Text translated from “CYBERDROIT 2009/2010, le droit à l’épreuve de l’internet”
5e édition, DALLOZ
Author : Christiane Féral-Schuhl

3. CYBER-SURVEILLANCE AT WORK

Published with the financial support of the European Commission

SECTION 0
ORIENTATION

3.00

Overview.

3.01

Applicable texts

> French texts.

Labour code, esp. Art. L. 1121-1, L. 1221-6, L. 2323-13, L. 2323-32 — Penal code, esp. Art. 226-15, 226-24 and 432-9 — Act no. 78-17, 6 Jan. 1978 on data processing and individual liberties ("*Data Privacy Act*")– Act no. 2004-801, 6 August 2004, on the protection of individuals with regard to the processing of personal data, amending Act no. 78-17, 6 January 1978

3.03

Relevant literature.

> Reports and Guidelines.

FDI, *Relations du travail et internet,* rapp. (relations between work and internet): *panorama législatif et jurisprudentiel*, (legislative and jurisprudential overview) 26 Jan. 2006 — CNIL, H. Bouchet (dir.), *La cybersurveillance sur les lieux de travail* (cyber-surveillance in the workplace), March 2004 — CNIL, *Guide pratique pour les employeurs* (practical guide for employers).

> Works

M.-P. Fenoll-Trousseau and G. Haas, *La cybersurveillance dans l'entreprise et le droit : Traquer, être traqué,* Litec, 2002 — J.-E. Ray, *L'employeur, le salarié et les TIC,* Éd. Liaisons, 2007 ; *Le droit du travail à l'épreuve des NTIC,* Éd. Liaisons, Rueil-Malmaison, 2001; *Droit du travail – Droit vivant,* 15th Edition., Éd. Liaisons, August 2006.

> Colloquia.

The ADIJ Tuesday (*Mardi de l'ADIJ*) (C. Baudoin), "Droit du travail et nouvelles technologies : actualités législatives et jurisprudentielles" (*Employment law and new technologies, current legislative and jurisprudential situation*) Summary J.-B. Auroux, *RLDI* no. 14, March 2006, p. 83 ; Summary by L. Teyssandier, *Lexbase* N5659AKS

> Articles.

Special issue of the journal *Dr. social,* "Le droit du travail à l'épreuve des NTIC" (*Employment law in the face of new ICT technologies*), January 2002.

CHAPTER

31. Employer monitoring of tools of work

SECTION 0
ORIENTATION

31.00

Overview.

Sect. 1 Employer monitoring powers

Sect. 2 Employee loyalty obligation

Sect. 3 Responsibilities

31.01

Applicable texts

> French texts.

See s[s] no. 3.01.

Act no. 2004-575, 21 June 2004, promoting confidence in the digital economy — Act no. 82-689, 4 August 1982, relating to employee rights at work, *JO* 6 August, 1982.

31.02

Reference court rulings

> Regarding an employee's general loyalty obligation.

• **Soc. 16 June 1998,** *D.* 1998, IR 77.

See s[s] no. 31.21.

> Regarding the introduction of password access to work stations.

• **Soc. 6 Feb. 2001,** no. 98-46.345, Sté Laboratoires pharmaceutiques Dentoria v. Mme Bardagiet et al., *Bull. civ.* V, no. 43; *JCP G* 25 July 2001, no. 30, p. 1514, note C. Puigelier; *RTD civ.* Oct.-Dec. 2001, no. 4, 880-882, note J. Mestre and B. Fages — cassation of **Toulouse Court of Appeal, 4th soc. law chamber, 23 Oct. 1998.**

• **Soc. 18 Oct. 2006** no. 04-48.025, Jérémy L… v. Sté Techni-Soft, *Bull. civ.,* no. 308; *CCE* Jan. 2007, note E. Caprioli, p. 40 ff. — confirmation of **Rennes Court of Appeal, soc. law chamber, 21 Oct. 2004.**

* See s[s] no. 31.24, also nos. 33.22 and 35.21.

> Regarding the abusive use of company equipment.

• **Soc. 10 Oct. 2007** no. 06-03.007, Claude G… v. Assoc. Ogec Emmanuel d'Alzon — confirmation by **Montpellier Court of Appeal, soc.law chamber, 17 May 2006,** Claude G… v. Assoc. Ogec Emmanuel d'Alzon, http://www.legalis.net/jurisprudence-decision.php3?id_article=2066 (accessing pornographic websites).

• With regard to the (confirmed) 1st instance ruling, see **Montpellier Industrial Tribunal, 26 Sept. 2005,** Claude G… v. Assoc. Ogec Emmanuel d'Alzon.

* See s[s] no. 31.23, also no. 32.24.

• **Soc. 14 March 2000,** no. 1270, no. 98-42.090, M. Dujardin v. Sté Instinet France *Bull. civ.* V, no. 101; *Gaz. Pal.* 28 Oct. 2000, no. 302, p. 34, note J. Berenguer-Guillon and L. Guignot; *JCP G* 7 Feb. 2001, no. 6, p. 325, note C. Puigelier; *LPA* 11 July 2000, no 137, p. 5, note G. Picca and A. Sauret — confirmation by **Paris Court of Appeal, 18th chamber, sect. A, 16 Feb. 1998,** no. 020563.

• With regard to the (partially annulled) 1st instance ruling, see **Paris Industrial Tribunal, 2nd chamber, supervision sect. , 13 Dec. 1995.**

* See s[s] no. 31.22, also nos. 32.11 and 30.23.

• **Soc. 11 March 1998,** no. 96-40.147, NPB, *RJS* 4/1998, no. 415 — confirmation of **Paris Court of Appeal, 21st chamber, sect. C, 7 Nov. 1995.**

* See s[s] no. 31.12, also no. 32.24 (abusive use of the telephone).

• **Aix-en-Provence Court of Appeal, 1st chamber A, 25 Nov. 2003,** no. 2003/798.

* See s[s] no. 31.21.

> Regarding an employer's responsibility.

• **plenary session, 19 May 1988,** no. 87-82.654, Cie d'assurance "La Cité", *Bull. civ.,* no. 5; *RTD civ.* 1989, 89, obs. P. Jourdain — confirmation of **Lyon Court of Appeal, 24 March 1987.**

* See s[s] no. 31.32.

• **2nd Civ., 19 June 2003,** no. 00-22.626, AGV Vie et al. v. Cts X… et al., *Bull. civ.* II, no. 202; *D.* 2003, 1808 — cassation of **Lyon Court of Appeal, 6th civil chamber, 18 Oct. 2000.**

* See s[s] no. 31.23.

• **Aix-en-Provence Court of Appeal, 2nd chamber, 13 March 2006,** SA Lucent Technologies v. SA Lycos France, M. Nicolas B… — confirmation of **Marseille TGI, 11 June 2003,** RG no. 01/390.

* See s[s] no. 31.33.

31.03

Relevant literature.

> Reports and Guidelines.

FDI, *Relations du travail et internet,* rapp. (relations between work and internet): Report of 17 Sept. 2002 — CNIL, H. Bouchet (dir.), *La cybersurveillance sur les lieux de travail* (cyber-surveillance in the workplace), March 2004 — CNIL, *Guide pratique pour les employeurs* (practical guide for employers).

> Articles.

J.-B. Auroux, The ADIJ Tuesdays ("*Les mardis de l'ADIJ*"): "droit du travail et nouvelles technologies: actualités législative et jurisprudentielle" (*Employment Law and new technologies: the current legislative and jurisprudential situation*), *RLDI* March 2006 no. 14, p. 83; see also the summary of L. Teyssandier, *Lexbase* N5659AKS — F. Bitan, "Messagerie électronique de l'entreprise: le pouvoir de contrôle de l'employeur à l'épreuve du secret des correspondances" (*E-mails at work: employer monitoring rights v. the secrecy of correspondence*), *CCE* 2004, study 15 — P. Bonneau, "Le contrôle des fichiers informatiques des salariés" (*Monitoring employees' IT files*), *Décideurs: Stratégies, Finance & Droit* no. 68, 15 Aug.-15 Sept. 2005, p. 52 s. — G. Haas and O. de Tissot, "Des restrictions inacceptables à la liberté d'action des syndicats" (*Restrictions unacceptable to trade unions' freedom of action*), *Expertises* Apr. 2005, p. 145 — D. Lebeau-Marianna, "Alertes éthiques: quelles orientations suite aux décisions de la Cnil ?" (Whistleblowing: which direction following the CNIL resolutions?), *RLDI* Oct. 2005, no. 9, p. 35 s. — M. Mélin and D. Melison, "Salarié, employeur et données informatiques : brefs regards croisés sur une pièce à succès" (*Employee, employer and computer data: a quick glance at a success story*), *RLDI* Jan. 2007, no. 23, p. 69 s. — A. Saint Martin, "Contrôle des messages électroniques du salarié et mesures d'instruction in futurum" (*Monitoring employee e-mails and guidelines for the future*), *RLDI* June 2007, no. 28; "Une présomption de professionnalité des messages électroniques du salarié ?" (*Assuming business-related content in employee e-mails*?) , *RLDI* May 2007, no. 27 — Master 2 students of multimedia and computer law at the University of Paris II headed by Professor J. Huet, "Le blog: nouvelle arme des salariés" (*The blog, a new weapon for employees*), *RLDI* no. 27, May 2007, p. 90 ff.

31.04

The main questions.

• Under which conditions may an employer set limits to the use of Internet within his company?

* See s[s] no. 31.12.

• What responsibilities does an employee have when accessing Internet at his workplace?

* See s[s] no. 31.21.

• Can an employer be held responsible when an employee distributes illegal content?

* See s[s] no. 31.32.

31.09

Internet access is a tool of work. Internet access, and e-mailing in particular, has become a work tool comparable to the telephone. It is proving to be more and more useful, if not indispensable, for the majority of employees in the conduct of their business work.

However this tool provides an employer with the potential to technically monitor his employees. He is in a position to intercept messages sent by them, to know the purpose and the recipients of such messages, the nature and content of any attached files. He can find out which websites have been accessed, in which forums his employees participate. He is in a position to know whether his employees are using the Internet for business or private reasons, how much time they spend surfing the Web, when they go surfing. Just like in PBXs (private

branch exchanges)[1], the automatic registering of e-mail addresses or websites can be used to build a profile of an employee and to collect information on his private life (membership of a trade union or political party, interest in pornography, revisionism, etc.). These technical means permit employee surveillance, the tracking of employees via the data they send out or receive via the Internet (their electronic footprints). They constitute practices condemned by CNIL, the French data protection authority (*la Commission nationale de l'informatique et des libertés*), following the 2001 publication of its report[2] on "cyber-surveillance" of employees by their employers.

This inevitably poses the question of how the fundamental rights of an employee can be protected. In this area the CNIL has issued a series of recommendations on "cyber-surveillance at work". But the no less difficult is the question regarding the extent of employee rights.

SECTION 1
EMPLOYER MONITORING POWERS

31.11
Toleration of the private use of tools of work made available to employees. Internet access, e-mailing and a telephone constitute resources made available to an employee for the purpose of executing his work. When private use, for example of a telephone, is tolerated, the question of proportionality arises. What is to be said when 75% of the 100 e-mails exchanged daily concern private matters? An employer is subjected to the loss of the employee's working time as well as the associated costs (mainly the logged-on time) when e-mails are being sent or the Web surfed for private purposes. A survey has revealed that 20 – 50% of time spent logged on to the Internet is used for non-business purposes.

31.12
Limitation of the use of tools of work made available to employees. In this context, it would seem legitimate for an employer to seek ways of ensuring that tools of work made available to employees are not used abusively. However, in doing so, he must act in total transparency and with "proportionality"[3]. In line with the principles set down by the CNIL and the recommendations of the Forum on Internet Rights (*Forum des droits sur l'internet*) [4], he needs to find the right balance between his power of monitoring and the protection of the fundamental rights of his employees.

In its 18 December 2003 version of its report "Cyber-surveillance in the workplace", the CNIL pointed out that "a general and absolute prohibition of any use of the Internet for other than professional purposes does not seem realistic in an information and communication society. It also seems disproportionate with respect to the applicable paragraphs." "A reasonable use, not likely to impinge on the conditions of professional access to the network and not endangering productivity, appears to be generally and socially admissible by most companies or administrations". Nevertheless, the CNIL is of the opinion that such tolerated use of IT tools and the Internet network by an employee for private purposes may be subjected to conditions or limits determined by the employer. In this respect, the CNIL recommends the introduction of filtering tools against non-authorised sites, in association with firewalls, and the implementation of global *a posteriori* monitoring of Internet connection data (for example for the whole company or individual departments) without it being necessary to carry out an individualised monitoring of sites accessed by an individual employee. In other words, it is justifiable for an

---

[1] See also CNIL, *5e Rapport d'activité,* (5th Activity report) p. 109 and *15e Rapport d'activité,* p. 74, Doc. fr.

[2] H. Bouchet (dir.), *La cybersurveillance des employés dans l'entreprise,* CNIL, March 2001, http://www.CNIL.fr/index.php?id=1432.

[3] Soc. 11 March 1998, no. 1375, *RJS* 4/1998, no. 415.

[4] FDI, *Relations du travail et internet* (Relations between work and Internet), FDI report, 17 Sept. 2002, http://www.foruminternet.org/recommandations/lire.phtml?id=394.

employer to set down the conditions for using Internet access and e-mailing for private purposes. He may prohibit access to sites deemed to be illicit (sites offering pornographic or paedophile content, inciting racial hatred, etc.), or further prohibit software downloads, logging on to forums or chatrooms, or accessing private mail-boxes (due to viruses risk). However, when any such monitoring system is instituted by an employer, it needs to be declared to the CNIL, broken down item by item.

SECTION 2
EMPLOYEE LOYALTY OBLIGATION

31.21

General loyalty obligation After initially ruling in favour of employees, judges are tending more and more to uphold the right of an employer to expect an employee to fulfil his work contract, respecting a general obligation of loyalty towards his employer[5].

In this respect, a ruling of the Aix-en-Provence Court of Appeal on 25 November 2003[6] stressed that "the whole national and international legislation aimed at protecting privacy, in particular with respect to employees at their place of work, has not been able to establish a zone of immunity or impunity for misdemeanours committed against employers or third-parties".

31.22

Playing while at work. In a ruling dated 14 March 2000[7], the Court of Cassation ruled that playing while at work was "illegal"[8]. It upheld the decision of an employer to sack an employee for gross misconduct: the employee had taken part in gaming – in particular sport bets – with third parties during working hours and using company equipment.

31.23

Accessing pornographic websites. Likewise, accessing pornographic websites at one's place of work and during working hours is accepted as a reason for sacking an employee – as shown in a ruling of the social law chamber of the Court of Cassation on 10 October 2007[9] (Montpellier Court of Appeal: dismissal of appeal, 17 May 2006).

31.24

Security measures. The CNIL repeats that "a computer placed at the disposal of an employee may be protected by a password or a login, but such a security measure is designed to avoid malevolent or abusive use by a third-party: it is not aimed at transforming the company computer into a private computer". In this respect, an employee, as the sole person with knowledge of the password, is obliged, when requested to do so by his employer, to back-up the material elements and to hand over the information in his possession necessary for conducting company business[10].

Likewise, concerning the use of cryptology, the Court of Cassation also found an employee, who encrypted access to his data on his work station of his own accord and without the authorisation of his employer, to be guilty of gross misconduct[11].

