Texto traducido de « CYBERDROIT 2009/2010, le droit à l'épreuve de l'internet »
5e édition, DALLOZ
Dirección: Christiane Féral-Schuhl

3. La cibervigilancia en la empresa

Publicado con el apoyo financiero de la Comisión Europea

SECCIÓN 0

ÍNDICE

3.00

Índice del capítulo.

3.01

Textos vigentes

> Textos franceses.

C. trab., not. art. L. 1121-1, L. 1221-6, L. 2323-13, L. 2323-32 — C. pen., not. art. 226-15, 226-24 et 432-9 — L. n° 78-17, 6 ene. 1978, relativa a la informática y a las libertades — L. n° 2004-801, 6 ago. 2004, relativa a la protección de las personas físicas con respecto al tratamiento de datos personales y que modifica la ley n° 78-17 del 6 ene. 1978.

3.03

Bibliografía indicativa

> Informes y Guía

FDI, *Relations du travail et Internet,* inform.: panorama législatif et jurisprudentiel, 26 ene. 2006 — Cnil, H. Bouchet (dir.), *La cybersurveillance sur les lieux de travail,* marzo 2004 — Cnil, *Guide pratique pour les employeurs.*

> Libros

M.-P. Fenoll-Trousseau et 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-Malmay.son, 2001; *Droit du travail – Droit vivant,* 15ª edición., Éd. Liaisons, agosto 2006.

> Coloquio

Martes del ADIJ (C. Baudoin), « Droit du travail et nouvelles technologies: actualités législatives et jurisprudentielles », informe J.-B. Auroux, *RLDI* n° 14, marzo 2006, p. 83; informe L. Teyssandier, *Lexbase* N5659AKS

> Artículos

Número especial de la revista *Dr. social,* « Le droit du travail à l'épreuve des NTIC », enero 2002.

CAPÍTULO

31. Control de la herramienta de trabajo por parte del empleador

SECCIÓN 0
ÍNDICE

31.00

Índice del capítulo.

31.01

Textos vigentes.

> Textos franceses.

Ver s^{s} n^{o} 3.01.

Leer n^{o} 2004-575, 21 jun. de 2004, para la confianza en la economía digital — L. n^{o} 82-689, 4 ago. 1982, relativa a las libertades de los trabajadores en la empresa, *JO* 6 ago., 2518.

31.02

Jurisprudencia de referencia

> Sobre la obligación general de lealtad del trabajador

• **Soc. 16 jun. de 1998,** *D.* 1998, IR 77.

* Ver s^{s} n^{o} 31.21.

> Sobre el uso de contraseñas en los puestos de trabajo

• **Soc. 6 de febrero de 2001,** n^{o} 98-46.345, Sté Laboratoires pharmaceutiques Dentoria c/Mme Bardagiet et a., *Bull. civ.* V, n^{o} 43; *JCP G* 25 jul. 2001, n^{o} 30, p. 1514, nota C. Puigelier; *RTD civ.* oct.-dic. 2001, n^{o} 4, 880-882, nota J. Mestre et B. Fages — sentencia del TA **Toulouse, 4ª sala de lo social, 23 oct. 1998.**

• **Soc. 18 oct. 2006,** n^{o} 04-48.025, Jérémy L… c/Sté Techni-Soft, *Bull. civ.,* n^{o} 308; *CCE* ene. 2007, nota E. Caprioli, p. 40 s. — confirmación del TA **Rennes, sala de lo social, 21 oct. 2004.**

* Ver s^{s} n^{o} 31.24, también n^{os} 33.22 y 35.21.

> Sobre el uso abusivo de las herramientas de la empresa

• **Soc. 10 oct. 2007,** n^{o} 06-03.007, Claude G… c/Assoc. Ogec Emmanuel d'Alzon — confirmación del **TA Montpellier, sala de lo social, 17 may. 2006,** Claude G… c/Assoc. Ogec Emmanuel d'Alzon, http://www.legalis.net/jurisprudence-decision.php3?id_article=2066 (consulta sitios pornográficos).

• Por la sentencia (confirmada) dictada en primera instancia, v. **Consejo de Conciliación Montpellier, 26 sept. 2005,** Claude G… c/Assoc. Ogec Emmanuel d'Alzon.

* Ver s^{s} n^{o} 31.23, también n^{o} 32.24.

• **Soc. 14 mar. 2000,** n^{o} 1270, n^{o} 98-42.090, M. Dujardin c/Sté Instinet France *Bull. civ.* V, n^{o} 101; *Gaz. Pal.* 28 oct. 2000, n^{o} 302, p. 34, nota J. Berenguer-Guillon y L. Guignot; *JCP G* 7 feb. 2001, n^{o} 6, p. 325, nota C. Puigelier; *LPA* 11 jul. 2000, n^{o} 137, p. 5, nota G. PicTA y A. Sauret — confirmación del **TA París, sala 18ª, Sección A, 16 feb. 1998,** n^{o} 020563.

• Por la sentencia (parcialmente revocada) dictada en 1ª instancia, v. **Consejo de Conciliación París, sala 2^{e}, Sección Encadrement, 13 dic. 1995.**

* Ver s^{s} n^{o} 31.22, también n^{os} 32.11 et 30.23.

• **Soc. 11 mar. 1998,** n^{o} 96-40.147, NPB, *RJS* 4/1998, n^{o} 415 — confirmación del TA **París, sala 21^{e}, Sección C, 7 nov. 1995.**

* Ver s^{s} n^{o} 31.12, también. n^{o} 32.24 (uso abusivo del teléfono).

• **TA Aquisgrán, sala 1ª A, 25 nov. 2003,** n^{o} 2003/798.

* Ver s^{s} n^{o} 31.21.

> Sobre la responsabilidad del empleador

• **Asam. Plen. 19 may. 1988,** n° 87-82.654, Cie d'assurance « La Cité », *Bull. civ.,* n° 5; *RTD civ.* 1989, 89, obs. P. Jourdain — confirmación del TA **Lyon, 24 mar. 1987.**

* Ver s^s n° 31.32.

• **Civ. 2^e^, 19 jun. 2003,** n° 00-22.626, AGV Vie et a. c/ Cts X… et a., *Bull. civ*. II, n° 202; *D.* 2003, 1808 — sentencia del TA **Lyon, sala 6^e^civ., 18 oct. 2000.**

* Ver s^s n° 31.23.

• **TA Aquisgrán, sala 2^e^, 13 mar. 2006,** SA Lucena Technologies c/ SA Locos France, M. Nicolás B… — confirmación del **TGI Martille, 11 jun. 2003,** RG n° 01/390.

* Ver s^s n° 31.33.

31.03

Bibliografía indicativa

> Informes y Guía

FDI, *Relations du travail et Internet,* inform., 17 sept. 2002 — Cnil, H. Bouchet (dir.), *La cybersurveillance sur les lieux de travail,* mar. 2004 — Cnil, *Guide pratique pour les employeurs.*

> Artículos

J.-B. Auroux, « Les mardis de l'ADIJ: droit du travail et nouvelles technologies: actualités législative et jurisprudentielle », *RLDI* marzo 2006 n° 14, p. 83; v. también informe de 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 », *CCE* 2004, étude 15 — P. Bonneau, « Le contrôle des fichiers informatiques des salariés », *Décideurs: Stratégies, Finance & Droit* n° 68, 15 agosto-15 sept. 2005, p. 52 s. — G. Haas et O. de Tissot, « Des restrictions inacceptables à la liberté d'action des syndicats », *Expertises* abr. 2005, p. 145 — D. Lebeau-Marianna, « Alertes éthiques: quelles orientations suite aux décisions de la Cnil? », *RLDI* oct. 2005, n° 9, p. 35 s. — M. Mélin et D. Melison, « Salarié, employeur et données informatiques: brefs regards croisés sur une pièce à succès », *RLDI* ene. 2007, n° 23, p. 69 s. — A. Saint Martin, « Contrôle des messages électroniques du salarié et mesures d'instruction in futurum », *RLDI* junio 2007, n° 28; « Une présomption de professionnalité des messages électroniques du salarié ? », *RLDI* mayo 2007, n° 27 — Estudiantes de Master 2 de derecho multimedia e informática de la Universidad de París II dirigido por el profesor J. Huet, « Le blog: nouvelle arme des salariés », *RLDI* n° 27, mayo 2007, p. 90 s.

31.04

Pregunta principal

• ¿En qué condiciones el empleador puede enmarcar las condiciones de uso de acceso a Internet en el seno de la empresa?

* Ver s^s n° 31.12.

• ¿Qué responsabilidades tiene el trabajador con respecto al uso de Internet en su lugar de trabajo?

* Ver s^s n° 31.21.

• ¿El empleador puede ser considerado responsable de la difusión de contenidos ilícitos por parte de un trabajador?

* Ver s^s n° 31.32.

31.09

El acceso a Internet es una herramienta de trabajo. El acceso a Internet, y más concretamente a la mensajería, se ha convertido, al igual que el teléfono, en una herramienta de trabajo. En efecto, es cada vez más útil, incluso indispensable, para que la mayoría de los trabajadores realicen su trabajo.

Ahora bien, el empleador tiene sobre esta herramienta un poder de control técnico que le permite interceptar los mensajes de su trabajador, conocer a los destinatarios de dichos mensajes, el objeto del mensaje, la naturaleza y el contenido de los ficheros adjuntos, los sitios consultados, los foros en los que participa… Por ejemplo, puede saber si sus trabajadores utilizan Internet por razones profesionales o personales, cuánto tiempo pasan navegando en Internet, los horarios de navegación… Al igual que con los auto conmutadores[1] telefónicos, el archivado automático de las direcciones *e-mails* o de los sitios *web* es susceptible de permitir que se esboce un perfil del trabajador y, por ende, recabar informaciones sobre su vida privada (tendencia sindical, política, interés por la pornografía, el revisionismo, etc.). Estos medios permiten "vigilar" a los

[1] Ver también Cnil, *5^e^ Rapport d'activité,* p. 109 et *15^e^ Rapport d'activité,* p. 74, Doc. fr.

trabajadores, “seguirles la huella” a través de los datos emitidos o recibidos a través de Internet, prácticas éstas denunciadas por la Commission nationale de l’informatique et des libertés (Cnil) desde 2001, con motivo de la presentación de su informe[2] sobre la “cibervigilancia” de los trabajadores por parte de sus empleadores.

Y todo ésto plantea, inevitablemente, la cuestión de la protección de las libertades fundamentales del trabajador (precisamente a este respecto, la Cnil presentó una serie de recomendaciones sobre la « cibervigilancia en la empresa ») y la cuestión, no menos complicada si cabe, de los límites de los derechos del trabajador.

SECCIÓN 1
PODERES DE CONTROL DEL EMPLEADOR

31.11

Tolerancia del uso a título privado de la herramienta de trabajo. El acceso a Internet y a la mensajería, o a un teléfono son algunos de los medios puestos a disposición del trabajador para que pueda efectuar su trabajo. Aunque existe una cierta tolerancia para permitir su uso a título privado –como es el caso del teléfono-, todo es cuestión de proporción. ¿Qué decir si de una centena de e-mail intercambiados al día, el 75% fueran mensajes con temas privados? En efecto, ya se trate de mensajes personales intercambiados por e-mail o de la consulta a título personal de sitios Internet, el empleador padece la pérdida del tiempo de trabajo así como los gastos asociados sobre todo durante las horas de conexión. Un sondeo ha revelado que del 20 al 50% del tiempo que se pasa en Internet en la empresa es para temas de ocio.

31.12

Marco de las condiciones de uso de la herramienta de trabajo. Dentro de este contexto, parece pues legítimo que el empleador se asegure del carácter no abusivo del uso por parte de sus trabajadores de las herramientas de trabajo puestas a su disposición. Ahora bien, el empleador debe actuar de manera transparente y « proporcionada »[3]. Se trata de buscar, de acuerdo con los principios enunciados por la Cnil y las propuestas preconizadas por el Forum des droits sur l’Internet[4], el justo medio entre el poder de control del empleador y la protección de las libertades fundamentales de los trabajadores.

La Cnil, en su informe « *La Cybersurveillance sur les lieux de travail »,* modificado el 18 de diciembre de 2003, indicaba que « aunque una prohibición general y absoluta del uso de Internet a otros fines que los profesionales, por parte de los trabajadores, no parece realista en una sociedad de la información y de la comunicación, y parece, además, desproporcionada con respecto a los textos vigentes », « un uso razonable, no susceptible de reducir las condiciones de acceso profesional a la red sin cuestionar por ello la productividad es algo general y socialmente admitido por la mayoría de las empresas o administraciones ». Sin embargo, la Cnil estima que este uso tolerado de la herramienta informática y de la red Internet por un trabajador, a título privado, puede estar sometido a unas condiciones o límites establecidos por el empleador. Así, la Cnil preconiza la colocación de dispositivos del filtrado de sitios no autorizados, asociados a un cortafuego como la aplicación de un control a posteriori de los datos de conexión a Internet, restituido de manera global (por ejemplo a nivel del organismo o de un servicio del mismo), sin que haya que proceder por ello a un control individualizado de los sitios visitados por un trabajador determinado. Dicho de otra manera, el empleador da la pauta de las

---

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

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

[4] FDI, *Relations du travail et Internet,* informe del FDI, 17 sept. 2002, http://www.forumInternet.org/recommandations/lire.phtml?id=394.

condiciones de acceso a Internet y del uso de la mensajería con fines personales. Puede prohibir el acceso a sitios ilícitos (contenido pornográfico, pederasta, incitación al racismo, etc.) o incluso prohibir la descarga de programas, la conexión a foros o chats, el acceso a buzones personales invocando el riesgo de propagación de virus. Ahora bien, cuando el control lo realiza el empleador, detallado puesto por puesto, este dispositivo debe ser objeto de una declaración ante la Cnil.

SECCIÓN 2
OBLIGACIÓN DE LEALTAD DEL TRABAJADOR

31.21
Obligación general de lealtad. En un principio a favor de los trabajadores, los jueces recuerdan cada vez más a menudo que el empleador tiene derecho legítimo a esperar de un trabajador que ejecute su contrato de trabajo respetando la obligación general de lealtad[5].

