CASE OF LÓPEZ RIBALDA AND OTHERS v. SPAIN

ZBIRNI PODATKI
Številka zadeve: 1874/13;8567/13
Ključne besede: (Art. 35) Admissibility criteria, (Art. 8) Positive obligations, (Art. 35-1) Exhaustion of domestic remedies, Proportionality, (Art. 6-1) Fair hearing, Margin of appreciation, (Art. 6) Civil proceedings, (Art. 8) Right to respect for private and family life, (Art. 6) Right to a fair trial, (Art. 8-1) Respect for private life
Domače pravo: Section 5 of the Personal Data Protection Act ; Instruction no. 1/2006 of 8 November 2006 ; Article 20.3 of the Labour Regulations (Estatuto de los Trabajadores) approved by Royal Legislative Decree no. 1/1995
Domače pravo_2: Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data
ECLI: ECLI:CE:ECHR:2019:1017JUD000187413
Praksa ESČP: M.C. v. Bulgaria, no 39272/98, § 150, ECHR 2003 XII, Söderman v. Sweden [GC], no 5786/08, § 78, ECHR 2013, Schüssel v. Austria (dec.), no 42409/98, 21 February 2002, Allan v. the United Kingdom, no 48539/99, § 35, ECHR 2002 IX, K. and T. v. Finland [GC], no 25702/94, §§ 140-141, ECHR 2001 VII, Herbecq and the Association "Ligue des droits de l'homme" v. Belgium, nos. 32200/96 and 32201/96, decision of the Commission of 14 January 1998, Decisions and Reports 92-A, p. 92, Schüth v. Germany, no 1620/03, §§ 54 and 57, ECHR 2010, Peck v. the United Kingdom, no 44647/98, §§ 58-63, ECHR 2003 I, Carmel Saliba v. Malta, no 24221/13, § 67, 29 November 2016, Perry v. the United Kingdom, no 63737/00, §§ 36-43, ECHR 2003 IX (extracts), Bărbulescu v. Romania [GC], no 61496/08, 5 September 2017, Schenk v. Switzerland, 12 July 1988, §§ 46-48, Series A no 140, Vukota-Bojić v. Switzerland, no 61838/10, §§ 55-59, 18 October 2016, Ilnseher v. Germany [GC], nos. 10211/12 and 27505/14, § 100, 4 December 2018, Köpke v. Germany (dec.), no 420/07, 5 October 2010, Palomo Sánchez and Others v. Spain [GC], nos. 28955/06 and 3 others, § 62, ECHR 2011, Angelov v. Bulgaria, no 44076/98, § 28, 22 April 2004, De La Flor Cabrera v. Spain, no 10764/09, § 31, 27 May 2014, Navalnyy v. Russia [GC], nos. 29580/12 and 4 others, § 61, 15 November 2018, P.G. and J.H. v. the United Kingdom, no 44787/98, ECHR 2001 IX, Von Hannover v. Germany (no 2) [GC], nos. 40660/08 and 60641/08, §§ 95 and 98, ECHR 2012, Fernández Martínez v. Spain [GC], no 56030/07, § 110, ECHR 2014 (extracts), Malhous v. the Czech Republic (dec.) [GC], no 33071/96, ECHR 2000-XII, Bochan v. Ukraine (no 2) [GC], no 22251/08, § 61, ECHR 2015, X and Y v. the Netherlands, 26 March 1985, §§ 23, 24 and 27, Series A no 91, Antović and Mirković v. Montenegro, no 70838/13, §§ 42-45, 28 November 2017, Gäfgen v. Germany [GC], no 22978/05, § 163, ECHR 2010, Reklos and Davourlis v. Greece, no 1234/05, §§ 34-43, 15 January 2009, Nicola v. Turkey, no 18404/91, § 15, 27 January 2009, Denisov v. Ukraine [GC], no 76639/11, §§ 95 and 100, 25 September 2018
Povezava do dokumenta na portalu IUS-INFO

GRAND CHAMBER

CASE OF LÓPEZ RIBALDA AND OTHERS v. SPAIN

(Applications nos. 1874/13 and 8567/13)

JUDGMENT

STRASBOURG

17 October 2019

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

In the case of López Ribalda and Others v. Spain,

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

Linos-Alexandre Sicilianos, *President,* Guido Raimondi, Angelika Nußberger, Robert Spano, Vincent A. De Gaetano, Jon Fridrik Kjølbro, Ksenija Turković, Işıl Karakaş, Ganna Yudkivska, André Potocki, Aleš Pejchal, Faris Vehabović, Yonko Grozev, Mārtiņš Mits, Gabriele Kucsko-Stadlmayer, Lətif Hüseynov, María Elósegui, *judges,* and Søren Prebensen, *Deputy Grand Chamber Registrar ,*

Having deliberated in private on 20 June 2019,

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

PROCEDURE

1. The case originated in two applications (nos. 1874/13

and 8567/13) against the Kingdom of Spain lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by five Spanish nationals, whose details are set out in the Annex ("the applicants"), on 28 December 2012 and 23 January 2013 respectively.

2. They were represented before the Court by Mr J.A. González Espada, a lawyer practising in Barcelona. The Spanish Government ("the Government") were represented by their Agent, Mr R.A. León Cavero, State Attorney.

3. The applicants submitted that the decision by which their employer had dismissed them had been based on video-surveillance implemented in breach of their right to respect for their private life, as guaranteed by Article 8 of the Convention, and that the domestic courts had failed in their obligation to ensure the effective protection of that right. Under Article 6 of the Convention, they complained about the admission in evidence during the proceedings of the recordings obtained by means of the video-surveillance. Under the same provision, the third, fourth and fifth applicants further complained of the acceptance by the domestic courts of the settlement agreements that they had signed with their employer.

4. The applications were allocated to the Third Section of the Court (Rule 52 § 1 of the Rules of Court). By a judgment of 9 January 2018 a Chamber of that Section, composed of Helena Jäderblom, President, Luis López Guerra, Dmitry Dedov, Pere Pastor Vilanova, Alena Poláčková, Georgios A. Serghides, Jolien Schukking, judges, and Stephen Phillips, Section Registrar, decided to join the applications, declared them partly admissible and found a violation of Article 8 of the Convention and no violation of Article 6. The dissenting opinion of Judge Dedov was appended to the Chamber judgment.

5. On 27 March 2018, under Article 43 of the Convention, the Government requested the referral of the case to the Grand Chamber. On 28 May 2018 the panel of the Grand Chamber granted that request.

6. The composition of the Grand Chamber was determined in accordance with Article 26 §§ 4 and 5 of the Convention and Rule 24.

7. The applicants and the Government each filed further written observations (Rule 59 § 1). The European Trade Union Confederation (ETUC), which had been granted leave to submit written comments in the Chamber proceedings (Article 36 § 2 of the Convention and Rule 44 § 3), had submitted such comments before the Chamber but did not make any additional comments before the Grand Chamber.

8. A hearing took place in public in the Human Rights Building, Strasbourg, on 28 November 2018 (Rule 59 § 3).

There appeared before the Court:

(a) *for the Government* Mr R.A. León Cavero, *Agent* , Mr A. Brezmes Martínez de Villarreal, *Co-Agent* , Mr A. Ramos de Molins Sainz de Baranda, Mr M. Montobbio, Ambassador, Permanent Representative of the Kingdom of Spain to the Council of Europe, Mr A. Antón, Adviser, Permanent Representation of the Kingdom of Spain to the Council of Europe, *Advisers* ;

(b) *for the applicants* Mr J.A. González Espada, *Counsel* , Ms À. Ortiz López, *Adviser.*

The Court heard addresses by Mr González Espada, Mr León Cavero and Mr Brezmes Martínez de Villarreal and their replies to questions from judges.

9. On 23 January 2019 the Court was made aware of the death of the second applicant. Her husband expressed the wish to continue the proceedings before the Court in her stead and gave authority to Mr J.A. González Espada to represent him.

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

A. The applicants' dismissal

10. At the time of the relevant events, the applicants were all working in a supermarket of the M. chain situated in Sant Celoni (Barcelona province). The first three applicants were cashiers, while the fourth and fifth applicants were sales assistants behind a counter.

11. From March 2009 onwards the supermarket's manager noticed some inconsistencies between the stock level and the sales figures. In the following months he identified losses of 7,780 euros (EUR) in February, EUR 17,971 in March, EUR 13,936 in April, EUR 18,009 in May and EUR 24,614 in June.

12. In the context of an internal investigation to shed light on the losses, on 15 June 2009 the manager installed CCTV cameras, some visible and others hidden. The visible cameras were directed towards the entrances and exits of the supermarket. The hidden cameras were placed at a certain height and directed towards the checkout counters. Three tills were covered by the range of each camera, including the areas in front of and behind the counters. The exact number of tills being monitored was not stated by the parties; the documents in the file show that at least four tills were filmed.

13. During a meeting the supermarket's staff were informed of the installation of the visible cameras on account of the management's suspicions about thefts. Neither the staff nor the staff committee were informed of the hidden cameras. Beforehand, in 2007, the company had notified the Spanish

Data Protection Agency that it intended to install CCTV cameras in its shops. The Agency had pointed out the obligations to provide information under the legislation on personal data protection. A sign indicating the presence of CCTV cameras had been installed in the shop where the applicants worked but the parties did not indicate its location or precise content.

14. On 25 June 2009 the management of the supermarket informed the union representative that the footage recorded by the hidden cameras had revealed thefts of goods at the tills by a number of employees. The representative watched the recordings.

15. On 25 and 29 June 2009 all the workers suspected of theft were called to individual interviews. Fourteen employees were dismissed, including the five applicants. Prior to each interview, the applicants and other employees concerned had a meeting with the union representative, who told them she had watched the video recordings. During the meeting a number of employees admitted that they had been involved in the thefts with other colleagues.

16. During the individual interviews, which were attended by the manager, the legal representative of the company M. and the union representative, the employees concerned were notified of their dismissal on disciplinary grounds with immediate effect. The dismissal letters given to the applicants indicated that the hidden CCTV cameras had filmed them, on several occasions between 15 and 18 June 2009, helping customers or other supermarket employees to steal goods and stealing goods themselves. Among the facts, the letters stated that the first three applicants, who worked at the tills, had allowed customers and colleagues to go to the cash till and leave the shop with goods they had not paid for. They added that those applicants had scanned items presented at the checkout by customers or colleagues and had then cancelled the purchases, with the result that the goods had not been paid for. They explained that a comparison between the goods actually taken away by customers and the sales receipts had made it possible to prove this. As to the fourth and fifth applicants, the cameras had reportedly caught them stealing goods with the help of their colleagues at the tills. According to the employer, these acts constituted a serious breach of the obligations of good faith and loyalty required in the employment relationship and justified the termination of the contract with immediate effect.

17. In addition, the third, fourth and fifth applicants signed an agreement entitled “settlement agreement” (*acuerdo transaccional*) with the company’s legal representative. These agreements were co-signed by the union representative. Under the agreements, the two parties confirmed the termination of the employment contract by the employer and declared that they had reached an agreement in order to avoid uncertainty as to any future legal dispute. The applicants acknowledged the thefts of the goods, as set out in the dismissal letters, and endorsed the employer’s decision to terminate their employment contracts. The company undertook not to bring criminal proceedings against the employees. A final settlement of outstanding accounts was attached to the agreement and the parties declared that they waived any claims against each other under the employment contract.

18. At no time before their dismissal, either during the meeting with the union representative or during their individual interviews, were the applicants able to view the recordings from the CCTV cameras.

B. Judicial proceedings brought by the applicants

1. The proceedings before the Employment Tribunal

19. On 22 July 2009 the first applicant brought proceedings for unfair dismissal before the Granollers Employment Tribunal no. 1 (“the Employment Tribunal”). The same day the other four applicants brought similar proceedings before the Employment Tribunal.

20. The applicants objected in particular to the use of the covert video-surveillance, arguing that it had breached their right to protection of their privacy. They thus requested that any recordings obtained by such means should not be admitted in evidence in the proceedings.

21. As regards the proceedings brought by the third, fourth and fifth applicants, the employer opposed them, relying on the settlement agreements signed by them. Those applicants sought the annulment of the agreements, arguing that they had signed them under the threat of criminal proceedings and that their consent had been vitiated by duress and by the deceitful manipulation of the employer with the complicity of the union representative.

22. A hearing was held in each of the two sets of proceedings, on 3 December 2009 and 23 November 2009 respectively. The CCTV recordings were produced in evidence by the employer.

23. On 20 January 2010 the Employment Tribunal issued two judgments dismissing the applicants’ actions, declaring their dismissals fair.

24. As regards the first and second applicants, who had not signed any settlement agreements, the tribunal took the view that it first had to ascertain whether the recordings obtained by the hidden cameras could constitute lawful evidence, given that, pursuant to section 11 of the Law on the Judiciary and Article 287 of the Code of Civil Procedure, any evidence obtained in breach of a fundamental right had to be excluded.