---

[5] Soc. 16 June 1998, *D.* 1998, IR 77.

[6] Aix-en-Provence Court of Appeal, 1st ch. A, 25 Nov. 2003, no. 2003/798.

[7] Soc. 14 Mar. 2000, no. 98-42.090, *Bull. civ.* V, no. 101; *Gaz. Pal.* 28 Oct. 2000, no. 302, p. 34, note J. Berenguer-Guillon and L. Guignot; *JCP G* 7 Feb.. 2001, no. 6, p. 325, note C. Puigelier; *LPA* 11 July 2000, no. 137, p. 5, note G. Picca and A. Sauret.

[8] F. Lemaître, "Jouer sur le lieu de travail est illégal, estiment les juges" (*Judges rule that playing at work is illegal*), *Le Monde* 28 March 2000.

[9] Soc. 10 Oct. 2007, no. 06-43.816, dismissal of an appeal, Montpellier Court of Appeal, 17 May 2006, cf. http://www.legalis.net/jurisprudence-decision.php3?id_article=2065.

[10] Soc. 6 Feb. 2001, no. 98-46.345, *Bull. civ.* V, no. 43 ; *JCP G* 25 July 2001, no. 30, p. 1514, note C. Puigelier; *RTD civ.* Oct.-Dec. 2001, no. 4, p. 880-882, note J. Mestre and B. Fages.

[11] Soc. 18 Oct. 2006, *CCE* Jan. 2007, note E. Caprioli, p. 40 ff.

SECTION 3
RESPONSIBILITIES

31.31

The responsibility of an employee while exercising his freedom of speech. In the field of freedom of speech, an employee benefits from the right of expressing himself freely both inside and outside the company where he works. This right is enshrined in the Act of 4 August 1982 granting employees "direct and collective freedom of speech with regard to work content, the conditions for conducting their work and its organisation" (on the general principles relating to the respect of an employee's privacy – see s[s] nos. 34.00 ff).

However, court rulings state that this principle also has a corollary: the principle of the responsibility of those making use of it. Though it is correct that the implicit subordination to a work contract does not deprive the employee of the fundamental rights attached to his person, and in particular his freedom of opinion, conscience and expression, the commitment still remains that a loyal execution of the contract imposes on him an obligation of discretion vis-à-vis both third parties and other employees within the company"[12]. Furthermore, an employee exercising his freedom of speech can only do so when this does not lead to any abuse such as the denigration of persons or slanderous accusations.

This last court ruling provides for the definition of conditions for using systems in which employees may digitally let off steam ("*défouloirs électroniques*")[13]. These are becoming more and more popular, either as forums created for this purpose by the employer or as sites or forums created on the initiative of an employee or a group of employees.

In addition, it should be stated here that the rule on discretion applies similarly to employee representatives (within the limits set down with regard to the freedom of communication for trade unions; cf. s[s] no. 37.14).

31.32

The responsibility of an employer faced with certain excesses of employees. Article 1384.5 of the Civil Code provides for a principle of an employer's civil responsibility for misconduct by one of his employees committed while executing his job. This is what is referred to as the responsibility of a superior towards his subordinates.

The linking up of an employee's misconduct with his work is perceived in jurisprudence as the connectedness of the misconduct and the execution of the work contract. This connectedness is generally upheld when the misconduct is committed by the employee during working hours, at the place of work, in connection with resources placed at his disposal by the employer, when carrying out instructions given by the employer or through a willingness to act on behalf of the employer. Court rulings also uphold an employer's responsibility for acts committed by one of his employees outside working hours or the place of work, using private resources or not, when these acts have been commissioned by the employer and are likely to be considered as being linked to the employee's work. Though old court rulings rejected making an employer responsible for any damage caused by a work tool when it was used outside the place of work and outside working hours, the situation has since become less clean-cut. Quite a number of rulings link up damage caused by the sole use of a work-related resource to an employee's work functions. Examples of such resources are blogs or forums.

The employer is obviously not responsible when an employee's misconduct cannot be linked up with his work functions and when it does not relate to these. If the misconduct is liable to be linked up to work, an employer may exempt himself from his responsibility if he can prove the three cumulative conditions defined by the Court of Cassation[14] : the employee has acted outside the scope of his work,

---

[12] *Francis Lefebvre,* PB II, page 1.

[13] M.-J. Gros and L. Lamprière, « J'irai cracher sur ma boîte », archives payantes du journal Libération.

[14] Plen. Ass. 19 May 1988, no. 87-82.654, *RTD civ.* 1989, 89, obs. P. Jourdain.

without authorisation and for purposes not related to his remit. On the basis of these three conditions, an Aix-en-Provence Court of Appeal ruling sanctioned an employer with regard to the misuse of Internet by one of his employees. In the case in question, the employee had taken the initiative to distribute a personal web-page criticising a third company. The judges recalled that on this occasion it was the responsibility of the employer "to monitor employees' correct use of equipment belonging to the company". They considered that the employee (i) had acted within the scope of his work, as he had found the opportunity and the means, and in particular the IT means, within this scope to commit an unlawful act, (ii) had acted with authorisation of the employer who had sent out an internal memo declaring the toleration of private use of the Internet for lawful purposes, and (iii) had not acted for purposes unrelated to his remit on the grounds that the internal rule authorised him to make use of Internet access even outside his working hours[15].

A similar hard decision was pronounced by the Court of Cassation with regard to an insurance agent who had committed various abuses by means of IT during working hours and at her place of work. "The employee had acted during working hours and at her place of work within the scope of the work for which she was employed, using the resources placed at her disposition. This rules out her having committed the abuses outside the scope of her work".

The Paris Court of Appeal upheld the negligence of an employer who had let his employees access websites (multimedia files, games, pornographic material, etc) in an uncontrolled manner and without relevance to their business activity. In this case, the employer was in dispute with his service provider commissioned to provide data and antivirus protection. Although the judges of first instance had upheld that "the presence of a virus in a (customer) installation is proof that (the service provider) has not correctly carried out antivirus control", the court of appeal considered that the customer was at fault. "In allowing his staff to link up to such sites, he had rendered ineffective the protection that (the service provider) was commissioned to provide. In such circumstances, the court could not consider the failure of the antivirus protection as justifiable grounds for the termination of the contracts"[16].

However it has been ruled that the sole fact of keeping a personal online blog is not sufficient to justify damage to an employer's reputation (industrial tribunal, 30 March 2007, cf. s^{s} no. 125.28).

These court rulings demonstrate the usefulness of defining, in internal company regulations or as an appendix thereof, the conditions under which employees can use the IT resources and Internet access placed at their professional disposal.

[15] Marseille TGI, 1st civil chamber, 11 June 2003, Escota v. Lucent Technologies, http://www.juriscom.net; confirmed by Aix-en-Provence Court of Appeal, 13 March 2006, appeal no. 2006/170.

CHAPTER

32. Principle of transparency

SECTION 0
ORIENTATION

32.00

Overview.

Sect. 1 Obligation to inform

Sect. 2 Consequences of breaches of transparency

32.01

Applicable texts

> French texts.

See s^s no. 3.01.

32.02

Reference court rulings.

> On the obligation to inform employees.

• **Soc. 22 May 1995,** no. 93-44.078, *Bull. civ.* V, no. 164; *Rev. soc. Francis Lefebvre* 1995, no. 7, p. 489, note Y. Chauvy — confirmation of **Douai Court of Appeal, 30 June 1993.**

* See s^s no. 32.11, also s^s no. 30.23.

> On the obligation to inform and consult the works council.

• **Soc. 7 June 2006,** no. 04-43.866, Girouard v. Continent France, *Bull. civ.* V, no. 206; *D.* 2006, 1704 — confirmation of **Bourges Court of Appeal, soc. law chamber, 24 Oct. 2003.**

* See s^s no. 32.12, also no. 30.24.

> Challenging evidence on the grounds that employees were not previously informed.

• **Soc. 6 June 2007,** no. 05-43.996, sté Eliophot v. M. X — confirmation of **Aix-en-Provence Court of Appeal, 18th chamber, 7 June 2005.**

• **Soc. 2, 20 Nov. 1991,** no. 88-43.120, *Bull. civ.* V, no. 519; *D.* 13 Feb. 1992, no. 7, 73, note Y. Chauvy — cassation of **Colmar Court of Appeal, soc. law chamber, 17 Dec. 1987.**

* See s^s no. 32.11 and 32.22, also no. 30.23.

• **Paris Court of Appeal, 31 May 1995,** *Juris-Data* no. 024755; *RLDI* May 2007, no. 27, comm. A. Saint Martin.

* See s^s no. 32.23.

> Challenging evidence on the grounds that it breaches CNIL rules.

• **Paris Court of Appeal, 7 March 1997,** *Gaz. Pal.* 21 Jan. 1999.

See also **Paris Court of Appeal, 31 May 1995** (prec.).

* See s^s no. 32.23.

> Admissibility of telephone records as evidence.

• **Soc. 29 Jan. 2008,** no. 06-45.279, Touati v. sté Canon France, *JS Lamy* 2008, no. 228, comm. J.-E. Tourreil; *Gaz. Pal.* 24 Apr. 2008, no. 115, p. 39, note L. Boncourt — confirmation of **Versailles Court of Appeal, 11th chamber, 5 Sept. 2006.**

* See s^s no. 32.23.

> Admissibility of evidence.

• **Soc. 11 March 1998,** no. 96-40.147, Pisani v. sté Pisani, *Sem. soc. Lamy* 28 May 2001, no. 1030 — confirmation of **Paris Court of Appeal, 21st chamber, 7 Nov. 1995.**

* See s^s no. 32.24.

• **Montpellier Court of Appeal, 17 May 2006,** no. 05/01954, Claude G… v. Assoc. Ogec Emmanuel d'Alzon, http://www.legalis.net/jurisprudence-decision.php3?id_article=2066 -- confirmation by **Soc. 10 Oct. 2007,** no. 06-03.007, Claude G… v. Assoc. Ogec Emmanuel d'Alzon.

• With regard to the (confirmed) 1st instance ruling, see **Montpellier Industrial Tribunal, 26 Sept. 2005,** Claude G… v. Assoc. Ogec Emmanuel d'Alzon.

* See s^s no. 32.24, also no. 31.23.

• See also **Soc. 10 Oct. 2007,** Claude G… v. Assoc. Ogec Emmanuel d'Alzon (prec.)

* See s^s no. 32.24.

• **Aix-en-Provence Court of Appeal, 18th chamber, 4 Jan. 1994**, Perez v. Beli Intermarchés, *Dr. soc.* 1995, 332; S. Darmaisin, "L'ordinateur, l'employeur et le salarié" (*the computer, the employer and the employee*), *Dr. soc.* 2000, p. 580; *Juris-Data* no. 041281 — annulment by **Nice Industrial Tribunal, comm. sect.,**

10 Dec. 1990.

* See s[s] no. 32.25.

• **Soc. 14 March 2000,** no. 1270, no. 98-42.090, *Bull. civ.* V, no. 101; *Gaz. Pal.* 28 Oct. 2000, no. 302, p. 34, note J. Berenguer-Guillon and L. Guignot; *JCP G* 7 Feb. 2001, no 6, p. 325, note G. Picca and A. Sauret — confirmation by **Paris Court of Appeal, 18th chamber, sect. A, 16 Feb. 1998,** no. 020563.

• With regard to the (partially annulled) 1st instance ruling, see **Paris Industrial Tribunal, 2nd chamber, supervision sect. , 13 Dec. 1995.**

* See s[s] no. 32.11 and 32.24, also no. 30.23 and 31.22.

> On the legal value of charters.

• **Soc. 21 Dec. 2006,** no. 05-41.165, J.-H. Pettre v. sté Ad 2 One SA — confirmation of **Versailles Court of Appeal, 5th chamber, sect. B, 25 Nov. 2004.**

* See s[s] no. 32.15.

> On the admissibility of evidence in criminal cases.

• **Crim. 6 Apr. 1994,** no. 93-82.717, *Bull. crim.,* no. 136 — confirmation of **Bordeaux Court of Appeal, 3rd chamber, 13 May 1993.**

• **Crim. 23 July 1992,** no. 92-82.721, *Bull. crim.,* no. 274 — confirmation of **Caen Court of Appeal, acc. chamber, 8 Apr. 1992.**

• **Crim. 31 May 2005,** no. 04-85.469 — confirmation of **Montpellier Court of Appeal, corr. chamber, 6 May 2004.**

* See s[s] no. 32.26, also nos. 30.26 and 30.23.

32.04

The main questions.

• What are the conditions with regard to the legitimacy of collecting and processing data of a personal nature?

* See s[s] nos. 32.11 and 32.12.

• What are the legal consequences of any failure to respect obligations to inform employees?

* See s[s] no. 32.22.

SECTION 1
OBLIGATION TO INFORM

32.11

Obligation to inform employees. French Labour Code explicitly foresees that "no information personally concerning an employee (or a candidate for a job) may be collected by a system which has not been made known beforehand to the employee (or the candidate for a job)" (Labour Code, Art. 1221-9 [prev. Art. L. 121-8]). The CNIL also states that the employees concerned must always be individually informed of the introduction of any monitoring systems, the modalities with regard to their right of access to the data, and the purpose of the monitoring measures.

This rule has been recalled several times by the Court of Cassation: "Though an employer has the right to control and monitor the activity of his staff during working hours, he may not introduce a monitoring system without previously informing employees"[17]. Or: "The employer has the right to control and monitor the activity of his employees during working hours. However any use of secret monitoring is excluded[18]"

It is thus to be noted that it is not so much the introduction of control and monitoring systems that is condemnable but the fact that they may be installed behind employees' backs. It is therefore advisable to set down, as part of internal company regulations, as a code of conduct or even as a "charter", the conditions under which Internet access, and in particular e-mails, are to be used, and to refer to such in work contracts. These conditions can additionally be referred to when

[17] Soc. 20 Nov. 1991, n° 88-43.120, *Bull. civ.* V, no. 519; *D.* 13 Feb. 1992, no. 7, 73, note Y. Chauvy: on a concealed camera — Soc. 22 May 1995, no. 93-44.078, *Bull. civ.* V, no. 164; *Rev. soc. Francis Lefebvre* 1995, no. 7, p. 489, note Y. Chauvy: on the shadowing of an employee by a private detective.
[18] Soc. 14. March 2000, no. 1270, no. 98-42.090, *Bull. Civ.* V, no. 101: On a system for listening in to telephone conversations.

allocating an access code, on certain screen pages or even when sending memos. The CNIL "supports this initiative when such "charters" or "usage guidelines" have the explicit purpose of providing users with comprehensive information, increasing the awareness of employees and public-sector officials for the demands of security, and calling their attention to certain behaviour patterns detrimental to the collective interests of the company or institution"[19].

32.12

The obligation to inform and consult the works council. Where a works council exists, the employer is also obliged to provide this body with information before introducing "automated HR procedures and on any modifications thereof" (Labour Code, Art. L. 2323-32; prev. L. 432-2-1) [20]. He must also consult it before any major project involving the introduction of "new technologies, when such are likely to have consequences on the jobs, qualifications, remuneration, training or working conditions of staff" (Labour Code, Art. L. 2323-13; prev. L. 432-2. 1). Finally, he is obliged to inform and consult "prior to any decision on the introduction of any means or technologies permitting the monitoring of employee activities in the company" (Labour Code, Art. L. 2323-32). The information to be provided to the works council must be precise and in written form (Labour Code, Art. L. 2323-4; prev. L. 431-5.2). However, the opinion expressed by the works council is purely consultative and not binding for the employer.