Un decreto del Tribunal de Apelación de Aquisgrán del 25 de noviembre de 2003[6] subraya a este respecto que « todos los textos nacionales o internacionales destinados a proteger la vida privada sobre todo de los trabajadores en su lugar de trabajo no puede crear una zona de inmunidad o de impunidad por las faltas cometidas contra su propio empleador o de un tercero ».

31.22
Jugar en el lugar de trabajo. El Tribunal de Casación enuncia, en una decisión del 14 de marzo de 2000[7], que jugar en el lugar de trabajo es « ilegal »[8]. A este respecto, dio razón al empleador que había despedido por falta grave a su trabajador por haber jugado (sobre todo haciendo apuestas deportivas) con terceros durante su tiempo de trabajo y utilizando el material de la empresa.

31.23
Consultar sitios pornográficos. Del mismo modo, consultar sitios pornográficos por parte del trabajador en su lugar de trabajo y durante sus horas de trabajo es susceptible de provocar el despido de dicho trabajador, como ilustra una decisión del 10 de octubre de 2007[9] de la sala de lo social del TC (rechazo del recurso del TA Montpellier, 17 may. 2006).

31.24
Medidas de seguridad. La Cnil recuerda que « el ordenador puesto a disposición del trabajador puede estar protegido por una contraseña o log-in, pero esta medida de seguridad está destinada a evitar el uso malintencionado o abusivo de un tercero: no tiene por objeto transformar el ordenador de la empresa en un ordenador para uso privado ». A este título, el trabajador, único conocedor de la contraseña, debe, cuando el empleador se lo pide, restituir los elementos materiales y comunicar las informaciones que están en su posesión y que son necesarias para continuar la actividad de la empresa[10].

Del mismo modo, al tratarse del uso de los medios de criptología, el Tribunal de Casación ha considerado también que el trabajador que cripte voluntariamente el acceso a sus datos, en su puesto informático, sin autorización de su empleador, comete una falta grave[11].

---

[5] Soc. 16 jun. 1998, *D.* 1998, IR 77.
[6] TA Aquisgrán, sala 1ª 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, nota J. Berenguer-Guillon et L. Guignot; *JCP G* 7 feb. 2001, nº 6, p. 325, nota C. Puigelier; *LPA* 11 jul. 2000, nº 137, p. 5, nota G. PicTA et A. Sauret.
[8] F. Lemaître, « Jouer sur le lieu de travail est illégal, estiment les juges », *Le Monde* 28 mar. 2000.
[9] Soc. 10 oct. 2007, nº 06-43.816, desestimación del recurso TA Montpellier, 17 may. 2006, v. 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 jul. 2001, nº 30, p. 1514, nota C. Puigelier; *RTD civ.* oct.-dic. 2001, nº 4, p. 880-882, nota J. Mestre et B. Fages.
[11] Soc. 18 oct. 2006, *CCE* ene. 2007, nota E. Caprioli, p. 40 s.

SECCIÓN 3
RESPONSABILIDADES

31.31

Responsabilidad del trabajador en el ejercicio de su libertad de expresión. Sobre el terreno de la libertad de expresión, el trabajador tiene un derecho de expresión dentro y fuera de la empresa, tal y como nos lo recuerda la ley del 4 de agoto de 1982, la cual le reconoce « un derecho de expresión directa y colectiva sobre el contenido, las condiciones de ejercicio y la organización de su trabajo » (sobre los principios generales para que se respete la vida privada del trabajador Ver s^{s} n^{os} 34.00 s).

Sin embargo, la jurisprudencia recuerda que este principio tiene como corolario el de la responsabilidad de aquellos que lo utilizan. Si bien es exacto que la subordinación inherente al contrato de trabajo no tiene como consecuencia privar al trabajador de los derechos fundamentales ligados a su persona, y sobre todo a su libertad de opinión, de conciencia y de expresión, también es cierto que « la ejecución leal del contrato le impone una obligación de discreción tanto con respecto a terceros como con respecto a los demás trabajadores de la empresa »[12]. Del mismo modo, el trabajador que ejerce su derecho de expresión debe hacerlo sin que ello lleve a abusos como denigrar a las personas o hacer acusaciones calumniosas.

Esta última jurisprudencia permite circunscribir las condiciones de uso de los « espacios de desquite electrónicos»[13] que se están generalizando, ya sea en el marco de los foros creados a tal efecto por el empleador, ya sea en el marco de los sitios o foros creados por iniciativa de un trabajador o de un grupo de trabajadores.

Por otro lado, hay que precisar también que la regla de discreción también se impone a los representantes de los trabajadores (sobre los límites ligados a la libertad de comunicación sindical existentes v. s^{s} n^{o} 37.14).

31.32

Responsabilidad del empleador a causa de algunas derivas de los trabajadores. El artículo 1384 párrafo 5 del Código Civil enuncia un principio de responsabilidad civil del empleador en caso de falta cometida por uno de sus trabajadores que haya actuado en el marco de sus funciones. Es lo que se denomina la responsabilidad del comitente por los actos de sus trabajadores.

Esta vinculación de la falta del trabajador a sus funciones es considerada por la jurisprudencia en función de la conexión que haya entre la falta y la ejecución del contrato de trabajo. Esta conexión suele retenerse cuando la falta la comete el trabajador durante el tiempo de trabajo, en el lugar de trabajo, con los medios puestos a su disposición por el empleador, para seguir las instrucciones del empleador o incluso con la voluntad de actuar en nombre del empleador. La jurisprudencia retiene también la responsabilidad del empleador por aquellos actos cometidos por uno de sus trabajadores fuera del tiempo y del lugar de trabajo, con medios personales o no, encargados por el empleador cuando los actos son susceptibles de ser considerados como vinculados a las funciones. En efecto, si una jurisprudencia antigua rechazaba considerar responsable al empleador del daño provocado con un instrumento de trabajo cuando había sido ocasionado fuera del lugar y del tiempo de trabajo, la solución es ahora menos tajante y muchas sentencias vinculan a las funciones los daños provocados por el único uso de una cosa o de una herramienta de trabajo, como por ejemplo un blog o un foro.

El empleador no es, evidentemente, responsable cuando la falta del trabajador no puede relacionarse con sus funciones y no tiene relación alguna con las mismas. Si la falta es susceptible de ser relacionada con las funciones, el empleador puede liberarse de su responsabilidad si demuestra las tres

---

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

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

condiciones acumuladas definidas por el Tribunal de Casación[14]: el trabajador ha actuado al margen de sus funciones, sin autorización y con fines ajenos a sus atribuciones. A partir de estas tres condiciones mencionadas, el Tribunal de Apelación de Aquisgrán dictó una sentencia por la que sancionaba a un empleador por el mal uso de Internet por parte de uno de sus trabajadores. En este caso, el trabajador había tomado la iniciativa de difundir una página personal en la web criticando a una tercera empresa. Los jueces recordaron entonces que el empleador es quien debe "controlar el buen uso de una herramienta que pertenezca a la empresa por parte de los trabajadores". Consideraron que el trabajador (1) había actuado en el marco de sus funciones, pues había encontrado en sus funciones la ocasión y los medios, sobre todo informáticos, para cometer un acto ilícito, (ii) había actuado con la autorización del empleador, quien había declarado, en una nota interna, que toleraba el uso personal y lícito de Internet, (iii) no había actuado con fines ajenos a sus atribuciones porque el reglamento de orden interno le autorizaba a disponer de una acceso a Internet incluso fuera de sus horas de trabajo[15].

El Tribunal de Casación pronunció una sentencia tan severa como la anterior con respecto a un corredor de seguros que había cometido malversaciones con los medios informáticos durante su tiempo de trabajo y en su lugar de trabajo: « El trabajador había actuado durante su tiempo y en su lugar de trabajo en el marco de las funciones para las que estaba trabajador, con el material puesto a su disposición, lo que excluía que hubiera cometido las malversaciones al margen de sus funciones ».

Por último, el Tribunal de Apelación de París retuvo la culpa del empleador que había dejado a sus trabajadores conectarse sin control a distintos sitios (ficheros multimedia, juegos, sitios pornográficos, etc), sin relación alguna con su actividad profesional. En este caso, el empleador estaba en litigio con su prestatario de archivado de datos informáticos y de protección antivirus. Y mientras que los jueces de primera instancia retuvieron que « la presencia de virus en las instalaciones (del cliente) es la prueba de que [el proveedor] no ha ejecutado correctamente la acción antivirus », el Tribunal de Apelación consideró que el cliente « al dejar al personal conectarse a tales sitios hizo, por su culpa, ineficaz la protección que [el proveedor] se había comprometido a proporcionar de manera que no podía invocar el malfuncionamiento de la protección antivirus como único motivo para rescindir los contratos»[16].

Sin embargo, también se juzgó que el sólo hecho de tener un blog personal en línea no bastaba para justificar un atentado contra la reputación de su empleador (Consejo Conciliación, 30 marzo 2007, v. s^{s} n^{o} 125.28).

Estas jurisprudencias demuestran la utilidad de definir, en el reglamento de orden interno o en anexo al mismo, las condiciones en las que los trabajadores pueden utilizar los recursos informáticos y el acceso a Internet puesto a su disposición en el ejercicio de su profesión.

---

[14] Asamb. plenaria 19 may. 1988, n^{o} 87-82.654, *RTD civ.* 1989, 89, obs. P. Jourdain.

[15] TGI Mar.eille, sala 1ª civ., 11 jun. 2003, Escota c/Lucent Technologies, http://www.juriscom.net; confirmado por el TA Aquisgrán, 13 mar. 2006, recurso n^{o} 2006/170.

CAPÍTULO

32. Principio de transparencia

SECCIÓN 0
ÍNDICE

32.00

Índice del capítulo.

32.01

Textos vigentes.

> Textos franceses.

Ver s^{s} n^{o} 3.01.

32.02

Jurisprudencia de referencia.

> Sobre la obligación de información de los trabajadores

• Soc. 22 may. 1995, n° 93-44.078, *Bull. civ.* V, n^{o} 164; *ReVer soc. Francis Lefebvre* 1995, n^{o} 7, p. 489, nota Y. Chauvy — confirmación del **TA Douai, 30 junio 1993.**

* Ver s^{s} n^{o} 32.11, tamb. s^{s} n^{o} 30.23.

> Sobre la obligación de información y consulta del comité de empresa

• Soc. 7 jun. 2006, n^{o} 04-43.866, Girouard c/Continent France, *Bull. civ.* V, n^{o} 206; *D.* 2006, 1704 — confirmación del TA **sala Bourges. soc, 24 oct. 2003.**

* Ver s^{s} n^{o} 32.12 et tamb. n^{o} 30.24.

> Recusación de los medios de prueba por falta de información de los trabajadores

• Soc. 6 jun 2007, n^{o} 05-43.996, sté Eliophot c/M. X — confirmación del TA **Aquisgrán, sala 18^{a}, 7 jun 2005.**

• Soc. 2, 20 nov. 1991, n^{o} 88-43.120, *Bull. civ.* V, n^{o} 519; *D.* 13 feb. 1992, n^{o} 7, 73, nota Y. Chauvy — casación del **TA Colmar, sala de lo social, 17 dic. 1987.**

* Ver s^{s} n^{o} 32.11 y 32.22, tamb. n^{o} 30.23.

• TA París, 31 mayo 1995, *Juris-Data* n^{o} 024755; *RLDI* mayo 2007, n^{o} 27, coment. A. Saint Martin.

* Ver s^{s} n^{o} 32.23.

> Recusación de los medios de prueba por incumplimiento de las reglas Cnil.

• TA París, 7 mar. 1997, *Gaz. Pal.* 21 ene. 1999.

V. tamb. **TA París, 31 may. 1995** (prec.).

* Ver s^{s} n^{o} 32.23.

>Admisión a título de prueba del desglose de las llamadas telefónicas.

• Soc. 29 ene. 2008, n^{o} 06-45.279, Touati c/sté Canon France, *JS Lamy* 2008, n^{o} 228, coment. J.-E. Tourreil; *Gaz. Pal.* 24 abr. 2008, n^{o} 115, p. 39, nota L. Boncourt — confirmación del TA **Versailles, sala 11^{e}, 5 sept. 2006.**

* Ver s^{s} n^{o} 32.23.

>Admisión de la prueba

• Soc. 11 mar. 1998, n^{o} 96-40.147, Pisani c/sté Pisani, *Sem. soc. Lamy* 28 mayo 2001, n^{o} 1030 — confirmación del TA **París, sala 21^{e}, 7 nov. 1995.**

* Ver s^{s} n^{o} 32.24.

• TA Montpellier, 17 mayo 2006, n^{o} 05/01954, Claude G… c/Assoc. Ogec Emmanuel d'Alzon, http://www.legalis.net/jurisprudence-decision.php3?id_article=2066 — confirmación del **Soc. 10 oct. 2007,** n^{o} 06-03.007, Claude G… c/Assoc. Ogec Emmanuel d'Alzon.

• Por la sentencia (confirmada) pronunciada en primera instancia, v. **Consejo de Conciliación Montpellier, 26 sept. 2005,** Claude G… c/Assoc. Ogec Emmanuel d'Alzon.

* Ver s^{s} n^{o} 32.24, tamb. n^{o} 31.23.

• V también **Soc. 10 oct. 2007,** Claude G… c/Assoc. Ogec Emmanuel d'Alzon (prec.)

* Ver s^{s} n^{o} 32.24.

• TA Aquisgrán, sala 18^{a}, 4 ene. 1994, Perez c/Beli Intermarchés, *Dr. soc.* 1995, 332; S. Darmay.sin, « L'ordinateur, l'employeur et le salarié », *Dr. soc.* 2000, p. 580; *Juris-Data* n^{o} 041281 — anulación del **Cons. Concil. Niza, Sección coment., 10 dic. 1990**.

* Ver s^{s} n^{o} 32.25.

