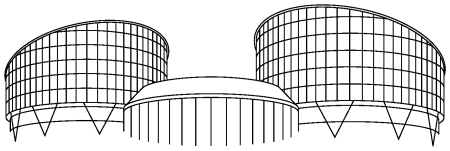

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

THIRD SECTION

CASE OF LÓPEZ RIBALDA AND OTHERS v. SPAIN

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

JUDGMENT

STRASBOURG

9 January 2018

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

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

The European Court of Human Rights (Third Section), sitting as a Chamber 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*,

Having deliberated in private on 12 December 2017,

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

PROCEDURE

1. The case originated in 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 attached Annex ("the applicants").

2. The first applicant lodged her application on 28 December 2012 and the other applicants lodged theirs on 23 January 2013. They are all 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 argued that the covert video surveillance ordered by their employer without previously informing them had violated their right to privacy protected by Article 8 of the Convention. They further complained under Article 6 of the Convention that the proceedings before the domestic courts had been unfair in that the video recordings had been used as the main evidence to justify the fairness of their dismissals. The third, fourth and fifth applicants also claimed that the domestic courts had determined the fairness of their dismissals on the basis of settlement agreements they had signed under duress, which had violated their right to a fair trial under Article 6 of the Convention. Lastly, the first applicant claimed that the judgments had lacked proper motivation as to her specific circumstances.

4. On 17 February 2015 the applications were communicated to the Government.

5. The European Trade Union Confederation (ETUC) was given leave to intervene in the written procedure (Article 36 § 2 of the Convention and Rule 44 § 3 of the Rules of Court).

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

6. At the time of the events the applicants were all working as cashiers for M.S.A., a Spanish family-owned supermarket chain.

7. At the beginning of February 2009 the applicants' employer noticed some irregularities between the supermarket stock levels and what was actually sold on a daily basis. In particular, the shop supervisor identified losses in excess of EUR 7,780 in February, EUR 17,971 in March, EUR 13,936 in April, EUR 18,009 in May and EUR 24,614 in June 2009.

8. In order to investigate and put an end to the economic losses, on 15 June 2009 the employer installed surveillance cameras consisting of both visible and hidden cameras. The purpose of the visible cameras was to record possible customer thefts and they were pointed toward the entrances and exits of the supermarket. The purpose of the hidden cameras was to record and control possible employee thefts and they were zoomed in on the checkout counters, which covered the area behind the cash desk. The company gave its workers prior notice of the installation of the visible cameras. Neither they nor the company's staff committee were informed of the hidden cameras.

9. On 25 and 29 June 2009 all the workers suspected of theft were called to individual meetings. During those meetings the applicants admitted their involvement in the thefts in the presence of the union representative and the company's legal representative.

10. Hereafter and for the sake of clarity, the applicants will be referred to as the first, second, third, fourth and fifth applicants (see the attached Annex).

A. Group A (the first and second applicants)

11. On 25 and 29 June 2009 the applicants were dismissed on disciplinary grounds: they had been caught on video helping co-workers and customers steal items and stealing them themselves. According to their letters of dismissal, the security cameras had caught them scanning items from the grocery baskets of customers and co-workers and afterwards cancelling the purchases. Security cameras had also caught them allowing customers and co-workers to leave the store with merchandise that had not been paid for.

12. On 22 July 2009 the first applicant brought proceedings for unfair dismissal before the Granollers Employment Tribunal no.1 (hereinafter "the Employment Tribunal"). The same day the second applicant brought similar proceedings before the Employment Tribunal in a joint application with the third, fourth and fifth applicants (see paragraph 20 below).

13. In the framework of the proceedings both applicants objected to the use of the covert video surveillance, arguing that it had breached their right to protection of their privacy.

14. On 20 January 2010 the Employment Tribunal issued two judgments ruling against the applicants, declaring both dismissals fair. The main evidence supporting the fairness of their dismissals was the recordings resulting from the covert surveillance, as well as the witness statements of co-workers dismissed for their involvement in the thefts, the shop manager, the union representative and the company's legal representative.

15. The Employment Tribunal found in both judgments – as regards these two applicants in particular – that the use of covert video surveillance in the workplace without prior notice had been in accordance with Article 20 of the Labour Regulations (*Estatuto de los Trabajadores*), which allowed an employer to use monitoring and surveillance measures which he or she deemed appropriate to verify that an employee was fulfilling his or her employment duties, as long as the employer respected "human dignity". This had been confirmed by the Constitutional Court in several judgments (see, among other authorities, judgment no. 186/2000 of 10 July 2000). According to the Constitutional Court's case-law, an employer's right to adopt organisational arrangements and act as a disciplinary authority had to be weighed against an employee's fundamental right to privacy recognised under Article 18 of the Constitution. In cases where there were substantiated suspicions of theft, special circumstances justified interference with an employee's right to privacy, which was considered to be appropriate to the legitimate aim pursued, necessary and proportionate. Following this case-law, the Employment Tribunal, having regard to the evidence before it, found that the employer had had sufficient grounds to conclude that the applicants' conduct amounted to a "breach of contractual good faith and abuse of trust" and thus declared both dismissals fair in conformity with Article 54.2.d of the Labour Regulations.

16. The applicants appealed before the High Court of Justice of Catalonia on 16 and 22 March 2010 respectively. On 28 January and 24 February 2011 the court upheld both first-instance judgments, referring to the Constitutional Court's case-law and endorsing the Employment Tribunal's finding that the defendant party had been authorised to carry out the covert video surveillance of the cash desks. While acknowledging that it was possible that the employer could face an administrative sanction for not informing its employees and the staff committee in advance of the installation of the cameras, that fact alone had no relevance from a constitutional point of view, since from that perspective the covert video surveillance had been justified (in that there had been reasonable suspicions of theft), appropriate to the legitimate aim pursued, necessary and proportionate. Consequently, their dismissals had been justified on the same grounds as already stated by the Employment Tribunal.

17. The applicants brought cassation appeals, 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, due to the "non-existence of a violation of a fundamental right".