Linking up to Internet, the installation of an Intranet, the introduction of an e-mail system are obviously to be seen "as new technologies and as techniques enabling employees' activities to be monitored" in the above sense. From a more general point of view, it is to be stated that an employer is obliged to inform and consult the works council (Labour Code, Art. L. 1221-9; prev. L.121-8), or, in a public-sector context, the joint technical council (*comité technique paritaire*) or any comparable body, before the introduction of a processing system or procedures enabling employee activities to be tracked, for example a system enabling access to the workstation of an absent employee.

The declaration to be submitted to the CNIL must contain the notification and the date when the employee representative bodies were consulted.

The Court of Cassation has had occasion to sanction the absence of consultation vis-à-vis the works council, applying Labour Code Art. L. 432-2-1 (now Art. L. 2323-32), even though it could hardly have been seriously contested that the employees had not been aware of cameras as these had been in use for a long time and there were signs indicating their presence[21].

32.13

Internet charters and codes of conduct. An employer may submit for signature to his employees a document setting down the conditions for the use of company IT tools. Such a document can become an appendix to the work contract.

If such a text foresees any injunctions, any prohibited activities or disciplinary sanctions, it is to be seen as an adjunct to internal company regulations. In this case, such a text is subject to more stringent publication and information requirements: it must be submitted to the works council for information and consultation, communicated to the work inspectorate (*l'inspection du travail*), deposited with the industrial tribunal, and publicised within the company. Such a document enables the establishment of internal rules of professional conduct and security relating to the use of IT and communication networks. Drawing up such a code of conduct has a number of advantages: though it helps an employer to avoid any potential disputes with his employees, it also fulfils his obligation to provide information about the employee monitoring systems installed in the company, vis-à-vis both employees and their representatives.

---

[19] H. Bouchet (dir.), *La cybersurveillance sur les lieux de travail,* ("cyber-surveillance in the workplace"), CNIL report, March 2004, http://www.CNIL.fr/index.php?id=1432.

[20] In the public sector, the employer is required to consult the joint technical committee or any other body equivalent to a works council: cf.. Law no. 84-16, 11 Jan. 1984; Law no. 84-53, 26 Jan. 1984 and Law no. 86-33, 9 Jan. 1986.

[21] Soc. 7 June 2006, no. 04-43.866, Girouard v. Continent France, *Bull. civ.* V, no. 206; *D.* 2006, 1704.

32.14
Internet charters and the CNIL. According to CNIL, the adopted document "must specify the technical possibilities of the tools and their use when actually implemented, especially with regard to their tracking potential". Stated more precisely, the modalities of the installed monitoring system, the back-up systems used by the employer and the retention period of the back-ups need to be mentioned in such a charter.

In its study report submitted to public consultation on cyber-surveillance of employees at work (*La cybersurveillance des employés dans l'entreprise*), published in March 2001, and in its report titled "Cyber-surveillance in the workplace" (*La cybersurveillance sur les lieux de travail*), modified on 18 December 2003, the CNIL warns against the excesses and abuse often encountered when drawing up charters on the use of IT tools. According to the CNIL, the imbalance between the employer and his employees on signing such a document often proves to be overt. Nevertheless the CNIL supports initiatives for creating such charters when the explicit purpose is "to provide users with comprehensive information, increasing the awareness [of employees] for the demands of security, and calling their attention to certain behaviour patterns detrimental to the collective interests of the company".

32.15
Charters and their legal status. A ruling of the social law chamber of the Court of Cassation attaches a legal value to IT charters, considering them, alongside internal company regulations, as documents opposable to employees. In the case in point, the behaviour of an employee who had attempted, without any legitimate motive and using the password of another employee, to log on to the workstation of the company's managing director, was seen to be contrary to the obligation to respect the IT charter in force at the company. Such behaviour constituted gross misconduct and made it impossible for him to stay on at the company during the period of notice[22].

SECTION 2
CONSEQUENCES OF BREACHES OF TRANSPARENCY

32.21
Invasion of privacy. The Labour Code specifies that the collection and processing of personal data without the knowledge of employees may lead to an employer incurring liability for breach of his general obligation of transparency. Furthermore, if neither the works council (or, in a public-sector context, the joint technical council (*comité technique paritaire*) or any other equivalent body) nor the employees have been previously informed in accordance with the conditions stated above, any system for monitoring an employee's e-mails or any tracking system to identify the websites visited by him could be considered as an invasion of the employee's privacy.Likewise the installation of a system without the knowledge of employees and deliberately kept out of sight (hidden cameras, for example) or aimed at monitoring the comings and goings of employees will be considered as an invasion of employees' privacy.

Court rulings have set down the legal contours applicable when introducing employee surveillance systems, in particular focussing on the admissibility of evidence based on cyber-surveillance systems, or challenging such.

32.22
Challenging evidence on the grounds that employees were not previously informed. An employer cannot make use of evidence obtained with the help of monitoring procedures installed without prior knowledge of employees. Such

[22] Soc. 21 Dec. 2006 no. 05-41.165, NPB, J.-H. Pettre v. sté Ad 2 One SA: dismissal of the appeal against the Versailles Court of Appeal, 5th chamber B, 25 Nov. 2004; *Gaz. Pal.*, 07 August 2007, no. 219, p. 22.

evidence would be rejected in legal disputes, with any sanctions taken against employees on the basis of such evidence possibly being annulled.

Since 1991, the Court of Cassation has been stating that "though an employer has the right to control and monitor the activities of his employees during working hours, all recordings, whatever the motives, of images or speech without their knowledge constitute illegal evidence"[23]. In the case in point, a shop assistant had been sacked for gross misconduct based on a recording made using a camera concealed in her cash register.

In a more recent case, a ruling of the Court of Cassation dated 6 June 2007 upheld a ruling of the court of appeal, which, underlining the private nature of an e-mail sent by the employee in question to one of his work colleagues, had argued that such an element of the employee's private life could not constitute a ground for dismissal[24].

32.23

Challenging evidence on the grounds that it breaches CNIL rules. The judges challenged the evidence gained from processing personal data, although this processing had been duly declared to the CNIL, considering that the data in question was without relevance to the purpose of the processing[25]. This means, for example, that an IT-based ticket reservation system made available to employees cannot be used behind their backs to monitor working hours.

Likewise, the 7 March 1997 ruling of the Paris Court of Appeal set down that the use as evidence of a list of telephone calls made from an employee's workplace, obtained from a PBX, was illegal. The reasoning was that "irrespective of what was done, the obligation of the company – as set down in Art. 6 of the Law of 6 January 1978 - to declare (monitoring) in advance had not been respected and that the records should not have been kept for any other reason that possibly billing the employee for his private calls"[26].

However, the ruling of the Court of Cassation dated 29 January 2008 should be pointed out here. This accepted that telephone records produced by an employer could be used to justify the dismissal of an employee on the grounds of abusive use of his business telephone[27]. With the help of these records, it had been established that the employee had spent a total of 63 hours between July 2002 and January 2003 calling adult telephone dating services from his workplace. The employee had tried in vain to take advantage of the inadmissibility of the evidence produced, arguing that he had not been informed of the monitoring. The High Court however ruled that the simple verification of records of the duration, the cost and the telephone numbers used in calls from each workplace and produced by the company's PBX, did not constitute illegal surveillance by not having been brought to the notice of the employee beforehand. One should however note that the question of conformity to the French Data Privacy Act (*la loi informatique et libertés*) with regard to collecting employee's personal data via telephone records was not raised here.

32.24

Admissibility of evidence. The judges ruled that the employer could make use of recordings of an employee's telephone conversations to establish that he had engaged in online gambling (bets on the presidential election or the results of football matches) during working hours, as he had been warned that he was being monitored[28]. They

---

[23] Soc. 20 Nov. 1991, no. 88-43.120, *Bull. civ.* V, no. 519.

[24] Soc. 6 June 2007, no. 05-43.996, NPB, sté Eliophot v. M. X…: dismissal of the appeal against the Aix-en-Provence Court of Appeal, 18th chamber, 7 June 2005.

[25] Paris Court of Appeal, 31 May 1995, *Juris-Data* no. 024755; *RLDI* May 2007, no. 27, comm. A. Saint Martin.

[26] Paris Court of Appeal, 7 March 1997, *Gaz. Pal.* 21 Jan. 1999, p. 30.

[27] Soc. 29 Jan. 2008, no. 06-45.279, Touati v. sté Canon France, *JS Lamy* 2008, no. 228, comm. J.-E. Tourreil; *Gaz. Pal.* 24 Apr. 2008, no. 115, p. 39, note L. Boncourt; http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000018074945.

[28] F. Lemaître, in " Jouer sur le lieu de travail est illégal, estiment les juges" (*Judges rule that playing at*

confirmed that "the employer has the right to control and monitor the activities of his employees during working hours and that solely the use of clandestine monitoring contravened the law"[29]. In the case in point, it should be noted that it involved a stock trading company where the professional regulations authorised the recording of telephone purchase orders.

Likewise, a ruling of 11 March 1998 pronounced by the social law chamber of the Court of Cassation accepted that the submission as evidence, by an employer, of telephone billing records sent to him by France Télécom for the settlement of calls from the employee's workplace, did not constitute a form of illegal evidence[30]. In a more recent case, a ruling of the Montpellier Court of Appeal of 17 May 2006 accepted that facts, revealed on the occasion of an employee calling in the company's IT service provider to look into a virus on his workstation, had been lawfully brought to the attention of the employer[31]. The judges considered that the dismissal for gross misconduct was justified, considering that the employee, by accessing pornographic sites on several occasions, had failed to honour his obligations as a teacher "to maintain the dignity inherent to his job and to respect the decent character of the institution", as set down in the collective agreement of secondary school teachers working in private schools. In a ruling dated 10 October 2007, the social law chamber of the Court of Cassation upheld this view[32].

32.25

In all cases, judges require high-quality evidence. A ruling of 4 January 1994 by the Aix-en-Provence Court of Appeal stated that a document submitted as evidence must present "sufficient guarantees of authenticity, impartiality and sincerity concerning both its date and its content"[33].

(For more comprehensive developments on the difficulty of establishing proof see s[s] nos. 141.31.)

32.26

In criminal terms. The Court of Cassation also noted that there was no legal provision allowing judges of criminal cases to reject evidence submitted by the parties with the sole justification that it had been obtained illegally or disloyally […] their duty was solely […] to assess its conclusiveness[34]. Furthermore, it noted that there was no text in criminal procedure forbidding the submission, by the plaintiff as substantiation of his complaint, of pieces of evidence such as to constitute charges against the persons who were the subject of the complaint […] the duty of criminal courts was to assess the value with regard to the regulations relating to the administration of the proof of the offences"[35].

As an example, one can cite the case of the recording of the activity in a pharmacy by a camera installed in public sight at the request of the pharmacist. The recordings had been able to demonstrate the abuse of confidence committed to his detriment by an employee. Or again the case of an employee sued for gang robbery on the basis of a surveillance-camera recording showing two people abducting various objects by passing them out through the toilet window and putting them in a car parked near to the window[36].

---

work is illegal), *Le Monde* 28 March 2000.

[29] Soc. 14 March 2000, no. 1270, no. 98-42.090, *Bull. civ.* V, no. 101; *Gaz. Pal.* 28 Oct. 2000, no. 302, p. 34, note J. Berenguer-Guillon and L. Guignot; *JCP G* 2001, no. 6, p. 325, note C. Puigelier.

[30] Soc. 11 March 1998, no. 96-40147 Pisani v. sté Pisani, *Sem. soc. Lamy* 28 May 2001, no. 1030, cf. http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechExpJuriJudi&idTexte=JURITEXT000007373394.

[31] Montpellier Court of Appeal, 17 May 2006, no. 05/01954, Claude G… v. Assoc. Ogec Emmanuel d'Alzon, cf. http://www.legalis.net/jurisprudence-decision.php3?id_article=2066.

[32] Soc. 10 Oct. 2007, no. 06-03.007; dismissal of appeal Montpellier Court of Appeal, 17 May 2006, v. http://www.legalis.net/jurisprudence-decision.php3?id_article=2065.

[33] Aix-en-Provence Court of Appeal, 4 Jan. 1994, *Dr. soc.* 1995, 332.; S. Darmaisin, "L'ordinateur, l'employeur et le salarié" (*the computer, the employer and the employee*), *Dr. soc.* 2000, p. 580.

[34] Crim. 6 Apr. 1994, no. 93-82.717, *Bull. crim.*, no. 136.

[35] Crim. 23 July 1992, no. 92-82.721, *Bull. crim.,* no. 274.

[36] Crim. 31 May 2005, no. 04-85.469.

However, one should note that, in at least two cases, the Court of Cassation confirmed that it was not possible to resort to police provocation to establish proof of an offence (Crim. 7 Feb. 2007[37] -- Crim. 4 June 2008[38] — for further developments see. s[s] no. 143.12).

[37] Crim. 7 Feb. 2007, no. 06-87.753, *Bull. crim.*, no. 37; cass. Paris Court of Appeal, 26 Sept. 2006 (referral to Versailles Court of Appeal); see also "Une procédure fondée sur une provocation à commettre une infraction, même commise à l'étranger, doit être annulée" (*A procedure based on a provocation to commit an offence, even when committed abroad, is to be annulled*), *AJ pénal* 2007, no. 5, May, juri. p. 233.

[38] Crim. 4 June 2008, no. 08-81.045 ; , P ; *JCP G* 2008, IV, 2287; http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000018946415.

CHAPTER

33. Principle of proportionality

SECTION 0
ORIENTATION

33.00

Overview.

Sect. 1 A justifiable system

Sect. 2 Conditions under which an employee's personal data may be accessed

Sect. 3 Sensitive systems and schemes

33.01

Applicable texts

> French texts.

Applicable texts

See s[s] no. 3.01.

Opinions and recommendations.

CNIL, Guideline doc. adopted by the Commission on 10 Nov. 2005 on the implementation of whistleblower schemes conforming to the 6 January 1978 Data Privacy Act (modified in August 2004) – CNIL resol. no. 2005-305, 8 Dec. 2005, on the authorisation of the processing of personal data implemented in connection with whistleblower systems -- CNIL resol.. no. 2006-067, 16 Mar. 2006, on the adoption of a simplified standard concerning the automated processing of personal data implemented by public or private bodies for the purpose of geo-tracking vehicles used by employees (simplified standard no. 51) *JO* n[o.] 1003, 3 May — Report presented to the Deputy Minister of Employment, 7 March 2007, *Charte d'éthique, alerte professionnelle et droit du travail français : état des lieux et perspectives* (Ethics charter, whistleblowing and French labour law) cf. http://lesrapports.ladocumentationfrancaise.fr/BRP/074000335/0000.pdf l

33.02

Reference court rulings

> Principle of prohibiting phone-tapping at work.

• **Soc. 7 Nov. 1995,** no. 92-44.498, NPB, Sté polyclinique Volney v. M. Bordeau — confirmation **Rennes Court of Appeal, 5th chamber, 29 Sept. 1992**.