• Soc. 14 mar. 2000, n^{o} 1270, n° 98-42.090, *Bull. civ.* V, n^{o} 101; *Gaz. Pal.* 28 oct. 2000, n^{o} 302, p. 34, nota de J. Berenguer-Guillon y L. Guignot; *JCP G* 7 feb. 2001, n^{o} 6, p. 325, nota C. Puigelier — confirmación del el **TA París, sala 18^{a}, Sección A, 16 feb. 1998,** n^{o} 020563.

Por la sentencia (impugnada

parcialmente) pronunciada en primera instancia, v. **Consejo de Conciliación París, sala 2e, Sección Encadrement, 13 dic. 1995**.

* Ver ss nos 32.11 et 32.24, tamb. ss nos 30.23 y 31.22.

> Sobre el valor jurídico de las cartas

• Soc. 21 dic. 2006, no 05-41.165, J.-H. Pettre c/sté Ad 2 One SA — confirmación del TA **Versailles, sala 5ª, Sección B, 25 nov. 2004.**

* Ver ss no 32.15.

> Sobre la admisión de los medios de prueba en materia penal

• Crim. 6 abr. 1994, no 93-82.717, *Bull. crim.,* no 136 — confirmación del TA **Burdeos, sala 3e ,13 may. 1993.**

• Crim. 23 jul. 1992, no 92-82.721, *Bull. crim.,* no 274 — confirmación del TA **Caen, sala acc., 8 abr. 1992.**

• Crim. 31 may. 2005, no 04-85.469 — confirmación del TA **Montpellier, sala corr., 6 may. 2004.**

* Ver ss no 32.26, tamb. nos 30.26 et 30.23.

32.04

Preguntas principales

• ¿Cuáles son las condiciones para que sean lícitos de la recogida y el tratamiento de los datos personales?

* Ver ss nos 32.11 y 32.12.

• ¿Cuáles son las consecuencias jurídicas si no se cumplen las obligaciones de informar a los trabajadores?

* Ver ss no 32.22.

SECCIÓN 1
OBLIGACIÓN DE INFORMACIÓN

32.11

Obligación de informar de los trabajadores. El Código de Trabajo prevé expresamente que « ninguna información que se refiera personalmente a un trabajador (o a un candidato a un empleo) podrá ser recogida por un dispositivo que no haya sido previamente presentado al trabajador (o candidato a un empleo) » (Cód. trab., art. L. 1221-9 [anct art. L. 121-8]). La Commission nationale de l'informatique et des libertés (Cnil) recuerda también que los trabajadores afectados deben ser siempre individualmente informados de la aplicación de los dispositivos de control, de las modalidades de su derecho de acceso a los datos y de la finalidad de las medidas de control.

Esta regla ha sido recordada en varias ocasiones por el Tribunal de Casación: « Si el empleador tiene derecho a controlar y vigilar la actividad de su personal durante el tiempo de trabajo, no podrá utilizar un dispositivo de control que no haya sido previamente presentado a los trabajadores.[17] » O incluso: « El empleador tiene derecho a controlar y vigilar la actividad de sus trabajadores durante el tiempo de trabajo, quedando sin embargo excluido el uso de procedimientos clandestinos de vigilancia [18] ».

Constatamos pues que no es tanto el uso de dispositivos para controlar y vigilar a los trabajadores como el hecho de hacerlo a escondidas lo que se condena. Es pues prudente organizar, en el marco de un reglamento de orden interno o de un código de conducta o incluso de una « carta », las condiciones de uso del acceso a Internet, sobre todo de la mensajería, y de hacer referencia a ello en los contratos de trabajo. Estas condiciones de uso pueden ser de hecho recordadas cuando se atribuya un código de acceso o en algunas páginas pantalla o incluso en la difusión de notas de servicio. La Cnil « apoya la iniciativa cuando estas « cartas » o « guías del buen uso » tienen por objeto garantizar una información perfecta a los usuarios, sensibilizar a los trabajadores o a los agentes públicos sobre las exigencias de seguridad, llamar su atención sobre ciertos

---

[17] Soc. 20 nov. 1991, no 88-43.120, *Bull. civ.* V, no 519; *D.* 13 feb. 1992, no 7, 73, nota Y. Chauvy: tratándose de una cámara disimulada — Soc. 22 may. 1995, no 93-44.078, *Bull. civ.* V, no 164; *ReVer soc. Francis Lefebvre* 1995, no 7, p. 489, nota Y. Chauvy: tratándose del seguimiento de pistas de un trabajador por un detective privado.

[18] Soc. 14 mar. 2000, no 1270, no 98-42.090, *Bull. civ.* V, no 101: a propósito de un sistema de escuchas telefónicas.

comportamientos de naturaleza a causar perjuicio al interés colectivo de la empresa o de la administración»[19].

32.12

Obligación de información y consulta del comité de empresa. Cuando existe un comité de empresa, el empleador también está obligado a informarle antes de utilizar « tratamientos automatizados de la gestión del personal y de cualquier modificación de los mismos » (Cód. trab., art. L. 2323-32; anc. L. 432-2-1)[20]. También debe consultarle previamente sobre cualquier proyecto que implique la introducción de « nuevas tecnologías, cuando estas son susceptibles de tener consecuencias en el empleo, la calificación, la remuneración, la formación o las condiciones de trabajo del personal » (Cód. trab., art. L. 2323-13; anc. L. 432-2, al. 1). Por último, debe informarle y consultarle « previamente a la decisión de utilización en la empresa, sobre los medios controlar la actividad de los trabajadores » (Cód. trab., art. L. 2323-32). La información que debe proporcionarse al comité de empresa debe ser precisa y por escrito (Cód. trab., art. L. 2323-4; anc. L. 431-5, al. 2). Ahora bien, la opinión expresada por el comité de empresa es puramente consultiva y no vincula al empleador.

La conexión a Internet, la creación de una red Intranet, el uso de una mensajería electrónica constituyen evidentemente « una nueva tecnología y una técnica que permiten controlar la actividad de los trabajadores » en el sentido de lo que precede. En general, hay que saber que el empleador debe informar y consultar al comité de empresa (Cód. trab., art. L. 1221-9; anc. L.121-8) o, en la función pública, al comité paritario o a cualquier otra instancia equivalente, previamente a el uso de un sistema de tratamiento o de procedimiento que permita « seguir las huellas » a los trabajadores en sus actividades, por ejemplo, que permitan acceder al puesto de un trabajador ausente.

El informe de declaración ante la Cnil debe de hecho incluir la indicación y la fecha en la que se consultó a las instancias representativas del personal.

El Tribunal de Casación tuvo la oportunidad de sancionar la falta de consulta del comité de empresa en aplicación del L. 432-2-1 (después art. L. 2323-32) del Código de trabajo, pues no podía contestarse seriamente que los trabajadores ignoraban la presencia de cámaras puesto que éstas se utilizaban desde hacía tiempo y había paneles que mencionaban su presencia[21].

32.13

Cartas « Internet » y Código de trabajo. El empleador puede pedir a sus trabajadores que firmen un documento que fije las condiciones de uso de las herramientas informáticas en la empresa. Dicho documento puede adjuntarse al contrato de trabajo.

Si este texto prevé recursos, prohibiciones o sanciones disciplinarias constituye un añadido al reglamento de orden interno. En esta hipótesis, este texto es objeto de unas condiciones de publicación y de información más consecuentes: en efecto, debe ser objeto de una información y consulta del comité de empresa, de una comunicación a la inspección de trabajo, de un depósito ante el Consejo de Conciliación y de un anuncio. Este documento permite establecer las reglas internas de deontología y de seguridad relativas al uso de la informatica y de las redes. La redacción de un código de conducta así comporta varias ventajas: permite prevenir al empleador de los posibles litigios que le oponen a sus trabajadores, cumple también la obligación de información en cuanto a los sistemas de control que los trabajadores utilizan en la empresa, tanto con respecto a los trabajadores como con respecto a las instancias representativas del personal.

32.14

Cartas « Internet » y Cnil. Según la Cnil, el documento adoptado « debe precisar el potencial técnico de las herramientas y el uso previsto efectivamente, sobre todo en materia de uso de las huellas ». Más concretamente, deben estar

---

[19] H. Bouchet (dir.), *La cybersurveillance sur les lieux de travail,* rapp. Cnil, mar. 2004, http://www.CNIL.fr/index.php?id=1432.

[20] Pour la fonction publique, l'employeur est tenu de consulter le comité technique ou tout autre organisme équivalent du comité d'entreprise: v. L. nº 84-16, 11 ene. 1984; L. nº 84-53, 26 ene. 1984 et L. nº 86-33, 9 ene. 1986.

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

mencionadas en esta carta las modalidades del control creado, los sistemas de archivado utilizados por el empleador así como la duración de los archivos.

En su informe de estudio y consulta pública sobre *La cybersurveillance des employés dans l'entreprise,* publicado en marzo de 2001, así como en su informe, titulado *La cybersurveillance sur les lieux de travail,* modificado el 18 de diciembre de 2003, la Commission nationale de l'informatique et des libertés (Cnil) avisa contra las derivas y los abusos con los que se ha topado siempre la redacción de Cartas de uso del material informático. El desequilibrio entre el empleador y los trabajadores, en el momento en el que se firma un documento así suele ser, según la comisió, evidente. Apoya sin embargo la iniciativa de creación de tales cartas cuando éstas tengan por objeto « garantizar una perfecta información de los usuarios, sensibilizar [a los trabajadores] sobre las exigencias de seguridad, llamar su atención sobre ciertos comportamientos de naturaleza a perjudicar el interés colectivo de la empresa ».

32.15

« Cartas» y estatuto jurídico. Una sentencia, pronunciada por la Sala de lo social del Tribunal de Casación, reconoce a las cartas informáticas un valor jurídico y las considera, junto con el reglamento de orden interno, como documento oponible a los trabajadores. En este caso concreto, el comportamiento de un trabajador que había intentado, sin motivo legítimo y tomando prestada al contraseña de otro trabajador, conectarse al puesto informático del director de la empresa, fue considerado contrario a la obligación del respeto de la carta informática vigente en la empresa. Un comportamiento así constituiría una falta grave e impediría que se quedara en la empresa durante el periodo de notificación previa de despido[22].

SECCIÓN 2
CONSECUENCIAS EN CASO DE FALTA DE TRANSPARENCIA

32.21

Intromisión en la vida privada. El Código de trabajo precisa que la recogida y tratamiento de datos personales a espaldas de los trabajadores puede comprometer al empleador por incumplimiento a su obligación general de transparencia. Del mismo modo, a falta de haber informado al comité de empresa (o en la función pública, al comité técnico paritario o cualquier otra instancia equivalente) y los trabajadores en las condiciones indicadas más arriba, un sistema de control de la mensajería del trabajador o incluso un dispositivo de trazabilidad para identificar los sitios web que haya consultado podría ser considerado como intromisión en la vida privada de éste. Del mismo modo, la instalación de un dispositivo a espaldas de los trabajadores de manera deliberadamente no visible (cámaras, por ejemplo) o destinado a vigilar las ideas y venidas de los trabajadores será considerado como intromisión en la vida privada de los trabajadores.

La jurisprudencia ha dibujado los contornos jurídicos de la aplicación de dispositivos de vigilancia de los trabajadores, sobre todo basándose en la admisión o la recusación de los medios de prueba basados en sistemas de cibervigilancia.

32.22

Recusación de los medios de prueba por falta de información de los trabajadores. El empleador no puede recurrir a unos medios de prueba obtenidos con la ayuda de procedimientos de control que no hayan sido previamente dados a conocer a los trabajadores. Tales pruebas serían rechazadas en los debates judiciales y las posibles sanciones tomadas contra los trabajadores, basadas en estas pruebas, podrían anularse.

El Tribunal de Casación precisó ya en 1991 que « si el empleador tiene derecho a controlar y a vigilar la actividad de los trabajadores durante el tiempo de trabajo, cualquier grabación, sean cuales sean los motivos, de imágenes o de

---

[22] Soc. 21 dic. 2006 nº 05-41.165, NPB, J.-H. Pettre c/sté Ad 2 One SA: desestimación del recurso contre TA Versailles, sala 5ª B, 25 nov. 2004; *Gaz. Pal.*, 07 ago. 2007, nº 219, p. 22.

palabras a sus espaldas, constituye un modo de prueba ilícito»[23]. En este caso concreto, se trataba del despido de una trabajadora de una tienda por falta grave basado en una grabación obtenida por medio de una cámara disimulada en la caja de la interesada.

Recientemente, una sentencia del Tribunal de Casación, con fecha del 6 de junio de 2007, aprobó una sentencia del Tribunal de Apelación que, al relevar el carácter privado del correo electrónico enviado por el trabajador a uno de sus compañeros de trabajo, dedujo que este elemento de la vida personal del interesado no podría ser considerado un motivo de despido[24].

32.23

Recusación de los medios de prueba por incumplimiento de las reglas Cnil. Los jueces recusaron la prueba presentada por un tratamiento de informaciones nominales, debidamente declarada a la Cnil, al considerar que la información en cuestión no tenía relación con la finalidad del tratamiento[25]. En efecto, a modo de ejemplo, no puede utilizarse, a espaldas del personal, un sistema informático de reserva de billetes, puesto a disposición de los trabajadores, para controlar el tiempo de trabajo de los trabajadores.

Del mismo modo, la sentencia del 7 de marzo de 1997 del Tribunal de Apelación de París consideró que la presentación ante la justicia del desglose de las comunicaciones telefónicas procedente de un puesto de un trabajo y obtenido por medio de un auto conmutador era ilícito considerando que "en todo caso, la obligación de declaración previa, artículo 6 de la ley del 6 de enero de 1978, no había sido cumplida y que dicho desglose sólo podía conservarse para la facturación eventual a la trabajadora de sus comunicaciones personales »[26].