25. In this connection, the Employment Tribunal found that in accordance with Article 20 § 3 of the Labour Regulations

(see paragraph 42 below), any employer was entitled to use monitoring and surveillance measures to verify that employees were fulfilling their employment duties, provided those measures were compatible with their "human dignity" and thus respected their fundamental rights. It referred in this connection to the case-law of the Constitutional Court, in particular judgment no. 186/2000 of 10 July 2000, which concerned a similar case of video-surveillance, using hidden cameras, of employees suspected of serious misconduct. In that judgment, the Constitutional Court had found that an employer's right to adopt monitoring measures in the exercise of its management power and for the purpose of ensuring the smooth running of the company was limited by the respect due to the employees' right to their privacy and to the protection of their image. It had explained that the lower court was supposed to strike a balance between the various interests of constitutional value by applying a proportionality test to the employer's measures. In the case at issue, it had found that the covert video-surveillance measure had been proportionate and had not breached the employee's fundamental right to privacy guaranteed by Article 18 of the Constitution given that, first, it was justified by reasonable suspicions of serious misconduct; that, secondly, it was appropriate to the aim pursued, namely to verify whether the employee was actually committing misconduct and to adopt sanctions if necessary; that, thirdly, it was necessary, because the recordings would provide evidence of the misconduct in question; and that, fourthly, it was proportionate, because the monitoring was limited in space and in time to what was sufficient to fulfil its aim. The court had, moreover, considered it not to be constitutionally pertinent to examine the question whether the employees or the staff committee had been informed beforehand of the installation of the video-surveillance. It had further taken the view that the right to effective judicial protection under Article 24 of the Constitution had not been breached by the admission in evidence of the recordings thus obtained, especially as the decision had also been based on other evidence.

26. Transposing the principles thus developed by the Constitutional Court in a similar case, the Employment Tribunal found that there had been no breach of the applicants' right to respect for their private life and that the recordings thus constituted valid evidence.

27. On the merits, the court took the view that the facts set out in the dismissal letters had been established by the evidence in the file and examined as a whole, namely: the video recordings, the witness statements of the supermarket manager, the union representative and other employees dismissed for their involvement in the thefts, and an expert's report drafted in the context of the criminal proceedings concerning the offences (see paragraph 40 below), which had compared the footage filmed by the cameras with the purchases registered at the tills.

28. In the tribunal's view, the applicants' conduct amounted to a breach of the principle of good faith and entailed the employer's loss of trust, thus rendering their dismissals lawful.

29. As regards the third, fourth and fifth applicants, the Employment Tribunal examined their arguments relating to the invalidity of the settlement agreements with their employer. It took the view that there was no evidence of any form of coercion or fraudulent intent on the part of the employer. It concluded from the union representative's testimony that the applicants had confessed to the facts during a meeting with her, thus rendering it plausible that they had signed the agreements in order to avoid criminal proceedings. It added that the failure of some employees in the same situation as the applicants (for example, the first and second applicants) to sign such an agreement confirmed the absence of any threat or duress. It also noted that the settlement agreements had no unlawful basis and could be seen as a means of settling a dispute by means of reciprocal concessions.

30. Having accepted the settlement agreements, the tribunal upheld the employer's objection to the proceedings and, finding that the three applicants in question had no *locus standi* , dismissed their actions without examining them on the merits.

2. The proceedings before the High Court of Justice

31. The applicants appealed before the High Court of Justice of Catalonia ("the High Court") on 16 and 22 March 2010 respectively. In her appeal, the first applicant expressly complained of a breach of the obligation of prior notification, as provided for in section 5 of the Personal Data Protection Act. In her view this should have been taken into account in the examination of the proportionality of the video-surveillance measure.

32. In judgments of 28 January and 24 February 2011 the High Court upheld both first-instance judgments.

33. Relying on its own case-law, on that of other courts and on that of the Constitutional Court already cited by the Employment Tribunal, the High Court took the view that the video-surveillance measures taken by the employer on the basis of Article 20 § 3 of the Labour Regulations did not require, in the light of section 6(2) of the Personal Data Protection Act, the prior consent of the employees concerned but had to be subjected to a proportionality test according to the criteria laid down by the Constitutional Court. It took the view that the measure at issue in the present case satisfied those criteria because it was justified by the existence of suspicions of misconduct, appropriate to the aim pursued, necessary for the fulfilment of that aim because a more moderate measure would not have been capable of fulfilling it, and proportionate because the recordings were limited, in time and space, to what was

necessary for the purpose of verifying the suspicions. Referring to previous judgments, the High Court found as follows in its judgment of 28 January 2011 in the proceedings concerning the first applicant:

"... the monitoring carried out by the employer by means of CCTV cameras (installed on the site where the [first applicant] was working and directed towards the cashiers' work-stations after the detection of missing goods ...) 'may be generally regarded as an appropriate and even a necessary means of monitoring the activity and it must therefore be considered that, despite the fact that it may give rise to sanctions ... because of the failure to inform staff representatives about the installation of the camera ..., the monitoring was not carried out in an excessive manner contrary to the test of appropriateness, necessity or proportionality, which would have resulted in an unjustified breach of the right to the protection of the person's image or in undermining the person's dignity, since it was an appropriate means and one that would have been difficult to replace for the purpose of proving possible thefts ...'"

The High Court further held that the failure to notify employees and staff representatives could probably be explained by the fact that "the company rightly feared that knowledge of the monitoring system would defeat its purpose".

34. Without expressly mentioning section 5 of the Personal Data Protection Act, the High Court noted that the question of the employer's compliance with the obligation of prior notification was one of ordinary legality and that the failure to inform employees exposed the employer to an administrative sanction but had no impact on the admissibility of the evidence where, as in the present case, the video-surveillance measure was justified and proportionate:

"... The alleged failure to inform the employees could, if appropriate, entail an administrative sanction but will not fall foul of the conditions regarding the lawfulness of evidence laid down by the Constitutional Court, for it is indeed a justified measure (there were reasonable suspicions that the appellant had committed serious misconduct in the workplace), which was appropriate to the aim pursued by the company (to verify whether the employee had actually committed the acts and if so to take relevant disciplinary measures), and was necessary (since the recordings would be used as evidence of the wrongdoing) and proportionate (the cameras were only zoomed in on the checkout counters and solely for a limited period of time, sufficient to verify that it was not a one-off act or a misunderstanding but indeed repeated unlawful conduct)."

Using a similar line of reasoning, the High Court arrived at the same conclusion in its judgment of 24 February 2011, in the proceedings concerning the second, third, fourth and fifth applicants.

35. With regard to the third, fourth and fifth applicants, the High Court upheld the Employment Tribunal's conclusion that the settlement agreements were valid and that no defects in consent could be found, noting in particular that the agreements had been signed in the presence of the union representative and that their wording left no doubt as to the employees' knowledge of the facts or their willingness to accept the termination of their employment contracts.

36. The High Court noted, however, that it was not procedurally correct to consider, as the Employment Tribunal had done, that the signing of the agreements had deprived the applicants of their right to take legal action. It took the view that it nevertheless appeared from these agreements that they had expressly acknowledged the facts of which they were accused, that they had accepted the employer's decision to discontinue their employment and that they had thus given their consent to the termination of their contracts. It therefore reached the conclusion, with reference to case-law of the Supreme Court relating to similar agreements entered into by the same employer with other employees, that the employment contracts had been terminated by mutual agreement. In its view, this was sufficient to consider the facts to be established and the termination of the employment contracts to be lawful, regardless of whether the video recordings were lawful and could be admitted in evidence, a question to which the court had in fact responded in the affirmative.

37. Moreover, in response to the ground of appeal raised by all the applicants to the effect that the evidence was insufficient to establish the facts, the High Court noted that the facts were proven by the video recordings, by the testimony of the union representative to whom several employees had admitted the thefts, and by the acknowledgment of the facts in the settlement agreements, in the cases of the three applicants who had signed them. As regards more specifically the first applicant, whose face did not appear in the video footage, the court found that an analysis of the recordings of the cameras directed towards the till at which she worked and the sales receipts sufficiently demonstrated her involvement in the acts of which she was accused.

38. After examining the other grounds of appeal put forward by the applicants in support of their claims, the High Court concluded that the dismissals were lawful and upheld the judgments handed down at first instance.

3. The proceedings before the Supreme Court and the Constitutional Court

39. The applicants brought appeals on points of law, which were declared inadmissible on 5 October 2011 and 7 February 2012 respectively. Ultimately the applicants lodged *amparo* appeals with the Constitutional Court, which were declared inadmissible on 27 June and 18 July 2012 respectively, owing to the "non-existence of a violation of a

fundamental right".

C. The criminal proceedings against the applicants

40. On 31 July 2009, after the applicants and other employees had appealed against their dismissals before the Employment Tribunal, the employer filed a criminal complaint against fourteen employees, including the five applicants. Criminal proceedings were opened against them. On 15 July 2001, finding that the investigation had not established that there had been any concerted action between the defendants in committing the offences, and that the value of the goods stolen by each defendant had not exceeded EUR 400, the investigating judge decided to reclassify the charges as a minor offence (*falta*). In a decision of 27 September 2011 the judge declared that the prosecution was time-barred on account of the statutory limitation of proceedings for that type of offence.

II. RELEVANT DOMESTIC LAW AND PRACTICE

D. The Spanish Constitution

41. The relevant provisions of the Spanish Constitution read as follows:

Article 18

"1. The right to respect for honour, for private and family life and for one's own image shall be guaranteed.

...

4. The law shall restrict the use of data processing in order to guarantee respect for the honour and private and family life of citizens and the full exercise of their rights."

Article 24

"1. Everyone has the right to effective protection by judges and the courts in the exercise of his or her legitimate rights and interests, and in no case may defence rights be curtailed.

2. Likewise, everyone has the right to ... a public trial without undue delay and with full guarantees ..."

Article 33

"1. The right to private ownership ... shall be recognised."

Article 38

"Free enterprise shall be recognised within the framework of a market economy. ..."

E. Relevant provisions of labour law

42. The Labour Regulations (*Estatuto de los Trabajadores*), approved by Royal Legislative Decree no. 1/1995 of 24 March 1995, as in force at the relevant time, provided in particular as follows:

Article 5 – Workers' duties

"Workers have the following basic duties:

(a) To fulfil the obligations inherent in their post, in keeping with the principles of good faith and diligence.

..."

Article 20

"2. ... In all cases, the worker and the employer shall be bound by the requirement of good faith in the fulfilment of their reciprocal obligations.

3. An employer may use monitoring and surveillance measures which it deems most appropriate to verify that an employee is fulfilling his or her employment duties, taking into account, in their adoption and application, of the consideration due to his or her human dignity ..."

43. The relevant provisions of the Employment Proceedings Act, approved by Royal Legislative Decree no. 2/1995 of 7 April 1995, as in force at the relevant time, read as follows:

Article 90

"1. The parties may rely on all the evidence prescribed by law ... save where it has been gathered directly or indirectly in breach of fundamental rights and freedoms.

..."

Article 108

"...

2. A dismissal based on any of the grounds of discrimination provided for by the Constitution or the law, or implemented in breach of fundamental rights and freedoms, shall be regarded as null and void."

F. Relevant procedural provisions

44. Section 11 of Organic Law no. 6/85 of 1 July 1985 on the Judiciary provides as follows:

"1. The principle of good faith must be complied with in all proceedings. Evidence obtained, directly or indirectly in violation of fundamental rights or freedoms will be excluded ..."

G. Legislation regarding the protection of personal data

4. Organic Law no. 15/1999

45. Organic Law no. 15/1999 on the protection of personal data (*Ley Orgánica de protección de datos de carácter personal* – the "Personal Data Protection Act"), as in force at the material time, was enacted on 13 December 1999 by transposing Directive 95/46/EC (see paragraph 63 below) and entered into force on 14 January 2000. Its aim was to safeguard the fundamental rights of individuals in connection with the processing of personal data, and more specifically their right to respect for their honour and their personal and family privacy (section 1 of the Act). It applied to the collection of personal data, defined as any information concerning identified or identifiable individuals recorded on a physical medium which may be subject to processing, and also covered the future usage of such data for public or private purposes (sections 2 and 3 of the Act).

46. The Spanish Data Protection Agency, created by the Act, is the authority responsible for the supervision of its application. In that capacity it is entitled to carry out inspections, examine complaints and impose penalties for contraventions of the Act, namely fines of up to EUR 600,000 (sections 35 et seq.).

47. The provisions of the Act concerning information and the consent of those concerned by the collection of their personal data, as applicable in the present case, read as follows:

Section 5 – Right to information on the collection of data

"1. Data subjects whose personal data are requested must be previously, explicitly, precisely and unambiguously informed of the following:

(a) the existence of a personal data file or the fact that the data will be processed, the purpose thereof and the recipients of the information;

(b) the obligatory or optional nature of their response to the questions asked;

(c) the consequences of providing or refusing to provide the data;

(d) the existence of rights of access, rectification, erasure and objection;

(e) the identity and address of the controller or, as appropriate, his representative.

...

4. Where personal data have been collected without the data subject being approached, the person must be informed thereof in an express, precise and unequivocal manner by the file manager or his or her representative, within three months from the recording of the data, except where the data subject has already been informed of the content of the processing, the origin of the data, and the information referred to in letters (a), (d) and (e) of subsection 1 of the present section.

5. The provisions of the preceding subsection shall not apply in cases where the law expressly provides otherwise, where the data-processing has historical, statistical or scientific purposes, or where it is impossible to inform the data subject, or where this would involve a disproportionate effort in the opinion of the Data Protection Agency or the corresponding regional body, in view of the number of data subjects, the age of the data and the possible compensation measures.

Furthermore, the provisions of the preceding subsection shall also not apply where the data are obtained from sources accessible to the public and are intended for advertising or market research, in which case each communication sent to the data subject shall inform him or her of the origin of the data, the identity of the person/entity responsible for processing the data and the rights of the data subject."

Section 6 – Consent of data subjects

"1. Processing of personal data shall require the unambiguous consent of the data subject, unless laid down otherwise by law.