• **Soc. 3 Feb. 1999,** no. 97-40.495, NPB, Sté Locamion v. Belgacem ben Mariem — confirmation **Lyon Court of Appeal, soc. law chamber. coll. B, 5 Dec. 1996**.

• **Soc. 30 March 1999,** no. 97-40.850, NPB — confirmation **Lyon Court of Appeal, soc. law chamber. coll. B, 8 Nov. 1996**.

• **Soc. 18 Nov. 1998,** no. 96-43.902, Sté Cegeor, SARL v. Mme I. NPB — confirmation **Lyon Court of Appeal, soc. law chamber, 5 June 1996.**

* See s[s] no. 33.13.

> On the principle of inviolability of private correspondence.

• **TGI Paris, 12th chamber, 1 June 2007,** Oddo et Cie v. Trinh Nghia T… and Trung T…, http://www.legalis.net/breves-article.php3?id_article=2178.

* See s[s] no. 33.20.

> On reading e-mails and files created by an employee.

• **Soc. 2 Oct. 2001, Nikon ruling,** no. 99-42.942, *Bull. civ.* V, no. 291; *D.* 8 Nov. 2001, no. 39, jur., comm. 3148-3153; *Sem. soc. Lamy* 15 Oct. 2001, no. 1046; *JCP E and A* 29 Nov. 2001, no. 48, p. 1918, note C. Puigelier; *JCP G* no. 2, 9 Jan. 2002, doctr., I, 102, p. 63-69, note M. Bourrié-Quenillet and F. Rodhain; *RTD civ.* Jan.-Mar. 2002, no. 1, 72-73, note J. Hauser; *RJPF* Jan. 2002, no. 1, p. 10-11, note B. Bossu; *RJS* no. 12/01, Dec. 2001, chron. p. 940-946, note F. Favennec-Hery; *Gaz. Pal.* 16 May 2002, no. 136, p. 47, note H. Vray; *LPA* 10 Dec. 2001, no. 245, p. 6, note G. Picca — cassation of **Paris Court of Appeal, 18th chamber, sect. A, 22 Sept. 1999**.

* See s[s] no. 33.21.

• **Soc. 18 Oct. 2006,** no. 04-48.025, NPB, Jérémy L. F… v. Techni-Soft: *Bull. civ.* V, 18 Oct. 2006 comm. Ray J.-E., L'envers de l'arrêt Nikon (*The other side of the Nikon ruling*), *Sem. soc. Lamy* 2006, no. 1280, p. 10; P. Alix, "L'accès par l'employeur aux fichiers personnels stockés sur l'ordinateur du salarié" (*Employer access to private files on an employee's PC*), *JSL* no. 189-1, p. 4; J.-

E. Tourreil, "Les documents détenus par un salarié dans l'entreprise sont présumés avoir un caractère professionnel" (*documents kept by an employee at work are assumed to be of a business nature*), *JSL* no. 200, p. 15 see http://www.legalis.net/jurisprudence-decision.php3?id_article=1774; *LPA* 28 Apr. 2008, no. 85, p. 7, note X. Daverat and S. Tournaux — confirmation of **Rennes Court of Appeal, soc. law chamber, 21 Oct. 2004,** *Gaz. Pal.* 18 Jan. 2007, no. 18, p. 37, note S. Hadjali and C. Fagot; *LPA* 28 Apr. 2008, no. 85, p. 7, note X. Daverat.**• Toulouse Court of Appeal, 4th soc. law chamber, 6 Feb. 2003,** aff. No. 02-02519.

* See s[s] no. 33.22, 33.21 and also no. 31.24.

• Soc. 17 May 2005, no. 03-40.017, NPB, Philippe K… v. Sté Cathnet-Science, *Juris-Data* no. 028449; *CCE* July-Aug. 2005, p. 34 s., comm. A. Lepage; *Gaz. Pal.* 20 Oct. 2005, no. 293, p. 36, note S. Hadjali; *LPA* 23 Apr. 2007, no. 81, p. 6, note S. Tournaux — cassation of **Paris Court of Appeal, 22nd chamber, sect. A, 6 Nov. 2002**.

• Besançon Court of Appeal, soc. law chamber, 21 Sept. 2004, RG no. 2003-1807, SNC General Electric Energy Products France v. Girardot et al., *RJS* 4/2005, no. 342.

• Soc. 23 May 2007, no. 05-17.818, Datacep v. Hansart, NPB, *Bull. civ.* V; *D.* 2007, AJ 1590, note A. Fabre; *Gaz. Pal.* 18 Mar. 2008, no. 78, p. 20; *LPA* 28 Apr. 2008, no. 85, p. 7, note X. Daverat and S. Tournaux — cassation of **Douai Court of Appeal, 1st chamber, sect. 2, 18 May 2005**.

* See s[s] no. 33.23.

• Versailles Court of Appeal, 2 Apr. 2003, aff. no. 02-00293 and **Besançon Court of Appeal, soc. law chamber, 21 Sept. 2004,** RG no. 2003-1807, SNC General Electric Energy Products France v. Girardot et al., *RJS* 4/2005, no. 342.

* See s[s] no. 33.21.

> On the "justified and commensurate" nature of a monitoring system.

• Soc. 26 Nov. 2002, no. 00-42.401, Montaigu Meret v. Wieth Lederle, NPB, *Bull. civ.* V, no. 352; *RTD civ.* 2003, 58; *Gaz. Pal.* 1 Feb. 2003, no. 32, p. 23, note C.-E. Brault: on the subject of geo-tracking — cassation of **Nancy Court of Appeal, soc. law chamber, 23 Feb. 2000**.

* See s[s] no. 33.31.

• Paris TGI, 19 Apr. 2005, *CCE* Oct. 2005, comm. 164, p. 46.

* See s[s] no. 33.11.

• TGI Paris, 1st chamber, 19 Apr. 2005, CE Effia Services, Synd. Sud Rail v. Effia Services, *CCE* Oct. 2005, p. 46 s, http://www.legalis.net/breves-article.php3?id_article=1434.

* See s[s] no. 33.11.

> On the presumed private or presumed business nature of an e-mail or file.

• Soc. 18 Oct. 2006, no. 04-48.025, NPB, Jérémy L. F… v. Techni-Soft (prec.) — confirmation of **Rennes Court of Appeal, soc. law chamber, 21 Oct. 2004** (prec.).

• Bordeaux Court of Appeal, soc. law chamber, sect. A, 8 Feb. 2005, no. 04/02449.

* See s[s] no. 33.22.

> on whistleblowing schemes.

• TGI Libourne, int. ruling, 15 Sept. 2005, RG no. 05/00143, BSN Glasspack works council, CGT repr. of staff of BSN Glasspack v. SAS BSN-Glasspack, see chron. F. Naftalski, *Lamy Dr. informatique et réseaux* 2005: indent.

• TGI Nanterre, int. ruling, 27 Dec. 2006: suspension of the scheme.

• *CONTRA:* in favour of keeping the scheme, **TGI Lyon, ch. urg., 19 Sept. 2006**, CGT Union, département du Rhône, CGT repr. at Bayer Cropscience v. Bayer Cropscience.

• TGI Nanterre, int. ruling, 1 Apr. 2005, ING Bank Works Council v. ING Bank France.

* See s[s] no. 33.32.

33.03

Relevant literature.

> Guidelines.

Cnil, *Guide pratique pour les employeurs* (Practical Guide for Employers) —CNIL publication on the introduction of fingerprint recognition systems where prints are stored in a database see http://www.cnil.fr/index.php?id=2363&news[uid]=508&cHash=0a2ef80a3e.

> Articles.

G. Haas and L. Goutorbe, "Cyber-surveillance: l'employeur doit être prudent en matière de collecte de preuve" (*an employer must take care when collecting evidence*)", *Expertises* Aug.-Sept. 2005, p. 304 — R. de Quenaudon, « Liberté et sécurité dans l'entreprise (*data privacy and protection at work*): une conciliation de plus

en plus problématique" (*increasingly difficult to reconciliate*), *RDT* 2006, p. 395 ; "Quelques remarques à propos de connexions illicites du salarié" (*some comments on unlawful Internet connections by employees*), *RDT* 2007, p. 370.

33.04

The main questions.

• How to reconcile an employer's right to monitor use of company equipment with his respect of employee privacy?

* See s[s] no. 33.11.

• Under which conditions may an employee's personal data be accessed?

* See s[s] no. 33.20 ff.

• What are the assessment criteria for obtaining authorisation for biometric access control to work premises?

* See s[s] no. 33.30, also no. 28.00 ff.

SECTION 1
A JUSTIFIABLE SYSTEM

33.11

When is a monitoring system "justified". The Act of 31 December 1992 set down a "principle of proportionality", since inserted into Art. 1121-1 of the Labour Code: "Nothing may infringe civil rights and individual and collective liberties which could not be justified by the nature of the task to be accomplished or is not commensurate to the intended goal" (formerly art. L. 120-2).

This was cited by the Paris TGI (tribunal de grande instance) in its decision of 19 April 2005[39], with regard to a biometric recognition system whose introduction was being disputed in the court by the works council and the trade union Sud-Rail. The latter considered that a fingerprint reading system installed to manage and control employee working hours at various work sites was an infringement of employees' rights and individual liberties.

An employer can only monitor activity when he is confronted with an employee's suspect behaviour: abnormally long link-up times or exceptionally long downloads (possibly linking up to and downloading games or even pornographic pictures) could for instance constitute circumstantial evidence justifying surveillance and interception measures. It is to be noted however that such screening could be considered as a restriction of freedom, when a "protected" employ is involved (i.e. a trade union or employee representative, a member of a works council, etc).

33.12

Legal framework with regard to PBXs (private branch exchanges). In an initial recommendation dated 18 September 1984, the CNIL specified that an employer could record neither telephone conversations nor the complete numbers dialled by his employees (he was only allowed to record the first four digits, in order to know whether the employee had been making long-distance calls, etc.) [40]At a later date, following discussions on 20 December 1994, the CNIL drew up a simplified standard as a legal framework with regard to the use of PBXs.These systems allow the storage of the telephone numbers dialled by employees from their workplaces. The CNIL quite clearly set down that the use of company phones for private purposes was allowed. The employer could however claim reimbursement for such calls from his employees. While an employer was in a position to store the numbers dialled by employees from their workplaces, these numbers were under no circumstances to be divulged in full to other employees. Furthermore, an employer was not permitted to store these numbers for longer than six months. Finally, the CNIL repeated that employee representatives needed to be consulted before any PBX was installed.

---

[39] TGI Paris, 1st chamber, 19 Apr. 2005, CE Effia Services, Sud Rail trade union v. Effia Services, *CCE* Oct. 2005, p. 46 ff.

[40] CNIL, resol. No. 84-31, 18 Sept. 1984, on the use of PBXs at work, *3e Rapport d'activités de la Cnil,* (3rd Report of CNIL Activities) Doc. fr., p. 109, http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017654576&fastReqId=227990&fastPos=1.

33.13

Conditions under which employee calls may be intercepted. The practice of phone-tapping has been regulated by the Act of 17 July 1970. This was complemented by the Act of 10 July 1991 enlarging the scope of the principle of prohibiting phone-tapping. Art. 226-15.2 was introduced into the Penal Code, making it a crime to "malevolently intercept, divert, use or divulge calls sent out, transmitted or received by means of telecommunication channels or to go ahead with the installation of equipment built to carry out such interceptions" (punishable by one year imprisonment and a 45 000 EUR fine).

It is similarly punishable to malevolently open, delete, delay or return correspondence that has or has not reached its final destination or to fraudulently gain knowledge of the contents thereof (Penal Code, Art. 226-15.1).

Art. 432-9 of the Penal Code also makes it a crime for any person invested with public authority or holding a public mandate, to order, commit or facilitate, in any other cases than those foreseen by law, the interception or diversion of correspondence sent out, transmitted or received by means of telecommunication channels, or the usage or divulging of the contents thereof (punishable by three years imprisonment and a 45 000 EUR fine).

In addition, the Penal Code makes the possession of any equipment built to perform such interceptions subject to a special authorisation granted by a commission specially formed for such purposes in accordance with Art. R. 226-2 of the Penal Code and chaired by the Secretary General of National Defence.

But doubt remained with regard to the application of this prohibition to employers. The CNIL authorised an employer to intercept calls made by company employees, on the condition that the purpose of the listening-in system is specified, that employees are warned in advance of the introduction of such a system, of the possible consequences of interceptions, and of the periods during which their conversations might be recorded. In addition it is foreseen that employees may benefit from phone lines not connected to the listening-in system for any conversations not directly linked to the purpose of listening-in. Finally it is specified that when listening-in is carried out for monitoring the quality of telephone answering, employees need to be able to have access to a report of the recorded conversation within a short time. Recordings are to be deleted once their analysis has been completed. This must take place within a timeframe in the region of two weeks to one month. Furthermore, customers must be informed that their calls are being recorded.

Court rulings set down a number of principles with regard to listening-in to phone calls. The use of a company phone for private purposes has, in a number of cases, been seen as constituting gross misconduct[41]. But other rulings have acknowledged that such use, though not constituting gross misconduct, was liable to constitute a genuine and serious cause for dismissal[42]. However, court rulings also considered that dismissals pronounced for such a cause were not justified, when they were to be seen as incommensurate to the facts behind the cause[43].

The sole admissible exceptions involve telephone marketing, distance selling, and quality assurance, for the purpose of allowing an employer to monitor work. Failing an acknowledged and commensurate necessity, an alternative solution would need to be looked into, other than, for example "recording all customer conversations as potential evidence, should a dispute arise , or asking the customer for written confirmation, in particular by e-mail"[44].

---

41 Soc. 7 Nov. 1995, No. 92-44.498, NPB, sté polyclinique Volney v. M. Bordeau ; cf. http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007286836.

42 Soc. 3 Feb. 1999, no. 97-40.495, NPB, sté Locamion v. Belgacem ben Mariem, http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007394923.

43 Soc. 30 March 1999, no. 97-40850; Soc. 18 Nov. 1998, no. 96-43902, NPB, sté Cégéor v. Mme I. Maulet, cf. http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007399898.

44 CNIL, *Guide pratique pour les employeurs* (Practical guide for employers), p. 21,

SECTION 2
CONDITIONS UNDER WHICH AN EMPLOYEE'S PERSONAL DATA MAY BE ACCESSED

33.21

Principle of inviolability of correspondence. Any violation thereof constitutes an offence as set down in Art. 226-15 of the Penal Code: "To malevolently open, delete, delay or return correspondence that has or has not reached its final destination and is addressed to a third party, or to fraudulently gain knowledge of the contents thereof, is a crime punishable by one year of imprisonment and a 45 000 EUR fine. The same punishment applies to malevolently intercepting, diverting, using or divulging calls sent out, transmitted or received by means of telecommunication channels or going ahead with the installation of equipment built to carry out such interceptions"[45].

There are several rulings underlining the principle that employers are not allowed to gain knowledge of private e-mails sent or received by their employees. The ruling of the Court of Cassation of 2 October 2001 (Nikon ruling[46]) specifies very clearly that "an employee has the right, even during working hours and at his place of work, to have his privacy respected. This applies in particular to the secrecy of correspondence. No employer may, without violating this fundamental liberty, gain knowledge of private e-mails sent out or received by an employee using equipment made available to him for his work, even if he (the employer) has stated that the use of the computer for non-business purposes is forbidden". In this matter, an employee had discovered that one of his employees was running a parallel activity during working hours and using his company workstation. The judges considered that the evidence collected from the employee's e-mail file had been obtained illegally and was therefore to be dismissed.