Ahora bien, conviene señalar que esta sentencia del Tribunal de Casación del 29 de enero de 2008 aceptó que los desgloses de las llamadas telefónicas presentados por el empleador podrían justificar el despido de trabajador por uso abusivo de su teléfono profesional[27]. Estos desgloses establecían que el trabajador había llamado, desde su puesto de trabajo, a mensajerías de encuentros entre adultos, por un total de 63 horas entre julio de 2002 y enero de 2003. El trabajador intentó en vano prevalecerse de la inadmisibilidad de la prueba presentada, argumentando que no había sido informado del procedimiento del control. Pero la alta jurisdicción consideró que la simple consulta de los desgloses, de la duración, del coste y del número de llamadas telefónicas efectuadas a partir de cada puesto, editados por medio de un auto conmutador telefónico de la empresa, no constituía un procedimiento de vigilancia ilícita por no haber sido previamente dado a conocer al trabajador. Ahora bien, hay que decir que el tema de la conformidad de la ley informática y las libertades de recogida de datos personales de los trabajadores a través de degloses telefónicos no se planteó en este caso específico.

32.24

Admisión de los medios de prueba. Los jueces consideraron que el empleador podía prevalecerse de la grabación de las conversaciones telefónicas de su trabajador para demostrar que éste había estado, durante el tiempo de trabajo, jugando a juegos de azar con terceros (apuestas sobre las elecciones presidenciales, resultados de los partidos de fútbol) pues éste había sido avisado que se le estaba grabando[28].

---

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

[24] Soc. 6 jun. 2007, nº 05-43.996, NPB, sté Eliophot c/M. X…: desestimación del recurso contre TA Aquisgrán, sala 18ª, 7 jun. 2005.

[25] TA París, 31 may. 1995, *Juris-Data* nº 024755; *RLDI* may. 2007, nº 27, coment. A. Saint Martin.

[26] TA París, 7 mar. 1997, *Gaz. Pal.* 21 ene. 1999, p. 30.

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

[28] F. Lemaître, dans « Jouer sur le lieu de travail est illégal, estiment les juges », *Le Monde* 28 mar. 2000.

Confirmaron que « el empleador tiene derecho a controlar y vigilar la actividad de sus trabajadores durante el tiempo de trabajo; que sólo el uso de procedimientos clandestinos de vigilancia es ilícito » [29]. En este caso concreto, hay que decir que se trataba de una empresa de bolsa cuya reglamentación profesional autoriza la grabación de las órdenes de compra hechas por teléfono.

Del mismo modo, una sentencia del 11 de marzo de 1998 pronunciada por la sala de lo social del Tribunal de Casación admitió que « no constituía un modo de prueba ilícita la presentación por el empleador de los desgloses de facturación telefónica que le fueron enviados por la sociedad France Telecom para abonar las comunicaciones correspondientes al puesto del trabajador »[30]. O incluso, recientemente, una sentencia del Tribunal de Apelación de Montpellier del 17 de mayo de 2006 admitió que los hechos revelados con motivo de la intervención de la empresa gestora del sistema informático del establecimiento llamada por la presencia de un virus informático en su puesto de trabajo, habían sido lícitamente dados a conocer al empleador[31]. Los jueces estimaron que el despido por falta grave estaba justificado, considerando que el trabajador, al consultar en varias ocasiones sitios pornográficos, había incurrido en falta con respecto a sus obligaciones de profesor y de educador « de conservar la dignidad inherente a su función y respetar el carácter mismo del centro », que figuran en el convenio colectivo de los profesores de enseñanza secundaria de la enseñanza privada. La sala de lo social del Tribunal de Casación, en su sentencia del 10 de octubre de 2007, confirmó este análisis[32].

32.25

En todo caso, los jueces exigen pruebas de buena calidad. Así, una sentencia del 4 de enero de 1994 del Tribunal de Apelación de Aquisgrán precisó que el documento de prueba presentado debía contener « garantías suficientes de autenticidad, de imparcialidad y de sinceridad en cuanto tanto a su fecha como a su contenido»[33].

(Explicaciones más completas sobre la dificultad de establecer la prueba, Ver s[s] n[os] 141.31.)

32.26

En materia penal. El Tribunal de Casación también recordó que « ninguna disposición legal permitirá a los jueces represivos desechar los medios de prueba presentados por las partes por la única razón de que hayan sido obtenidos de manera ilícita o desleal […] sólo tienen que […] apreciar su valor probatorio»[34]. O incluso que « ningún texto de procedimiento penal prohíbe la presentación por el demandante para apoyar su denuncia, de piezas de naturaleza a constituir cargas contra las personas contempladas en ella […], corresponde a las jurisdicciones penales apreciar su valor con respecto a las reglas relativas a la presentación de la prueba de las infracciones»[35].

Así, a título de ejemplo, se puede citar el caso de la grabación de la actividad de una farmacia por una cámara instalada en un lugar abierto al público a la demanda del farmacéutico que permitió demostrar el abuso de confianza en su detrimento cometido por un trabajador. O incluso el caso de un trabajador perseguido por robo en reunión basado en una grabación del sistema de vídeo

---

[29] Soc. 14 mar. 2000, n° 1270, n° 98-42.090, *Bull. civ.* V, n° 101; *Gaz. Pal.* 28 oct. 2000, n° 302, p. 34, nota J. Berenguer-Guillon et L. Guignot; *JCP G* 2001, n° 6, p. 325, nota C. Puigelier.

[30] Soc. 11 mar. 1998, n° 96-40147 Pisani c/sté Pisani, *Sem. soc. Lamy* 28 may. 2001, n° 1030, v. http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechExpJuriJudi&idTexte=JURITEXT000007373394.

[31] TA Montpellier, 17 may. 2006, n° 05/01954, Claude G… c/Assoc. Ogec Emmanuel d'Alzon, v. http://www.legalis.net/jurisprudence-decision.php3?id_article=2066

[32] Soc. 10 oct. 2007, n° 06-03.007; desestimación del recurso TA Montpellier, 17 may. 2006, v. http://www.legalis.net/jurisprudence-decision.php3?id_article=2065.

[33] TA Aquisgrán, 4 ene. 1994, *Dr. soc.* 1995, 332.; S. Darmay.sin, « L'ordinateur, l'employeur et le salarié », *Dr. soc.* 2000, p. 580.

[34] Crim. 6 abr. 1994, n° 93-82.717, *Bull. crim.,* n° 136.

[35] Crim. 23 jul. 1992, n° 92-82.721, *Bull. crim.,* n° 274.

vigilancia que mostraba a dos personas cogiendo distintos objetos y haciéndolos pasar por la ventana de los servicios y metiéndolos en un vehículo situado cerca de la ventana[36].

Ahora bien, hay que decir que el Tribunal de Casación confirmó en al menos dos ocasiones que no se podría recurrir a la provocación policial para demostrar de infracción (Crim. 7 feb. 2007[37] — Crim. 4 jun 2008[38] — (explicaciones Ver s^{s} n^{o} 143.12).

[36] Crim. 31 may. 2005, n^{o} 04-85.469.

[37] Crim. 7 feb. 2007, n^{o} 06-87.753, *Bull. crim.,* n^{o} 37; casación TA París, 26 sept. 2006 (renvoi devant TA Versailles); ver también « Une procédure fondée sur une provocation à commettre une infraction, même commise à l'étranger, doit être annulée », *AJ pénal* 2007, n^{o} 5, may., juri. p. 233.

[38] Crim. 4 jun. 2008, n^{o} 08-81.045; , P; *JCP G* 2008, IV, 2287; http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000018946415.

CAPÍTULO

33. Principio de proporcionalidad

SECCIÓN 0
ÍNDICE

33.00

Índice del capítulo.

33.01

Textos vigentes

> Textos franceses

Textos legislativos

Ver s^{s} n^{o} 3.01.

Dictámenes y recomendaciones

Cnil, doc. de orientación adoptado por la Comisión el 10 nov. 2005 sobre el uso de dispositivos de alerta profesionales de acuerdo con la ley del 6 de enero de 1978 /modifcada en agosto de 2004) – Cnil, resol. n^{o} 2005-305, 8 dic. 2005, sobre la autorización única de tratamiento de datos personales creado en el marco de los dispositivos de alerta profesional — Cnil, resol. n^{o} 2006-067, 16 mar. 2006, sobre la adopción de una norma simplificada en cuanto a los tratamientos automatizados de datos personales usados por los organismos públicos o privados destinados a geolocalizar los vehículos utilizados por sus trabajadores (norma simplificada nº 51), *JO* n^{o} 1003, 3 mayo — Informe presentado al ministro de Empleo, Trabajo e Inserción profesional de los jóvenes, 7 mar. 2007, *Charte d'éthique, alerte professionnelle et droit du travail français: état des lieux et perspectives,* en http://lesinformes.ladocumentationfrancaise.fr/BRP/074000335/0000.pdf l

33.02

Jurisprudencia de referencia

> Principio de prohibición de las escuchas telefónicas en el lugar de trabajo.

• **Soc. 7 nov.1995,** n^{o} 92-44.498, NPB, Sté polyclinique Volney c/M. Burdeos — confirmación del TA **Rennes, sala 5ª, 29 sept. 1992**.

• **Soc. 3 feb. 1999,** n^{o} 97-40.495, NPB, Sté Locamion c/Belgacem ben Mariem — confirmación del TA **Lyon, sala de lo social coll. B, 5 dic. 1996**.

• **Soc. 30 mar. 1999,** n^{o} 97-40.850, NPB — confirmación del TA **Lyon, sala de lo social coll. B, 8 nov. 1996**.

• **Soc. 18 nov. 1998,** n^{o} 96-43.902, Sté Cegeor, SARL c/Mme I. NPB — confirmación del TA **Lyon, sala de lo social, 5 jun. 1996**.

* Ver s^{s} n^{o} 33.13.

> Sobre el principio de inviolabilidad de la correspondencia.

• **TGI París, sala 12ª, 1 jun.007,** Oddo et Cie c/Trinh Nghia T… et Trung T…, http://www.legalis.net/breves-article.php3?id_article=2178.

* Ver s^{s} n^{o} 33.20.

> Sobre la consulta de la mensajería y de los ficheros creados por el trabajador

• **Soc. 2 oct. 2001, sentencia Nikon,** n^{o} 99-42.942, *Bull. civ.* V, n^{o} 291; *D.* 8 nov. 2001, n^{o} 39, jur., coment. 3148-3153; *Sem. soc. Lamy* 15 oct. 2001, n^{o} 1046; *JCP E y A* 29 nov. 2001, n^{o} 48, p. 1918-1922, nota C. Puigelier; *JCP G* n^{o} 2, 9 ene. 2002, doctr., I, 102, p. 63-69, nota M. Bourrié-Quenillet y F. Rodhain; *RTD civ.* ene.-mar. 2002, n^{o} 1, 72-73, nota J. Hauser; *RJPF* ene. 2002, n^{o} 1, p. 10-11, nota B. Bossu; *RJS* n^{o} 12/01, dic. 2001, cronolog. p. 940-946, nota F. Favennec-Hery; *Gaz. Pal.* 16 may. 2002, n^{o} 136, p. 47, nota H. Vray; *LPA* 10 dic. 2001, n^{o} 245, p. 6, nota G. PicTA — sentencia del TA **París, sala 18ª, Sección A, 22 sept. 1999**.

* Ver s^{s} n^{o} 33.21.

• **Soc. 18 oct. 2006,** n^{o} 04-48.025, NPB,

Jérémy L. F… c/Techni-Soft: *Bull. civ.* V, 18 oct. 2006 coment. Ray J.-E., L'envers de l'arrêt Nikon, *Sem. soc. Lamy* 2006, n° 1280, p. 10; P. Alix, « L'accès par l'employeur aux fichiers personnels stockés sur l'ordinateur du salarié », *JSL* n° 189-1, p. 4; J.-E. Tourreil, « Les documents détenus par un salarié dans l'entreprise sont présumés avoir un caractère professionnel », *JSL* n° 200, p. 15 v. http://www.legalis.net/jurisprudence-decision.php3?id_article=1774; *LPA* 28 abr. 2008, n° 85, p. 7, nota X. Daverat et S. Tournaux — confirmación del TA **Rennes, sala de lo social, 21 oct. 2004,** *Gaz. Pal.* 18 ene. 2007, n° 18, p. 37, nota S. Hadjali et C. Fagot; *LPA* 28 abr. 2008, n° 85, p. 7, nota X. Daverat.

• TA Toulouse, 4ª sala de lo social, 6 feb. 2003, caso n° 02-02519.

* Ver s^s n° 33.22, 33.21 et tamb. n° 31.24.

• Soc. 17 may. 2005, n° 03-40.017, NPB, Philippe K… c/Sté Cathnet-Science, *Juris-Data* n° 028449; *CCE* jul.-ago. 2005, p. 34 s., coment. A. Lepage; *Gaz. Pal.* 20 oct. 2005, n° 293, p. 36, nota S. Hadjali; *LPA* 23 abr. 2007, n° 81, p. 6, nota S. Tournaux — sentencia del TA **París, sala 22ª, Sección A, 6 nov. 2002**.

• TA Besançon, sala de lo social, 21 sept. 2004, RG n° 2003-1807, SNC General Electric Energy Products France c/Girardot et a., *RJS* 4/2005, n° 342.

• Soc. 23 may. 2007, n° 05-17.818, Datacep c/Hansart, NPB, *Bull. civ.* V; *D.* 2007, AJ 1590, nota A. Fabre; *Gaz. Pal.* 18 mar. 2008, n° 78, p. 20; *LPA* 28 abr. 2008, n° 85, p. 7, nota X. Daverat et S. Tournaux — sentencia del TA **Douai, sala 1ª Sección 2, 18 may. 2005**.

* Ver s^s n° 33.23.

• TA Versailles, 2 abr. 2003, caso n° 02-00293 y **TA Besançon, sala de lo social, 21 sept. 2004,** RG n° 2003-1807**,** SNC General Electric Energy Products France c/Girardot a., *RJS* 4/05, n° 342.

* Ver s^s n° 33.21.

> Sobre el carácter « justificado y proporcional » de un dispositivo de control.

• Soc. 26 nov. 2002, n° 00-42.401, Montaigu Meret c/ Wieth Lederle, NPB, *Bull. civ.* V, n° 352; *RTD civ.* 2003, 58; *Gaz. Pal.* 1 feb. 2003, n° 32, p. 23, nota C.-E. Brault: au sujet de la géolocalisation — sentencia del TA **Nancy, sala de lo social, 23 feb. 2000**.