2. Consent shall not be required where the personal data are collected for the exercise of the functions proper to public authorities within the scope of their duties; where they relate to the parties to a contract or preliminary contract for a business, employment or administrative relationship, and are necessary for its maintenance or fulfilment; where the purpose of processing the data is to protect a vital interest of the data subject under the terms of section 7(6) of this Act or where the data are contained in sources accessible to the public and their processing is necessary to satisfy the legitimate interest pursued by the controller or that of the third party to whom the data are communicated, unless the fundamental rights and freedoms of the data subject are jeopardised."

48. Under sections 13 to 18 of the Act, data subjects had, in particular, a right of access, rectification and deletion in respect of their personal data. Section 19 of the Act provided for a right to compensation as follows:

Section 19 – Right to compensation

"1. Persons who, as a result of any failure by the data-processing manager or controller, have sustained any damage to their property or to their rights, shall be entitled to compensation. ...

3. If the files are held by private-law entities, any proceedings shall be brought in the ordinary courts."

49. On that basis a judgment of the Supreme Court ordered

an employer to pay compensation to one of its former employees, who had been dismissed two years earlier, for providing potential employers with personal information concerning the employee's dismissal and thus apparently reducing the employee's chances of finding a new job (judgment no. 609/2015 of 12 November 2015).

5. Instruction no. 1/2006

50. Instruction no. 1/2006 of 8 November 2006 on the processing of personal data for monitoring purposes using video-surveillance devices, issued by the Spanish Data Protection Agency, contains the following provisions:

Article 3 - Information

"Everyone who uses video-surveillance devices must fulfil all the obligations prescribed in section 5 of Organic Law no. 15/1999 of 13 December. For that purpose they must:

(a) place at least a sufficiently visible information board in the areas monitored ... and

(b) make available to the data subjects a document containing the information provided for in section 5.1 of Organic Law no. 15/1999 ..."

Article 4 – Principles of quality, proportionality and purpose of data processing

"1. In accordance with section 4 of Organic Law no. 15/1999 ..., images may only be processed if they are appropriate, relevant and not excessive in relation to the scope and to the legitimate and explicit aims justifying the installation of video-surveillance.

2. The installation of cameras ... is permitted only where the aim of the monitoring cannot be fulfilled, without disproportionate effort, by other means that would be less intrusive for the privacy of individuals and their right to the protection of personal data.

3. ... In all situations, any data processing should be avoided if it is not necessary for the aim pursued."

51. The website of the Data Protection Agency, moreover, provides a factsheet on video-surveillance and a model board indicating the information required by law.

6. Law no. 3/2018

52. Law no. 15/1999 was repealed by a new Organic Law, no. 3/2018, on the protection of personal data and the safeguarding of digital rights, enacted on 5 December 2018, which entered into force on 7 December 2018. Section 22 of the new Law expressly governs the processing of personal data collected by means of video-surveillance. It provides in particular as follows:

"4. The obligation to provide information under Article 12 of Regulation (EU) 2016/679 is deemed to be fulfilled by the placing of an information board in a sufficiently visible place, indicating at least the existence of the processing, the identity of the person responsible and the possibility of exercising the rights provided for by Articles 15 to 22 of Regulation (EU) 2016/679. ..."

53. As regards video-surveillance in the workplace, section 89(1) of the Law provides as follows:

"1. Employers are entitled to process images obtained by means of video-surveillance devices in the exercise of their authority to monitor employees or officials, as laid down in Article 20 § 3 of the Labour Regulations ... provided that this possibility is used in the statutory framework and within its inherent limits. Employers must inform employees or officials of the introduction of such a measure beforehand and in an explicit, clear and concise manner.

In the event that CCTV cameras film employees or officials clearly committing an illegal act, the obligation to provide information shall be deemed fulfilled when at least the mechanism provided for in section 22(4) hereof has been put in place."

H. Case-law of the Constitutional Court

54. On 10 July 2000 the Constitutional Court delivered a leading judgment on the lawfulness of video-surveillance in the workplace in the light of the protection provided by Article 18 § 1 of the Spanish Constitution (judgment no. 186/2000). In that case the employer had set up a system of hidden CCTV cameras in the ceiling of the clothing and footwear department of a shop, directed towards three tills and the reception desk. The Constitutional Court held that the measure at stake had to pass a threefold test to be considered acceptable: there had to be a legitimate aim ("appropriateness test"), and the measure had to be necessary ("necessity test") and proportionate ("strict proportionality test"). In other words, the courts had to ascertain whether a fair balance had been struck between the interference with a fundamental right and the importance of the legitimate aim pursued. On the subject of the video-surveillance at issue in that case, it found as follows:

"In the present case, the covert video-surveillance ... was a justified measure (since there was a reasonable suspicion that the person investigated had committed some wrongdoing at work); it was suited to the purpose pursued by the company (to verify that the worker was in fact committing the suspected wrongdoing, in which case he would be subjected to an appropriate disciplinary sanction); it was necessary (the recordings were to be used as evidence of the wrongdoing); and it was proportionate (since the cameras were only zoomed in on the checkout counters and solely for a limited period of time) ... ; it follows

that there has been no interference with the right to [respect for] privacy as enshrined in Article 18.1 of the Spanish Constitution."

55. As to the alleged failure to inform the employees and the staff committee, the Constitutional Court found that it was a question of ordinary legality that was not pertinent in terms of the constitutional protection of fundamental rights. The facts of the case nevertheless predated the entry into force of the Personal Data Protection Act in January 2000 and, at that time, the applicable law did not lay down any obligation to provide information that was comparable to the obligation subsequently enshrined in section 5(1) of that Act.

56. In a previous judgment of 10 April 2000 (no. 98/2000), applying a similar proportionality test, the Constitutional Court had taken the view that video and audio recording devices placed at the checkout and on a gaming table in a casino, complementing the existing security system, had been a disproportionate measure in view of the resulting major interference with the right of employees and customers to respect for their private life. The court noted that the employer had failed to show how the sound recording, which was particularly intrusive for the right to privacy of those concerned, had been necessary for the protection of its legitimate rights and interests.

57. Subsequently, in judgment no. 29/2013 of 11 February 2013, which concerned events after the Personal Data Protection Act had entered into force, the Constitutional Court held that the permanent installation of a video-surveillance system, initially as a security measure for the purpose of monitoring employees' activity, required that the workers' representatives and employees be given prior notification and that a failure to do so would be in breach of Article 18 § 4 of the Constitution. In that case, an employee of Seville University had been suspended from his duties without pay for unjustified late arrivals and absences that had been established by means of video-surveillance installed with the approval of the administration. The Constitutional Court found as follows:

"7. ... In conclusion, it must not be overlooked that the [Constitutional Court has] established, in an invariable and continuing manner, that an employer's power is limited by fundamental rights (among many other [authorities], STC no. 98/2000, of 10 April, legal ground no. 7, or STC no. 308/2000, of 18 December, legal ground no. 4). Consequently, in the same way that the 'public interest' behind the punishment linked to an administrative offence is not enough to allow the State to deprive the citizen concerned of his or her rights derived from [sections 5(1) and (2) of the Personal Data Protection Act] (STC 292/2000, of 30 November, legal ground no. 18), the 'private interest' of an employer cannot justify using the worker's personal data to his or her detriment without previously informing him or her of the monitoring measures that have been implemented. There is no reason in the employment sphere ... to restrict the right to be informed, a fundamental right that is protected by Article 18.4 of the Constitution. Accordingly, it is not enough that the data processing itself is lawful, being prescribed by law (section 6(2) of the Personal Data Protection Act), or proves, in a given case, to be proportionate to the aim pursued; monitoring by the employer, while certainly possible, must also guarantee the requisite prior information.

8. In the instant case, the CCTV cameras installed on the campus recorded the appellant's image and allowed [the employer] to verify the appellant's compliance with the working time [regulations] ... The owner of the cameras was Seville University and it was this entity that used the recordings, thus becoming the entity responsible for processing the appellant's data without previously informing him of the use of cameras to monitor his work. This infringed Article 18.4 of the Constitution.

The fact that signs were put up indicating the existence of a video-surveillance system on the campus, or that the Data Protection Agency had been informed of the installation of the system, does not detract from this conclusion. The employees, moreover, should have been informed, beforehand and in an express, precise and unambiguous manner, that the system could be used to monitor their work. The information should specify the characteristics and scope of the data processing, indicating the situations in which the images could be examined, together with the time-frame and purpose, specifically stating that the images could be used to impose disciplinary sanctions on the workers for non-compliance with the contract of employment."

58. In a judgment of 3 March 2016 (no. 39/2016) the Constitutional Court consolidated its case-law concerning the use of hidden surveillance cameras. In this case the manager of a clothing shop had detected some thefts from the till and suspected one of its employees. He had temporarily installed hidden cameras zoomed in on the area where the till was located. The employer had placed a sign indicating in a general manner the presence of CCTV cameras, including the information provided for by section 5 of the Personal Data Protection Act, as required by Article 3 of Instruction no. 1/2006 issued by the Spanish Data Protection Agency. The Constitutional Court explained in the following terms the relevance of the fulfilment of the obligation to provide information under section 5 of that Act:

"4. ... as has been emphasised, even though the express consent of the employee is not required to implement a monitoring measure which involves the processing of [personal data], the obligation to provide information under section 5 of the Personal Data Protection Act remains. Without prejudice to any legal sanctions which may be

entailed by an employer's failure to comply with the obligation, for it to constitute a violation of Article 18.4 of the Constitution it is necessary to ascertain whether the proportionality principle has been upheld. The right to data protection should be weighed in the balance against any limitations that may be justified by the employee's work obligations and the corresponding power of monitoring and supervision granted to the employer by Article 20.3 of the Labour Regulations, in relation to Articles 33 and 38 of the Constitution. The assessment of the constitutional relevance of a total or partial lack of information in cases of video-surveillance in the workplace requires the balancing in each case of the competing constitutional rights and values: on the one hand the employees' right to the protection of personal data and, on the other, the employer's management power, which, essential as it is to the proper running of a productive organisation, reflects the constitutional rights recognised in Articles 33 and 38 of the Constitution and ... is enshrined in Article 20.3 of the Labour Regulations, which expressly empower the employer to adopt monitoring and supervision measures in order to verify that the workers comply with their employment duties ... This general monitoring power provided for by law legitimises the supervision carried out by the employer of the employees' performance of their professional tasks (see ... the judgment of the European Court of Human Rights *Bărbulescu v. Romania* of 6 [*sic*] January 2016), without prejudging the particular circumstances of each case, which will determine whether or not the monitoring implemented by the employer has entailed a violation of the fundamental right at stake.

It is clear that, in order to ascertain whether the proportionality test is satisfied where the provision of information is insufficient or absent, it will be necessary first to determine, in each case, whether there has actually been a failure in the duty to provide information."

59. In that case the Constitutional Court found that there had been no violation of Article 18 § 4 of the Constitution, in particular on the ground that the employer had placed a board indicating that video-surveillance was in place, in accordance with the regulations. It considered that the board contained sufficient information as to the existence of monitoring and the purpose of the data processing. After examining the proportionality of the interference with the employee's private life, using the criteria laid down in the case-law (see paragraph 54 above), it further found that there had not been any breach of the right to personal privacy protected by Article 18 § 1 of the Constitution.

III. RELEVANT EUROPEAN AND INTERNATIONAL LAW

I. Council of Europe

7. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

60. This Convention (ETS No. 108) entered into force on 1 October 1985, having been ratified by Spain on 31 January 1984. Under Article 1, its purpose is to secure in the territory of each State Party, for every individual, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him. It provides, *inter alia* , as follows:

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;

c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this Convention;

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."

8. The Venice Commission

61. In 2007 the Venice Commission, the Council of Europe's advisory body on constitutional matters, adopted an Opinion on "video surveillance by private operators in the public and private spheres and by public authorities in the private sphere and human rights protection" at its 71st plenary session (Venice, 1-2 June 2007, CDL-AD(2007)027). The relevant parts read as follows:

"18. For the purposes of this study, the private sphere will also include workplaces and the use of video surveillance in workplace premises, which raises legal issues concerning the employees' privacy rights.

...

52. As regards workplaces, the introduction of video monitoring requires respecting the privacy rights of the employees.

53. Here, video surveillance would, in general, be allowed to prevent or detect fraud or theft by employees in case of a well-founded suspicion. However, except in very specific circumstances, videotaping would not be allowed at places such as toilets, showers, restrooms, changing rooms, or smoking areas and employee lounges where a person may trust to have full privacy.

54. Moreover, secret surveillance should only be allowed, and then only on a temporary basis, if proven necessary because of lack of adequate alternatives.

...

57. As regards shops, camera surveillance may be justified to protect the property, if such a measure has proven to be necessary and proportional. It may also be justified at certain locations in the shop to prevent and prosecute robberies under threat but, again, only if proven necessary, and no longer than necessary.

58. National legislation will have to clearly define the legal basis of the surveillance and the necessity of the infringement in view of the interests protected.

... "

IV. Conclusions and recommendations

" ...

99. The Venice Commission would hence reiterate the Recommendations made in its previous study:

- Video surveillance [performed on grounds of security or safety requirements, or for the prevention and control of criminal offences], shall respect the requirements laid down by Article 8 of the ECHR.

- With regard to the protection of individuals concerning the collection and processing of personal data, the regulations shall at least follow the requirements laid down by Directive 95/46/EC, especially its Articles 6 and 7 which are based on Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data in its Article 5.