B. Group B (the third, fourth and fifth applicants)

18. On 25 and 29 June 2006 the applicants were dismissed on disciplinary grounds: they had been caught on video helping co-workers and customers steal items and stealing them themselves. According to the employer, the security cameras had caught the third applicant scanning items from the grocery baskets of customers and co-workers and afterwards voiding the receipts. Security cameras had also caught her allowing customers or co-workers to leave the store with merchandise that had not been paid for. As regards the fourth and fifth applicants, security cameras had caught them stealing goods with the help of their co-workers, such as the second applicant.

19. On the days that they were dismissed all three applicants signed a document called a "settlement agreement" *(acuerdo transaccional)*, by which they committed themselves not to bring proceedings against their employer for unfair dismissal, while the employer committed itself not to bring criminal charges against them for theft. In the meetings at least one union representative and the company's legal representative were also present.

20. Despite the settlement agreements, on 22 July 2009 the applicants, together with the second applicant (see paragraph 12 above), brought proceedings for unfair dismissal before the Employment Tribunal. According to the applicants, the settlement agreements had to be declared void. They claimed that the consent they had given was not valid, since they had been under duress at the time they had signed the settlement agreements (a company representative had allegedly threatened to bring criminal proceedings against them if they did not sign the agreements). They also argued that the evidence derived from the covert video surveillance had been obtained illegally.

21. On 20 January 2010 the Employment Tribunal ruled against the applicants and declared the dismissals fair. It carefully analysed the settlement agreements signed by the applicants. In particular, it addressed their allegation of invalid consent, finding that there was no evidence proving the existence of any kind of duress or intention to commit a crime (*dolo*) at the time the applicants had signed the settlement agreements. The court concluded that the applicants had signed the settlement agreements freely and voluntarily with the clear purpose of avoiding criminal

proceedings for the alleged thefts they had been accused of (and to which they had already confessed). Further evidence as to the lack of any threat or coercion was the fact that other employees in the same situation as the applicants (such as the first and second applicants) had refused to sign the settlement agreements. Accordingly, the settlement agreements were declared valid under Article 1.809 of the Civil Code and, consequently, the Employment Tribunal ruled against the third, fourth and fifth applicants. As the signing of the settlement agreements rendered their dismissals fair, the use and analysis of the impugned videos as evidence in the proceedings was deemed unnecessary.

22. The applicants appealed before the High Court of Justice of Catalonia on 16 March 2010. On 24 February 2011 it upheld the first-instance judgment and endorsed the Employment Tribunal's finding that the settlement agreement signed by the applicants was valid. The court also analysed, for the sake of clarity, the legality of the covert video surveillance. Referring to the Constitutional Court's case-law, it confirmed that the defendant party had been authorised to carry out the covert video surveillance on the applicants.

23. The applicants brought a joint cassation appeal, which was declared inadmissible on 7 February 2012. Ultimately, they lodged a joint *amparo* appeal with the Constitutional Court, alleging a violation of Articles 18 and 24 of the Constitution. It was declared inadmissible on 18 July 2012 due to the "non-existence of a violation of a fundamental right".

II. RELEVANT DOMESTIC AND INTERNATIONAL LAW AND PRACTICE

A. Domestic law and practice

1. Constitution

24. 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."

Article 18 § 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 obtain the effective protection of judges and the courts in the exercise of their legitimate rights and interests, and in no case may their defence rights be curtailed.

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

Article 53 § 2

“Every citizen shall be entitled to seek protection of the freedoms and rights recognised in Article 14 and in the first section of Chapter II by bringing an action in the ordinary courts under a procedure designed to ensure priority and expedition and, in appropriate cases, by an appeal (*recurso de amparo*) to the Constitutional Court ...”

2. Civil Code

25. The relevant provisions of the Civil Code read as follows:

Article 1.809

“A settlement is a contract whereby the parties, by each giving, receiving or retaining something, prevent [proceedings] or end [those] which had already begun.”

3. Judiciary Act (Law no. 6/1985 of 1 July 1985)

26. The relevant provision reads as follows:

Section 11

“1. The rules 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 ...”

4. Labour Regulations (approved by Royal Legislative Decree no. 1/1995 of 24 March 1995) – Estatuto de los Trabajadores

27. The relevant provision (in force at the relevant time) read as follows:

Article 20.3

“An employer may use monitoring and surveillance measures which he/she deems appropriate to verify that an employee is fulfilling his/her employment duties, in so far the employer respects human dignity ...”

5. Spanish Labour Procedure Act (Law no. 36/2011)

28. The relevant provision reads as follows:

Section 90

“2. Evidence obtained, directly or indirectly in violation of fundamental rights or freedoms will be excluded ...”

6. Personal Data Protection Act (Law no. 15/1999)

29. The relevant provisions read as follows:

Section 5

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

a) the existence of a personal data file or 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.

...

5. The provisions of the preceding paragraph shall not apply in cases where it is expressly provided for by law, where the processing data 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 paragraph shall also not apply where the data are obtained from sources accessible to the public and are intended for advertising activity 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

"1. [The] 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 administrations 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 section7(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.

3. The consent to which the section refers may be revoked when there are justified grounds for doing so and the revocation does not have retroactive effect.

4. In cases where the consent of the data subject is not required for processing personal data, and unless provided otherwise by law, the data subject may object to such processing when there are compelling and legitimate grounds relating to a particular personal situation. In such an event, the controller shall exclude the data relating to the data subject from the processing."

7. Instruction no. 1/2006 of 8 November issued by the Spanish Data Protection Agency

30. The relevant provision reads as follows:

Article 3

"Everyone who uses video surveillance systems must fulfil all the obligations prescribed in section 5 of the Personal Data Protection Act. For that purpose they must:
a. Place a distinctive sign indicating the areas that are under surveillance...
b. Have documents available containing the information provided in section 5 of the Personal Data Protection Act [...]."