* Ver s^s n° 33.31.

• TGI París, 19 abr. 2005, *CCE* oct. 2005, coment. 164, p. 46.

* Ver s^s n° 33.11.

• TGI París, sala 1ª 19 abr. 2005, CE Effia Services, Synd. Sud Rail c/Effia Services, *CCE* oct. 2005, p. 46 s, http://www.legalis.net/breves-article.php3?id_article=1434.

* Ver s^s n° 33.11

> Sobre el carácter presumiblemente privado o profesional de un mensaje o de un fichero.

• Soc. 18 oct. 2006, n° 04-48.025, NPB, Jérémy L. F… c/Techni-Soft (prec.) — confirmación de **TA Rennes, sala de lo social, 21 oct. 2004** (prec.).

• TA Burdeos, sala de lo social, Sección A, 8 feb. 2005, n° 04/02449.

* Ver s^s n° 33.22.

> Sobre los dispositivos de alerta profesional

• TGI Libourne, ord. ref., 15 sept. 2005, RG n° 05/00143, Comité de establecimiento BSN Glasspack, Synd. CGT del personal de BSN Glasspack c/SAS BSN-Glasspack, v. cronolog. F. Naftalski, *Lamy Dr. informatique et réseaux* 2005: retrait.

• TGI Nanterre, ord. ref., 27 dic. 2006: suspensión del dispositivo

• *CONTRA:* por el mantenimiento del dispositivo, **TGI Lyon, sala urg. , 19 sept. 2006**, Union départementale CGT du Rhône, sindic. CGT Bayer Cropscience c/Bayer Cropscience.

• TGI Nanterre, ord. ref., 1 abr. 2005, CE ING Bank c/ING Bank France.

* Ver s^s n° 33.32.

33.03

Bibliografía indicativa.

> Guías.

Cnil, *Guide pratique pour les employeurs* — Comunicación de la Cnil relativa al uso de dispositivos de reconocimiento por huella digital con almacenamiento en un banco de datos, v. http://www.cnil.fr/index.php?id=2363&news[uid]=508&cHash=0a2ef80a3e.

> Artículos

G. Haas et L. Goutorbe, « Cybersurveillance: l'employeur doit être prudent en matière de collecte de preuve », *Expertises* ago.-sept. 2005, p. 304 — R. de Quenaudon, « Liberté et sécurité dans l'entreprise: une conciliation de plus en plus problématique », *RDT* 2006, p. 395; « Quelques remarques à propos de

connexions illicites du salarié », *RDT* 2007, p. 370.

33.04

Preguntas principales.

• ¿Cómo conciliar el derecho de control del empleador sobre la herramienta de trabajo y el respeto de la vida privada del trabajador?

* Ver s^{s} n^{o} 33.11.

• ¿En qué condiciones se puede acceder a los datos personales de un trabajador?

* Ver s^{s} n^{os} 33.20 s.

• ¿Cuáles son los criterios de apreciación para obtener una autorización de control biométrico de acceso al lugar de trabajo?

* Ver s^{s} n^{o} 33.30, tamb. n^{os} 28.00 s.

SECCIÓN 1
UN DISPOSITIVO JUSTIFICADO

33.11

Un dispositivo de control « justificado ». La ley del 31 de diciembre de 192 instauró un « principio de proporcionalidad », desde entonces incluido en el artículo L. 1121-1 del Código de trabajo: « Nadie puede aportar a los derechos de las personas y a las libertades individuales restricciones que no estuvieran justificadas por la naturaleza de la tarea a realizar ni proporcionales con respecto al objetivo buscado » (anc^{t} art. L. 120-2).

Esto fue lo que recordó el Tribunal de Gran Instancia de París, en su decisión del 19 de abril de 2005[39], con respecto a un dispositivo biométrico, cuyo uso era contestado judicialmente por el comité de empresa y el sindicato Sud-Rail. Estos últimos consideraban que el sistema de lectura de huellas digitales para administrar y controlar el tiempo de presencia de los trabajadores en distintos lugares de trabajo iba en contra de los derechos y libertades individuales de los trabajadores.

El empleador por lo tanto sólo puede ejercer un control cuando esté ante un comportamiento sospechoso de su trabajador: tiempos de conexión anormalmente largos o incluso descargas anormalmente largas (conexión y descarga de juegos o incluso de imágenes pornográficas) podrían, por ejemplo, constituir índices que justifiquen una medida de vigilancia y de intercepción. Hay que apuntar sin embargo que tales comprobaciones podrían ser consideradas con un « obstáculo » si se trata de un trabajador « protegido » (delegado sindical, delegado de personal, miembro del comité de empresa, *etc.*).

33.12

Marco jurídico de los auto conmutadores. En una primera recomendación del 18 de septiembre de 1984, la Commission nationale de l'informatique et des libertés (Cnil) precisaba que el empleador no puede grabar las conversaciones telefónicas, ni la totalidad de los números de teléfono marcados por sus trabajadores (sino sólo los cuatro primeros números, para saber si el trabajador ha llamado al extranjero o a otra provincia, *etc.*[40]).

Desde entonces, por decisión del 20 de noviembre de 1994, la Cnil ha elaborado una norma simplificada que constituye el marco jurídico para usar auto conmutadores. Este dispositivo permite conservar en la memoria los números de teléfono marcados por los trabajadores, desde su lugar de trabajo. La Comisión establece claramente que el uso con fines privados de las líneas telefónicas por parte de los trabajadores está permitido, aunque el empleador puede exigir a los trabajadores afectados el reembolso de las comunicaciones hechas con tales fines. Ahora bien, si el empleador tiene la posibilidad conservar los números de teléfono marcados por los trabajadores desde su puesto de trabajo, estos número

---

[39] TGI París, sala 1ª 19 abr. 2005, CE Effia Services, Synd. Sud Rail c/Effia Services, *CCE* oct. 2005, p. 46 s.

[40] Cnil, recomend. n^{o} 84-31, 18 sept. 1984, sobre el uso de auto conmutadores telefónicos en el lugar de trabajo, *3^{e} Rapport d'activités de la Cnil,* Doc. fr., p. 109, http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017654576&fastReqId=227990&fastPos=1.

no podrán en ningún caso divulgarse íntegramente a otros trabajadores. Además, el empleador no puede conservar restos números durante un periodo superior a seis meses. Por último, la Cnil recuerda que los representantes del personal deben ser consultados antes de que se coloque un sistema de auto conmutador semejante.

33.13

Condiciones de intercepción de las comunicaciones hechas por los trabajadores. La práctica de las escuchas telefónicas está reglamentada por la ley del 17 de julio de 1970. Ha sido completada por la ley del 10 de julio de 1991, que amplia el alcance del principio de prohibición de las escuchas telefónicas. De esta manera, inscribió en el Código penal, un artículo 226-15 párrafo 2 que incrimina « el hecho, cometido de mala fe, de interceptar, desviar, utilizar o divulgar correspondencia emitira, transmitida o recibida haciendo uso de las telecomunicaciones o proceder a la instalación de aparatos concebidos para realizar tales intercepciones" (un año de carcel y 45.000 euros de multa).

Y también se castiga, cometido de mala fe, de abrir, suprimir, posponer o devolver la correspondencia llegada o no a destino y de enterarse de su contenido de manera fraudulenta (C. penal, alrt. 226-15, al. 1).

El artículo 432-9 del Código penal incrimina también el hecho, para una persona depositaria de la autoridad pública o encargada de una misión de servico publico, de ordenar, cometer o facilitar, excepto en los caso previstos por la ley, que se intercepte o se desvíe correspondencia emitida, transmitida o recibida haciendo uso de las telecomunicaciones, de usar y divulgar su contenido (tres años de cárcel, 45.000 euros de multa).

Además, el Código penal subordina la posesión de aparatos concebidos para realizar tales intercepciones a la concesión de una autorización entregada por una comisión, especialmente instituida a tal efecto por el artículo R. 226-2 del mismo código, y presidida por el secretario general de la Defensa nacional.

Una duda quedaba en cuanto a la aplicación de esta prohibición a los empleadores. La Cnil autorizó al empleador a interceptar las comunicaciones hechas por los trabajadores de la empresa con la condición de que la finalidad del dispositivo de escuchas se precise, que los trabajadores estén avisados de la instalación de tal dispositivo, previamente a su instalación, de las posibles consecuencias de la intercepción de comunicacionesm de las horas durante las cuales sus conversaciones podrían ser grabadas. Además, está previsto que los trabajadores puedan contar con líneas no conectadas al dispositivo de escucha para las conversaciones que no estén directamente relacionadas con el motivo de la escucha. Por último, se precisa que cuando la escucha se lleve a cabo con fines de control de calidad de la respuesta telefónica, los trabajadores deben conocer en un plazo muy breve el informe de la conversación grabada. Las grabaciones deben ser después borradas, una vez efectuado el análisis, en un plazo de entre 15 días y un mes. Por otro lado, los clientes que llamen deben ser informados de que su llamada va a ser grabada.

La jurisprudencia dedica algunos principios en materia de escuchas telefónicas. En efecto, el uso con fines personales de la línea telefónica profesional ha sido considerado, en muchos casos, como falta grave[41]. Pero otras sentencias han reconocido que tal uso, si bien no es constitutivo de una falta grave, si es susceptible de constituir una causa real y seria de despido[42]. Ahora bien, la jurisprudencia también ha considerado que los despidos pronunciados por esta razón eran injustificados cuando parecían desproporcionados con respeto a los hechos de la causa[43].

---

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

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

[43] Soc. 30 mar. 1999, nº 97-40850; Soc. 18 nov. 1998, nº 96-43902, NPB, sté Cégéor c/Mme I. Maulet, v. http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT0000073

Nos quedaremos pues con que se consideran derogaciones admitidas las actividades de marketing telefónico, venta por correspondencia, centralita, para que el empleador pueda controlar el trabajo. A falta de una necesidad reconocida y proporcionada, habrá que buscar una solución alternativa, por ejemplo « en lugar de grabar todas las conversaciones con los clientes para constituir pruebas materiales con las que hacer frente en caso de un posible contencioso, solicitar una confirmación escrita al cliente, sobre todo por vía electrónica »[44].

SECCIÓN 2
CONDICIONES DE ACCESO A LOS DATOS PERSONALES DEL TRABAJADOR

33.21

Principio de inviolabilidad de la correspondencia. Toda violación a este principio constituye la infracción contemplada y reprimida por el artículo 226-15 del Código penal: « El hecho, cometido de mala fe, de abrir, suprimir, retrasar o desviar las cartas llegadas o no a destino y dirigidas a terceros o de enterarse de su contenido de manera fraudulenta, será castigado con un año de cárcel y 45.000 euros de multa. Se castiga con las mismas penas el hecho de interceptar, desviar, utilizar o divulgar cartas emitidas, transmitidas o recibidas haciendo uso de las telecomunicaciones o de proceder la instalación de aparatos concebidos para realizar tales intercepciones»[45].

Varias decisiones recuerdan así la prohibición hecha a un empleador de enterarse de los mensajes emitidos y recibidos por sus trabajadores. La sentencia del Tribunal de Casación del 2 de octubre de 2001 (sentencia Nikon[46]) precisa especialmente que « el trabajador tiene derecho, incluso durante y en el lugar de trabajo, a que se respete la intimidad de su vida privada; que ésta implica concretamente el secreto de la correspondencia; que el empleador no puede pues, sin violar esta libertad fundamental, enterarse de los mensajes personales enviados por el trabajador y recibidos por él gracias a una herramienta informática puesta a su disposición para su trabajo y ello incluso en el caso de que el empleador haya prohibido un uso no profesional del ordenador ». En este caso, el empleador había descubierto que su trabajador mantenía una actividad paralela que desarrollaba durante sus horas de trabajo y a partir de su puesto informático puesto a disposición por la empresa que le empleaba. Los elementos de prueba recogidos en la mensajería del trabajador se obtuvieron, según los jueces, de manera ilícita y, a por esta razón, fueron suprimidos de los debates.

Recientemente, el Tribunal de Casación aprobó una sentencia del Tribunal de Apelación que, al darse cuenta del carácter privado del correo electrónico enviado por un trabajador a uno de sus compañeros de trabajo, dedujo que este elemento de la vida personal del interesado no podría ser invocado como motivo de despido[47].

El principio de inviolabilidad de la correspondencia también se aplica a los

---

99898.

[44] Cnil, *Guide pratique pour les employeurs,* p. 21, http://www.cnil.fr/fileadmin/documents/La_CNIL/publications/CNIL_GuideTravail.pdf.

[45] Este artículo ha sido extraido de la decisión judicial nº 2000-916, 19 sept. 2000, art. 3, *JO* 22 sept. 2000, en vigueur le 1 janvier 2002.

[46] Soc. 2 oct. 2001, nº 99-42.942, Nikon France c/M. Onof, casación TA París, 22 mar. 1999 (devolución ante el TA París con composición diferente), *D.* 2001, 3148, nota P.-Y. Gautier; *D.* 2002, somm. 2296, nota C. Caron; *CCE* 2001, coment. 120 et obs.; *Dr. soc.* nov. 2001, p. 915, nota J.-E. Ray — ver también debate sobre la sentencia Nikon France, 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, nota H. Vray; *LPA*, 10 dic. 2001, nº 245, p. 6, nota G. Picca.

[47] Soc. 6 jun. 2007, nº 05-43.996, NPB, sté Eliophot c/M. X….: desestimación del recurso contra el TA Aquisgrán, sala 18ª, 7 jun. 2005.

trabajadores, tal y como ilustra esta sentencia del Tribunal de gran instancia de París (TGI París, 1 jun. 2007[48]) que condenó a un antiguo consultor informático de una empresa que habría conservado, incluso mucho después de haberse marchado, los códigos que le permitían acceder a las mensajerías electrónicas del director general y del director de recursos humanos. En este caso, ambos dirigentes descubrieron que eran objeto de vigilancia electrónica. El registro efectuado en casa del consultor permitió encontrar huellas de conexiones a las mensajerías en cuestión. Declaró que había comunicado los códigos a su hermano, un antiguo trabajador de esta empresa, que trabajaba actualmente para la competencia, para vigilar la posible compra de la empresa Oddo por su empleador. Como recordaron los jueces, el simple hecho de consultar los correos electrónicos de terceros utilizando sus códigos de acceso constituye un acceso fraudulento a un sistema informático y un perjuicio al secreto de la correspondencia violando así el artículo 226-15 del Código penal.