100. Furthermore the Commission recommends, in view of the specificities of video surveillance, that the following measures should also be taken on a systematic basis:

- People should be notified of their being surveyed, unless the surveillance system is obvious. This means that the situation has to be such that the person observed may be assumed to be aware of the surveillance, or has unambiguously given his /her consent."

9. The Committee of Ministers

62. On 1 April 2015, at the 1224th meeting of the Ministers' Deputies, the Committee of Ministers of the Council of Europe adopted Recommendation CM/Rec(2015)5 on the processing of personal data in the context of employment. The relevant extracts provide as follows:

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. ..."

15. Information systems and technologies for the monitoring of employees, including video surveillance

"15.1. The introduction and use of information systems and technologies for the direct and principal purpose of monitoring employees' activity and behaviour should not be permitted. Where their introduction and use for other legitimate purposes, such as to protect production, health and safety or to ensure the efficient running of an organisation has for indirect consequence the possibility of monitoring employees' activity, it should be subject to the additional safeguards set out in principle 21, in particular the consultation of employees' representatives.

15.2. Information systems and technologies that indirectly monitor employees' activities and behaviour should be specifically designed and located so as not to undermine

their fundamental rights. The use of video surveillance for monitoring locations that are part of the most personal area of life of employees is not permitted in any situation."

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;

d. consult, in accordance with domestic law, the national supervisory authority on the processing of personal data."

J. European Union material

10. Directive 95/46/EC

63. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, in its relevant parts, provides:

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. ..."

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 ..."

Article 10 – Information in cases of collection of data from the data subject

"Member States shall provide that the controller or his representative must provide a data subject from whom data relating to himself are collected with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(b) the purposes of the processing for which the data are intended;

(c) any further information such as

- the recipients or categories of recipients of the data, ...

- the existence of the right of access to and the right to rectify the data concerning him ..."

Article 11 – Information where the data have not been obtained from the data subject

"1. Where the data have not been obtained from the data subject, Member States shall provide that the controller or his representative must at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it:

(a) the identity of the controller and of his representative, if any;

(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

in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject. ..."

Article 13 – Exemptions and restrictions

"1. Member States may adopt legislative measures to restrict the scope of the obligations and rights provided for in Articles 6 (1), 10, 11 (1), 12 and 21 when such a restriction constitutes a necessary measures to safeguard:

(a) national security;

(b) defence;

(c) public security;

(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;

(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;

(f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);

(g) the protection of the data subject or of the rights and freedoms of others."

Article 22 – Remedies

"Without prejudice to any administrative remedy for which provision may be made, inter alia before the supervisory authority referred to in Article 28, prior to referral to the judicial authority, Member States shall provide for the right of every person to a judicial remedy for any breach of the rights guaranteed him by the national law applicable to the processing in question."

Article 23 – Liability

"1. Member States shall provide that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to this Directive is entitled to receive compensation from the controller for the damage suffered. ..."

11. The Data Protection Working Party

64. A Data Protection Working Party was established under Article 29 of Directive 95/46/EC in order to contribute to the uniform implementation of its provisions. It is an independent EU advisory body. In September 2001 it issued Opinion 8/2001 on the processing of personal data in an employment context, which summarises the fundamental principles of data protection: purpose, transparency, legitimacy, proportionality, accuracy, security and staff awareness. With regard to the monitoring of employees, it recommended as follows:

"Any monitoring, especially if it is conducted on the basis of Article 7(f) of Directive 95/46/EC and, in any case, to satisfy Article 6 must be a proportionate response by an employer to the risks it faces taking into account the legitimate privacy and other interests of workers.

Any personal data held or used in the course of monitoring must be adequate, relevant and not excessive for the purpose for which the monitoring is justified. Any monitoring must be carried out in the least intrusive way possible. It must be targeted on the area of risk, taking into account that data protection rules and, where applicable, the principle of secrecy of correspondence.

Monitoring, including surveillance by camera, must comply with the transparency requirements of Article 10. Workers must be informed of the existence of the surveillance, the purposes for which personal data are to be processed and other information necessary to guarantee fair processing. The Directive does not treat less strictly monitoring of a worker's use of an Internet and email system if the monitoring takes place by means of a camera located in the office."

65. Another opinion, issued on 11 February 2004, "on the Processing of Personal Data by means of Video Surveillance" (opinion no. 4/2004), pointed out that Directive 95/46/EC applied to such means and that the proportionality principle had to be upheld both in the decision to use it and for the processing of the personal data thus obtained. As regards video-surveillance in the workplace, it explained as follows:

"In addition to the considerations made in the above documents, to the extent that they are actually applicable to video surveillance, it is appropriate to point out that video surveillance systems aimed directly at controlling, from a remote location, quality and amount of working activities, therefore entailing the processing of personal data in this context, should not be permitted as a rule.

The case is different as regards video surveillance systems that are deployed, subject to appropriate safeguards, to meet production and/or occupational safety requirements and also entail distance monitoring – albeit indirectly.

The implementing experience has shown additionally that surveillance should not include premises that either are reserved for employees' private use or are not intended for the discharge of employment tasks – such as toilets, shower rooms, lockers and recreation areas; that the images collected exclusively to safeguard property and/or detect, prevent and control serious offences should not be used to charge an employee with minor disciplinary breaches; and that employees should always be allowed to lodge their counterclaims by using the contents of the images collected.

Information must be given to employees and every other person working on the premises. This should include the identity of the controller and the purpose of the surveillance and other information necessary to guarantee fair processing in respect of the data subject, for instance in which cases the recordings would be examined by the management of the company, the recording period and when the recording would be disclosed to the law enforcement authorities. The provision of information for instance through a symbol can not be considered as sufficient in the employment context."

12. The General Data Protection Regulation

66. 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, has been applicable since 25 May 2018. It incorporates most of the provisions of Directive 95/46/EC and reinforces some of the safeguards contained therein.

IV. COMPARATIVE-LAW MATERIAL

67. The following information was gleaned from the Court's research into the legislation of the member States of the Council of Europe, and in particular a study covering forty-two States.

68. The twenty-eight member States of the European Union have legislation transposing Directive 95/46/EC. Among them, twenty-one States have adopted instruments specifically regulating video-surveillance in the workplace. The majority of States which have such rules prohibit covert video-surveillance. Some of them (Germany, United Kingdom) allow it, however, in the event of suspicion of a criminal offence or serious misconduct.

69. As regards the States which are not members of the EU, seven of them have specific rules on video-surveillance in the workplace, three States have regulations on video-surveillance in general and five States have only general legislation on the collection and processing of personal data. The States which have specific rules require that such monitoring should have a legitimate purpose and that the employees should be informed. In one State (Switzerland) covert video-surveillance may be used in the case of suspicion of an offence.

70. Almost all States enable any person who has been the subject of video-surveillance to go before the courts to seek compensation for any damage sustained and/or an order to terminate the monitoring or delete the data obtained by that means. In some countries, criminal liability may also be engaged. In all member States of the European Union and in ten of the other States, it is possible to complain to an independent authority for the protection of personal data, which has powers to investigate and impose sanctions.

THE LAW

V. PRELIMINARY ISSUES

K. *Locus standi*

71. The Court observes that the second applicant, Ms A. Gancedo Giménez, died on 25 October 2018, while the case was pending before the Grand Chamber. Her husband and legal heir, Mr J. López Martínez, expressed his wish to continue the proceedings before the Court.

72. The Court would point out that, in a number of cases where an applicant died during the proceedings, it has taken account of the wish expressed by heirs or close relatives to continue them (see, among other authorities, *Malhous v. the Czech Republic* (dec.) [GC], no. 33071/96, ECHR 2000XII; *Angelov v. Bulgaria* , no. 44076/98, § 28, 22 April 2004; and *Nicola v. Turkey* , no. 18404/91, § 15, 27 January 2009).

73. In the present case, the Court finds that the heir of the second applicant may have a sufficient interest in the

continued examination of the application and thus recognises his capacity to act in her stead.

L. Subject matter of the case before the Grand Chamber

74. In their oral observations before the Grand Chamber, the Government requested that the Court should only re-examine the complaint under Article 8 of the Convention, in respect of which the Chamber had found a violation in its judgment of 9 January 2018 and which was the subject of the Government's request for referral, as accepted by the panel of the Grand Chamber. They added that the applicants had not submitted any referral request concerning the complaints under Article 6, in respect of which the Chamber had found no violation.

75. The applicants did not comment on the Government's request but nevertheless asked the Court to review the Chamber's finding of no violation.

76. The Court reiterates that the content and scope of the "case" referred to the Grand Chamber are delimited by the Chamber's decision on admissibility (see *K. and T. v. Finland* [GC], no. 25702/94, §§ 140-41, ECHR 2001VII, and *Ilnseher v. Germany* [GC], nos. 10211/12 and 27505/14, § 100, 4 December 2018). The "case" referred to the Grand Chamber thus necessarily encompasses all the aspects of the application that the Chamber found admissible and is not confined to the "serious issue" of general importance or affecting the interpretation or application of the Convention or the Protocols thereto, under Article 43 of the Convention, in respect of which the referral request has been accepted by the panel (see *K. and T. v. Finland* , cited above, §§ 140-41). Accordingly, in the present case, the Grand Chamber's examination will concern all the complaints under Articles 6 and 8 of the Convention that were declared admissible by the Chamber.

VI. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

77. The applicants argued that their employer's decision to dismiss them had been based on recordings obtained by means of video-surveillance in their workplace, in breach of their right to respect for their private life, and that, by refusing to declare their dismissal null and void, the domestic courts had failed in their duty to protect that right. They relied on Article 8 of the Convention, which reads as follows:

"1. Everyone has the right to respect for his private ... life ...

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."

M. The Chamber judgment

78. In its judgment of 9 January 2018 the Chamber found that Article 8 of the Convention was applicable in the present case. As the disputed video-surveillance measure had been implemented by a private party, it examined the complaint in terms of the State's positive obligations and sought to ascertain whether the national authorities had struck a fair balance between the applicants' right to respect for their private life, on the one hand, and their employer's interest in protecting its rights in connection with the organisation and management of its property, on the other.

79. The Chamber noted that, while the video-surveillance had been set up on account of legitimate suspicions of theft, it had been broad in scope – not being limited in time, affecting all the employees working at the tills and covering all working hours – and had breached the obligation under domestic law to give prior information, to those persons who were concerned by the collection and processing of their personal data, of the existence, purpose and implementation of the measures. Having regard to those factors, the Chamber did not share the opinion of the domestic courts as to the proportionality of the video-surveillance measure taken by the employer. It was of the view, in particular, that the employer's rights could have been secured by informing the applicants, even in a general manner, of the installation of a video-surveillance system.

80. Consequently, the Chamber found that the domestic courts had failed to strike a fair balance between the applicants' right to respect for their private life and the other interests at stake, and that there had thus been a violation of Article 8 of the Convention.

N. The Government's preliminary objection

81. The Government argued that the applicants could have complained to the Data Protection Agency, alleging an infringement by the employer of the Personal Data Protection Act, or could have brought criminal proceedings to complain of a breach of their right to respect for their private life. In their view, those remedies could have resulted in the imposition of an administrative or criminal sanction on the employer. They concluded that the applicants had failed to exhaust the domestic remedies available under domestic law.

82. The applicants submitted that the Data Protection Agency was merely an administrative organ whose authority was confined to imposing pecuniary sanctions in the event of a breach of the data-protection legislation. They took the view that such a sanction, if it were to be imposed on their employer, would not bring them redress for the damage caused to them by the breach of their right to respect for

their private life and by their dismissal based on that breach. They added that it was not mandatory to complain to the Agency before the ordinary courts, which had full jurisdiction to interpret and apply the Personal Data Protection Act.

83. The Court notes that the Government only raised the issue of non-exhaustion of domestic remedies for the first time in their written pleadings before the Grand Chamber. It discerns no exceptional circumstances in this case which could have released them from their obligation pursuant to Rule 55 to raise their preliminary objection prior to the adoption of the Chamber's decision on admissibility. It thus takes the view that the Government are estopped from raising that objection at this stage of the proceedings and that it must be dismissed (see *Navalnyy v. Russia* [GC], nos. 29580/12 and 4 others, § 61, 15 November 2018).

84. However, in so far as the parties' arguments on the objection of non-exhaustion raised by the Government have a bearing on the merits of the applicants' complaint under Article 8 of the Convention, the Court will examine them below.

0. Applicability of Article 8 of the Convention

13. The parties' submissions

(a) The applicants

85. The applicants submitted that the fact they had been continuously filmed in their workplace throughout their entire working day, without their knowledge and without being able to evade the monitoring, resulted in Article 8 of the Convention being applicable.

(b) The Government

86. The Government argued that the applicants had been working in a public place, in direct contact with the public. They took the view that, in the absence of a consensus among the member States as to whether such a situation was comprised within the notion of "private life", the Court should not extend that concept accordingly. They added that the protection of Article 8 could not extend to criminal conduct.

14. The Court's assessment

Principles derived from the Court's case-law

87. The Court reiterates that the concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person. It can therefore embrace multiple aspects of the person's physical and social identity (see, as a recent example, *Denisov v. Ukraine* [GC], no. 76639/11, § 95, 25 September 2018). It extends in particular to aspects relating to personal identity, such as a person's name or picture (see *Schüssel v. Austria* (dec.), no. 42409/98, 21 February 2002, and *Von Hannover v. Germany (no. 2)* [GC], nos. 40660/08 and 60641/08, § 95, ECHR 2012).