In a more recent case, the Court of Cassation upheld a ruling of the court of appeal, which, underlining the private nature of an e-mail sent by the employee in question to one of his work colleagues, had argued that such an element of the employee's private life could not constitute a ground for dismissal[47].

The principle of the inviolability of correspondence also applies to employees. This has been illustrated by a ruling of the Paris TGI (tribunal de grande instance) of 1 June 2007[48] which found a former IT consultant of a company guilty of having kept in his possession the codes needed to access the e-mail files of both the managing director and the HR director after he had left the company. In this matter, the two directors had discovered that they were being subjected to electronic surveillance. The search carried out at the consultant's home had revealed links to the e-mail files concerned. He claimed to have passed the codes on to his brother, a former employee of the company in question (Oddo), who was now working for a competitor, so that he could see whether this company was possibly going to take over Oddo. The judges recalled that the simple fact of accessing e-mail files of third-parties by the use of their access codes constitutes fraudulent access to an IT system and a violation of the secrecy of

---

http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_GuideTravail.pdf.

[45] This article emerged from Regulation No. 2000-916, 19 Sept. 2000, Art. 3, *JO* 22 Sept. 2000, which came into effect on 1st January 2002.

[46] Soc. 2 Oct. 2001, no. 99-42.942, Nikon France v. M. Onof, cass. Paris Court of Appeal, 22 March 1999 (referral to the Paris Court of Appeal), *D.* 2001, 3148, note P.-Y. Gautier; *D.* 2002, summ. 2296, note C. Caron; *CCE* 2001, comm. 120 et obs.; *Dr. soc.* Nov. 2001, p. 915, note J.-E. Ray — see also the debate on the Nikon France ruling, no. 99-42.942, *Bull. civ.* V, no. 291; *Sem. soc. Lamy* 15 Oct. 2001, no. 1046, http://www.legifrance.gouv.fr/WAspad/UnDocument?base=CASS&nod=CXCXAX2001X10X05X00291X000; *Gaz. Pal.*, 16 May 2002, no. 136, p. 47, note H. Vray; *LPA*, 10 Dec. 2001, no. 245, p. 6, note G. Picca.

[47] Soc. 6 June 2007, no. 05-43.996, NPB, sté Eliophot v. M. X…: dismissal of the appeal against the Aix-en-Provence Court of Appeal, 18th chamber, 7 June 2005.

[48] Paris TGI, 1 June 2007, Oddo et Cie v. Trinh Nghia T… and Trung T…, available at: http://www.legalis.net/jurisprudence-decision.php3?id_article=2179.

correspondence as set down in Art. 226-15 of the Penal Code.

33.22

E-mails presumed to be of business nature. According to CNIL, "it needs to be generally accepted that an e-mail sent or received from a workstation made available to an employee by his company or government institution takes on a business character, unless the e-mail's subject or directory where it might have been filed by the recipient clearly indicates its character as being correspondence falling under the protection of secrecy of correspondence"[49].

This is the reasoning followed by the judges at Bordeaux Court of Appeal for admitting evidence produced by an employer. They specified that "files on employees' workstations or documents kept in their offices were to be seen as being of business nature when they were not specifically marked as private. It followed that an employer had legitimate access to these business files or documents, even when the employee concerned was not present. It follows that employees' workstations may be accessed by an employer. Therefore (the employer) could quite legally gain access to (an employee's) computer. Without the employee having specifically marked the e-mails sent by her from her company workstation (as private), the employer is within his rights when producing such as evidence at court. As a result, the existence of the e-mails in question was recognised and the facts proven" (Bordeaux Court of Appeal, social law chamber, sect. A, 8 Feb. 2005[50]).

Following this logic, *a contrario,* if the e-mail subject indicates its private nature, an employer has in principle no right to open it in order to read its contents.

However, there are other rulings stating that the inviolability rule applies under all circumstances, even when the e-mail subject is not explicit, and that it is up to the employer to verify those elements likely to clearly indicate the private character of the e-mail in question (as was the case with an e-mail whose subject involved vacation and which was filed in a directory marked as "private")[51].

Employers use different ways to get around this regulation, such as including specific stipulations in charters on the use of company IT equipment. As an example of this, the following ruling of Nanterre Industrial Tribunal of 15 September 2005 may be cited. In this case, an employee who had sent a number of e-mails to a competing company had been dismissed for gross misconduct. Although the e-mails had been marked as "strictly private and confidential", the counsellors considered that the applicant's request for the dismissal to be classified as unfair dismissal (*licenciement privé de cause réelle et sérieuse*) could not be granted, arguing that the company's "ICT Charter" (as a supplement to the internal regulations) clearly stated that "private e-mails need to be marked 'PRV'". This meant that the employer was completely free to gain knowledge of all e-mails not marked 'PRV'.

33.23

Access to private files in the presence of the employee. The Bordeaux Court of Appeal considered that the violation of the secrecy of private correspondence could not be invoked, as the employer had not himself accessed the files in question (of a pornographic nature). These had been opened and read by a legal expert commissioned by the industrial tribunal and in the presence of the parties concerned or their legal advisors (Besançon Court of Appeal, 24 Sept. 2004[52]). The Court of Cassation confirmed that an employer may have access to an employee's private files. In the case in question, the employer had discovered erotic photos in the drawer of the employee's desk and had thereupon decided to take a look at the employee's computer hard-disk. There he found a file named "perso", in which there were a series of documents not relating to the employee's job. According to the Court, "apart from cases of risk or specific events, an

[49] CNIL, Guide pratique pour les employeurs (*Practical guide for employers*).

[50] Bordeaux Court of Appeal, soc. law chamber, sect. A, 8 Feb. 2005, no. 04/02449.

[51] Toulouse Court of Appeal, 4th soc. law chamber, 6 Feb. 2003, aff. no. 02-02519.

[52] Besançon Court of Appeal, soc. law chamber, 21 Sept. 2004, RG no. 2003-1807, SNC General Electric Energy Products France v. Girardot et al., *RJS* 4/2005, no. 342.

employer may only open files on the hard-disk of a company computer that have been defined by an employee as private when the latter is present or has been duly summoned" (Soc. 17 May 2005[53]). Since then, the High Court has ruled that "files created by an employee using IT equipment made available to him by his employer for carrying out his work, are presumed to be of business nature and accessible by the employer without the employee actually being present, unless the employee has specifically marked such files as being private" (Soc. 18 Oct. 2006[54]).

Following the same logic, the Versailles Court of Appeal rejected e-mails produced as evidence by an employer to prove that his employee was in the process of establishing a competing company, arguing that these had been retrieved from the employee's laptop without respecting the employee's prior wish to back-up his private files (Versailles Court of Appeal, 2. Apr. 2003[55]).

33.23

Producing SMS text messages as evidence. The Court of Cassation had to give a ruling on the admissibility of SMS text messages as evidence in a case where the employee, dismissed for gross misconduct, was contesting her dismissal on the grounds of the sexual harassment she had been subjected to. These grounds were established by SMS text messages which the court of appeal had admitted as evidence. The employer lodged an appeal, contesting the admissibility of the evidence produced (text messages re-created and transcribed by a huissier (a French judicial officer) without the knowledge of the sender, and a conversation recorded by the employee on a microtape without the knowledge of her employer). The Court of Cassation considered that, though the recording of a private telephone conversation without the knowledge of the person making the proposals was effectively an act of disloyalty, this was not comparable to the recipient's use of SMS text messages, where the sender must have known that they were recorded by the receiving device. It was therefore found that the SMS text messages were proof of the sexual harassment that the employee was complaining about (Soc. 23 May 2007[56]).

SECTION 3
SENSITIVE SYSTEMS AND SCHEMES

33.30

Biometric access control. One can observe a major development of biometric systems used for gaining access to work premises or to IT systems (cf. s[s] nos. 28.20 ff.).

Their introduction is subject to an authorisation issued by the CNIL. In a guide published on 28 December 2007[57], the CNIL sets out the main assessment criteria

---

[53] Soc. 17 May 2005, no. 03-40.017, NPB, Philippe K… v. Sté Cathnet-Science, *Juris-Data* no. 028449; *CCE* July-Aug. 2005, p. 34 s., comm. A. Lepage; see also G. Haas and L. Goutorbe, "Cybersurveillance: l'employeur doit être prudent en matière de collecte de preuve" (*an employer must take care when collecting evidence*), *Expertises* Aug.-Sept. 2005, p. 304; *Gaz. Pal.*, 20 Oct. 2005, no. 293, p. 36, note S. Hadjali; *LPA* 23 Apr. 2007, no. 81, p. 6, note S. Tournaux

[54] Soc. 18 Oct. 2006, no. 04-48.025, Jérémy L… v. Sté Techni-Soft, *Bull. civ.,* V, 18 Oct. 2006 comm. Ray J.-E., L'envers de l'arrêt Nikon (*The other side of the Nikon ruling*), *Sem. soc. Lamy* 2006, no. 1280, p. 10; P. Alix, "L'accès par l'employeur aux fichiers personnels stockés sur l'ordinateur du salarié" (*Employer access to private files on an employee's PC*), *JSL* no. 189-1, p. 4; J.-E. Tourreil, "Les documents détenus par un salarié dans l'entreprise sont présumés avoir un caractère professionnel" (*documents kept by an employee at work are assumed to be of a business nature*), *JSL* no. 200, p. 15, see http://www.legalis.net/jurisprudence-decision.php3?id_article=1774; *Gaz. Pal.* 18 Jan. 2007, no. 18, p. 37, note S. Hadjali and C. Fagot ; *LPA* 28 Apr. 2008, no. 85, p. 7, note X. Daverat.

[55] Versailles Court of Appeal, 2 Apr. 2003, aff. no. 02-00293.

[56] Soc. 23 May 2007, no. 05-17.818, NPB, *Bull. civ.* V; *D.* 2007, AJ 1590, note A. Fabre; *Gaz. Pal.* 18 March 2008, no. 78, p. 20; *LPA* 28 Apr. 2008, no. 85, p. 7, note X. Daverat and S. Tournaux.

[57] http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf.

and risks to which companies expose themselves when implementing such systems, and employee rights in this area (cf. s[s] nos. 28.21 ff.).

Generally speaking, the system must respond to a "major security requirement". In addition, the purpose of the system needs to be limited to controlled access to a well-defined zone for a fixed number of people (1st criterion). In view of the associated data privacy risks, the system must be "commensurate", i.e. tailored to its purpose (2nd criterion). Guarantees need to be given that the authentication and/or identification does not lead to data being divulged (3rd criterion). Finally, the persons concerned must be informed (4th criterion).

The CNIL thus authorised, on 13 September 2007[58], the introduction of a system automatically processing personal data based on voice recognition. Such a system, enabling the generation and automatic re-initialisation of access passwords to a company's IT system, is based on the recognition of employees' voice patterns.

On 8 November 2008, the CNIL also authorised, in five resolutions (no. 2007-335 to no. 2007-339)[59], the introduction of several systems based on finger scans for the purpose of access control to work premises or IT systems.

33.31

Geo-Tracking. An increasing number of companies are introducing geo-tracking systems enabling them to see exactly where their employees are (their geographic position), either at a set point in time or continuously, by tracking equipment they are using. This applies especially to vehicles placed at their disposal by their employer. These systems are mainly based on GSM/GPS technology which allows the permanent localisation of a vehicle equipped with such a system. They enable the collection and processing of such data as the length of time the vehicle was used, the mileage covered or the speed.

The CNIL is of the opinion that such permanent surveillance of employees' movements is disproportionate when the task to be accomplished is not part of the movement itself but part of a service that can itself be the subject of verification[60]. In a ruling of 26 November 2002[61], the Court of Cassation thus ruled that "any tracking organised by an employer to control and monitor an employee's activities constitutes unlawful evidence, without making any distinction as to whether the employee had been informed or not of the existence of such surveillance"[62]. Furthermore, the CNIL initiated a consultation with the stakeholders involved, in particular ministries, trade unions, professional organisations and geo-tracking system integrators, with a view to drawing up a framework for the use of these systems[63].

These discussions led to the adoption, on 16 March 2006, of two recommendations, no. 2006-066 and no. 2006-067, containing respectively a recommendation and a simplified standard "concerning the automated processing of data of a personal nature by public or private bodies and collected in connection with tracking the location of vehicles used by their employees"[64]. Bearing in mind the intrusive nature of geo-tracking systems, the CNIL is drawing up a list of purposes for which the use of such systems is deemed legitimate and therefore permissible (safety or security of employees or merchandise, improved allocation of resources, monitoring and billing transport services for people or goods or service provision directly linked to the use of a vehicle, monitoring working hours).

---

[58] CNIL, resol. no. 2007-248, 13 Sept. 2007, http://www.wk-rh.fr/mybdd/upload/bdd_80/Cnil-D2007-248.pdf.

[59] CNIL, resol. nos. 2007-335 to 2007-339, 8 Nov. 2007, http://www.wk-rh.fr/mybdd/upload/bdd_80/Cnil-D2007-335-339.pdf.

[60] CNIL, Guide pratique pour les employeurs (*Practical guide for employers*), p. 23.

[61] Soc. 26 Nov. 2002, no. 00-42.401, *Bull. civ.* V, no. 352; *RTD civ.* 2003, 58.

[62] CNIL, Guide pratique pour les employeurs (*Practical guide for employers*), p. 23.

[63] CNIL, communiqué 29 Sept. 2005.

[64] CNIL, resol. No. 2006-067, 16 March 2006, on the adoption of a simplified standard concerning the automated processing of data of a personal nature by public or private bodies and collected in connection with tracking the location of vehicles used by their employees (simplified standard no. 51), *JO* no. 1003, 3 May.

Furthermore, the CNIL points out that the use of such a system must not lead to a permanent monitoring of the employee involved. It foresees a considerable reduction in the administrative burden for companies conforming to the proposed requirements, especially with regard to the types of data collected and the length such data is retained (simplified standard no. 51). In this respect, the resolution contains a list of purposes with which such a process of collecting data must comply. The CNIL also sets limits on the data which can be processed when a geo-tracking system is introduced. Furthermore, it sets narrow limits as to who may receive such data.

Finally, the CNIL specifies that those wishing to introduce a geo-tracking system must inform and consult staff representatives before implementing such a system. It is further required to inform all employees affected by the system. Furthermore, those in charge of such processing must ensure that all necessary safety precautions have been taken.

33.32

Whistleblowing schemes. The US Sarbanes-Oxley Act (July 2002) imposes on all US public companies and their foreign subsidiaries the requirement to provide their employees with a whistleblowing scheme, enabling them to "blow the whistle" on any financial offences they gain knowledge of.