33.22

Mensajes supuestamente profesionales. Según la Cnil, « en general, hay que considerar que un mensaje enviado o recibido desde el puesto de trabajo puesto a disposición por la empresa o la administración reviste un carácter profesional, excepto indicación expresa en el objeto del mensaje o en el nombre del repertorio en el que hubiera sido archivado por su destinatario, quien le daría entonces el carácter y la naturaleza de una correspondencia privadas protegida por el secreto de correspondencia»[49].

Este fue el razonamiento seguido por los jueces del Tribunal de Apelación de Burdeos para admitir las pruebas presentadas por el empleador. En efecto, precisaron que « las carpetas y ficheros presentes en el ordenador de los trabajadores, o incluso los documentos que están en su oficina, tiene necesariamente un carácter profesional cuando no se les ha identificado como personales. De ello resulta que el trabajador tiene legítimamente acceso a estas carpetas, ficheros o documentos profesionales, sin que sea necesario que el trabajador en cuestión esté presente. Por lo tanto, los ordenadores de los trabajadores están al alcance del empleador. Así pues, (el empleador) podría legalmente acceder al ordenador (del trabajador). A falta de mención particular inscrita (por el trabajador) en los correos electrónicos enviados desde su ordenador profesional […], (el empleador) tiene derecho a presentarlos ante la justicia. En consecuencia, la existencia de los mails quedaba reconocida y los hechos quedaban claramente establecidos » (TA Burdeos, sala de lo social, Sección A, 8 feb. 2005[50]).

Dentro de esta lógica, *a contrario,* cuando el objeto de un mensaje indica el carácter privado de este último, el empleador no puede, en principio, abrir este mensaje para leer su contenido.

Ahora bien, otras decisiones recuerdan que la regla de la inviolabilidad se aplica en cualquier circunstancia, incluso cuando el objeto del mensaje no está explícitamente indicado, con lo que el empleador es quien tiene que comprobar los elementos susceptibles de conferir al susodicho mensaje un carácter manifiestamente personal (tal sería el caso de un mensaje cuyo objeto se refiera a las vacaciones y que esté clasificado en una carpeta que lleve la mención «Personal »)[51].

Del mismo modo, para dar al traste con esta regla, los empleadores recurren a distintos medios, sobre todo la inserción de disposiciones específicas en la carta relativa al uso de las herramientas informáticas. Como ejemplo podemos citar la sentencia del 15 de septiembre de 2005 del Consejo de conciliación de Nanterre. En este caso, un trabajador, que mandaba muchos mensajes a una empresa de la competencia, fue despedido por falta grave. Los asesores consideraron que,

---

[48] TGI París, 1 jun. 2007, Oddo et Cie c/Trinh Nghia T… et Trung T…, se puede consultar en el sitio legalis.net: http://www.legalis.net/jurisprudence-decision.php3?id_article=2179.

[49] Cnil, *Guide pratique pour les employeurs.*

[50] TA Bordeaux, sala de lo social, Sección A, 8 feb. 2005, nº 04/02449.

[51] TA Toulouse, 4ª sala de lo social, 6 feb. 2003, caso nº 02-02519.

aunque llevara la mención « mensaje estrictamente privado y confidencial », no había lugar de acoger favorablemente la demanda del demandante que solicitaba la declaración de despido privado por causa real y seria invocando que la « carta de los medios de comunicación », usada en la empresa, como complemento del reglamento de orden interno, precisaba que « los mensajes con carácter privado deben llevar la mención PRV ». Por ello, el empleador era libre de enterarse del contenido de cualquier mensaje que no llevara dicha mención

33.23

Acceso a los ficheros personales en presencia del trabajador. El Tribunal de Apelación de Besançon consideró que la violación del secreto de la correspondencia privada no podía invocarse, pues el empleador no tenía acceso directo a los ficheros en cuestión (con carácter pornográfico), y su apertura y su lectura fueron realizadas por un experto judicial enviado por el Consejo de conciliación en presencia de las partes o de sus abogados (TA Besançon, 24 sept. 2004[52]). El Tribunal de Casación confirmó que el empleador podría tener acceso a los ficheros personales de un trabajador. En este caso, el empleador había descubierto fotos eróticas en el cajón de la mesa del despacho de su empelado y había decidido entonces investigar el disco duro del ordenador del mismo. Un fichero titulado « perso » contenía una serie de documentos ajenos a las funciones del trabajador. Según el tribunal, « excepto en caso de riesgo o evento particular, el empleador sólo puede abrir los ficheros identificados por el trabajador como personales que se encuentren en el disco duro del ordenador puesto a su disposición en presencia de éste último o después de haber sido llamado» (Soc. 17 may. 2005[53]). Desde entonces, la Alta jurisdicción ha precisado que « las carpetas y ficheros creados por un trabajador gracias a la herramienta informática puesta a su disposición por su empleador para hacer su trabajo, se supone, excepto si el trabajador los identifica como personales, que tienen carácter profesional con lo que el empleador puede acceder a ellos sin que el trabajador esté delante» (Soc. 18 oct. 2006[54]).

Siguiendo con la misma lógica, el Tribunal de Apelación de Versailles descartó los mensajes presentados por un empleador para demostrar que su trabajador estaba creando una empresa competidora pues éstos fueron recuperados del portátil del trabajador sin satisfacer la demanda previa de este último de que se le restituyeran sus ficheros personales (TA Versailles, 2 abr. 2003[55]).

33.23

Presentación de SMS a título de prueba. El Tribunal de Casación tuvo que pronunciarse sobre la admisibilidad de SMS a título de prueba en un caso en el que la trabajadora, despedida por falta grave, impugnaba su despido invocando acoso sexual. Estos hechos, demostrados por SMS, fueron admitidos por el Tribunal de Apelación. El empleador presentó un recurso de casación, en el que contestaba la admisibilidad de los elementos de las pruebas presentados (mensajes telefónicos reconstituidos y retranscritos pour un ujier a espaldas de su autor y una entrevista grabada por la trabajadora en un micro-casete a escondidas). El Tribunal de Casación consideró que si la grabación de una

---

[52] TA Besançon, sala de lo social, 21 sept. 2004, RG nº 2003-1807, SNC General Electric Energy Products France c/Girardot et a., *RJS* 4/2005, nº 342.

[53] Soc. 17 may. 2005, nº 03-40.017, NPB, Philippe X. c/Cabinet-Science, *Juris-Data* nº 2005-028449; *CCE* jul.-ago. 2005, p. 34 s., coment. A. Lepage; v. aussi G. Haas et L. Goutorbe, « Cybersurveillance: l'employeur doit être prudent en matière de collecte de preuve », Expertises ago.-sept. 2005, p. 304; *Gaz. Pal.*, 20 oct. 2005, nº 293, p. 36, nota S. Hadjali; *LPA* 23 abr. 2007, nº 81, p. 6, nota S. Tournaux

[54] Soc. 18 oct. 2006, nº 04-48.025, Jérémy L. F… c/Techni-Soft, *Bull. civ.* V, 18 oct. 2006, coment. J.-E. Ray, L'envers de l'arrêt Nikon, *Sem. soc. Lamy* 2006, nº 1280, p. 10; P. Alix, « L'accès par l'employeur aux fichiers personnels stockés sur l'ordinateur du salarié », *JSL* nº 189-1, p. 4; J.-E. Tourreil, « Les documents détenus par un salarié dans l'entreprise sont présumés avoir un caractère professionnel », *JSL* nº 200, p. 15, v. http://www.legalis.net/jurisprudence-decision.php3?id_article=1774; *Gaz. Pal.* 18 ene. 2007, nº 18, p. 37, nota S. Hadjali et C. Fagot; *LPA* 28 abr. 2008, nº 85, p. 7, nota X. Daverat.

[55] TA Versailles, 2 abr. 2003, caso nº 02-00293.

conversación telefónica privada, efectuada sin que el autor de los propósitos se enterara es un efectivamente un procedimiento desleal que hace inadmisible ante la justicia la prueba así obtenida, lo mismo ocurre con el uso del destinatario de los SMS cuyo autor no puede ignorar que son grabados por el aparto receptor. Los SMS establecían la prueba de acoso sexual de la que se quejaba la trabajadora (Soc. 23 may. 2007[56]).

SECCIÓN 3
UN DISPOSITIVO SENSIBLE

33.30

Control de acceso biométrico. Se observa un desarrollo importante de los dispositivos biométricos con objeto de controlar los accesos al lugar de trabajo o a los sistemas de información (Ver s^{s} n^{os} 28.20 s.).

Su puesta en marcha está subordinada a una autorización otorgado por la Cnil. Esta precisa, en una guía publicada el 28 de diciembre de 2007[57], sus principales criterios de apreciación así como los riesgos a los que se exponen las empresas que recurren ellos y los derechos de los trabajadores (Ver s^{s} n^{os} 28.21 s.).

En general, el dispositivo debe responder a un « fuerte imperativo de seguridad ». Por otro lado, debe limitarse al control de acceso a una zona bien definida para un número determinado de personas (1 criterio). En razón de los riesgos asociados para la protección de los datos personales, el dispositivo debe ser "proporcional" es decir, adaptado a la finalidad que persigue (2º criterio) Hay que tomar medidas para garantizar que la autentificación y/o identificación no provoquen la divulgación de los datos (3er criterio). Por último, las personas afectadas deben ser informadas (4º criterio).

La Cnil autorizó pues, el 13de septiembre de 2007[58], el uso de un tratamiento automatizado de datos personales que descansa en un procedimiento de reconocimiento vocal. Este dispositivo, que pretende generar y reinicializar automáticamente las contraseñas de acceso al sistema de información de la empresa, descansa en el reconocimiento del modelo de la huella de la voz de los trabajadores.

La Cnil también autorizó el 8 de noviembre de 2008, por cinco deliberaciones (n^{o} 2007-335 à n^{o} 2007-339)[59], el uso de varios dispositivos que descansan sobre el reconocimiento de la red venosa del dedo de la mano y que tiene por objeto controlar el acceso a los locales o los sistemas de información.

33.31

Geolocalización. Cada vez hay más empresas que recurren a dispositivos de geolocalización que permiten identificar la posición geográfica en un momento dado o de manera continua, de sus trabajadores gracias a la localización de los materiales que utilizan, sobre todo los vehículos confiados por la empresa. Estos dispositivos se basan sobre todo en el uso de la tecnología GSM/GPS que permite localizar en cualquier momento la posición de un vehículo equipado con dicho sistema. El tratamiento de los resultados de estos dispositivos permite recabar datos como la duración del uso del vehículo, los kilómetros recorridos o la velocidad de circulación. La Cnil considera que esta "vigilancia permanente de los desplazamientos de los trabajadores es desproporcionada cuando la tarea que hay que realizar no reside en el desplazamiento mismo sino en la realización de

---

[56] Soc. 23 may. 2007, n^{o} 05-17.818, NPB, *Bull. civ.* V; *D.* 2007, AJ 1590, nota A. Fabre; *Gaz. Pal.* 18 mar. 2008, n^{o} 78, p. 20; *LPA* 28 abr. 2008, n^{o} 85, p. 7, nota X. Daverat et S. Tournaux.

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

[58] Cnil, resol. n^{o} 2007-248, 13 sept. 2007, http://www.wk-rh.fr/mybdd/upload/bdd_80/Cnil-D2007-248.pdf.

[59] Cnil, resol. n^{os} 2007-335 a 2007-339, 8 nov. 2007, http://www.wk-rh.fr/mybdd/upload/bdd_80/Cnil-D2007-335-339.pdf.

una prestación la cual puede ser también objeto de comprobaciones»[60]. El Tribunal de Casación, en una sentencia del 26 de noviembre de 2002[61], consideró que "una red organizada por el empleador para controlar y vigilar la actividad de un trabajador es un medio de prueba ilícito, al margen de si el trabajador ha sido informado o no de la existencia de tal control»[62]. Del mismo modo, la Cnil puso en marcha una consulta entre los actores implicados, sobre todo ministerios, organizaciones sindicales y profesionales e integradores de los servicios de geolocalización para enmarcar adecuadamente las condiciones de uso de estos dispositivos[63].

Esta reflexión llevó a la aprobación, el 16 de marzo de 2006, de dos deliberaciones nº 2006-066 y nº 2006-067 relativas, respectivamente, a una recomendación y a una norma simplificada "sobre los tratamientos automatizados de datos personales utilizados por los órganos públicos o privados destinados a geolocalizar los vehículos utilizados por sus trabajadores»[64]. Teniendo en cuenta el carácter intrusivo del uso de dispositivos de geolocalización, al Cnil presenta una lista de finalidades por las cuales la inserción de un dispositivo así le parece legítimo y, por ende, admisible (seguridad del trabajador o de las mercancías, mejor reparto de los medios, seguimiento y facturación de una prestación de transporte de personas o mercancías o de una prestación de servicio directamente ligada al uso del vehículo, seguimiento del tiempo de trabajo). Por otro lado, la comisión indica que el uso de un dispositivo así no debe llevar al control permanente del trabajador en cuestión. Prevé un aligeramiento considerable de las formalidades administrativas para las empresas que respondan a las condiciones contempladas, sobre todo en cuanto a los tipos de datos recogidos y a la duración de su conservación (norma simplificada nº 51). Esta resolución esboza, a este respecto, una lista de las finalidades a las que debe responder imperativamente la recogida de información con un procedimiento semejante. La Cnil delimita también los datos que pueden tratarse con el uso de un dispositivo de geolocalización. También establece una lista sucinta de destinatarios de estos datos.