88. The concept of private life is not limited to an "inner circle" in which the individual may live his or her own personal life without outside interference, but also encompasses the right to lead a "private social life", that is, the possibility of establishing and developing relationships with others and the outside world (see *Bărbulescu v. Romania* [GC], no. 61496/08, § 70, 5 September 2017). It does not exclude professional activities in that connection (see *Fernández Martínez v. Spain* [GC], no. 56030/07, § 110, ECHR 2014 (extracts); *Köpke v. Germany* (dec.), no. 420/07, 5 October 2010; *Bărbulescu* , cited above, § 71; *Antović and Mirković v. Montenegro* , no. 70838/13, § 42, 28 November 2017; and *Denisov* , cited above, § 100) or activities taking place in a public context (see *Von Hannover (no. 2)* , cited above, § 95). There is thus a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life" (see *P.G. and J.H. v. the United Kingdom* , no. 44787/98, § 56, ECHR 2001-IX; *Perry v. the United Kingdom* , no. 63737/00, § 36, ECHR 2003-IX (extracts); and *Von Hannover (no. 2)* , cited above, § 95).

89. There are a number of elements relevant to a consideration of whether a person's private life is concerned by measures effected outside a person's home or private premises. Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor in this assessment (see *P.G. and J.H. v. the United Kingdom* , cited above, § 57; *Bărbulescu* , cited above, § 73; and *Antović and Mirković* , cited above, § 43). As to the monitoring of an individual's actions using photographic or video devices, the Convention institutions have taken the view that the monitoring of the actions and movements of an individual in a public place using a camera which did not record the visual data does not constitute in itself a form of interference with private life (see *Herbecq and the Association "Ligue des Droits de l ' Homme " v. Belgium* , nos. 32200/96 and 32201/96, Commission decision of 14 January 1998, Decisions and Reports 92-B, p. 92, and *Perry* , cited above, § 41). Private-life considerations may arise, however, once any systematic or permanent record of such personal data comes into existence, particularly pictures of an identified person (see *Peck v. the United Kingdom* , no. 44647/98, §§ 58-59, ECHR 2003I; *Perry* , cited above, §§ 38 and 41; and *Vukota-Bojić v. Switzerland* , no. 61838/10, §§ 55 and 59, 18 October 2016). As the Court has stated in this connection, a person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers. The right of each person to the protection of his or her image is thus one

of the essential components of personal development and presupposes the right to control the use of that image. Whilst in most cases the right to control such use involves the possibility for an individual to refuse publication of his or her image, it also covers the individual's right to object to the recording, conservation and reproduction of the image by another person (see *Reklos and Davourlis v. Greece* , no. 1234/05, § 40, 15 January 2009, and *De La Flor Cabrera v. Spain* , no. 10764/09, § 31, 27 May 2014).

90. In order to determine whether Article 8 applies, the Court also finds it relevant to address the question whether the individual in question was targeted by the monitoring measure (see *Perry* , cited above, § 40; *Köpke* , cited above; and *Vukota-Bojić* , cited above, §§ 56 and 58) or whether personal data was processed, used or made public in a manner or to a degree surpassing what those concerned could reasonably have foreseen (see *Peck* , cited above, §§ 62-63; *Perry* , cited above, §§ 40-41; and *Vukota-Bojić* , cited above, § 56).

91. As regards, more specifically, the issue of video-surveillance in the workplace, the Court has found that video-surveillance implemented by an employer without the employee's knowledge, for about fifty hours over a two-week period, and the use of the recordings thus obtained in the proceedings before the employment courts to justify her dismissal, interfered with her right to respect for her private life (see *Köpke* , cited above). The non-covert video-surveillance of university lecturers while they were teaching, where the recordings had been kept for one month and could be consulted by the dean of the faculty, was also found to have interfered with the applicants' right to respect for their private life (see *Antović and Mirković* , cited above, §§ 44-45).

Application of those principles to the present case

92. The Court notes that in the present case the applicants were subjected to a video-surveillance measure implemented by their employer in their workplace for a period of ten days, the cameras being directed towards the supermarket checkout area and its surroundings. Thus, while the applicants were not individually targeted by the video-surveillance, it is not in dispute that the first three of them, who were working behind the tills, could have been filmed throughout their working day, while the fourth and fifth applicants were filmed when they were passing through that area.

93. As to whether the applicants had a reasonable expectation that their private life would be protected and respected, the Court observes that their workplace, a supermarket, was open to the public and that the activities filmed there, namely the taking of payments for purchases by the customers, were not of an intimate or private nature. Their expectation as to the protection of their private life was thus necessarily limited. However, even in public places, the creation of a systematic or permanent recording of images of identified persons and the subsequent processing of the images thus recorded could raise questions affecting the private life of the individuals concerned (see paragraph 89 above and the case-law cited therein). The Court notes that in the present case domestic law provided a formal and explicit statutory framework which obliged a person responsible for a video-surveillance system, even in a public place, to give prior information to the persons being monitored by such a system (see paragraphs 47 and 50 above). The applicants had, moreover, been informed about the installation by their employer of other CCTV cameras in the supermarket, those cameras being visible and positioned such as to film the shop's entrances and exits. In those circumstances the applicants had a reasonable expectation that they would not be subjected to video-surveillance in the other areas of the shop without being informed beforehand.

94. As to the processing and use of the video recordings, the Court notes that they were viewed by a number of people working for the applicants' employer even before the applicants were informed of their existence. In addition, they constituted the basis of their dismissal and were used in evidence in the Employment Tribunal proceedings.

95. Having regard to the foregoing, the Court finds that Article 8 is applicable in the present case.

P. Compliance with Article 8 of the Convention

15. The parties' submissions

(c) The applicants

96. The applicants began by drawing attention to the fact that the only questions for discussion in the present case were whether their right to respect for their private life had been infringed on account of the introduction of the video-surveillance measure without their knowledge, together with that of the limits imposed by Article 8 of the Convention on the monitoring that an employer was entitled to use against its employees. They took the view that, contrary to what the Government had suggested, the question of their possible criminal liability had already been settled at domestic level and could not be a matter of debate before the Court.

97. The applicants acknowledged that an employer had to be able to install surveillance systems to protect its property but argued that this right should be limited in order to preserve the employees' right to respect for their private life. They explained that, in the present case, they and all the supermarket staff had been filmed for weeks, throughout the working day, without having been informed beforehand. The monitoring had been implemented in breach of Spanish law, which provided for an obligation for the employer, if not to obtain the consent of the employees, at least to inform them

beforehand of the installation of the cameras and of their rights under the data-protection legislation. If such indications had been given, both their right to respect for their private life and the employer's interests would have been preserved. The applicants thus concluded that, by refusing to find fault with this omission on the part of the employer, the domestic courts had not granted them sufficient protection under Article 8 of the Convention.

98. The applicants were of the opinion that the present case had to be distinguished from that of *Köpke v. Germany* (decision cited above) on a number of points. They argued that in the *Köpke* case there had been no specific legislation on video-surveillance in the workplace and the employer had complied with the conditions laid down by the domestic case-law, whereas, in the present case, their employer had breached the domestic legislation without being penalised. Furthermore, the monitoring had been more extensive in their case because it had been introduced without a time-limit, had continued throughout the working day and had involved filming not only the employees under suspicion but the whole staff.

99. The applicants asked the Court to follow the approach adopted in its recent judgment in *Bărbulescu v. Romania* (cited above), a case about an employer's monitoring of messaging and internet use by an employee, which in their view laid down the proportionality criteria to be met by any interference by an employer with the right to privacy of its employees. They argued that the measure taken by their employer clearly did not meet these requirements, given the lack of prior information about the introduction of video-surveillance and the rights provided for in the data-protection legislation. They added that this measure was not proportionate since the employer's interests could have been safeguarded while providing employees with the information required by law.

100. The applicants concluded that, by refusing to acknowledge that the video-surveillance by means of hidden cameras had infringed their right to respect for their private life and by holding, consequently, that their dismissals were lawful, the domestic courts had deprived them of the protection to which they were entitled against improper interference with their privacy by their employer. Contrary to what the Government had argued, this complaint was distinct from those that they had made under Article 6 of the Convention.

101. Moreover, as regards the possibility of complaining to the Spanish Data Protection Agency, the applicants repeated the arguments they had made in response to the Government's objection of non-exhaustion of domestic remedies (see paragraph 81 above) and submitted that, even if that Agency had found an administrative offence, the imposition of an administrative sanction on the employer would not have provided appropriate redress for the alleged breach of their right to respect for their private life. As to the possibility of seeking redress in the ordinary civil courts, they explained that those courts had no jurisdiction in respect of relations under an employment contract and that the case-law cited by the Government by way of example, concerning a situation in which the employment relationship had been severed two years earlier, could not be transposed to the present case (see paragraph 49 above). In their view, the main consequence of the video-surveillance had been their dismissal, in respect of which only the employment courts had jurisdiction.

(d) The Government

102. The Government observed that, as the breach of privacy alleged by the applicants was attributable to a private company and not to the authorities, the Grand Chamber should follow the approach adopted in the case of *Von Hannover (no. 2) v. Germany* (cited above), in which the Court had examined whether the domestic courts had weighed up the various individual interests at stake and had struck a fair balance between them. In their view, the Spanish courts had performed such a balancing exercise and had taken due account of the applicants' right to respect for their private life.

103. The Government argued that, even if it would have been desirable for the applicants to have been informed of the installation of the CCTV cameras, the measures taken by the employer had not been disproportionate. They observed that the applicants had been working in an area that was open to the public, that they had been informed of the installation of certain CCTV cameras following the suspicions of theft and that they had knowingly committed criminal acts. The present application was similar to the *Köpke* case and the distinction made by the Chamber judgment was not justified. They explained in this connection that the monitoring had lasted for only ten days, from 15 to 25 June, on which date the employees under suspicion had been called for individual interview, and that it had been directed not at the whole staff but only at those working in the checkout area, who were in direct contact with the customers. The present case should, by contrast, be distinguished from *Bărbulescu* as in that case the impugned interference had concerned compliance with the employer's instructions, which the Court found to have "reduce[d] private social life in the workplace to zero", whereas the video-surveillance measure at issue had pursued a legitimate aim, namely to shed light on an offence of which the company had been the victim. They added that, as the applicants had worked in an area where they were in direct contact with the public, their expectation of privacy had necessarily been reduced in comparison with a situation involving the confidentiality of communications exchanged via a messaging account.

104. Moreover, relying on their arguments in support of

their objection of non-exhaustion of domestic remedies (see paragraph 81 above), the Government maintained that the applicants could have submitted a complaint to the Spanish Data Protection Agency alleging a failure to comply with the Personal Data Protection Act. This agency was an independent body, empowered to monitor the application of data-protection legislation and to impose fines on offenders, whereas the employment courts to which the applicants had taken their case only had jurisdiction to rule on the lawfulness of dismissals. Any failure to comply with data-protection legislation did not automatically lead to a violation of the right to respect for private life, and these two concepts were not to be confused.

105. The Government submitted that the applicants could also have brought an action before the ordinary civil courts to claim compensation for any damage caused by the alleged breach of the Personal Data Protection Act. In support of their argument they submitted a judgment of the Supreme Court, which had awarded compensation to an employee for the unlawful transmission of personal data by his former employer (see paragraph 49 above).

106. The Government concluded that the respondent State had complied with its positive obligations under Article 8 of the Convention and that its responsibility should not be engaged on account of any infringements by a private company or for a failure by the applicants to complain of such infringements to the competent domestic authorities.

16. The third-party's submissions

107. The European Trade Union Confederation (ETUC), intervening as a third party, expressed its concern that States might not sufficiently protect the privacy of workers in the workplace. It emphasised that the protection of privacy in general and in employment relations in particular was a relatively new aspect of international human rights protection and that the risks for privacy deriving from new technologies were increasing. In its view, this was why international, and in particular European, human rights protection had developed in the sense that, irrespective of the question of permitted processing of personal data as such, those concerned had to be informed.

108. The ETUC stressed that the right to be informed of the collection of personal data was expressly recognised in domestic law under section 5(1) of the Personal Data Protection Act. Highlighting how several European legal instruments (at Council of Europe as well as European Union level) had addressed the protection of privacy, either in the general form of protection of personal data or more specifically in the case of video-surveillance in the workplace, it concluded that the right of the data subject to be informed prior to the processing of his or her personal data was to be regarded as a right derived from Article 8 of the Convention, constituting a procedural safeguard. Moreover, in situations where it was not required to give prior information to the employees themselves, the notification and consultation of their representatives would be essential.

17. The Court's assessment

(e) Positive obligations of the respondent State

109. The Court observes that, in the present case, the video-surveillance measure complained of by the applicants was imposed by their employer, a private company, and cannot therefore be analysed as an "interference", by a State authority, with the exercise of Convention rights. The applicants nevertheless took the view that, by confirming their dismissals on the basis of that video-surveillance, the domestic courts had not effectively protected their right to respect for their private life.

110. The Court reiterates that although the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in effective respect for private or family life. These obligations may necessitate the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves (see *Söderman v. Sweden* [GC], no. 5786/08, § 78, ECHR 2013, and *Von Hannover (No. 2)* , cited above, § 98). The responsibility of the State may thus be engaged if the facts complained of stemmed from a failure on its part to secure to those concerned the enjoyment of a right enshrined in Article 8 of the Convention (see *Bărbulescu* , cited above, § 110, and *Schüth v. Germany* , no. 1620/03, §§ 54 and 57, ECHR 2010).