In France, there is no legislation regarding such schemes. However it may well be introduced, as this road has been recommended in a report submitted to the Deputy Minister of Labour on 7 March 2007[65]. Indeed, this report, entitled *Charte d'éthique, alerte professionnelle et droit du travail français: état des lieux et perspectives* ("Business standards, whistleblowing and French labour legislation: status and outlook"), recommends several ways of tightening up the legal safety of business standards and corporate governance and establishing a framework for whistleblowing schemes. One particular proposal is to insert into the Labour Code specific rules to enable companies to introduce schemes opening up the possibility of employees blowing the whistle, not just on illegal or irregular acts, infringements of civil rights and breaches of employee health and safety regulations, but also on non-ethical or non-professional acts. This new regulation would have as its principal objectives: "to define whistleblowing; to determine the legal instruments for introducing such schemes; to set down the organisational framework for the legal instrument chosen; to protect the whistleblower".

At present, the CNIL is drawing up a framework of requirements for introducing such schemes. It describes them as "systems placed at the disposal of employees by a public or private institution to encourage them, in addition to the normal alerts given when a system is not working properly, to indicate to their employers any behaviour which they deem as being contrary to the regulations in force, and to organise the verification of the alert thus received from within the institution concerned".

Initially (in May 2005[66]), the CNIL had refused to authorise the introduction of such schemes, considering they "were disproportionate with regard to the objectives pursued, and to the risks of false accusations and stigmatisation of employees who were the subject of any whistleblowing". It also stressed that "the employees subject to whistleblowing would not, by definition, be informed of the recording of data questioning their business integrity (or citizen integrity) and would therefore have no way of opposing the processing of the data on them. The modalities of collecting and processing such data, certain of which could involve actions liable to constitute criminal offences, can therefore be classified as disloyal". This position had the effect of causing difficulties to the French

---

[65] See the report "Charte d'éthique, alerte professionnelle et droit du travail français: état des lieux et perspectives" (*Business standards, whistleblowing and French labour legislation: status and outlook*) cf. http://lesrapports.ladocumentationfrancaise.fr/BRP/074000335/0000.pdf l

[66] CNIL, resol.. no. 2005-110, 26 May 2005, relating to a request for authorisation from Mc Donald's France for the introduction of a business integrity scheme, http://www.cnil.fr/index.php?id=1833&delib[uid]=73&cHash=ed7a84e6a7 — and CNIL, resol. no. 2005-111, 26 May 2005, relating to a request for authorisation from the Compagnie européenne d'accumulateurs for the introduction of a "whistleblowing hotline", http://www.cnil.fr/index.php?id=1834&delib[uid]=74&cHash=89a931a002.

subsidiaries of US companies which were obliged to respect the contradictory requirements of the French Data Privacy Act and the *Sarbanes-Oxley Act*.

This led to the CNIL revising its position. It first aligned its position with the *Securities and Exchange Commission (SEC)* to find guarantees compatible with both the French Data Privacy Act and the *Sarbanes-Oxley Act*, publishing on 10 November 2005[67] a guideline document setting out the conditions under which it was possible to introduce a whistleblowing scheme. It subsequently adopted on 8 December 2005[68] a special authorisation resolution setting out the requirements to be respected in order to be able to benefit from the simplified authorisation procedure. In principle, it accepted the principle of whistleblowing, while limiting its scope to well-defined areas (accounting, financial business, banking, and combating corruption). In addition, it foresees that such a scheme requires the introduction of precautionary measures when collecting, processing and transferring to countries outside the EU the data involved. At the same time, employee rights of information, access and rectification have been modified correspondingly.

The G 29 group (cf. s[s] no. 15.18) similarly adopted on 1 February 2006[69] an opinion on whistleblowing schemes in the banking, accounting, audit sectors and in the fight against corruption and financial irregularities. It essentially takes up the principles stated in the guideline document and the special authorisation procedure issued by the CNIL in November and December 2005.

As a corollary to these stipulations, the court rulings need to be taken into account, due to the increase in cases aimed at stopping whistleblowing schemes. By order of 15 September 2005[70], the judge in chambers at the Libourne (Gironde) tribunal demanded that the French subsidiary of a US company withdraw its whistleblowing scheme, ruling that this measure imposed itself on employees due to the "sole existence of potential imminent damage to the individual liberties of employees who were the victims of anonymous whistleblowing received by means of a private and completely uncontrolled scheme without any serious justification for its existence on the part of the company and its interests". An order of the judge in chambers at Nanterre TGI of 27 December 2006 similarly called for the stop of a questionnaire being sent out to employees that they were obliged to fill in. In it, they were supposed to "indicate whether any family member had any significant holding in any other company wanting to cooperate with or in competition with the company" or to specify "whether any family or private relationship might stand in the way of their acting in the best interests of the company"[71]. The judge in chambers ruled that this whistleblowing scheme did not conform with the CNIL resolution of 8 December 2005, especially insofar as the CNIL had specified that "only voluntary whistleblowing schemes could benefit from the special authorisation".

But the decisions upholding whistleblowing schemes also need to be taken into account. One example is the following ruling of the Lyon TGI of 19 September 2006. It ruled that, "though the claimants had initially brought the case against the whistleblowing scheme, it needed to be stated that the modified document, presenting the scheme as optional and only to be used in areas where the legitimacy had been established (accounting, auditing and fighting corruption),

---

[67] Guideline doc. adopted by the CNIL on 10 Nov. 2005 on the introduction of whistleblowing schemes conforming to the Data Privacy Act Law of 6 January 1978 (and modified in August 2004), http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/CNIL-docori-10112005.pdf.

[68] CNIL, resol. no. 2005-305, 8 Dec. 2005, on the special authorisation regarding the processing of personal data within the framework of whistleblowing schemes, http://www.cnil.fr/index.php?id=1969.

[69] G 29, opinion., 1 Feb. 2006, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf.

[70] Libourne TGI, 15 Sept. 2005, BSN Glasspack, cited in "Alertes éthiques: quelles orientations suite aux décisions de la Cnil ?" (Whistleblowing: which direction following the CNIL resolutions?), *RLDI 2005*/11, no. 318, obs. F. Naftalkski; *CCE* Dec. 2005, A. Lepage, comm. 191, p. 37 and A. Caprioli, comm. 194, p. 44.

[71] TGI Nanterre, 27 Dec. 2006, Dupont de Nemours central works council v. SAS Dupont de Nemours, no. 20006/02550.

treating the identity of the whistleblower confidentially and providing the person targeted with the benefit of a right of access to legal advice and a right of rectification, conformed with the CNIL resolution of 8 December 2005"[72]. Back in April 2005, the judge in chambers had already ruled that the document presented to the works council on the introduction of a whistleblowing system did not seem to pose, at that interim stage and on the basis of the evidence available, any problem either in the interpretation or violation of employee rights, as it was an optional system without any sanctions or consequences[73].

In the view of certain people, these legal precedents outline, in a sufficiently precise way, the framework applicable to whistleblowing schemes. For their part, the authors of the March 2007 report, note that "in an era when there are numerous people legitimately calling for greater legal security […], it would be better to avoid a legal construction for whistleblowing that is by definition slow and conflict-ridden".

The legalisation of whistleblowing schemes indisputably remains subject to debate.

[72] TGI Libourne, chamber for urgent cases, 19 Sept. 2006, CGT Union département du Rhône, CGT CGT Bayer Cropscience v. Bayer Cropscience, cf. http://www.legalis.net/jurisprudence-decision.php3?id_article=1760.

[73] TGI Nanterre, int. ruling., 1 Apr. 2005, ING Bank Works Council v. ING Bank France.

CHAPTER

34. General principles regarding the respect of employee privacy

SECTION 0

Orientation34.00

Overview.

Sect. 1 Employee rights

Sect. 2 Relevance and purpose of processing measures

Sect. 3 Protective measures

34.01

Applicable texts

> French texts.

Legal texts

Labour Code., Art. L. 1121-1 and L. 1134-1 ff.

Opinions and recommendations.

CNIL, resol. no. 20028, 8 Jan. 2002, concerning the automated processing of personal information implemented at places of work for managing access to premises, working hours and company canteens— CNIL, resol. No. 2007-368, 11 Dec. 2007, with an opinion on the draft government decree modifying decree no. 2005-1726 of 30 December 2005 relating to electronic passports.

34.02

Reference court rulings

> On employees' right to be informed.

• **Soc. 6 Apr. 2004,** no. 01-45.227, Sté Allied signal industrial Fibers v. M. Pacheco NPB, *Bull. civ.* V, no. 103; *Gaz. Pal.* 20 July 2004, no. 202, p. 31, note J. Bérenguer-Guillon and L. Maurel-Guignot — confirmation of **Nancy Court of Appeal, social law chamber, 25 June 2001,** M. Pacheco v. Sté Allied signal industrial Fibers, *Juris-Data* no. 145997; *Dr. ouvrier* 2002, no. 652.

For the 1st instance ruling (annulled), see **Longwy Industrial Tribunal, 3 Dec. 1999.**

* See s[s] no. 34.10, also no. 14.24.

> On the access to annual assessment data.

• **Soc. 23 Oct. 2001,** no. 99-44.215, NPB, CANSSM v. Mme Vicheney, cf. http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007628680 — confirmation of **Paris Court of Appeal, 18th chamber, sect. A, 1 June 1999.**

* See s[s] no. 34.12.

> On the appraisal of the relevance of the data.

• **Civ. 1st, 29 May 1984,** no. 82-12.232, CEMU v. Mme D… et al., *Bull. civ.* I, no. 176 — confirmation of **Rouen Court of Appeal, 3rd chamber, 17 Dec. 1981**.

* See s[s] no. 34.21.

34.03

> Report.

H. Bouchet (dir.), *La cybersurveillance sur les lieux de travail,* ("cyber surveillance in the workplace"), CNIL, March 2004, http://lesrapports.ladocumentationfrancaise.fr/BRP/044000175/0000.pdf.

> Article.

A. Saint-Martin, "La reconnaissance d'une présomption de professionnalité des messages électroniques du salarié", (*The recognition of a presumption of business content of employees' e-mails*) *RLDI* no. 34, Jan. 2008, p. 29.

34.04

The main questions.

• What rights does an employee have with regard to his personal data?

* See s[s] no. 34.10 ff.

• What are an employer's responsibilities?

* See s[s] no. 34.21 ff.

SECTION 1
EMPLOYEE RIGHTS

34.10
Right to be informed. cf.. s[s] nos. 12.30 ff. and 32.11 ff.

34.11
Rights of access, rectification and deletion. Each employee, as with any physical person, has the right to have all data on file concerning his person handed over to him, and to have erroneous data either corrected or deleted. He also has the right to be opposed to his data being kept on file, but only when there are legitimate reasons that his employer should accept. He cannot oppose the collection of data needed to fulfil a legal commitment, for example mandatory social security declarations. On the other hand, he may be against the works committee receiving data on his person. He must however be clearly informed of the consequences which he would incur (such as not being able to benefit from reduced fares). If the data have already been transmitted, the works council must be informed of such so that it may delete the data in accordance with the employee's request. This obligation does not just hang over an employer, but similarly over a works council or any other body in the public sector, intent on implementing databases involving employees' personal data. Notices to this effect must be contained in any questionnaire aimed at gathering personal data on employees. In all other cases, the CNIL considers that "the posting of an information notice on a company bulletin board or the handing over of a document to this effect to the employee constitutes a suitable informational measure"[74] (on the rights of persons concerned, see. s[s] nos. 12.41 ff.).

34.12
Access to annual assessment data. Following several complaints made against employers for refusing to send managers their ranking results and information on their career potential, the CNIL ruled, on the occasion of its 8 March 2007 plenary session, that this type of data may be communicated to the employee concerned once they have been taken into account for deciding a salary increase, a promotion or a posting. The employee can, in accordance with Art. 39 of the Data Privacy Act, modified in August 2004, demand a copy of the document containing these data.

A ruling of the Court of Cassation dated 23 October 2001 had already had occasion to consider that the non-communication of an assessment file to an employee requesting it constituted one element of a behaviour pattern that could be characterised as discriminatory[75].

SECTION 2
RELEVANCE AND PURPOSE OF PROCESSING DATA

34.21
Relevance of data. Personal data must be "appropriate, relevant and not excessive" with regard to the objectives pursued. The collection of information, for example, on the health of an employee or on his close relatives would be contrary to this principle. The recording of the social security number is authorised in payroll and HR files to prepare pay-slips and mandatory social security declarations (Decr. no. 91-1404, 27 Dec. 1991 — CSS, Art. R. 115-1 and R. 115-2) and for keeping employee savings accounts (Labour Code., Art. L. 3341-6). Though the

---

[74] See CNIL, Guide pratique pour les employeurs (*Practical guide for employers*), p. 30.
[75] Soc. 23 Oct. 2001, no. 99-44.215, NPB, CANSSM v. Mme Vicheney, cf. http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007628680.

copy of an employee's tax certificate may be sent to a works committee so that the latter may calculate the employee's contributions, it is a different matter altogether with regard to an income statement, due to the private character of the data contained therein[76].

34.22

Legitimate usage Data of a personal nature must have a "predetermined and legitimate usage".

This means that a video-surveillance system installed in a place likely to cause a violation of intimate privacy (showers, for example) or which would put an employee or a group of employees under constant surveillance would be illegal. Furthermore, the purpose stated needs to be respected.

A badge-reader must not enable the monitoring of employees' comings and goings or provide access to detailed information on what employees are consuming in a company canteen. The CNIL issued a series of recommendations on how to avoid such distortions of purpose in its resolution no. 02-001 of 8 January 2002[77].

34.23

Remarks in HR files not to be excessive. On 11 December 2007, the CNIL fined a French company 40 000 EUR for subjective remarks in an HR file[78]. In its ruling, it stated that, though it was admissible that personal data files could include fields for remarks which could be used to record management information such as summaries of interviews or case progress indicators, these remarks had to be relevant, appropriate and non-excessive with regard to the processing purpose. Non-respect of this obligation is liable to lead to the application of Art. 226-18 of the Penal Code. In the case in point, it was about persons formerly employed by a company, but not to that company's satisfaction.

SECTION 3
PROTECTIVE MEASURES

34.31

Data retention period. This period must be specified for each file with respect to its purpose (for example, from a few days to one month for video-surveillance recordings). An unlimited retention period is not permitted.

With regard to telecommunications data (cf. s[s] nos. 27.00 ff.), an employer must be as precise as possible in specifying the retention period for telecommunications data permitting the identification of the workplace or the user. The CNIL recommends in this respect the introduction of an annual report: "Security measures involving the recording of traces of user activities or their use of ICT equipment (digital footprints) or which are based on the implementation of automated processing of information either directly or indirectly of a personal nature should be the subject of an "annual IT report" submitted to the works council or the joint technical committee or any other equivalent body for discussion, together with the social report"[79].

---

[76] Civ. 1st, 29 May 1984, no. 82-12.232, *Bull. civ.* I, no. 176.

[77] CNIL, resol. no. 02-001, 8 Jan. 2002, (simplified standard 42) regarding the automated processing of related personal information, implemented at places of work for managing access to premises, working time and canteens,
http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653507

[78] CNIL, resol. No. 2007-368, 11 Dec. 2007, on a draft government decree modifying decree no. 2005-1726 of 30 December 2005 on electronic passports.

[79] See. H. Bouchet (dir.), *La cybersurveillance sur les lieux de travail,* ("cyber surveillance in the workplace"), CNIL, March 2004, p.18,
http://lesrapports.ladocumentationfrancaise.fr/BRP/044000175/0000.pdf.