8. Case-law of the Constitutional Court

31. On 10 July 2000 the Constitutional Court rendered a leading judgment on the lawfulness of covert video surveillance in the workplace (judgment no. 186/2000) as regards the protection rendered by Article 18.1 of the Spanish Constitution. In it the court analysed the use of a covert surveillance camera system installed on the ceiling of a clothing and shoe section of a company, only focusing on three cash registers and the counter. In that case the Constitutional Court held that the measure at stake had to pass a three-fold test to be considered acceptable: there had to be a legitimate aim ("a suitability test"), necessary ("a necessity test") and proportionate ("a strict proportionality test") – that is to say, to determine whether a fair balance had been struck between the interference with a fundamental right and the importance of the legitimate aim pursued. As regards the covert video surveillance, the Constitutional Court found:

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

32. Later, 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 video surveillance as security and surveillance measures required that the workers' representatives and employees be given prior notification and that a lack thereof would be in violation of Article 18.4 of the Spanish Constitution. In that case, an employee of the Seville University was suspended without pay for being late and absent from work, after evidence was obtained from video cameras installed after administrative approval. The Constitutional Court stated:

"7. ... In conclusion, it cannot be forgotten that the [Constitutional] Court has established, in an invariable and continuing manner that business power is limited by fundamental rights (among many other [authorities], STC no. 98/2000, of 10 April, legal argument no. 7, or STC no. 308/2000, of 18 December, legal argument no. 4). Consequently, in the same way 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/her rights derived from [sections 5(1) and (2) of the Personal Data Protection Act] (STC 292/2000, of 30 November, legal basis no. 18), the "private interest" of an employer cannot justify that the worker's personal data be treated against the worker without previously informing him/her of the monitoring measures that have been implemented.

There is no reason in the employment sphere ... which allows the restriction of 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 has a legitimate aim ... or is proportionate to the aim pursued; business control must also secure the right to be previously informed [of the existence of a means of data collection and processing].

In the instant case, the video surveillance cameras installed on the campus reproduced the appellant's image and allowed [the employer] to control 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 videotapes, thus becoming the one responsible for processing the appellant's data without previously informing him of the [existence] of that work monitoring system .... This infringed ... Article 18.4 of the Spanish Constitution.

The facts 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 video surveillance system do not outweigh this conclusion; it was necessary, moreover, previously and expressly, precisely, clearly and unambiguously to inform the workers of the aim of the work monitoring system .... The information should specify the characteristics and scope of the data processing, ... *i.e.*, in which cases the images could be examined, during how much time and for what purpose, specifically stating in a particular manner that the images could be used to impose on the workers a disciplinary sanction for non-compliance with the contract of employment."

33. In a relatively recent judgment of 3 March 2016 (no. 39/2016 of 3 March 2016), the Constitutional Court developed its case-law concerning the use of covert surveillance cameras. In this case the company had detected some irregularities in the cash register allegedly committed by one of its employees. It temporarily installed hidden cameras zoomed in on the area where the cash register was located. The employer had placed a sign indicating in a general manner the presence of video surveillance, as well as a document containing the text of section 5 of the Personal Data Protection Act, as required by Article 3 of the Instruction 1/2006 of 8 November issued by the Spanish Data Protection Agency (hereinafter "Instruction no. 1/2006"). According to the Constitutional Court, one of the reasons why Article 18.4 of the Constitution had not been infringed was the fact that the employer had installed a sign in the shop window indicating the installation of video surveillance, in accordance with section 5 of the Personal Data

Protection Act as well as Instruction no. 1/2006. According to the Constitutional Court, the employee was aware of the installation of the monitoring system and of its purpose. As a result of the video surveillance, the employee was caught stealing money from the cash register and was therefore dismissed. The Constitutional Court concluded that:

> "... the use of security cameras was justified (since there was a reasonable suspicion that some of the employees were stealing cash from the cash register), appropriate (to verify if the irregularities were committed by some of the employees, and if so, to adopt the respective disciplinary measures) necessary (the video surveillance would be used as evidence of those irregularities) and proportionate (the image recording was limited to the area where the cash register was located)."[1]

B. International law

1. Council of Europe

34. On 1 October 1985 the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No.108), which was ratified by Spain on 31 January 1984, entered into force. Under Article 1, the purpose was "to secure in the territory of each Party for every individual, whatever his nationality or residence, 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 ('data protection')". It provided, *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 7 – Data security**
>
> Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.
>
> **Article 8 – Additional safeguards for the data subject**
>
> Any person shall be enabled:

1. *Ibid*., legal argument no. 5.

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."

35. 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 (document CDL-AD(2007)027 of 8 June 2007). The relevant parts read:

"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.

...

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."

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

"10. Transparency of processing

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

10.2. Employers should provide employees with the following information:

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

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

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

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

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

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

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."

2. European Union

37. 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 provides:

Article 7

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

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

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

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

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

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

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

..."

Article 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,

- whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply,

- 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 collected, to guarantee fair processing in respect of the data subject.

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.

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law. In these cases Member States shall provide appropriate safeguards."

38. A Data Protection Working Party ("the Working Party") was established under Article 29 of the Directive in order to examine the issue of surveillance of electronic communications in the workplace and to evaluate the implications of data protection for employees and employers. It is an

independent EU advisory body. In September 2001 the Working Party issued Opinion 8/2001 on the processing of personal data in an employment context, which summarises the fundamental principles of data protection: finality, transparency, legitimacy, proportionality, accuracy, security and staff awareness. With regard to the monitoring of employees, it suggested:

> "It should be also clear that
>
> 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."

39. In February 2004 the Working Party issued Opinion 4/2004 on the processing of personal data, which stated:

> "In the light of its peculiar features and the existence of specific provisions also related to the investigational activities carried out by police and judicial authorities as well as for State security purposes - which may include video surveillance that is "hidden", i.e. carried out without providing information on the premises -, this category of processing operations will not be addressed in detail in this document.
>
> However, the Working Party would like to stress that, similar to several other processing operations of personal data that likewise fall outside the scope of the Directive, video surveillance performed on grounds of actual public security requirements, or else for the detection, prevention and control of criminal offences should respect the requirements laid down by Article 8 of the Convention of Human Rights and Fundamental Freedoms and both be provided for by specific provisions that are known to the public and be related and proportionate to the prevention of concrete risks and specific offences – *e.g.*, in premises that are exposed to such risks, or in connection with public events that are likely reasonably to result in such offences. The effects produced by video surveillance systems should be taken into account – e.g. the fact that unlawful activities may move to other areas or sectors -, and the data controller should always be specified clearly in order for data subjects to exercise their rights."

THE LAW

I. JOINDER OF THE APPLICATIONS

40. In accordance with Rule 42 § 1 of the Rules of Court, the Court decides to join the applications, given their similar factual and legal background.

II. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

41. The applicants complained that the covert video surveillance ordered by their employer as well as the recording and use of the data obtained therefrom in the proceedings before the domestic courts had breached their right to privacy under Article 8, which provides:

> "1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

A. Admissibility

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

B. Merits

1. The parties' submissions

(a) The applicants

43. All the applicants considered that the covert video surveillance of their place of work had seriously interfered with their right to privacy. They contended that the purpose of Article 8 of the Convention was not limited to protect the individual against interference by the public authorities, but also to secure respect for private life even in the sphere of the relations of individuals between themselves.

44. The applicants further noted that, in the present case, a video recording of them at their workplace had been made without their employer giving them prior notice, as was required by the domestic law in force at the time (and, in particular, by the Personal Data Protection Act).

45. They also argued that the covert video surveillance had not been limited in time as it had had a permanent nature with the purpose of monitoring all staff during working hours.

46. The applicants further alleged that the use of the video recordings as evidence in the proceedings before the domestic courts had seriously interfered with their right to privacy.

(b) The Government

47. The Government firstly noted that installation of the covert video surveillance had been carried out by a private company, which meant that any violation of the Convention could not be attributable to the State.

48. They further stated that the employer had informed the employees of the installation of a system of video surveillance for theft prevention purposes. They also acknowledged, however, that the employees had not been informed of the installation of covert video surveillance zoomed in on the cash desks. According to the Government, the employees also had not specifically been informed of their rights under the Personal Data Protection Act.

49. The Government also noted that the legislation in force at the time provided every citizen with a means to complain about the use of covert video surveillance to the Data Protection Agency, which could have led to the company being administratively sanctioned.

50. Lastly, the Government concluded that the installation of covert video surveillance without prior notice to the applicants had not been in conformity with Article 18.4 of the Spanish Constitution or Article 8 of the Convention. Nonetheless, they reiterated that, under Article 1 of the Convention, the State should bear no responsibility, since the covert video surveillance had been carried out by a private company.

(c) European Trade Union Confederation (ETUC), third-party intervener

51. The ETUC, intervening as a third party, expressed its concern as regards the fact that States might not sufficiently protect the privacy of workers in the workplace. The ETUC 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. 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, the person(s) concerned had to be informed. For the ETUC, a person's consent was, in principle, necessary.

52. The ETUC also stressed that the right to be informed of the existence of personal data was expressly recognised in domestic law under section 5(1) of the Personal Data Protection Act. It also highlighted 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 as video surveillance at the workplace.

53. The ETUC concluded that the right of the data subject to be informed before the processing of personal data was to be considered as a right derived from Article 8 of the Convention as a procedural safeguard, a right which was also enhanced by the principle of prior consent before data processing.

2. The Court's assessment

(a) General principles

54. The Court reiterates that "private life" within the meaning of Article 8 of the Convention is a broad term not susceptible of exhaustive definition. The choice of the means calculated to secure compliance with Article 8 in the sphere of the relations of individuals between themselves is in principle a matter that falls within the Contracting State's 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 (*Söderman v. Sweden* [GC], no. 5786/08, § 79; and *Bărbulescu v. Romania* [GC], no. 61496/08, § 113).

55. The concept of private life extends 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. 59320/00, § 50, ECHR 2004-VI). It may include activities of a professional or business nature and may be concerned in measures effected outside a person's home or private premises (compare *Peck v. the United Kingdom*, cited above, §§ 57-58; *Perry v. the United Kingdom*, cited above, §§ 36-37; and *Benediktsdóttir v. Iceland* (dec.), no. 38079/06, 16 June 2009).

56. In the context of the monitoring of the actions of an individual by the use of photographic equipment, the Court has found that private-life considerations may arise concerning the recording of the data and the systematic or permanent nature of the recording (compare *P.G. and J.H. v. the United Kingdom*, no. 44787/98, § 57, ECHR 2001-IX; *Peck*, cited above, §§ 58-59; and *Perry*, cited above, § 38). A person's image constitutes one of the chief attributes of his or her personality, as it reveals unique characteristics and distinguishes him or her from his or her peers. The right to the protection of one's image is thus one of the essential components of personal development and presupposes the right to control the use of that image (see *Reklos and Davourlis v. Greece*, no. 1234/05, § 40, 15 January 2009).

57. The Court has considered relevant in this connection whether or not a particular individual was targeted by the monitoring measure (compare

Rotaru v. Romania [GC], no. 28341/95, §§ 43-44, ECHR 2000-V; *Peck*, cited above, § 59; and *Perry*, cited above, § 38) and whether personal data was processed or used in a manner constituting an interference with respect for private life (see, in particular, *Perry*, cited above, §§ 40-41, and *I. v. Finland*, no. 20511/03, § 35, 17 July 2008). A person's reasonable expectation as to privacy is a significant though not necessarily conclusive factor (see *Halford v. the United Kingdom*, 25 June 1997, § 45, *Reports of Judgments and Decisions* 1997-III; and *Perry*, cited above, § 37; and *Bărbulescu,* cited above, § 73).

(b) Application of the above principles to the present case

58. The Court observes that, in the present case, the employer decided to install surveillance cameras consisting of both visible and hidden cameras. The employees were only aware of the visible cameras zoomed in on the supermarket exits – they were not informed of the installation of video surveillance covering the cash desks.

59. The Court observes that the covert video surveillance of an employee at his or her workplace must be considered, as such, as a considerable intrusion into his or her private life. It entails a recorded and reproducible documentation of a person's conduct at his or her workplace, which he or she, being obliged under the employment contract to perform the work in that place, cannot evade (see *Köpke*, cited above). The Court is therefore satisfied that the applicants' "private life" within the meaning of Article 8 § 1 was concerned by these measures.

60. According to the Government, the video surveillance was carried out on the instructions of the applicants' employer, a private company which could not by its actions engage State responsibility under the Convention. The Court reiterates, however, that, although the purpose of Article 8 is essentially to protect 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 an effective respect for private life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves (see *von Hannover*, cited above, § 57; *I. v. Finland*, cited above, § 36; *K.U. v. Finland*, no. 2872/02, §§ 42-43, ECHR 2008; *Söderman*, cited above, § 78 and *Bărbulescu,* cited above, § 108).