111. Accordingly, in line with the approach it has followed in similar cases, the Court takes the view that the complaint should be examined from the standpoint of the State's positive obligations under Article 8 of the Convention (see *Bărbulescu* , cited above, § 110; *Köpke* , cited above; and *De La Flor Cabrera* , cited above, § 32). 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 private and public interests, 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, and *Bărbulescu* , cited above, § 112). The margin of appreciation goes hand in hand with European supervision, embracing both the legislation and the decisions applying it, even those given by independent courts. In exercising its supervisory function, the Court does not have to take the place of the national courts but to review, in the light of the case as a whole, whether their decisions were compatible with the

provisions of the Convention relied upon (see *Peck* , cited above, § 77, and *Von Hannover (no. 2)* , cited above, § 105).

112. 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 *Von Hannover (no. 2)* , cited above, § 104; *Söderman* , cited above, § 79; and *Bărbulescu* , cited above, § 113).

113. The Court has already held that, in certain circumstances, the fulfilment of positive obligations imposed by Article 8 requires the State to adopt a legislative framework to protect the right at issue (see *X and Y v. the Netherlands* , 26 March 1985, §§ 23, 24 and 27, Series A no. 91, and *M.C. v. Bulgaria* , no. 39272/98, § 150, ECHR 2003XII, concerning cases of sexual assault on minors; and *Codarcea v. Romania* , no. 31675/04, §§ 10204, 2 June 2009, as regards medical negligence). Concerning the gravest acts, such as rape, this obligation may go as far as requiring the adoption of criminal-law provisions (see *M.C. v. Bulgaria* , cited above, § 150). In respect of less serious acts between individuals which may affect the rights protected under Article 8, the Court takes the view that Article 8 leaves it to the discretion of States to decide whether or not to pass specific legislation and it verifies that the existing remedies were capable of providing sufficient protection of the rights at issue (see, concerning the protection of a minor's personal integrity, *Söderman* , cited above, §§ 86-91; and on the right to the protection of one's image, *Von Hannover (no. 2)* , cited above, §§ 95-126, and *Reklos and Davourlis* , cited above, §§ 34-43).

114. As regards, more specifically, the monitoring of employees in the workplace, the Court has taken the view that Article 8 leaves it to the discretion of States to decide whether or not to enact specific legislation on video-surveillance (see *Köpke* , cited above) or the monitoring of the non-professional correspondence and other communications of employees (see *Bărbulescu* , cited above, § 119). It has nevertheless pointed out that, regardless of the discretion enjoyed by States in choosing the most appropriate means for the protection of the rights in question, the domestic authorities should ensure that the introduction by an employer of monitoring measures affecting the right to respect for private life or correspondence of its employees is proportionate and is accompanied by adequate and sufficient safeguards against abuse (see *Bărbulescu* , cited above, § 120, and *Köpke* , cited above).

115. In the *Bărbulescu* judgment, the Court set out a certain number of requirements that must be met by any monitoring of the correspondence and communications of employees if it is not to breach Article 8 of the Convention (see *Bărbulescu* , cited above, § 121). It also found in that judgment that, to ensure effective compliance with those requirements, the employees concerned must have access to a remedy before an independent judicial body with jurisdiction to determine, at least in substance, whether the relevant conditions were satisfied (ibid., § 122).

116. The Court is of the view that the principles established in the *Bărbulescu* judgment, a number of which came from the decision in *Köpke* , which concerned facts that were similar to those in the present case, are transposable, *mutatis mutandis* , to the circumstances in which an employer may implement video-surveillance measures in the workplace. These criteria must be applied taking into account the specificity of the employment relations and the development of new technologies, which may enable measures to be taken that are increasingly intrusive in the private life of employees. In that context, in order to ensure the proportionality of video-surveillance measures in the workplace, the domestic courts should take account of the following factors when they weigh up the various competing interests:

(i) Whether the employee has been notified of the possibility of video-surveillance measures being adopted by the employer 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 notification should normally be clear about the nature of the monitoring and be given prior to implementation.

(ii) The extent of the monitoring by the employer and the degree of intrusion into the employee's privacy. In this connection, the level of privacy in the area being monitored should be taken into account, together with any limitations in time and space and the number of people who have access to the results.

(iii) Whether the employer has provided legitimate reasons to justify monitoring and the extent thereof. The more intrusive the monitoring, the weightier the justification that will be required.

(iv) Whether it would have been possible to set up a monitoring system based on less intrusive methods and measures. In this connection, there should be an assessment in the light of the particular circumstances of each case as to whether the aim pursued by the employer could have been achieved through a lesser degree of interference with the employee's privacy.

(v) The consequences of the monitoring for the employee subjected to it. Account should be taken, in particular, of the use made by the employer of the results of the monitoring

and whether such results have been used to achieve the stated aim of the measure.

(vi) Whether the employee has been provided with appropriate safeguards, especially where the employer's monitoring operations are of an intrusive nature. Such safeguards may take the form, among others, of the provision of information to the employees concerned or the staff representatives as to the installation and extent of the monitoring, a declaration of such a measure to an independent body or the possibility of making a complaint.

117. The Court will thus ascertain in the present case whether the domestic law, and in particular its application by the employment courts which examined the applicants' cases, provided sufficient protection, in weighing up the competing interests, of their right to respect for their private life.

(f) Application to the present case of the above-mentioned principles

118. In the present case, the positive obligations imposed on the State by Article 8 of the Convention required the national authorities to strike a fair balance between two competing interests, namely, on the one hand, the applicants' right to respect for their private life and, on the other, the possibility for their employer to ensure the protection of its property and the smooth operation of its company, particularly by exercising its disciplinary authority.

119. The Court notes at the outset that, at the material time, Spanish law had laid down a legal framework intended to protect the private life of employees in situations such as that in the present case. Thus, the Personal Data Protection Act and Instruction no. 1/2006 specifically on video-surveillance provided for a certain number of safeguards and conditions to be satisfied by any measure of video-surveillance and the ensuing processing of personal data. Failure to provide these safeguards could give rise to administrative sanctions and could engage the civil liability of the person responsible for the data processing (see paragraphs 46 and 48 above). In addition, Article 20 § 3 of the Employment Regulations limited the employer's use of monitoring, as regards the fulfilment by employees of their employment duties, by requiring that the measures taken in that regard were compatible with their human dignity. Moreover, the applicable rules of procedure required the domestic courts to exclude any evidence obtained in breach of a fundamental right. Lastly, there was case-law of the ordinary courts and the Constitutional Court requiring that any measures interfering with the privacy of employees had to pursue a legitimate aim ("appropriateness test"), and had to be necessary for the fulfilment of the aim pursued ("necessity test") and proportionate to the circumstances of each case ("strict proportionality test") (see paragraphs 54 et seq. above).

120. In these circumstances the Court observes that the regulatory framework which was in place under domestic law is not at issue in the present case. The applicants have not in fact questioned the pertinence of that framework (see paragraph 97 above), but they argued that it was precisely the refusal of the employment courts to draw the appropriate conclusions from the employer's failure to fulfil its domestic-law obligation to provide information which had breached the Convention.

121. Accordingly, the Court will consider the manner in which the domestic courts to which the applicants appealed examined their complaint that their right to respect for their private life in the workplace had been breached and whether, as the Government argued, other domestic-law remedies could have provided them with appropriate protection.

122. The Court would begin by noting that the employment courts identified the various interests at stake, referring expressly to the applicants' right to respect for their private life and the balance to be struck between that right and the employer's interest in ensuring the smooth running of the company by exercising its management powers. It will thus ascertain how those courts took into account the factors listed above when they weighed up these interests.

123. The domestic courts first found, in accordance with the requirements of the Constitutional Court's case-law, that the installation of the video-surveillance had been justified by legitimate reasons, namely the suspicion, put forward by the supermarket manager on account of the significant losses recorded over several months, that thefts had been committed. They also took account of the employer's legitimate interest in taking measures in order to discover and punish those responsible for the losses, with the aim of ensuring the protection of its property and the smooth functioning of the company.

124. The domestic courts then examined the extent of the monitoring and the degree of intrusion into the applicants' privacy, finding that the measure was limited as regards the areas and staff being monitored – since the cameras only covered the checkout area, which was likely to be where the losses occurred – and that its duration had not exceeded what was necessary in order to confirm the suspicions of theft. In the Court's opinion this assessment could not be regarded as unreasonable. It notes that the monitoring did not cover the whole shop but targeted the areas around the tills, where thefts were likely to have been committed. The three applicants who worked as cashiers were indeed monitored by CCTV cameras throughout their working day. As a result of their jobs within the company, they could not evade these recordings, which were aimed at all the staff working in the checkout area, and were operated permanently and without any limitation (contrast *Köpke* , cited above, concerning an applicant who was both a shop

assistant and cashier of the store in question, the video-surveillance measure thus not covering the entirety of her place of work). To some extent, they thus found themselves in limited areas (see, *mutatis mutandis* , *Allan v. the United Kingdom* , no. 48539/99, § 35, ECHR 2002IX, and *Perry* , cited above, §§ 39-43). As to the fourth and fifth applicants, the CCTV cameras filmed them whenever they passed through the checkout area.

125. At the same time it should be pointed out that the applicants' duties were performed in a place that was open to the public and involved permanent contact with customers. The Court takes the view in this connection that it is necessary to distinguish, in the analysis of the proportionality of a video-surveillance measure, the various places in which the monitoring was carried out, in the light of the protection of privacy that an employee could reasonably expect. That expectation is very high in places which are private by nature, such as toilets or cloakrooms, where heightened protection, or even a complete ban on video-surveillance, is justified (see, to this effect, the relevant international instruments cited in paragraphs 61 and 65 above). It remains high in closed working areas such as offices. It is manifestly lower in places that are visible or accessible to colleagues or, as in the present case, to the general public.

126. As regards the extent of the measure over time, the Court notes that while, as the applicants argued, the employer had not set the duration of the video-surveillance beforehand, in actual fact it lasted for ten days and ceased as soon as the employees responsible had been identified. The length of the monitoring does not therefore appear excessive in itself (compare *Köpke* , cited above, where a duration of fourteen days was not found to be disproportionate). Lastly, only the supermarket manager, the company's legal representative and the union representative viewed the recordings obtained through the impugned video-surveillance before the applicants themselves had been informed. Having regard to these factors, the Court takes the view that the intrusion into the applicants' privacy did not attain a high degree of seriousness.

127. As regards the consequences of the impugned monitoring for the applicants, the Court finds that they were significant because the employees concerned were dismissed on the basis of recordings obtained by that means. It nevertheless observes, as the domestic courts also noted, that the video-surveillance and recordings were not used by the employer for any purposes other than to trace those responsible for the recorded losses of goods and to take disciplinary measures against them (compare *Peck* , cited above, §§ 62-63, where the images recorded by a CCTV camera of public places showing the applicant's attempted suicide had been distributed to the media).

128. The domestic courts additionally found that, in the circumstances of the case, there were no other means by which to fulfil the legitimate aim pursued and that the measure should therefore be regarded as "necessary" within the meaning of the Constitutional Court's case-law (see paragraph 33 above). Even if it would have been desirable for the domestic courts to examine in a more in-depth manner the possibility for the employer to have used other measures entailing less intrusion into the private life of the employees, the Court cannot but note that the extent of the losses identified by the employer suggested that thefts had been committed by a number of individuals and the provision of information to any staff member might well have defeated the purpose of the video-surveillance, which was, as those courts noted, to discover those responsible for the thefts but also to obtain evidence for use in disciplinary proceedings against them.

129. The Court further observes that domestic law prescribed a certain number of safeguards for the purpose of preventing any improper interference with the rights of individuals whose personal data was subject to collection or processing. The Personal Data Protection Act in particular conferred on those individuals the right to be informed of such safeguards beforehand, as provided for in section 5 of the Act, together with a right of access, rectification and deletion in respect of the data collected. A requirement of proportionality in the collection and use of the images obtained through video-surveillance was expressly laid down by Instruction no. 1/2006 and, according to the Constitutional Court's case-law, the domestic courts had to review the appropriateness, necessity and proportionality of such measures in the light of the fundamental rights guaranteed by the Constitution (see paragraphs 47, 50 and 54 above).

130. As to whether, lastly, the applicants had been informed of the installation of the video-surveillance, the Court notes that it was not in dispute that two types of camera had been installed in the supermarket where they worked: on the one hand, visible cameras directed towards the shop's entrances and exits, of which the employer had informed the staff; and, on the other, hidden cameras directed towards the checkout areas, of which neither the applicants nor the other staff members had been informed. It was stated in the parties' observations that one or more information boards had been placed in the supermarket to notify the public of the presence of CCTV cameras but the exact content of the information on these boards has not been ascertained.

131. The Court observes that, while both Spanish law and the relevant international and European standards do not seem to require the prior consent of individuals who are placed under video-surveillance or, more generally, who have their personal data collected, those rules establish that it is, in principle, necessary to inform the individuals

concerned, clearly and prior to implementation, of the existence and conditions of such data collection, even if only in a general manner (see paragraphs 47, 60 and 63 above). It takes the view that the requirement of transparency and the ensuing right to information are fundamental in nature, particularly in the context of employment relationships, where the employer has significant powers with regard to employees and any abuse of those powers should be avoided (see paragraphs 61-62 and 64-65 above). It would point out, however, that the provision of information to the individual being monitored and its extent constitute just one of the criteria to be taken into account in order to assess the proportionality of a measure of this kind in a given case. However, if such information is lacking, the safeguards deriving from the other criteria will be all the more important.