Por último, la Cnil precisa que los responsables del tratamiento que deseen utilizar un dispositivo de geolocalización deben informar y consultar obligatoriamente a las instancias representativas del personal antes de utilizar dicho dispositivo. Esta obligación de información debe llegar también a los trabajadores sometidos a tal dispositivo. Por otro lado, los responsables del tratamiento de los datos deben asegurarse de que se han tomado todas las medidas de seguridad necesarias.

33.32

Dispositivos de alerta profesional. La ley americana Sarbanes-Oxley (julio 2002) impone a las empresas que cotizan en bolsa en Estados Unidos y a sus filiales en el extranjero proporcionar a sus trabajadores un dispositivo de *whistleblowing* (denominado, en francés "alerta profesional" o incluso "alerta ética") con el que denunciar los delitos financieros de los que estén al corriente.

No existe ninguna ley francesa sobre estos dispositivos, pero podrían llegar un día ya que se preconiza esta vía en un informe entregado el 7 de marzo de 2007[65] al ministro delegado de Empleo, de Trabajo y de Inserción profesional de los jóvenes En efecto, este informe, titulado *Charte d'éthique, alerte professionnelle et droit du travail français: état des lieux et perspectives,* preconiza varias vías para reforzar la seguridad jurídica de las cartas éticas y para crear el marco para un sistema de alerta profesional. Propone sobre todo introducir en el Código de

---

[60] Cnil, *Guide pratique pour les employeurs,* 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,* p. 23.

[63] Cnil, comunicado 29 sept. 2005.

[64] Cnil, resol. nº 2006-067, 16 mar. 2006, sobre la adopción de una norma simplificada relativa al tratamiento automático de datos personales utilizado por los organismos públicos o privados destinados a geolocalizar los vehículos utilizados por sus trabajadores (norma simplificada nº 51), *JO* nº 1003, 3 may.

[65] Ver el informe *Charte d'éthique, alerte professionnelle et droit du travail français: état des lieux et perspectives,* en http://lesinformes.ladocumentationfrancaise.fr/BRP/074000335/0000.pdf l.

trabajo unas reglas específicas para permitir a las empresas utilizar unos dispositivos con los que señalar no sólo actos en contra de los dispositivos legislativos o reglamentarios y si se atenta contra los derechos de las personas y la salud de los trabajadores sino también actos contrarios a las reglas de origen ético o profesional. Así, esta nueva reglamentación tendría sobre todo como objetivo "-definir la alerta profesional; - determinar los instrumentos jurídicos para utilizar dicho dispositivo; - fijar las reglas de organización que deben contener el instrumento jurídico elegido; - proteger al emisor".

De momento, la Cnil marca las condiciones de uso de estos dispositivos, a los que define como "sistemas a disposición de los trabajadores de un organismo público o privado para incitarles, como complemento a los medios normales de alerta sobre el malfuncionamiento del organismo, a señalar a su empleador comportamientos que consideren contrarios a las reglas vigentes y para organizar la veracidad de la alerta así recogida en el seno del organismo en cuestión"

En un principio, la Cnil rechazó, en mayo de 2005[66], autorizar el uso de tales dispositivos, considerando que "eran desproporcionados con respecto a los objetivos perseguidos y los riesgos de denuncia calumniosa y de estigmatización de los trabajadores objeto de una alerta ética". También subrayó que "los trabajadores afectados por un aviso no no estarían informados en cuanto se pusiera en marcha el registro de datos que3 pongan en tela de uuido su integridad profesional o de ciudadano y que no terndrían pues medios para oponerse a este tratamiento de datos relativos a sus personas. Las modalidades de recogida y tratamiento de estos datos, algunos de los cuales podrían referirse a hechos susceptibles de ser considerados como infracción penal, pueden ser pues ser calificados de desleales". Esta postura tuvo como consecuencia que las filiales francesas de empresas americanas se han topado conciertas dificultades, pues están obligadas a respetar disposiciones contradictorias de la ley informática y de libertades y las de ley *Sarbanes-Oxley.*

Así pues, la Cnil revisó su postura. Primero se acercó a la *Securities and Exchange Commission (SEC)* para encontrar garantías compatibles tanto con la ley informática y de libertades como con la ley *Sarbanes-Oxley* y publicó el 10 de noviembre de 2005[67] un documento de orientación para precisar las condiciones en las que se puede utilizar un dispositivo de alerta ética. Después adoptó, el 8 de diciembre de 2005[68] una decisión de autorización única por la que se fijan las condiciones que hay que respetar para poder beneficiarse de las formalidades simplificadas. En general, admite el principio de alerta profesional, pero restringe su campo de aplicación a unos ámbitos bien precisos (contable, financiero, bancario y de lucha contra la corrupción). Por otro lado, prevé que un dispositivo de esa índole exige el uso de medidas de precaución para recoger, tratar y transferir fuera de la Unión Europea los datos en cuestión. Paralelamente se perfilaron los derechos de información, de acceso y de rectificación de los trabajadores.

El grupo G 29 (v. s^{s} n^{o} 15.18) también adoptó el uno de enero de 2006[69] un dictamen sobre los dispositivos de alerta profesional en los ámbitos bancario, contable, de control interno de cuentas, de auditoria y lucha contra la corrupción y

---

[66] Cnil, resol. n^{o} 2005-110, 26 may. 2005, relativa a una solicitud de autroización de Mc Donald's France para utilizar un dispositivo de integridad profesional,
http://www.cnil.fr/index.php?id=1833&delib[uid]=73&cHash=ed7a84ª6a7 — y Cnil, resol. n^{o} 2005-111, 26 may. 2005, relativa a una solicitud de autorización de la Compagnie européenne d'accumulateurs para utilizar un dispositivo de línea ética,
http://www.cnil.fr/index.php?id=1834&delib[uid]=74&cHash=89a931a002.

[67] Doc. de orientación adoptado por la Comisión el 10 nov. 2005 para el uso de dispositivos de alerta profesional de acuerdo con la ley del 6 de ene. 1978 modificada en ago. 2004, relativa la informática, a los ficheros y a las libertades,
http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/CNIL-docori-10112005.pdf.

[68] Cnil, delib. n^{o} 2005-305, 8 dic. 2005, sobre la autorización única de tratamientos de datos personales utilizados en el marco de dispositivos de alerta profesional,
http://www.cnil.fr/index.php?id=1969.

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

de los plazos financieros. En general, retoma los principios del documento de orientación y de la autorización única emitidos por la Cnil en noviembre y diciembre de 2005.

Al margen de estas prescripciones, hay que tener en cuenta la jurisprudencia, a causa de la inflación de las acciones destinadas a conseguir que se supriman los sistemas de alerta ética. Así, por providencia de urgencia del 15 de septiembre de 2005[70], el juez de los recursos de urgencia del tribunal de Libourne (Gironde) pidió a la filial francesa de una empresa americana, que retirara su dispositivo de alerta ética considerando que esta medida se imponía invocando "la simple existencia de un perjuicio potencial inminente para las libertades individuales de los trabajadores víctimas de denuncias anónimas obtenidas a través de un dispositivo privado que escapa a cualquier control, sin que el interés de la empresa permita justificarlo seriamente". Una providencia de urgencia del 27 de diciembre de 2006 del tribunal de gran instancia de Nanterre también ordenó la suspensión de la difusión de un cuestionario titulado « business ethics » que los trabajadores tenían que cumplimentar y les imponía sobre todo "señalar si un miembro de su familia tiene intereses significativos en una empresa exterior que quiera trabajar o esté en competencia con la empresa" o incluso precisar "si una relación familiar o personal podría disuadirles de actuar en el mejor interés de la empresa»[71]. El juez de los recursos de urgencia estimó que este dispositivo de alerta ética no respondía a la resolución de la Cnil del 8 de diciembre de 2005, concretamente en la medida en que la Cnil precisaba que sólo podrían beneficiarse del régimen de autorización única "los dispositivos de alerta que no tengan carácter obligatorio".

Pero también hay que contar con las decisiones que validan los dispositivos de alerta ética, como el de la sentencia del 19 de septiembre de 2006 del tribunal de gran instancia de Lyon que consideró que "si los demandantes evocaron y criticaron inicialmente el dispositivo de alerta profesional utilizada, hay que decir que aunque el texto retocado lo presenta como medio facultativo que sólo puede utilizarse para responder a los intereses cuya legitimidad está establecida (ámbitos contables, control de cuentas y lucha contra la corrupción), dado que la identidad del emisor se trata de manera confidencia y que la persona contemplada se beneficia de un derecho de acceso a las informaciones y de un derecho de rectificación, es conforme con la resolución de la Cnil del 8 de diciembre de 2005 »[72]. Ya en abril de 2005, el juez de los recursos de urgencia consideró que el documento presentado en el comité de empresa por el que se ponía en marcha un procedimiento de alerta no parecía plantear, en la situación del procedimiento judicial de urgencia y de la evidencia, problema alguno ni de interpretación, ni de violación de los derechos del trabajador, porque se trataba de un procedimiento facultativo sin sanciones ni consecuencias de ningún tipo[73].

Para algunos, estos precedentes judiciales dibujan de manera bastante precisa el marco vigente a los dispositivos de alerta profesional. Los autores del informe de marzo de 2007, por su parte, notan que "ahora que muchos son los que aspiran a una mayor seguridad jurídica [...], más vale evitar una construcción judicial, lenta y confidencial por naturaleza, de un derecho de alerta profesional"

La legalización de los dispositivos de alerta ética profesional sigue suscitando el debate.

---

[70] TGI Libourne, 15 sept. 2005, BSN Glasspack, citado en « Alertes éthiques: quelles orientations suite aux décisions de la CNIL ? », *RLDI* 2005/11, nº 318, obs. F. Naftalkski; *CCE* dic. 2005, A. Lepage, coment. 191, p. 37 et A. Caprioli, coment. 194, p. 44.

[71] TGI Nanterre, 27 dic. 2006, Comité central d'entreprise Dupont de Nemours c/SAS Dupont de Nemours, nº 20006/02550.

[72] TGI Lyon, ch. urgences, 19 sept. 2006, Union départmentale CGT du Rhône, synd. CGT Bayer Cropscience c/Bayer Cropscience, v.
http://www.legalis.net/jurisprudence-decision.php3?id_article=1760.

[73] TGI Nanterre, ord. ref., 1 abr. 2005, CE ING Bank c/ING Bank France, inédit

CAPÍTULO

34. Principios generales para el respeto de la vida privada del trabajador

SECCIÓN 0
ÍNDICE

34.00

Índice del capítulo.

34.01

Textos vigentes.

> Textos franceses.

Textos legislativos.

Cód. trab., art. L. 1121-1 y L. 1134-1 s.

Dictámenes y recomendaciones.

Cnil, resol. n° 2002-001, 8 ene. 2002, sobre el tratamiento automatizado de informaciones nominales usadas en el lugar de trabajo en la gestión de los controles de acceso a los locales, de los horarios de trabajo y de la restauración — Cnil, resol. n° 2007-368, 11 dic. 2007, sobre un proyecto de decreto en el Conseil d'État por el que se modifica el decreto n° 2005-1726 del 30 de diciembre de 2005 relativo a los pasaportes electrónicos.

34.02

Jurisprudencia de referencia.

> Sobre el derecho de información del trabajador

• **Soc. 6 abr. 2004,** n° 01-45.227, Sté Allied signal industrial Fibers c/M. Pacheco NPB, *Bull. civ.* V, n° 103; *Gaz. Pal.* 20 jul. 2004, n° 202, p. 31, nota J. Bérenguer-Guillon y L. Maurel-Guignot — confirmación del TA **Nancy, sala de lo social, 25 jun. 2001,** M. Pacheco c/Sté Allied signal industrial Fibers, *Juris-Data* n° 145997; *Dr. ouvrier* 2002, n° 652.

Para la sentencia (revocada) presentada en 1ª instancia, v. **Consejo de Conciliación Longwy, 3 dic. 1999.**

* Ver s^s n° 34.10, tamb. n° 14.24.

> Sobre el acceso a los datos de notación anual

• **Soc. 23 oct. 2001,** n° 99-44.215, NPB, CANSSM c/Mme Vicheney, v. http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007628680 — confirmación del TA **París, sala 18, Sección A, 1 jun. 1999.**

* Ver s^s n° 34.12.

> Sobre la apreciación de la pertinencia de los datos

• **Civ. 1ª, 29 may. 1984,** n° 82-12.232, CEMU c/Mme D… et a., *Bull. civ.* I, n° 176 — confirmación del TA **Rouen, sala 3^e^, 17 dic. 1981**.

* Ver s^s n° 34.21.

34.03

> Informe

H. Bouchet (dir.), *La cybersurveillance sur les lieux de travail,* Cnil, mar. 2004, http://lesinformes.ladocumentationfrancaise.fr/BRP/044000175/0000.pdf.

> Artículo

A. Saint-Martin, « La reconnaissance d'une présomption de professionnalité des messages électroniques du salarié », *RLDI* n° 34, ene. 2008, p. 29.

34.04

Preguntas principales.

• ¿Cuáles son los derechos del trabajador sobre los datos personales relativos a su persona?

* Ver s^s n^os 34.10 s.

• ¿Cuáles son la obligaciones del empleador?

* Ver s^s n^os 34.21 s.