61. Therefore, the Court has to examine whether the State, in the context of its positive obligations under Article 8, struck a fair balance between the applicants' right to respect for their private life and both their employer's interest in the protection of its organisational and management rights concerning its property rights, as well as the public interest in the proper administration of justice (see *Bărbulescu,* cited above, § 112).

62. The Court firstly notes that the covert video surveillance was carried out after losses had been detected by the shop supervisor, raising an arguable suspicion of theft committed by the applicants as well as other employees and customers.

63. The Court also observes that the visual data obtained entailed the storage and processing of personal data, closely linked to the private sphere of individuals. This material was thereby processed and examined by several persons working for the applicants' employer (among others, the union representative and the company's legal representative) before the applicants themselves were informed of the existence of the video recordings.

64. The Court further notes that the legislation in force at the time of the events contained specific provisions on personal data protection. Indeed, under section 5 of the Personal Data Protection Act, the applicants were entitled to be "previously and explicitly, precisely and unambiguously informed" of "the existence of a personal data file or that the data will be processed, the purpose thereof and the recipients of the information; the obligatory or optional nature of their response to the questions asked; the consequences of providing or refusing to provide the data; the existence of rights of access, rectification, erasure and objection; and the identity and address of the controller or, as appropriate, his representative" (see paragraph 29 above). Article 3 of Instruction no. 1/2006 issued by the Spanish Data Protection Agency also specified that this obligation also applied to anyone using video surveillance systems, in which case, he or she had to place a distinctive sign indicating the areas that were under surveillance, and to make a document available containing the information provided in section 5 of the Personal Data Protection Act (see paragraph 30 above).

65. The Court observes that, as acknowledged by the domestic courts, the applicants' employer did not comply with the obligation to inform the data subjects of the existence of a means of collecting and processing their personal data, as prescribed in the aforementioned domestic legislation. In addition to this, the Court notes that the Government have specifically acknowledged that the employees were not informed of the installation of covert video surveillance zoomed in on the cash desks or of their rights under the Personal Data Protection Act (see paragraph 48 above).

66. Despite this, the domestic courts considered that the measure had been justified (in that there had been reasonable suspicions of theft), appropriate to the legitimate aim pursued, necessary and proportionate, since there had been no other equally effective means of protecting the employer's rights which would have interfered less with the applicants' right to respect for their private life. This was stated by the Employment Tribunal in respect of the first and second applicants and later confirmed by the Catalonia High Court of Justice in respect of all the applicants, which

specifically declared that the covert video surveillance (and its use as valid evidence in the framework of the proceedings) had been in conformity with Article 20.3 of the Labour Regulations, and had been proportionate to the legitimate aim pursued and necessary.

67. The Court observes that, in the present case, the situation differs from that in *Köpke*. Indeed, in that case, at the time the employer carried out the covert video surveillance following suspicions of theft against two employees, the conditions under which an employer could resort to the video surveillance of an employee in order to investigate a criminal offence had not yet been laid down in statute (although the German Federal Employment Tribunal had developed in its case-law important guidelines regulating the legal framework governing covert video surveillance in the workplace). In the present case, however, the legislation in force at the time of the facts of the case clearly established that every data collector had to inform the data subjects of the existence of a means of collecting and processing their personal data (see paragraphs 29 and 30 above). In a situation where the right of every data subject to be informed of the existence, aim and manner of covert video surveillance was clearly regulated and protected by law, the applicants had a reasonable expectation of privacy.

68. Furthermore, in the present case and unlike in *Köpke*, the covert video surveillance did not follow a prior substantiated suspicion against the applicants and was consequently not aimed at them specifically, but at all the staff working on the cash registers, over weeks, without any time limit and during all working hours. In *Köpke* the surveillance measure was limited in time – it was carried out for two weeks – and only two employees were targeted by the measure. In the present case, however, the decision to adopt surveillance measures was based on a general suspicion against all staff in view of the irregularities which had previously been revealed by the shop manager.

69. Consequently, the Court cannot share the domestic courts' view on the proportionality of the measures adopted by the employer with the legitimate aim of protecting the employer's interest in the protection of its property rights. The Court notes that the video surveillance carried out by the employer, which took place over a prolonged period, did not comply with the requirements stipulated in Section 5 of the Personal Data Protection Act, and, in particular, with the obligation to previously, explicitly, precisely and unambiguously inform those concerned about the existence and particular characteristics of a system collecting personal data. The Court observes that the rights of the employer could have been safeguarded, at least to a degree, by other means, notably by previously informing the applicants, even in a general manner, of the installation of a system of video surveillance and providing them with the information prescribed in the Personal Data Protection Act.

70. Having regard to the foregoing, and notwithstanding the respondent State's margin of appreciation, the Court concludes in the present case that the domestic courts 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.

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

71. The applicants complained under Article 6 § 1 that, when deciding their case, the domestic courts had used the surveillance footage proving the commission of the thefts as the main evidence.

72. The third, fourth and fifth applicants also claimed that the settlement agreement on which the fairness of their dismissals had been based should not have been used as evidence, since they had been signed under duress on the basis of the illegally obtained video recordings. Accordingly, the consent they had given in the settlement agreements had not been valid and the agreements should have been declared void.

73. Article 6 § 1 provides as follows:

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

A. Admissibility

74. The Court notes that these complaints are not manifestly ill-founded within the meaning of Article 35 § 3 (a) of the Convention and that they are not inadmissible on any other grounds. They must therefore be declared admissible.

B. Merits

1. The parties' submissions

(a) The applicants

75. All the applicants argued that the domestic courts had based the judgments mainly on the findings of the unlawful surveillance carried out by the employer. They further pointed out that they had not been aware of the existence of the covert video surveillance and had only had access to the obtained data once they had already been dismissed. Consequently, they had been prevented from exercising their rights of access, rectification, erasure and objection, as prescribed by section 5 of the Personal Data Protection Act. They added that the videos, which had been obtained in violation of

domestic and international law, had been declared admissible by the domestic courts in violation of the applicants' right to a fair trial.