132. In the present case, the Court observes that the employment courts which examined the applicants' claims carried out a detailed balancing exercise between, on the one hand, their right to respect for their private life, and on the other the employer's interest in ensuring the protection of its property and the smooth operation of the company. It notes that the proportionality criteria established by the Constitutional Court's case-law and followed in the present case are close to those which it has developed in its own case-law. The domestic courts thus verified whether the video-surveillance was justified by a legitimate aim and whether the measures adopted for that purpose were appropriate and proportionate, having observed in particular that the legitimate aim pursued by the employer could not be attained by measures that were less intrusive for the applicants' rights.

133. Admittedly, the employment courts did not take account of the employer's failure, as alleged by the applicants, to provide them with the prior information required by section 5 of the Personal Data Protection Act, having considered the matter irrelevant and not capable of calling into question the proportionality, in the constitutional sense, of the measure, provided that the other criteria laid down by the Constitutional Court were satisfied. Given the importance of the right to information in such cases, the Court finds that only an overriding requirement relating to the protection of significant public or private interests could justify the lack of prior information.

134. However, in the specific circumstances of the present case, having regard particularly to the degree of intrusion into the applicants' privacy (see paragraphs 125-26 above) and to the legitimate reasons justifying the installation of the video-surveillance, the Court finds that the employment courts were able, without overstepping the margin of appreciation afforded to national authorities, to take the view that the interference with the applicants' privacy was proportionate (see, for a similar situation, *Köpke* , cited above). Thus, while it cannot accept the proposition that, generally speaking, the slightest suspicion of misappropriation or any other wrongdoing on the part of employees might justify the installation of covert video-surveillance by the employer, the existence of reasonable suspicion that serious misconduct has been committed and the extent of the losses identified in the present case may appear to constitute weighty justification. This is all the more so in a situation where the smooth functioning of a company is endangered not merely by the suspected misbehaviour of one single employee, but rather by the suspicion of concerted action by several employees, as this creates a general atmosphere of mistrust in the workplace.

135. Moreover, as the Government argued, the applicants had other remedies available to them, as provided for by the Personal Data Protection Act, for the specific purpose of obtaining sanctions for breaches of that legislation. The applicants could thus have complained to the Data Protection Agency of a failure by the employer to fulfil its obligation to provide prior information, as required by section 5 of that Act. The Agency had the power to investigate the alleged breach of the law and impose financial penalties on the person responsible. They could also have referred the matter to the ordinary courts in order to obtain redress for the alleged breach of their rights under the Personal Data Protection Act. The Court notes in this connection that while the case-law cited by the Government (see paragraph 49 above) does indeed concern a situation which is not identical to that of the present case, the right to obtain redress for damage caused by a breach of the Personal Data Protection Act was expressly provided for in section 19 thereof and there is no reason to question the effectiveness of that remedy now.

136. Domestic law had thus made available to the applicants other remedies by which to secure the specific protection of personal data, but they chose not to use those remedies. The Court reiterates in this connection that the effective protection of the right to respect for private life in the context of video-surveillance in the workplace may be ensured by various means, which may fall within employment law but also civil, administrative or criminal law (see, *mutatis mutandis* , *Bărbulescu* , cited above, § 116).

137. Under those circumstances, having regard to the significant safeguards provided by the Spanish legal framework, including the remedies that the applicants failed to use, and the weight of the considerations justifying the video-surveillance, as taken into account by the domestic courts, the Court concludes that the national authorities did not fail to fulfil their positive obligations under Article 8 of the Convention such as to overstep their margin of appreciation. Accordingly, there has been no violation of that provision.

VII. ALLEGED VIOLATION OF ARTICLE 6 OF THE CONVENTION

138. Under Article 6 of the Convention, the applicants complained that recordings obtained in breach of their right to respect for their private life had been admitted and used in evidence by the employment courts.

139. The third, fourth and fifth applicants further argued that the acknowledgment of the validity of the settlement agreements that they had signed, allegedly following deceitful manipulation by the employer, had also breached their right to a fair hearing.

140. The relevant parts of Article 6 provide as follows:

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

Q. Chamber judgment

141. In its judgment of 9 January 2018 the Chamber reiterated that, in order to assess compliance with Article 6 of the Convention, it was required to determine whether the proceedings as a whole, including the way in which evidence had been taken, had been fair. Finding that the applicants had been able to challenge both the authenticity and the admission in evidence of the footage obtained by means of video-surveillance and that this was not the only evidence on which the courts had based their decisions, it concluded that there had been no violation of Article 6 on this point.

142. As regards the settlement agreements, the Chamber found that the three applicants in question had had ample opportunity to challenge their validity in the domestic courts, which had taken the view, without any appearance of arbitrariness, that no duress on the employer's part had vitiated the applicants' consent. It thus found that there had been no violation of Article 6 under this head either.

R. The parties' submissions

18. The applicants

143. The applicants submitted that the domestic courts had based their decisions mainly on recordings obtained by their employer in a manner that was unlawful and in breach of their right to privacy. Consequently, in their view, the mere admission of these recordings in evidence entailed a violation of Article 6 of the Convention. The applicants further submitted that both the obtaining of this evidence and its use in the proceedings constituted an abuse by the employer of its dominant position and a breach of the equality of arms. In this connection, they pointed out that they had not been aware of the existence of the video-surveillance and had not had access to the recordings until they had been produced in evidence in the context of the judicial proceedings to which they were parties. As to the other evidence, in particular the witness testimony, on which the domestic courts had relied, it had been "vitiated" by the prior viewing of the footage by those concerned.

144. The third, fourth and fifth applicants further argued that, when they had signed the settlement agreements, they had been misled as to the significance of the concession made by their employer. They stated that the law obliged any individual to report a criminal offence on becoming aware of it and that the employer could not therefore validly waive the right to file a criminal complaint. In those circumstances, the courts should have declared the settlement agreements null and void and excluded them from the case file. In support of their argument they adduced a judgment of the Catalonia High Court of 19 October 2010 in the case of one of their colleagues, Ms D.

19. The Government

145. The Government agreed with the findings of the Chamber judgment, which they invited the Grand Chamber to confirm. As to the use of footage recorded by means of video-surveillance, they asserted that the recordings had been used merely to complement other evidence in the file and that the applicants had had the opportunity to contest their use and authenticity in the domestic courts.

146. As regards the settlement agreements, the Government argued that, as found by the domestic courts, they had been signed without any pressure from the employer. They submitted that it was the applicants who had breached these agreements by bringing the matter before the Employment Tribunal in spite of the undertaking given and that, even so, their appeals had been duly examined by the courts. They argued that, while those courts had indeed taken into account the applicants' acknowledgment of the facts as reflected in the agreements, they had also had other evidence at their disposal. Lastly, with regard to the case of Ms D., cited by the applicants, they explained that, while the High Court had certainly overturned an initial judgment on the ground that, according to that judgment, the settlement agreement in question had deprived the employee of her right to take legal action, the courts examining the case after it was remitted had ultimately considered that the settlement agreement was nevertheless valid and could be used to prove the acknowledgment of the facts by the person concerned.

S. The third-party's submissions

147. The European Trade Union Confederation was of the view that a judgment mainly based on recordings from covert video-surveillance was in breach of Article 6 of the Convention.

148. As regards the settlement agreements signed by the third, fourth and fifth applicants, the ETUC pointed out that

such agreements were often used when confronting workers with alleged misconduct, creating a situation where the employees felt under specific pressure, were not properly advised and were not in a position to demand the recognition of their procedural and substantive rights. The ETUC concluded that the specificity of employment relations required a cautious approach to the recognition of such agreements.

T. The Court's assessment

20. General principles

149. The Court reiterates that its only duty, in accordance with Article 19 of the Convention, is to ensure the observance of the engagements undertaken by the States Parties to the Convention. In particular, it is not competent to deal with an application alleging that errors of law or fact have been committed by domestic courts, except where it considers that such errors might have involved a possible violation of any of the rights and freedoms set out in the Convention. While Article 6 guarantees the right to a fair hearing, it does not lay down any rules on the admissibility of evidence as such, which is primarily a matter for regulation under national law (see *Schenk v. Switzerland* , 12 July 1988, § 45, Series A no. 140, and *García Ruiz v. Spain* [GC], no. 30544/96, § 28, ECHR 1999I). Normally, issues such as the weight attached by the national courts to given items of evidence or to findings or assessments in issue before them for consideration are not for the Court to review. The Court should not act as a court of fourth instance and will not therefore question under Article 6 § 1 the judgment of the national courts, unless their findings can be regarded as arbitrary or manifestly unreasonable (see *Bochan v. Ukraine (no. 2)* [GC], no. 22251/08, § 61, ECHR 2015).

150. It is therefore not the role of the Court to determine, as a matter of principle, whether particular types of evidence – for example, evidence obtained unlawfully in terms of domestic law – may be admissible. The question which must be answered is whether the proceedings as a whole, including the way in which the evidence was obtained, were fair. This involves an examination of the unlawfulness in question and, where the violation of another Convention right is concerned, the nature of the violation found (see *P.G. and J.H. v. the United Kingdom* , cited above, § 76, and *Gäfgen v. Germany* [GC], no. 22978/05, § 163, ECHR 2010).

151. As regards the nature of the unlawfulness or of the Convention violation, while the use of evidence secured as a result of a measure found to be in breach of Article 3 always raises serious issues as to the fairness of the proceedings (see *Gäfgen* , cited above, § 165), the question whether the use in evidence of information obtained in violation of Article 8 or of domestic law 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. 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 question whether the circumstances in which it was obtained cast doubt on its reliability or accuracy (see *Schenk* , cited above, §§ 46-48; *P.G. and J.H. v. the United Kingdom* , cited above, §§ 77-79; and *Gäfgen* , cited above, § 164). While no problem of fairness necessarily arises where the evidence obtained was unsupported by other material, it may be noted that where the evidence is very strong and there is no risk of its being unreliable, the need for supporting evidence is correspondingly weaker (see *Gäfgen* , cited above, § 164).

152. The Court notes that the principles set out above concerning the admissibility of evidence were developed in a criminal-law context, although it has already had occasion to apply them in a case concerning the fairness of civil proceedings (see *Vukota-Bojić* , cited above, §§ 92-100). It observes that, while the "fair trial" guarantees are not necessarily the same in criminal-law and civil-law proceedings, the States having greater latitude when dealing with civil cases, it may nevertheless draw inspiration, when examining the fairness of civil-law proceedings, from the principles developed under the criminal limb of Article 6 (see *Carmel Saliba v. Malta* , no. 24221/13, § 67, 29 November 2016). In the present case, the Court takes the view that the principles in question are applicable to its examination of the fairness of the civil proceedings at issue.

21. Application to the present case

153. The Court will examine the complaint of a violation of Article 6, made by all five applicants on the basis of the admission in evidence of recordings from video-surveillance, and then the complaint of a violation of that provision made by the third, fourth and fifth applicants in respect of the acceptance of the settlement agreements signed by them.

(g) Consideration of the video-surveillance images as part of the evidence

154. The Court points out that it has not found a violation of Article 8 of the Convention on account of the video-surveillance to which the applicants were subjected (see paragraph 137 above). It notes, however, that the applicants argued that the video-surveillance had been installed in breach of the statutory obligation under domestic law to provide prior information and that the employment courts did not address that question, having deemed it not to be pertinent (see paragraph 34 above). The Court will thus examine whether the use in evidence of the images

obtained by means of the video-surveillance at issue undermined the fairness of the proceedings as a whole.

155. The Court begins by noting that, in the context of the proceedings before the Employment Tribunal, the applicants had access to the recordings obtained by means of the impugned video-surveillance and were able to contest their authenticity and oppose their use in evidence. The domestic courts examined the applicants' argument that the recordings had to be excluded from the case file because they had been obtained in breach of a fundamental right and in their decisions they gave extensive reasoning on this point. They thus found that, in line with the Constitutional Court's case-law, the video-surveillance had not been implemented in breach of the applicants' right to respect for their private life. They further found that the images obtained from the video-surveillance were not the only items of evidence in the file.

156. As regards the quality of evidence, the Court notes that the applicants did not at any time dispute the authenticity or accuracy of the footage recorded by means of video-surveillance, their main complaint being based on the lack of prior information about the installation of the cameras. The domestic courts, for their part, found that the recordings presented sufficient guarantees of authenticity. Given the circumstances in which the recordings were obtained, the Court does not see any reason to question their authenticity or reliability. It thus takes the view that they constituted sound evidence which did not necessarily need to be corroborated by other material.

157. The Court would nevertheless note that the recordings in question were not the only evidence on which the domestic courts based their findings. It can be seen from their decisions that they also took account of the applicants' statements, the testimony of the supermarket manager, the company's legal representative and the staff representative – to whom the applicants had admitted the misconduct – and the expert's report comparing the images recorded by the video-surveillance and the till receipts. The Court observes that the till receipts, which constitute objective evidence that cannot be "vitiated" by the viewing of the recordings, showed that a significant number of purchases had been cancelled without payment. As regards the third, fourth and fifth applicants, the courts also relied on their acknowledgment of the facts in the settlement agreements they had signed. Having examined this evidence as a whole, they found the facts to be comprehensively established.

158. In the light of the foregoing, the Court takes the view that the use in evidence of the images obtained by video-surveillance did not undermine the fairness of the proceedings in the present case.