34.32
Authorisation management An employer is obliged to define a security policy for ensuring data privacy (1978 Data Privacy Act, Art. 34). There are certain data that can only be accessed by special persons (unless they need to be transmitted to authorised third parties, such as employment inspectorates, tax authorities, etc.). Likewise, when a video-surveillance system is in operation, recorded image data may only be viewed by people with appropriate authorisation, within the framework of their job assignments (for more on video-surveillance, see s[s] nos. 30.00 ff.).

CHAPTER

35. Specific rules applicable to network administrators

SECTION 0
ORIENTATION

35.00

Overview.

Sect. 1 Principle of professional secrecy

Sect. 2 Exception: the presence of a potential risk to company security

35.01

Applicable texts

> French texts. See s[s] no. 3.01.

35.02

Reference court rulings

> Access to employee documents.

• **Soc. 6 Feb. 2001,** no. 98-46.345, Sté Laboratoires pharmaceutiques Dentoria v. Mme Bardagiet et al., *Bull. civ.* V, no. 43; *JCP G* 25 July 2001, no. 30, p. 1514, note C. Puigelier; *RTD civ.* Oct.-Dec. 2001, no. 4, 880-882, note J. Mestre and B. Fages —cassation of **Toulouse Court of Appeal, 4th soc. law chamber, 23 Oct. 1998.**

• **Soc. 18 March 2003,** no. 01-41.343, NPB, UMS v. Mme C…, *Gaz. Pal.* 25 Sept. 2003, no. 268, p. 37, note L. Maurel-Guignot — cassation of **St Denis de la Réunion Court of Appeal, soc. law chamber, 28 Nov. 2000**.

* See s[s] no. 35.21, also nos. 31.24 and 33.22.

> Measures justified for security reasons.

• **Paris Court of Appeal, 11th chamber, sect. A, 17 Dec. 2001,** no. 2000-07565, F. M…, H. H… and V. R… v. Min. Public and A. T…, *Gaz. Pal.* 8 May 2002, p. 31, comm. S. Le Guillas.

* See s[s] no. 35.21.

35.04

The main questions.

• What are the obligations and responsibilities of a network operator?

* See s[s] no. 35.12.

• How far can they go when intervening?

* See s[s] no. 35.21.

SECTION 1
PRINCIPLE OF PROFESSIONAL SECRECY

35.11

Means of remote monitoring. The question of violations of the secrecy of correspondence takes on a new dimension where network administrators are involved, who have the job of ensuring normal operations and security in company networks and IT systems. Their positions lead them to have access to user information (e-mails, internet links, log files, etc.). They generally have the wherewithal to remotely look into workstations, for example for remote software maintenance, or, more generally speaking, to take over control of the workstation from the user.

35.12

Respect of transparency and proportionality obligations. The conditions under which a network administrator may intervene need to be brought to the attention of employees and their representative bodies. This is part of an employer's obligation with regard to transparency (cf. s[s] nos. 32.00 ff. for this principle). The circumstances surrounding such interventions need to be strictly defined (prior information provided for the user and intervention only when his prior agreement

has been given (via e-mail if needed), and limited to ensuring the smooth operation of applications.

The control must likewise be in accordance with the principle of proportionality (see nos. 32.00 ff. for this principle) and the principle of justifiable purpose set down by the Data Privacy Act.

The CNIL had occasion to remind companies that any use of such tools on the sole initiative of network administrators or their superiors, for example for monitoring purposes, "is neither in accordance with the principle of proportionality nor respectful of the principle of justified purpose set down by the Data Privacy Act.[80].

35.13

Enhanced obligation with regard to confidentiality. Network administrators are bound to professional secrecy, and, in a more general way, to an obligation of professional discretion which forbids them to disclose information that comes to their knowledge while exercising their duties.

This rule is taken up by the CNIL in its report dedicated to cyber-surveillance at work ("*Cybersurveillance sur les lieux de travail* ") (Feb. 2004). "Network and system administrators are generally bound, by professional secrecy or an obligation of professional discretion, not to disclose information that might come to their knowledge in the exercise of their duties, particularly when this information is covered by the principle of secrecy of correspondence or relates to the user's private affairs and has no negative influence either on the smooth running of applications, their security or company interests". It further states that the administrators must not be forced to disclose such information, "unless required to by any special legal provision in this sense".

Finally, the Forum on Internet Rights points out that "a network administrator should take care not to disclose to anyone in the company, including his superiors and his colleagues, personal information on an employee of which he has gained knowledge in the exercise of his duties".

In addition, security measures need to be taken to guarantee the confidentiality of information to which network administrators have access in the course of exercising their functions. This obligation of confidentiality should be referred to in the employment contract, or even in company regulations or the IT usage charter.

SECTION 2
EXCEPTION: THE PRESENCE OF A POTENTIAL RISK TO COMPANY SECURITY

35.21

> Measures justified for security reasons. These rules are valid up to a certain point. They lose their validity when company or government security is at risk. In this context, the Paris Court of Appeal stated, in a ruling of 17 December 2001, that "concern for network security justifies network and system administrators in making use of their positions and the technical possibilities at their disposal to conduct investigations and take measures appropriate to this concern – in the same way that the Royal Mail would react when confronted with a suspicious package or letter. On the other hand, the disclosure of the content of e-mails, particularly of the latter one which was about a latent conflict within the laboratory, bore no relation to such objectives"[81].

Likewise, an employer must have access to documents stored in an employee's computer when the employee is away (on vacation, off sick, etc.)[82]. The Court of

---

[80] CNIL, Guide pratique pour les employeurs (*Practical guide for employers*), p. 14.

[81] • Paris Court of Appeal, 11th chamber, sect. A, 17 Dec. 2001, F. M..., H. H... and V. R... v. Min. public and A. T..., *Gaz. Pal.* 8 May 2002, p. 31, comm. S. Le Guillas; http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=240.

[82] Soc. 6 Feb. 2001, no. 98-46.345, NPB, *Bull. civ.* V, no. 43; *JCP G* 2001, no. 30, p. 1514, note C. Puigelier; *RTD civ.* Oct. - Dec. 2001, no. 4, 880-882, note J. Mestre and B. Fages; *Gaz. Pal.*

Cassation, in a ruling of 18 March 2003, had thus ruled that an employee was bound to communicate his password or the files in his possession when the smooth running of the company was dependent on the data kept by him[83].

20 March 2001, no. 79, p. 9.

[83] Soc. 18 March 2003, no. 01-41.343, NPB, *Gaz. Pal.* 25 Sept. 2003, no. 268, p. 37, note L. Maurel-Guignot.

CHAPTER

36. Specific rules applying to recruitment

SECTION 0
ORIENTATION

36.00

Overview.

36.01

Applicable texts

> French texts.

Legal texts

Labour Code., Art. L. 1221-6 and L. 1221-8.

Opinions and resolutions.

CNIL, resol. No. 02-017, 21 March 2002, on the adoption of a recommandation relating to the collection and processing of personal information during recruiting (abrogates and replaces CNIL recomm. 85-44, 15 Oct. 1985).

CNIL, Recomm. of 5 July 2005 - Measuring racial diversity in the fight against discrimination

> European text.

See s[s] no. 1.01: Dir. No. 95-46, 24 Oct. 1995, Art. 10.

36.04

The main questions.

• What rights does a candidate for a job have?

* See s[s] no. 36.21 ff.

• What guarantees does he benefit from?

* See s[s] no. 36.31 ff.

SECTION 1
CONDITIONS OF IMPLEMENTATION

36.11

Declaration formalities. Persons in charge of recruitment must declare to the CNIL automated processing procedures involving personal data before their introduction (1978 Data Privacy Act , Art. 22). Any breach of this rule makes the person responsible for the processing liable to criminal sanctions (Penal Code, Art 226-24).

36.12

The purpose is limited to the recruitment process. The Labour Code states that "the information requested from a job candidate, in whatever form, is gathered for the sole purpose of assessing his capability to carry out the proposed job or his professional ability. Such information must present a direct and necessary link to the job in question or to an assessment of professional ability. The candidate is bound to respond in good faith to such requests for information" (Labour Code, Art. L. 1221-6).

For its part, the CNIL is of the opinion that, apart from special cases justified by the nature of a vacancy or regulations in effect in a foreign country involving the vacancy, the following questions are contrary to legal requirements: date of entry into France, date of naturalisation, modalities of acquiring French nationality,

original nationality, matriculation or social security numbers, military service details, previous address, information on the family situation (especially on a spouse), state of health (especially height and weight), whether home-owner or tenant, club membership, details of bank account, loans taken out.

Furthermore, the use of vacancy notices to build up a file of candidates or the collection of information about a candidate's professional background without his knowledge could constitute a fraudulent, disloyal or prohibited collection of information (1978 Data Privacy Act, Art. 6).

Finally, the collection and retention of data directly or indirectly pointing to racial origins, political, philosophical or religious opinions, or trade union membership, as well as information on a candidate's health or sexual behaviour is forbidden (1978 Data Privacy Act, Art. 6). The only exemption, and only with prior assent of the candidate, involves information specific to the vacancy.

SECTION 2
CANDIDATE'S RIGHTS

36.21

Candidates' right to be informed. Candidates, as with all other people providing data of a personal nature, have a right to be informed about: (i) the nature of the requested information (obligatory or optional); (ii) any consequences of not providing the information; (iii) the recipients (both physical and legal persons) of the information; (iv) the existence of a right of access to and rectification of the information (1978 Data Privacy Act, Art. 32). Furthermore, they have the right to object (when there are legitimate reasons) to such personal data being processed (1978 Data Privacy Act, Art. 38).

The candidate must similarly be informed of the identity of the person in charge of processing the data and the purpose of the processing (Dir no. 95-46, 24 Oct. 1995, Art. 10). In this respect, the CNIL has issued two recommendations:

(1) "(that) the persons in charge of recruitment take all necessary steps to inform the candidate, within a reasonable period of time, of the outcome of his application, the retention period of the data concerning his person as well as the possibility of requesting the restitution of these data or their deletion."

(ii) "(that) persons whose coordinates are recorded in a file of potential candidates for the purpose of contacting them directly, be informed of the provisions contained in Art. 27 of the Data Privacy Act, at the latest on the occasion of the initial contact. When the identity of an employer has not been specified in the vacancy notice, the candidate's agreement must be gained before any personal data are transmitted to that employer. In the case of personal information being provided by means of telecommunications, the CNIL recommends that the candidate for the job be informed of the form (with or without his name) in which the information on his person will be sent online or transmitted to the employer. The candidate must also be informed beforehand of any potential transfer of information to other recruiting organisations and must also be given the chance to object to such transfers".

The CNIL likewise points out that, "the collected information may only be used with regard to the vacancy and for no other purpose, in particular customer acquisition".

Finally, the candidate must be explicitly informed, "prior to their use, of the methods and recruitment techniques used in his case" (Labour Code, Art. L. 1221-8; formerly L. 121-7). In this respect, the CNIL recommends that "information concerning recruitment software be made available in writing beforehand, either individually or in a standard letter".

36.22

Right of access and rectification. A candidate may exercise the right, available to everyone, of access to and rectification of data concerning his person, whether such data have been provided directly by himself or by third parties or whether they are data resulting from recruitment methods or recruitment software. He may

thus request information concerning his person and demand their rectification if they are found to be inexact (1978 Data Privacy Act, Art. 39). The CNIL consequently recommends that "every candidate be clearly informed of the modalities involved in exercising the right of access and may be provided, on demand, with all information concerning his person, including the results of any assessments, tests or professional appraisals conducted. Similarly, it recommends that "any communication of information contained in the candidate's file be sent in written form. Results of tests or assessments may be communicated by any means appropriate, taking into account the nature of the tool used".

SECTION 3
MEASURES PROTECTING CANDIDATES

36.31
Data retention period. Unless explicitly authorised by the CNIL, data of a personal nature may not be retained for longer than the period stated in the processing declaration (*déclaration du traitement*) (Data Privacy Act, Art. 36). Here, the CNIL recommends that the candidate "be informed of the retention period and of his right to demand at any time their deletion. In no case may the retention period extend beyond two years after the final contact with the person concerned". This measure is recommended for all candidates, whether recruited or not.

36.32
Security and confidentiality of data. The person in charge of the automated processing of candidates' data must commit himself to take all necessary precautions to ensure the security and confidentiality of the data (1978 Data Privacy Act, Art. 34). No parties not directly involved with the recruitment process may have access (either directly or indirectly) to the data.

36.33
Automatic profiling. The candidate has the right to be informed of the algorithms used in the automated selection of candidates (1978 Data Privacy Act, Art. 22). However, no selection decision implying an appraisal of human behaviour may be based solely on any IT processing providing a profile of the candidate or his personality (1978 Data Privacy Act, Art. 10). The CNIL also recommends the prohibition of "automated remote assessment tools without any individual appraisal".

36.34
Statistical tools used in search of discrimination. The CNIL recommends not to collect any data relating to an employee's or candidate's racial or ethnic origin and not to attempt to analyse names or forenames in this respect. On the other hand, such data as the name of the candidate for a job, his forename, nationality, original nationality, place of birth, nationality or place of birth of his parents or his address may be collected and processed.

In addition, the CNIL considers that any rejection of an application for an appointment or a promotion may be the result of the simultaneous consideration of several non-discriminatory criteria, for example professional experience. The discriminating factor may therefore be the result of a statistical analysis involving these various criteria. Furthermore, when the application forms contain data enabling the indirect identification of the person involved, the CNIL recommends that access to the content be restricted solely to persons specifically responsible for such analysis, that "the results be produced in aggregate form" to guarantee anonymity, and that the application forms be destroyed once the answers contained have been evaluated. When the application forms contain identifying data, the CNIL recommends the use of identifiers other than those used in HR management (such as a social security number), the recording of all information in a file held separately from those maintained by HR management as well the implementation of an anonymising process foreseeing the erasure not just of the candidate's identity, but also his address, his telephone number and e-mail

address, his photograph, and any other data permitting his identification".

This is the right place to point out the CNIL's adoption of the National Assembly laws[84] and an amendment to the draft law relating to immigration control, integration and asylum. This amendment, dated 12 September 2007, was based on the CNIL's observations and recommendations[85] with regard to measuring diversity. These are aimed at proposing modifications to the Data Privacy Act for the purpose of facilitating research into measuring racial diversity, discrimination and integration, while at the same time providing better protection of the data and improving the scientific character of the research. The text suggests in particular that data making apparent, either directly or indirectly, a person's racial or ethnic origin may be gathered for research purposes aimed at "measuring the diversity of people's origins, discrimination and integration", but that such processing must be submitted for CNIL authorisation and that the persons concerned retain their right of objecting to such processing.

[84] Report of the Law Commission (*Commission des lois*), http://www.assemblee-nationale.fr/13/rapports/r0160.asp.

[85] CNIL, Recomm., 5 July 2005 - Measuring racial diversity in the fight against discrimination, cf. http://www.cnil.fr/index.php?id=1844.

CHAPTER

37. Specific rules applying to trade unions

SECTION 0
ORIENTATION

37.00

Overview.

Sect. 1 Conditions for using the Internet and Intranet

Sect. 2 Rules protecting the employee

37.01

Applicable texts

> French texts. See s[s] no. 3.01: Labour Code, Art. L. 2142-6 — L. no. 82-689, 4 August 1982, relating to workers' liberties at work — L. no. 2004-391, 4 May 2004 relating to lifelong professional learning and social dialogue, *JO* no. 105, 5 May, 1983 — L. no. 2008-67, 21 Jan. 2008, ratifying ordinance no. 2007-329 of 12 March 2007 relating to the Labour Code (legislative section), *JO* no. 0018, 22 Jan., 1122.