76. The third, fourth and fifth applicants further stated that the settlement agreements by which the applicants had committed themselves not to bring proceedings for unfair dismissal against their employer should have been declared void since they had signed them against their will and under duress. They added that the employer had had no capacity to waive its right to bring criminal charges against the applicants and therefore no power to prevent a possible criminal complaint against them.

(b) The Government

77. The Government pointed out that the domestic judgments had not been solely based on the covert surveillance footage, but also on several other pieces of evidence, such as the witness statement issued by the union representative, the supporting documents proving the daily accounting irregularities, as well as the applicants' own behaviour at the time of their dismissals – they all acknowledged the commission of the thefts during the meetings, in the presence of the union representative and the company's legal representative, among others.

78. As regards the third, fourth and fifth applicants, the Government stressed that the settlement agreements had been valid since they had signed them freely and voluntarily.

(c) European Trade Union Confederation (ETUC), third-party intervener

79. The ETUC considered that a judgment mainly based on covert surveillance footage would be in breach of Article 6 of the Convention.

80. 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 aware and even less dared to require the recognition of their procedural and substantial rights. The ETUC concluded that the specificity of employment relations required a cautious approach in respect of recognising such agreements.

2. The Court's assessment

(a) General principles

81. The Court reiterates that, according to Article 19 of the Convention, its duty is to ensure the observance of the engagements undertaken by the Contracting Parties to the Convention. In particular, it is not its function to deal with errors of fact or law allegedly committed by a national court unless and in so far as they may have infringed rights and freedoms protected by the Convention.

82. While Article 6 of the Convention guarantees the right to a fair hearing, it does not lay down any rules on the admissibility of evidence or the way it should be assessed, which are therefore primarily matters for regulation by national law and the national courts (see *Schenk v. Switzerland*, 12 July 1988, Series A no. 140, p. 29, §§ 45-46; and *García Ruiz v. Spain* [GC], no. 30544/96, § 28, ECHR 1999-I).

83. The Court reiterates in this connection that it is not its function 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 (see *Van Mechelen and Others v. the Netherlands*, 23 April 1997, § 50, *Reports* 1997-III; and *Khan v. the United Kingdom*, no. 35394/97, § 34, ECHR 2000-V). The salient question is therefore not whether evidence that was obtained unlawfully or in breach of the Convention should or should not have been admitted, but whether the proceedings as a whole, including the way in which evidence was taken, were fair. This involves an examination of the unlawfulness in question and, where a violation of another Convention right is concerned, the nature of the violation found (see, *inter alia*, *Khan*, cited above, § 34; and *P.G. and J.H. v. the United Kingdom*, cited above, § 76).

84. As to the examination of the nature of the Convention violation found, the Court reiterates that the question whether the use as evidence of information obtained in violation of Article 8 rendered a trial as a whole unfair contrary to Article 6 has to be determined with regard to all the circumstances of the case, including respect for the applicant's defence rights and the quality and importance of the evidence in question (compare, *inter alia*, *Khan*, cited above, §§ 35-40; *P.G. and J.H. v. the United Kingdom*, cited above, §§ 77-79; and *Bykov v. Russia* [GC], no. 4378/02, 10 March 2009, §§ 94-98, in which no violation of Article 6 was found). Matters to be taken into account are whether the applicant was able to challenge the authenticity of the evidence and to oppose its use, whether the evidence was of sufficient quality – which entails an inquiry as to whether the circumstances in which it was obtained could cast doubt on its reliability or accuracy – and whether it was supported by other material (see *Schenk v. Switzerland*, cited above, §§ 46-48; *Khan*, cited above, §§ 34 and 35; *P.G. and J.H. v. the United Kingdom*, cited above, §§ 76 and 77; *Allan v. the United Kingdom*, no. 48539/99, §§ 42 and 43; and *Bykov* [GC], cited above, §§ 88-90). Lastly, the Court will attach weight to whether the evidence in question was or was not decisive for the outcome of the proceedings (compare, in particular, *Khan*, cited above, §§ 35 and 37).

(b) Application of the above principles to the present case

85. Turning to the present case and for the sake of clarity, the Court will firstly analyse the alleged violation of Article 6 § 1 as regards all the applicants and in connection with the use as evidence of the covert video

surveillance. It will then look at the alleged violation of that Article as regards the third, fourth and fifth applicants in connection with the validity of the settlement agreements signed by them.

(i) Alleged violation of Article 6 § 1 as regards all the applicants

86. The Court will now determine whether the fact that the domestic courts relied on evidence obtained in breach of Article 8 of the Convention also violated the applicants' right to a fair trial as guaranteed under Article 6 § 1 of the Convention.

87. In the present case the Court must examine whether the use in the proceedings of the covert surveillance footage obtained in breach of the Convention was capable of rendering them as a whole unfair.

88. The Court notes, firstly, that the applicants had ample opportunity to challenge both the authenticity and use of the material obtained through the devices in the adversarial procedure during the trials and in their grounds of appeal. The domestic courts at all levels (namely the Granollers Employment Tribunal no.1, the Catalonia High Court of Justice and the Supreme Court) dealt with their objections in that regard.

89. The Court further observes that the impugned recordings were not the only evidence relied on by the domestic court as the basis for the judgments declaring the dismissals fair. In fact, as regards the first applicant, the main pieces of evidence supporting the fairness of her dismissal were not only the recordings resulting from the covert surveillance, but also the witness statements of a co-worker also dismissed because of her involvement in the thefts, the shop manager, the union representative and the company's legal representative. In the same way, as regards the remaining applicants, the main evidence supporting the fairness of their dismissals were not only the recordings, but also the witness statements of co-workers also dismissed for their involvement in the thefts, the shop coordinator, the union representative and the company's legal representative.

90. In view of the above, the Court concludes that nothing has been shown to support the conclusion that the applicants' defence rights were not properly complied with in respect of the evidence adduced or that its evaluation by the domestic courts was arbitrary (see *Bykov* [GC], cited above, § 98).

91. The Court finds therefore that the use in the proceedings of the secretly recorded material did not conflict with the requirements of fairness guaranteed by Article 6 § 1 of the Convention.

(ii) Alleged violation of Article 6 § 1 as regards the third, the fourth and the fifth applicants

92. The Court will now turn to whether the domestic courts' finding that the settlement agreements were valid was in breach of Article 6 § 1 of the Convention.