(h) Consideration of the settlement agreements signed by the third, fourth and fifth applicants

159. The Court would begin by observing that the domestic courts accepted the settlement agreements signed by these three applicants, having taken the view that their consent had not been vitiated. However, unlike the Employment Tribunal, which had found that, by signing those agreements, they had waived their right to take legal action, the High Court, ruling on appeal, found that those agreements did not constitute a waiver by the applicants of their right of access to a court and it examined the case on the merits. It took the view that the agreements gave effect to the unequivocal acceptance by the applicants of the employer's decision to terminate their employment contracts on the grounds set out in the dismissal letter. In those circumstances, the Court finds that the complaint, as set out by the applicants, relates to the assessment by the domestic courts of the validity and weight of evidence.

160. It notes in this connection that the three applicants were able to dispute the validity of the settlement agreements and oppose their admission in evidence. The domestic courts analysed all the arguments put forward by those applicants and took the view that the circumstances of the present case did not indicate any intimidation or deceit on the part of the employer. They examined the circumstances in which the agreements had been signed and found that the presence of the union representative at the time of signing, the prior acknowledgment of the acts by the applicants during a meeting with that representative, and the fact that other employees who were dismissed had not signed the employer's proposed agreement, ruled out any indication of duress. Their findings in this connection appear neither arbitrary nor manifestly unreasonable. Lastly, as noted above, the domestic courts based their decisions on various items of evidence (see paragraph 157 above).

161. In the light of those observations, there is no reason for the Court to call into question the findings of the domestic courts as to the validity and weight of the settlement agreements signed by the third, fourth and fifth applicants. It thus finds that there has been no violation of Article 6 on this point either.

FOR THESE REASONS, THE COURT

Holds , unanimously, that the second applicant's legal heir has standing to continue the present proceedings in her stead;

Dismisses , unanimously, the Government's preliminary objection;

Holds , by fourteen votes to three, that there has been no violation of Article 8 of the Convention;

Holds , unanimously, that there has been no violation of Article 6 of the Convention on account of the use in evidence of the recordings obtained by means of video-surveillance;

Holds , unanimously, that there has been no violation of Article 6 of the Convention on account of the acceptance of the settlement agreements signed by the third, fourth and fifth applicants.

Done in English and French, and delivered at a public hearing in the Human Rights Building, Strasbourg, on 17 October 2019.

Søren Prebensen
Deputy to the Registrar

Linos-Alexandre Sicilianos
President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the separate opinion of Judges De Gaetano, Yudkivska and Grozev is annexed to this judgment.

L.A.S. S.C.P.

ANNEX

List of applicants

Application no. 1874/13

1. Isabel LÓPEZ RIBALDA, born in 1963, resident in Sant Celoni

Application no. 8567/13

2. María Ángeles GANCEDO GIMÉNEZ, born in 1967, died in 2018

3. Maria Del Carmen RAMOS BUSQUETS, born in 1969, resident in Sant Celoni

4. Pilar SABORIDO APRESA, born in 1974, resident in Sant Celoni.

5. Carmen Isabel POZO BARROSO, born in 1974, resident in Sant Pere de Vilamajor

JOINT DISSENTING OPINION OF JUDGES DE GAETANO, YUDKIVSKA AND GROZEV

1. We respectfully disagree with our colleagues that Article 8 of the Convention was not violated in the present case. We would share the position of our colleagues in the Chamber who found that in the light of the existing domestic legislation, the domestic courts had failed to strike a fair balance between the applicants' right to respect for their private life under Article 8 of the Convention and their employer's interest in the protection of its property rights.

2. This case demonstrates the growing influence and control that technology has in our world, and more particularly, the collection and use of our personal data in our everyday activities. As a living instrument, the Convention, and therefore the Court, not only needs to recognise the influence of modern technologies, but also has to develop more adequate legal safeguards to secure respect for the private life of individuals.

3. The widespread use of personal data in modern times was, eight years ago, already an area in which the Court expressed the need for "increased vigilance", when it heard the quite similar case of *Köpke v. Germany* ((dec.), no. 420/07, 5 October 2010). Since then, surveillance technologies and the data collected using them have been significantly developed. These new technologies allow the data stored to be viewed by anyone, in any place, at any given time, with little control and not much trace, thus calling into question the majority's finding in the present case that "only the supermarket manager, the company's legal representative and the union representative viewed the recordings obtained through the impugned video-surveillance" (paragraph 126).

4. In other words, new technologies have dramatically changed the ease with which video-surveillance can both be carried out and transmitted, thus multiplying significantly the potential infringement of privacy rights under Article 8 of the Convention. It is precisely for this reason that there is a need, at national level, for the legislative framework to be clear and foreseeable in relation to cases concerning electronic surveillance. This becomes crucial in cases such as the present one, where an employer uses covert video-surveillance in the workplace. Thus, our disagreement of principle with the majority stems from their endorsement of a legal response to the particular issue which was only developed after the facts and in relation to a specific case. While such an approach, where domestic courts are given leeway to develop a legal response to a conflict which has given rise to a specific case regarding competing Convention rights, might be appropriate in some cases, we consider it to be ill-suited to cases regarding electronic surveillance. This is precisely due to the technological ease with which electronic surveillance can be carried out and disseminated and the potentially vast and significant negative effects it could have on individuals' privacy rights. Therefore a clear and foreseeable legal framework, with appropriate and effective safeguards, becomes of paramount importance. In the case at hand, the existing legal framework provided for only one specific guarantee, namely the need for employees to be given prior warning of the installation and use of surveillance, and it did not allow of any exceptions to that guarantee. This point, in our view, is decisive for an effective legal analysis and the finding in the present case.

5. Moreover, the legal framework is of particular importance in the context of employment relationships, where the employer has significant powers with regard to employees and any abuse of those powers should be avoided.

Information on the implementation of surveillance measures is essential for the persons concerned to be able to assert the totality of the rights that they are guaranteed, such as the rights of access, of rectification or of deletion in respect of the personal data collected.

6. The failure of the national courts to strike a fair balance between the parties' competing rights is most apparent when analysing the domestic legislation. In the case of *S. and Marper v. United Kingdom* ([GC], nos. 30562/04 and 30566/04, ECHR 2008), the Court concluded that "detailed rules governing the scope and application of measures" were needed to provide sufficient guarantees against the risk of abuse and arbitrariness. Thus, in the Court's view, "the protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8". Although the legislation which governs personal data has created a social norm where there is recognition that individuals can control the dissemination of their image, this right was not granted to the applicants in this case. This was in direct contradiction with the Spanish national law under section 5 of the Data Protection Act. If the current regulatory framework is to be enforced, then prior notice must be given to individuals whose image is going to be collected and used. Regrettably, no such opportunity was given to all the employees as they were not made aware beforehand of the covert video-surveillance.

7. The majority agree that Spanish law requires that "it is necessary to inform the individuals concerned, clearly and prior to implementation, of the existence and conditions of such data collection", thus limiting the invasion of privacy and giving employees the opportunity to regulate their conduct. This requirement was clearly not met in the present case. However, the majority went on to hold that this was "just one of the criteria to be taken into account in order to assess the proportionality of a measure" (paragraph 131). It is true that the Court's clear structure in assessing any interference (requirement of lawfulness preceding assessment of proportionality) does not apply in the present case as we are talking about positive obligations and not interference; we nevertheless find it problematic that the domestic courts failed to examine whether the applicants had been informed of the installation of the covert video-surveillance. The Employment Tribunal, when judging the proportionality of the measure, did not expressly address the applicants' argument that they had not been informed of the monitoring specifically and prior to its implementation, as required by domestic law. Instead, it merely referred to Judgment no. 186/2000 of the Constitutional Court, which had taken the view that the question of the information given by the employer to the employees and to the staff committee was a question of ordinary legality and was not pertinent in terms of the constitutional right to respect for private life. Thus, the national courts failed to enforce the legal framework which ensures data protection or to take into account the applicants' case in a detailed and individual manner.

8. We also find unsatisfactory the assessment made by the domestic courts when determining whether the covert video-surveillance had been necessary. The Tribunal confirmed that it was a necessary measure for the legitimate aim pursued, to discover who had committed thefts in the supermarket. However, the Tribunal failed to consider whether a less restrictive measure could have been used by the employer to pursue the same aim. This failure takes on particular importance in the light of the majority's finding that the question whether it would have been possible "to set up a monitoring system based on less intrusive methods and measures" is an important factor to be assessed in order to ensure the proportionality of covert video-surveillance measures in the workplace (paragraph 116).

9. The national courts had to consider which alternative measures could have been used by the employer to pursue its legitimate aim – measures which would simultaneously have had a less invasive impact on the employees' right to respect for their private life. The employer had two legitimate aims: firstly, it wanted to stop further theft, for which purpose a warning about the installed video-surveillance system would have been sufficient. Secondly, it wanted to find out who was responsible for the losses it had sustained over the past months; here, prior notice of the visible and covert video-surveillance would not have proven useful. Nevertheless, since the theft committed was a criminal offence, the employer could have, and should have, gone to the police prior to taking such measures on its own initiative. The need to elucidate an offence does not justify private investigation, including in the form of covert video-surveillance, which amounts to an excessively intrusive measure and an abuse of power. By not condemning such behaviour committed by private parties, the Court is encouraging individuals to take legal matters into their own hands. Instead, it is for the competent authorities to take the appropriate measures as they are better equipped, in terms both of their powers to implement certain measures and of their responsibility and obligations to follow guidance on what is necessary in a situation like the present one.

10. The majority point out that they "cannot accept the proposition that ... the slightest suspicion of misappropriation or any other wrongdoing on the part of employees might justify the installation of covert video-surveillance by the employer", but nevertheless find that "the existence of reasonable suspicion that serious misconduct has been committed ... may appear to constitute weighty justification" for such a measure (paragraph 134). In our view, in the absence of a requirement of clear procedural safeguards, the existence of "reasonable suspicion of serious misconduct" is not sufficient as it may result in private investigations and might be used as

justification in an unacceptably large number of cases. While, in principle, the requirement of "reasonable suspicion" is an important safeguard, it is not sufficient to protect privacy rights when faced with electronic surveillance of a covert nature. Under circumstances such as those in the present case, where an employer uses covert video-surveillance without giving prior warning to its employees, there is a need for additional procedural safeguards; similar to those required under the Convention in the use of secret surveillance in criminal proceedings. Procedural requirements allowing for a reliable verification, by a third party, of the existence of a "reasonable suspicion of serious misconduct", and guarantees against the justification for the surveillance being given "after the fact", should be a requirement under Article 8 of the Convention. It is only with the implementation of these procedural safeguards that we could readily accept the majority's judgment.

11. Furthermore, unlike the Chamber, the Grand Chamber failed to differentiate the present case from that of *Köpke* (cited above). In that decision only two employees had been suspected of committing theft in the company, while in the present case all the employees had been subject to the covert video-surveillance installed behind the tills of the supermarket. This unlimited surveillance is much more significant and should thus have been given additional weight by the national courts and by this Court; especially as the surveillance lasted for the entire working day and the cameras were positioned in such a manner that the applicants, in their work as cashiers, could not have avoided being filmed. Such an extensive collection of personal data in respect of all the applicants should have adequately been recognised when determining the proportionality of the measure used by the employer.

12. As this case concerns private employers, in our view the Court had to confirm, extend, and transpose the *Bărbulescu* principles, as set out in paragraph 121, in respect of covert video-surveillance cases such as the present one. Although that case was not specific to covert video-surveillance, it established an important principle regarding the extent of control that can be exercised by an employer upon its employees, as well as a multitude of factors that the national courts have to consider in order to strike a fair balance between the competing interests of the parties.

13. Another factor which was undermined in the majority's assessment was "the consequences of the monitoring for the employee subjected to it". In the case of *Vukota-Bojić v Switzerland* (no. 61838/10, 18 October 2016), where the Court found a violation of Article 8 of the Convention, the applicant had been identified through the use of covert video-surveillance, which had ultimately led to a reassessment of her insurance benefits. In the present case, the majority found that although the applicants had been dismissed following the use of covert video-surveillance, "the recordings were not used by the employer for any purposes other than to trace those responsible for the recorded losses of goods and to take disciplinary measures against them" (paragraph 127). In our view, although not used for any other purpose, the consequence of collecting and using this personal data should not have been underestimated, especially given the wide array of possibilities that potential modern technologies provide.

14. Similar criteria, of importance for an assessment of proportionality in relation to covert video-surveillance, have been developed in other jurisdictions. For example, in the case of *R v. Oakes* ([1986] 1 S.C.R. 103) the Canadian Supreme Court considered the following factors: whether the measure is necessary to meet a specific need; whether it is effective in meeting that need; and whether the loss is proportionate to the benefit. This is an appropriate approach to follow in order to determine whether there has been a fair balance between competing Convention rights. Also of note is the same court's finding in *Ross v. Rosedale Transport Ltd* ([2003] C.L.A.D. No. 237) that "surveillance is an extraordinary step which can only be resorted to where there is, beforehand, reasonable and probable cause to justify it".

15. In sum, we find that both the national courts and this Court failed to strike a fair balance between the rights of the employer and the rights of the employees. By finding no violation of Article 8 of the Convention, the Court has decided to allow the unlimited use of covert video-surveillance in the workplace without affording sufficient legal safeguards to those whose personal data will be collected and used for purposes unknown to them. With the growing influence that technology has on our society, we cannot afford to let individuals take justice into their own hands and allow the right to a private life under Article 8 of the Convention to remain insufficiently protected when faced with such new challenges.