37.02

Reference court rulings

> Freedom of use of e-mail systems and the Intranet provided a company agreement on such exists.

• **Soc. 25 Jan. 2005,** no. 02-30.946, Fédération des services CFDT et al. v. Sté Clear Channel France *Bull. civ.* V, no. 19; *LPA* 8 March 2005, no. 47, p. 3, note A. Sauret and G. Picca — confirmation of **Paris Court of Appeal, 14th chamber, sect. B, 31 May 2002**.

• **Soc. 22 Jan. 2008,** no. 06-40.514, M. M. v. Crédit industriel et commercial, *RDT* 2008, p. 324; *Sem. soc. Lamy* no. 1339, 2008 — confirmation of **Paris Court of Appeal, 18th chamber, sect. D, 29 Nov. 2005**.

• **Crim. 10 May 2005,** no. 04-84705, *Bull. crim.,* no. 144.

* See s[s] no. 37.11.

> On freedom of speech for trade unionists.

• **Nancy Admin. Court of Appeal, 3th chamber, 2 August 2007,** the town of Lons le Saunier v. Elisabeth M…, *RLDI* 2007, no. 31 — annulment of **Besançon Admin. Trib., 1st chamber, 19 Dec. 2006,** Elisabeth M… v. the town of Lons-Le-Saunier, RG no. 0400718.

* See s[s] no. 37.12.

• **Soc. 5 March 2008,** no. 06-18.907, sté TNS Secodip v. Féd. CGT des stés d'études, *Gaz. Pal.* 26 Apr. 2008, no. 117, http://www.courdecassation.fr/jurisprudence_publications_documentation_2/actualite_jurisprudence_21/chambre_sociale_576/arrets_577/br_arret_11274.html — cassation pf **Paris Court of Appeal, 18th civil law chamber, 15 June 2006,** Féd. CGT des stés d'études v. TNS Secodip, followed by appeal before Paris Court of Appeal. For the 1st instance ruling (annulled), see **Bobigny TGI, 11 Jan. 2005,** TNS Secodip v. Fédération CGT des Sociétés d'Etudes.

• **Paris Court of Appeal, 18th chamber C, 15 June 2006,** Féd. CGT des stés d'études v. TNS Secodip, (prec.).

* See s[s] no. 37.14.

37.04

The main questions.

• Can trade unions have their own Internet sites (in a company)?

* See s[s] no. 37.11.

• What are the conditions under which such a site may be implemented?

* See s[s] no. 37.13 ff.

• What are the guarantees offered to employees whose personal data are used by trade unions?

* See s[s] no. 37.21 ff.

SECTION 1
CONDITIONS FOR USING THE INTERNET AND INTRANET

37.11

A company agreement is obligatory. Within the Labour Code, it is foreseen that "a company agreement may authorise the distribution of trade union publications and leaflets, either through a website on the company's Intranet or by using the company's e-mail system. In the latter case, such distribution must not compromise the smooth running of the company's IT network and must not get in the way of work. The company agreement sets out the modalities under which such information may be made available or distributed, defining particularly the conditions under which trade unions may access the network and the technical rules aimed at preserving employees' rights to choose whether to accept or reject such e-mails" (Labour Code, Art. L. 2142-6 — L. no. 2004-391, 4 May 2004 — L. no. 2008-67, 21 Jan. 2008).

Thus, trade unions may access the Intranet, in particular for establishing a trade union blog accessible to all within a company, and use the company's e-mail system provided that prior agreement has been reached with the company.

Without such a company agreement, courts are ruling in favour of prohibiting any such distribution — as confirmed in the Court of Cassation's ruling of 25 January 2005[86]. In this case, the trade union had sent a union e-mail to the business addresses of all employees. There was no company agreement in place and the employer had not given his authorisation.

Furthermore, when a company agreement does exist, the Court of cassation requires it to be strictly applied. In a ruling of 22 January 2008, it observes that, though the company agreement made the use of its e-mail system for distributing union publications subject to the existence of a link between the content and the social situation existing within the company, this had not been true in the case in point (Soc. 22 Jan. 2008[87]).

One needs to observe however that the text of the ruling does not concern the access to these IT resources by trade union representatives, in particular the works council or staff representatives.

37.12

The right to organise is a fundamental right. This rule, pronounced by the Besançon Administrative Tribunal on 19 December 2006, states that nobody may introduce "restrictions which would not be justified by the nature of the task to be achieved or commensurate with the goal sought"[88]. It considered that the mayor of the town of Lons-Le-Saunier was not right in sanctioning one of his employees, an administrative assistant and a trade union representative, who had called on employees to take part in a demonstration. She had done this with the help of the town's e-mail system. It rejected the mayor's argument claiming that the employee had failed in her professional duties by not respecting the ban on using the e-mail system for personal purposes.

But in a different analysis of the content of the disputed e-mail, the Nancy Administrative Court of Appeal considered, in its ruling of 2 August 2007[89], that it was an e-mail with a political nature. In the given circumstances, it considered that the mayor of Lons-le-Saunier had acted within his legal rights in sanctioning the trade union representative on the grounds that a memorandum sent on 18 November 2003 forbade staff to use the Internet for political purposes.

---

[86] Soc. 25 Jan. 2005, no. 02-30.946, *Bull. civ.* V, no. 19.

[87] Soc. 22 Jan. 2008, no. 06-40.514, *Sem. soc. Lamy* no. 1339, 2008.

[88] Besançon Admin. Trib., 1st chamber, 19 Dec. 2006, Elisabeh M… v. Town of Lons-Le-Saunier, cf. http://www.legalis.net/jurisprudence-decision.php3?id_article=1818.

[89] Nancy Admin. Court of Appeal, 3rd chamber, town of Lons le Saunier v. Elisabeth M…, *RLDI* 2007, no. 31.

37.13

Respect of the principle of legitimate purpose. The purpose of any processing must be held in strict respect. Thus, though the company agreement authorises the electronic distribution of trade union information, the e-mail addresses of employees may be used solely for the purpose of distributing publications of a trade union nature.

37.14

Respect of the rights of others. The question of the limits imposed on the freedom of trade union communication from a website outside a company was settled by the Social Law Chamber of the Court of Cassation on 5 March 2008[90].

In the case in point, a trade union had published on its own website company information that was confidential: two opinions of an accounting company on the company's accounts, minutes of several contractual negotiations, meetings of the works council and questions posed by staff delegates. The company was of the opinion that such distribution was prejudicial to its interests and had complained to the Bobigny TGI (*tribunal de grande instance*), requesting to have these items removed from the website.

The first instance judges had acceded to this request, considering that four items containing confidential company information were not to be brought to the knowledge of third parties and competitors and that an employee's obligation of discretion and confidentiality also applied to "trade unions representing employees within a company" (TGI Bobigny, 11 Jan. 2005[91]).

This finding was annulled by the Court of Appeal in its ruling of 15 June 2006. This set down that "as with any citizen, a trade union is free to create a website for exercising its freedom of speech, both directly and collectively, and that there is to be no restriction on exercising this right, and that there is no legal obligation or obligation of confidentiality imposed upon trade union members, other than that imposed by Art. L. 432-7.2 of the Labour Code on members of works committees or trade union representatives, even when these are one and the same person"[92].

Taken to appeal, the Court of Cassation in its turn censured the Court of Appeal, stating that "though a trade union has the right to freely communicate information to the public on a website, this right may be limited as far as necessary to prevent the disclosure of confidential information representing an invasion of the rights of third parties". The High Court ruling is based on Art. 10.2 of the European Convention for the Protection of Human Rights and Fundamental Freedoms which explicitly foresees that freedom of speech may be subjected to certain conditions and restrictions set down by law and constituting necessary measures protecting the rights and repute of others. The ruling is also based on the Act on Confidence in the Digital Economy which foresees that the exercise of freedom of electronic communication may be limited to the required extent, in particular with regard to the respect of the freedom and property of others.

In a previous ruling, the criminal chamber of the Court of Cassation had likewise censured proposals published on a trade union website on the grounds that they slandered a company director to an extent deemed to exceed the admissible limits

---

[90] Soc. 5 March 2008, no. 06-18.907, sté TNS Secodip v. féd. CGT des stés d'études: cass. ruling Paris Court of Appeal, 15 June 2006 (appeal before the Paris Court of Appeal), http://www.courdecassation.fr/jurisprudence_publications_documentation_2/actualite_jurisprudence_21/chambre_sociale_576/arrets_577/arret_no_11275.html;
http://www.legalis.net/jurisprudence-decision.php3?id_article=2227; *Gaz. Pal.* 26 Apr. 2008, no. 117.

[91] TGI Bobigny, 11 Jan. 2005, TNS Secodip v. Féd. CGT des stés d'études, *Gaz. Pal.* 20 July 2005, n° 101, p. 45-46 ; *Expertises* Apr. 2005, p. 156 — for a critical analysis of this ruling, see G. Haas and O. de Tissot, "Des restrictions inacceptables à la liberté d'action des syndicats" (*Unacceptable restrictions to trade unions' freedom of action*), *Expertises* Apr. 2005, p. 145.

[92] Paris Court of Appeal, 18th chamber C, 15 June 2006, Féd. CGT des stés d'études v. TNS Secodip,
http://www.courdecassation.fr/jurisprudence_publications_documentation_2/actualite_jurisprudence_21/chambre_sociale_576/arrets_577/br_arret_11274.html.

in such a case" (Crim. 10 May 2005[93]).

SECTION 2
RULES PROTECTING THE EMPLOYEE

37.21
Employees' right to object. Employees must be able to exercise their right of objection to a trade union's sending any e-mail to their business e-mail accounts. To this effect, they must be informed in advance of any agreement concluded and on how to exercise their right of objection. They must be able to exercise this right at any time and they need to be reminded of this right in every e-mail sent. In addition, the CNIL recommends always making it a clear that it is a trade union e-mail, so as to provide the greatest possible transparency with regard to the origin and nature of the e-mail.

37.22
Guarantee of confidentiality. E-mails sent between employees and trade unions are confidential. Here, the CNIL considers that, "in order to avoid all possibilities of misuse, the employer should not be able to exercise any control over distribution lists established for this purpose. These are liable to reveal an employee's favourable opinion towards an organisation, or even his membership of a certain union, on the basis of his choice in accepting or rejecting trade union e-mails.[94].

[93] Crim. 10 May 2005, no. 04-84,705, *Bull. crim.,* no. 144.
[94] CNIL, Guide pratique pour les employeurs (*Practical guide for employers*), p. 28.

CHAPTER

38. Rules and practices in other countries

SECTION 0
ORIENTATION

38.00

Overview.

Sect. 1 On a European level

Sect. 2 Other nations

38.04

The main question.

• What is the understanding of international bodies and legislation in other countries on the question of workplace technologies?

SECTION 1
ON A EUROPEAN LEVEL

38.11

The European Court of Human Rights. The principle of protecting an employee's privacy at work has been confirmed several times by the European Court of Human Rights[95] : "Every person has the right to respect for his private and family life, his home and his correspondence" ECHR, Art. 8). Even if not always understood in the same way, one finds again here the spirit and the letter of the European Convention for the Protection of Human Rights and Fundamental Freedoms. The concern remains the same: the search for a compromise between an employer's power of monitoring employees' activities and the respect of their privacy. There are several texts formalising, on both a European and international level, the obligation to inform employees in advance.

38.12

Recommandation no. R (89). The 18 January 1989 recommendation no. R (89) of the Council of Europe's Committee of Ministers to Member States on the protection of personal data used for employment purposes states:

"3. Information and consultation of employees:

3.1. In accordance with domestic law or practice and, where appropriate, in accordance with relevant collective agreements, employers should, in advance, fully inform or consult their employees or the representatives of the latter about the introduction or adaptation of automated systems for the collection and use of personal data of employees. This principle also applies to the introduction or adaptation of technical devices designed to monitor the movements or productivity of employees.

3.2. The agreement of employees or their representatives should be sought before the introduction or adaptation of such systems or devices where the consultation procedure referred to in paragraph 3.1 reveals a possibility of infringement of employees' right to respect for privacy and human dignity unless domestic law or practice provides other appropriate safeguards.

---

[95] Not. ECHR, 16 Dec. 1992, conf. Niemietz v. Germany, req. no 00013710/88, A-251 B § 29, *JDI* 1993, p. 755, obs. E. Decaux and P. Tavernier; *D.* 1993, summ. 386, obs. J.-F. Renucci.

38.13
The ILO (International Labour Office) code of practice (dated 7 October 1996) on the protection of workers' personal data states that: Personal data collected in connection with technical or organisational measures to ensure the security and proper operation of automated information systems should not be used to control the behaviour of workers (item 5.4).

This Code does however foresee that electronic surveillance may be introduced under certain conditions: on the one hand, personal data collected by electronic monitoring should not be the only factors in evaluating worker performance, and on the other hand, in cases where monitoring does take place, workers should be informed in advance of the reasons for monitoring, the time schedule, the methods and techniques used and the data to be collected, and the employer must minimise the intrusion to the privacy of workers (Item 6 of the Code). It further states that continuous monitoring should be permitted only if required for health and safety reasons or the protection of company property. Furthermore, secret monitoring should be permitted only if it is in conformity with national legislation, or if there is "suspicion on reasonable grounds of criminal activity or other serious wrongdoing" (including sexual harassment).

38.14
29 May 2002 opinion of the G 29. It is also appropriate to refer here to the opinion issued the G 29 on 29 May 2002 (v. s[s] no. 15.18). Dedicated to the "monitoring of electronic communications" at work [96], this opinion seems to be greatly influenced by the work and discussions of the CNIL.

SECTION 2
OTHER NATIONS

38.21
United States of America. The delicate question of cyber-surveillance is not understood in the same way in the USA where the employer often sees himself with a right to gain knowledge of employees' e-mails. The most recent surveys[97] do indeed indicate that 46.5 % of companies look into and store the contents of employees' e-mails. Though the secrecy of correspondence is protected by the *Electronic Communications Privacy Act of 1986*[98] (18 USC §§ 2510 s.), an employer is allowed to monitor the company's ICT network, thereby giving him the right to completely legally listen in to his employees' telephone conversations or to read their e-mails, even though these dispensations are only allowed for business purposes and are subject to an employee having been informed beforehand of any such surveillance.

38.22
England. The public body responsible for the protection of personal data, the Information Commissioner, has issued the *Employment Practices Data Protection Code* [99]. This contains the conditions under which an employer may monitor his employees. Based on the provisions of the *Data Protection Act of 1998* (c. 29)[100] this code makes the surveillance of employees at work subject to two principles: transparency and proportionality. Also, an employer must not just forewarn his employees of surveillance measures to be introduced, but must also eliminate all personal information that are "irrelevant or excessive" to the employment relationship.

---

[96] G 29, opinion., 29 May 2002,
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_fr.pdf
[97] Survey conducted by the Policy Institute: http://www.epolicyinstitute.com/survey/survey.pdf.
[98] http://cpsr.org/issues/privacy/ecpa86/.
[99] *The Employment Practices Data Protection Code,*
http://www.informationcommissioner.gov.uk/eventual.aspx?id=437.
[100] http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1.