93. The Court observes that, in the instant case, the domestic courts carefully addressed the admissibility and reliability of the settlement agreements. The applicants had ample opportunity to challenge the validity of the agreements and the domestic courts addressed all the relevant submissions made by them and gave ample reasons as to the validity of the applicants' consent (see paragraphs 21 and 22 above).

94. The Court further notes that the domestic courts did not find any evidence of any duress which allegedly led the applicants to signing the settlement agreements. In particular, the domestic courts found that the employer's behaviour could not be classed as a threat that would invalidate the applicants' consent, but as the legitimate exercise of its right to decide whether or not to initiate criminal proceedings against the applicants, who had also already and voluntarily admitted their involvement in the thefts. The absence of any sign of coercion or duress was corroborated at the hearing by the union representative as well as by the company's legal representative, who were present at those meetings.

95. In the instant case, the Court sees no reason to challenge the domestic courts' assessment of the evidence in this regard. Indeed, the Court cannot itself assess the facts which have led a national court to adopt one decision rather than another; otherwise, it would be acting as a court of fourth instance and would disregard the limits imposed on its action (see, *mutatis mutandis*, *Kemmache v. France (no. 3)*, 24 November 1994, § 44, Series A no. 296-C).

96. In view of the above, the Court finds that there has been no violation of Article 6 § 1 of the Convention in this connection as regards the third, fourth and fifth applicants.

IV. OTHER ALLEGED VIOLATION OF THE CONVENTION

97. Lastly, the first applicant also complained under Article 6 § 1 of the Convention of the unfairness of the proceedings in that the judgments had lacked proper motivation as to her specific circumstances and reasoning leading to the conclusion that her dismissal had been fair.

98. The Court has examined this complaint. Having carefully considered the applicant's submissions in the light of all material in its possession and in so far as the matter complained of are within its competence, the Court finds that it does not disclose any appearance of a violation of the rights and freedoms set out in the Convention or its Protocols.

99. It follows that this part of the application is manifestly ill-founded and must be rejected in accordance with Article 35 §§ 3 and 4 of the Convention.

V. APPLICATION OF ARTICLE 41 OF THE CONVENTION

100. Article 41 of the Convention provides:

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

A. Damage

1. Pecuniary damage

101. In respect of pecuniary damage, all the applicants sought compensation for the lost wages they would have received had the domestic courts declared their dismissals unfair and had they continued working at the company consequently.

102. The Government submitted that there was no causal link between the alleged violations and the compensation for pecuniary damage sought. They also added that the applicants had failed to prove that they had not found another job after their dismissals.

103. The Court does not discern any causal link between the violation found and the pecuniary damage alleged; it therefore rejects this claim.

2. Non pecuniary damage

104. The applicants alleged that they had suffered "considerable moral damages" and claimed EUR 6,250 each.

105. The Government contested this claim.

106. Having regard to all the circumstances of the present case, the Court accepts that the applicants have suffered non-pecuniary damage which cannot be compensated for solely by the finding of a violation. The Court awards each applicant EUR 4,000 in respect of non-pecuniary damage, plus any tax that may be chargeable on those amounts.

B. Costs and expenses

107. The applicants also claimed a lump sum of EUR 2,906.80 each for the costs and expenses incurred before the domestic courts.

108. The Government contested this claim.

109. According to the Court's case-law, an applicant is entitled to the reimbursement of costs and expenses only in so far as it has been shown

that these have been actually and necessarily incurred and are reasonable as to quantum. In the present case having regard to the documents in its possession and the above criteria, the Court considers it reasonable to award the applicants the amounts indicated in the table below for costs and expenses incurred in the proceedings before the domestic courts:

Application No.	Name of the applicant	Amount
1874/13	Isabel LÓPEZ RIBALDA	EUR 500.00
8567/13	María Ángeles GANCEDO GIMÉNEZ	EUR 568.86
8567/13	María Del Carmen RAMOS BUSQUETS	EUR 568.86
8567/13	Pilar SABORIDO APRESA	EUR 568.86
8567/13	Carmen Isabel POZO BARROSO	EUR 568.86

C. Default interest

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

FOR THESE REASONS, THE COURT

1. *Decides,* unanimously, to join the applications;

2. *Declares,* unanimously, the complaint under Article 8 of the Convention, as well as the complaint under Article 6 § 1 as regards the use of evidence allegedly obtained in breach of Article 8 of the Convention and the complaint under Article 6 § 1 as regards the validity of the settlement agreements admissible and the remainder of the first application inadmissible;

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

4. *Holds*, unanimously, that there has been no violation of Article 6 § 1 of the Convention in respect of all the applicants, as regards the use of evidence obtained in breach of Article 8 of the Convention;

5. *Holds*, unanimously, that there has been no violation of Article 6 § 1 of the Convention in respect of the third, fourth and fifth applicants, as regards the validity of the settlement agreement;

6. *Holds*, by four votes to three,
(a) that the respondent State is to pay the applicants, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, EUR 4,000 (four thousand euros) in respect of non-pecuniary damage, plus any tax that may be chargeable, in respect of non-pecuniary damage;
(b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

7. *Holds*, unanimously,
(a) that the respondent State is to pay, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, EUR 500 (five hundred euros), plus any tax that may be chargeable, to the first applicant and EUR 568.86 (five hundred and sixty-eight euros eighty-six cents), plus any tax that may be chargeable, to the second, third, fourth and fifth applicants each, in respect of costs and expenses;
(b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amounts at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

8. *Dismisses*, unanimously, the remainder of the applicants' claim for just satisfaction.

Done in English, and notified in writing on 9 January 2018, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Stephen Phillips
Registrar

Helena Jäderblom
President

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

(a) partly dissenting opinion of Judge Poláčková joined by Judge Pastor Vilanova;

(b) dissenting opinion of Judge Dedov.

H.J.
J.S.P.

PARTLY DISSENTING OPINION OF JUDGE POLÁČKOVÁ JOINED BY JUDGE PASTOR VILANOVA

1. We are in agreement with the majority's reasoning and conclusions relating to the complaint under Article 8 of the Convention, as well as to the complaint under Article 6 § 1 in respect of all the applicants, as regards the use of evidence obtained in breach of Article 8 of the Convention, and the complaint under Article 6 § 1 in respect of the third, fourth and fifth applicants, as regards the validity of the settlement agreements. We also fully share the majority's reasoning on the application of Article 41 of the Convention as regards costs and expenses.

2. We regret, however, that we are unable to subscribe to the findings by our colleagues in the majority that the respondent State is to pay the applicants EUR 4,000 (four thousand euros) in respect of non-pecuniary damage. That finding was based on the conclusion that the applicants have suffered non-pecuniary damage which cannot be compensated for solely by the finding of a violation.

3. We agree with our colleagues in the majority that notwithstanding the respondent State's margin of appreciation, the domestic courts 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. However, having regard to all the circumstances of the present case and the Court`s recent case law, we have come to the conclusion that the finding of a violation constitutes in itself sufficient just satisfaction for the non-pecuniary damage sustained by the applicant (compare *Barbulescu v. Romania* [GC], no. 61496/08, § 148).

DISSENTING OPINION OF JUDGE DEDOV

I regret that I cannot agree with my colleagues, because I believe that the conclusion in the present case is inconsistent with the Court's case-law, and also for other reasons.

As regards the lack of consistency with the Court's case-law, one might observe that the approach in the present case differs from a number of cases adjudicated by the Court, including *Barbulescu* (referred to in the judgment), where the employer had recorded the applicant's private conversations with members of his family. In the present case there was no interference with private life in such a context.

According to the general principle, covert video surveillance of an employee at his or her workplace must be considered, as such, as a major intrusion into the employee's private life. It entails the recorded and reproducible documentation of a person's conduct at his or her workplace, which the employee, being obliged under the employment contract to perform work in that place, cannot evade (see *Antović and Mirković v. Montenegro*, no. 70838/13, 28 November 2017, § 44, and *Köpke v. Germany* (dec.), no. 420/07, 5 October 2010). The national authorities therefore are required to strike a balance between the rights and the "competing interests" of the employer and the employees.

Unlike the present case, in *Antović* and *Mirković* the Court found that the visible cameras had been installed without any legitimate aim. By way of contrast, the circumstances in *Köpke* were similar to those of the present case. One might say that the interference in the case of *Köpke* was more serious because there had only been hidden cameras and the employee had at no stage been notified of any surveillance. Nevertheless, the Court found the complaint ill-founded. In the *Köpke* decision the Court accepted the domestic courts' view that there had been no other equally effective means to protect the employer's property rights which would have interfered to a lesser extent with the applicant's right to respect for her private life. Having regard to the circumstances of the case, the Court agreed with this finding because the stocktaking carried out in the drinks department could not clearly link the losses discovered to a particular employee. Surveillance by superiors or colleagues or open video surveillance would not have had the same prospects of success in discovering a covert theft.

I have already expressed my opinion in previous cases, such as *Vukota-Bojić v. Switzerland*, no. 61838/10 and *Trabajo Rueda v. Spain*, no. 32600/12, that offensive behaviour is incompatible with the right to private life under the Convention. That means that the public interest of society should prevail and that safeguards against unlawfulness and arbitrariness should be limited to protecting against an abusive interference. The majority have implicitly tried to correct a number of irregularities

which might be considered abusive. However, I have doubts as to whether there were any abusive elements in the present case.

Firstly, the Court stressed that the employer had installed both visible and hidden cameras. That might be considered an abusive element as the hidden cameras zoomed in on the checkout counters behind the cash desk. However, they were installed in public, and not in private, spaces. Moreover, the company used the records from both types of cameras in evidence of the commission of an offence during the national court proceedings. Thus, the visible cameras seemed necessary in order to provide a complete picture of how the applicants had organised the whole theft process.

Secondly, the employees had not been informed about the surveillance. However, the visible cameras themselves demonstrated that the video surveillance had been organised by the employer, so it could not be said that the employees had not been informed about it. Paragraph 33 of the judgment states that the same approach had been taken by the national Constitutional Court, which had found that a general indication of the operation of video surveillance did not amount to a violation of the right to private life. Equally, this Court cannot find a violation simply because the applicants could not have anticipated that they would be monitored in places where they had stored the stolen items.

Thirdly, another abusive element could be derived from the proposition that the visible cameras had been pointed towards customers, while the hidden cameras had targeted employees. This created an impression that the employer was trying to suggest that the employees were not being specifically monitored at all, while the visible cameras were neutral and could record the actions of both customers and employees, and even the manager himself.

Fourthly, the Court stressed that the decision to adopt surveillance measures had been based on a general suspicion against all staff members (p. 68 of the judgment). I must point out that the losses identified by the manager had been quite numerous (between some EUR 8,000 and EUR 25,000 per month) for a retail supermarket, where individual items were not too expensive, and that the losses had constantly increased over time, so that it could reasonably be concluded that the losses might not have been caused by one person. Therefore, it cannot be concluded that the surveillance was unnecessary. Again, the only place where the stolen items could be hidden from visible cameras was behind the cash desks.

In my view, therefore, the actions of the employer and the national authorities cannot be considered abusive, arbitrary or disproportionate. In the present case, as in the previous cases cited above, the conclusion of the majority contradicts the general principle of law: the applicants should not be legally allowed to profit form their own wrongdoing (see *Riggs v. Palmer*, 1889). Therefore, the Convention cannot be construed and

interpreted in such a way as to allow wrongdoing. The Russian writer Alexander Solzhenitsyn said that no system can survive without repentance and regret. It would be like an oak with a rotten trunk: it would not last long.

ANNEX

No.	Application no.	Applicant name date of birth place of residence
1.	1874/13	**Isabel LÓPEZ RIBALDA** 03/08/1963 Sant Celoni
2.	8567/13	**María Ángeles GANCEDO GIMÉNEZ** 14/03/1967 Sant Celoni
3.	8567/13	**María Del Carmen RAMOS BUSQUETS** 11/11/1969 Sant Celoni
4.	8567/13	**Pilar SABORIDO APRESA** 15/09/1974 Sant Celoni
5.	8567/13	**Carmen Isabel POZO BARROSO** 20/05/1974 Sant Pere de Vilamajor