SECCIÓN 1
DERECHOS DEL TRABAJADOR

34.10
Derecho de información. Ver s^{s} n^{os} 12.30 s. et 32.11 s.

34.11
Derechos de acceso, de rectificación y de supresión. Cada trabajador, como cualquier persona física, tiene derecho a que se le comuniquen todas las informaciones que se refieran a su persona en un fichero y que se rectifiquen o supriman las informaciones erróneas. También tiene derecho a oponerse a figurar en un archivo, aunque sólo por motivos legítimos que el empleador es quien debe considerarlos. No puede oponerse a la recogida de datos necesarios para cumplir con una obligación legal, por ejemplo para las declaraciones sociales obligatorias. Por el contrario, puede oponerse a que el comité de empresa sea destinatario de las informaciones relativas a su persona. Ahora bien, debe ser claramente informado de las consecuencias que de ello se derivan para él (exclusión del beneficio de precios reducidos, por ejemplo). Si los datos ya han sido transmitidos, el comité de empresa debe ser informado para suprimir los datos, de acuerdo con la solicitud del trabajador en cuestión. Esta obligación pesa no sólo sobre el empleador sino también sobre el comité de empresa o cualquier otro organismo que, en el sector público, utilice ficheros informáticos de datos personales de los trabajadores. Estas menciones deben estar obligatoriamente incluidas en el cuestionario destinado a recoger los datos personales relativos a los trabajadores. En los demás casos, la Commission nationale de l'informatique et des libertés (Cnil) considera que fijar una nota de información en los locales o entregar un documento al trabajador pueden constituir medidas de información adaptadas»[74] (sobre los derechos de las personas en cuestión Ver s^{s} n^{os} 12.41 s.).

34.12
Acceso a los datos de notación anual. Después de las muchas quejas presentadas contra un trabajador por rechazo de comunicación a sus mandos de su clasificación y de su potencial de carrera, la Cnil consideró, en su sesión plenaria del 8 de marzo de 2007, que este tipo de datos puede comunicarse al trabajador en cuestión porque fueron tenida en cuenta a la hora de decidir su aumento de sueldo, su ascenso o su afectación. El trabajador puede pues, de acuerdo con el artículo 39 de la ley del 6 de enero de 1978 modificada en agosto de 2004, solicitar una copia del documento en el que estén incluidos estos datos.

Una sentencia del Tribunal de Casación del 23 de octubre de 2001 consideró que no comunicar su ficha de notación a un trabajador que lo haya solicitado constituye uno de los elementos que permiten caracterizar un comportamiento discriminatorio en su contra[75].

SECCIÓN 2
PERTINENCIA Y FINALIDAD DEL TRATRAMIENTO

34.21
Pertinencia de los datos. Los datos personales deben ser "adecuados, pertinentes y no excesivos" con respcto a los objetivos perseguidos. La recogida de informaciones sobre la salud o los allegados del trabajador sería contrario a este principio. Registrar el número de la seguridad social está autorizado en las hojas de paga y de gestión del personal para poder redactar las nóminas y las distintas

---

[74] V. Cnil, *Guide pratique pour les employeurs,* p. 30.
[75] Soc. 23 oct. 2001, n° 99-44.215, NPB, CANSSM c/Mme Vicheney, v. http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007628680.

declaraciones sociales obligatorias (Decreto nº 91-1404, 27 dic. 1991 — CSS, art. R. 115-1 y R. 115-2) y para teneduría de las cartillas de ahorro salarial (Cód. trab., art. L. 3341-6). Si la copia de la notificación de liquidación de un trabajador puede comunicarse al comité de empresa para que éste calcule la contribución debida por el interesado, no ocurre lo mismo con la declaración de la renta dado el carácter privado de las informaciones que en ella figuran[76].

34.22

Uso legítimo. Los datos personales deben ser objeto de un "uso determinado y legítimo".

Así, un dispositivo de video vigilancia instalado en un lugar susceptible de atentar contra la intimidad de la vida privada de los trabajadores (duchas, por ejemplo) o que incluso vigilara a un trabajador o a un grupo de personas de manera permanente sería ilícito. Por otro lado, la finalidad anunciada debe ser respetada.

Un lector de etiquetas no deber permitir de los trabajadores o de acceder a informaciones detallas sobre su consumo en la cantina de la empresa. La Cnil ha presentado una serie de recomendaciones para evitar tales desvíos de finalidad en su resolución nº 02-001 del 8 de enero de 2002[77].

34.23

Pocos comentarios en los ficheros del personal. La Cnil condenó a una empresa francesa, el 11 de diciembre de 2007, a pagar 40.000 euros de multa causa de los comentarios subjetivos que figuraban en el fichero de gestión de los trabajadores[78]. En su resolución, la Cnil precisa que aunque se admite que el tratamiento de datos personales puede incluir zonas de comentarios destinados a archivar informaciones de gestión tales como los resúmenes de las entrevistas o indicadores de seguimiento de un expediente, estas menciones deben ser pertinentes, adecuadas y no excesivas con respecto a la finalidad del tratamiento. El incumplimiento de esta obligación conlleva la aplicación del artículo 226-18 del Código penal. En este caso, se trataba de personas que habían trabajado en la empresa pero de los que ésta no había quedado satisfecha.

SECCIÓN 3
MEDIDAS DE PROTECCIÓN

34.31

Duración de conservación de los datos. Hay que indicar la duración de cada fichero y en función de la finalidad (por ejemplo, desde unos días a un mes como máximo para las grabaciones de video vigilancia). Excluye que se hable de conservación por una duración indeterminada.

Al tratarse de datos de conexión (Ver s^{s} n^{os} 27.00 s.), el empleador tiene que proporcionar todas las precisiones posibles sobre durante cuánto tiempo se conservan o archivan los datos de conexión con los que se identifica el puesto o el usuario que se haya conectado . La Cnil preconiza a este respecto que se lleve a cabo un balance anual: "las medidas de seguridad que se toman para conservar una traza de la actividad de los usuarios o del uso que hacen de las tecnologías de la información y de la comunicación o que descansan en el uso de tratamientos automatizados de informaciones directa o indirectamente nominales deberían ser objeto de un "balance anual informático y ser liberados cuando se aborde el balance social que se presenta ante el comité de empresa o el comité técnico

---

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

[77] Cnil, resol. nº 02-001, 8 ene. 2002, (norma simplificada 42) relativa al tratamiento automatizado de informaciones nominales utilizado en el lugar de trabajo para la gestión dde los controles de acceso a los locales, de los horarios y de la restauración,
http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653507

[78] Cnil, resol. nº 2007-368, 11 dic. 2007, relativa al dictamen sobre un proyecto de decreto en Consejo de Estado por el que se modifica el decreto nº 2005-1726 del 30 dic. 2005 relativo a los pasaportes electrónicos.

paritario o cualquier otra instancia equivalente »[79].

34.32

Gestión de las habilitaciones. El empleador está obligado a definir una política de seguridad para garantizar la confidencialidad de los datos (L. 6 ene. 1978, art. 34). Algunos datos sólo pueden estar al alcance de ciertas personas, excepto la facultad de transmitirlos a terceros autorizados (inspección del trabajo, servicios fiscales, etc.). Del mismo modo, en presencia de un dispositivo de video vigilancia, las imágenes grabadas sólo pueden verlas las personas debidamente autorizadas a tal efecto, en el marco de sus atribuciones (para más información sobre la video vigilancia v s[s] n[os] 30.00 s.).

[79] V. H. Bouchet (dir.), *La cybersurveillance sur les lieux de travail,* Cnil, mar. 2004, p. 18, http://lesinformes.ladocumentationfrancaise.fr/BRP/044000175/0000.pdf.

CAPÍTULO

35. Reglas específicas para los administradores de redes

SECCIÓN 0
ÍNDICE

SECCIÓN 1
PRINCIPIO: EL SECRETO PROFESIONAL

35.11

Medios de control a distancia. El tema de la violación del secreto de la correspondencia adquiere una dimensión especial con los administradores de redes, cuya misión consiste en garantizar el funcionamiento normal y la seguridad de las redes y sistemas en el seno de la empresa. Su función les lleva a acceder a informaciones relativas a los usuarios (mensajería, datos de conexión a Internet, ficheros-logs, etc). Del mismo modo, disponen de medios para controlar a distancia los puestos de trabajo, por ejemplo para garantizar el mantenimiento a distancia de los programas o, de manera más general, para hacerse con el control del puesto de trabajo en lugar del trabajador.

35.12
Cumplir con las obligaciones de transparencia y de proporcionalidad. Las condiciones de intervención de los administradores de red deben darse a conocer a los trabajadores y a los órganos de representación del personal en nombre de la obligación de transparencia a cargo del empleador (sobre el principio, Ver s^{s} n^{os} 32.00 s.). Estas intervenciones deben estar estrictamente delimitadas (información previa al usuario e intervención con su acuerdo previo, o por e-mail si fuera necesario) y limitarse al buen funcionamiento de las aplicaciones.
El control también debe responder al principio de proporcionalidad (sobre el principio, Ver s^{s} n^{os} 32.00 s.) y respetar el principio de finalidad enunciados por la ley informática y de libertades.

La Commission nationale de l'informatique et des libertés (Cnil) recordó que cualquier uso de estas herramientas por iniciativa propia de los administradores de redes o por orden de la jerarquía, por ejemplo con fines de control, "no responde al principio de proporcionalidad, ni cumple el principio de finalidad impuesto por la ley informática y de libertades »[80].

35.13
Obligación de confidencialidad reforzada. Los administradores de redes deben atenerse al secreto profesional y, de manera más general, a una obligación de discreción profesional que les prohibe divulgar las informaciones de las que hubieran podido entretenerse en el ejercicio de sus funciones.

La Cnil recuerda esta regla en su informe dedicado a la *Cybersurveillance sur les lieux de travail* (feb. 2004) al indicar que "los administradores de redes y sistemas, que en general deben atenerse al secreto profesional o a una obligación de discreción profesional, no deben divulgar informaciones de las que hubieran podido enterarse en el marco de sus funciones, y concretamente cuando éstas están cubiertas por el secreto de la correspondencia o tienen que ver con la vida privada de los usuarios y no se ponen en tela de juicio ni el buen funcionamiento técnico de las aplicaciones, ni su seguridad, ni el interés de la empresa". Precisa además que los administradores no podrán ser obligados a divulgar estas informaciones, "excepto disposición legislativa particular en este sentido".

Por último, el Forum des droits sur l'Internet indica por su parte que "el administrador de red velará para no divulgar a nadie en la empresa, ni siquiera a sus superiores y a sus compañeros, las informaciones personales relativas a un trabajador de las que hubiera podido enterarse en el marco de sus funciones".

Des mismo modo, hay que tomar medidas de seguridad para garantizar la confidencialidad de las informaciones a las que tienen acceso los administradores de redes en el ejercicio de sus funciones. Esta obligación de confidencialidad deberá recordarse en el contrato de trabajo, e incluso en el reglamento de orden interno o en la carta de uso de las herramientas informáticas.

SECCIÓN 2
EXCEPCIÓN: EN PRESENCIA DE UN RIESGO DE ATENTADO CONTRA LA SEGURIDAD DE LA EMPRESA

35.21
Medidas justificadas en caso de atentado contra la seguridad. Estas reglas tienen sin embargo un límite, en caso de riesgo de atentado contra la seguridad de la empresa o de la administración. Dentro de este contexto, el Tribunal de Apelación de París precisó en una sentencia del 17 de diciembre de 2001, que « la preocupación de la seguridad de la red justifica que los administradores de sistemas y de redes hagan uso de sus posiciones y de las posibilidades técnicas que dispongan para investigar y tomar las medidas que esta seguridad imponga – igual que Correos debe reaccionar ante un paquete o una carta sospechosa. Por el contrario, la divulgación del contenido de los mensajes, y sobre todo del último que hacía referencia al conflicto latente en el laboratorio en el que era mando, no

[80] Cnil, *Guide pratique pour les employeurs,* p. 14.

tenía relación alguna con estos objetivos»[81].

Del mismo modo, el empleador debe poder acceder a los documentos almacenados en el ordenador del trabajador ausente de su puesto de trabajo (baja, enfermedad sobre todo)[82]. El Tribunal de Casación, en una sentencia del 18 de marzo, consideró que el trabajador estaba obligado a comunicar su contraseña o los ficheros en su posesión cuando el buen funcionamiento de su empresa dependa de los datos que están en manos de este trabajador[83].

---

[81] TA París, 11e ch., Sección A, 17 dic. 2001, F. M..., H. H... et V. R... c/Min. public et A. T..., *Gaz. Pal.* 8 may. 2002, p. 31, coment. 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, nota C. Puigelier; *RTD civ.* oct.-dic. 2001, nº 4, 880-882, nota J. Mestre et B. Fages; *Gaz. Pal.* 20 mar. 2001, nº 79, p. 9.

[83] Soc. 18 mar. 2003, nº 01-41.343, NPB, *Gaz. Pal.* 25 sept. 2003, nº 268, p. 37, nota L. Maurel-Guignot.

CAPÍTULO

36. Reglas específicas en las operaciones de reclutamiento

SECCIÓN 0
ÍNDICE

36.00

Índice del capítulo.

36.01

Textos vigentes.

> Textos franceses.

Texto legislativo.

Cód. trab., art. L. 1221-6 et L 1221-8.

Dictámenes y resoluciones.

Cnil, resol. n° 02-017, 21 mar. 2002, sobre la adopción de recomendación relativa a la recogida y al tratamiento de informaciones nominales durante las operaciones de reclutamiento (revoca y sustituye la Cnil, recomend. 85-44, 15 oct. 1985).

Cnil, Recomend. para medir la diversidad de los orígenes en la lucha contra las discriminaciones del 5 de julio de 2005

> Texto europeo.

Ver s^{s} n^{o} 1.01: Dir. n^{o} 95-46, 24 oct. 1995, art. 10.

36.04

Preguntas principales.

• ¿Cuáles son los derechos del candidato durante las operaciones de reclutamiento?

* Ver s^{s} n^{os} 36.21 s.

• ¿De qué garantías puede beneficiarse?

* Ver s^{s} n^{os} 36.31 s.

SECCIÓN 1
CONDICIONES DE USO

36.11

Formalidades declarativas. Las personas que se encargan de el reclutamiento deben declarar ante la Commission nationale de l'informatique et des libertés (Cnil) los tratamientos automatizados de informaciones nominales, antes de utilizarlas (L. 6 ene. 1978, art. 22). El incumplimiento de esta regla expone al responsable del tratamiento a sanciones penales (Cod. penal, art. 226-24).

36.12

Una finalidad limitada al reclutamiento. El Código de trabajo precisa que "las informaciones solicitadas, sea cual sea su forma, al candidato a un empleo no pueden tener como finalidad apreciar su capacidad para ocupar el empleo propuesto o sus aptitudes profesionales. Estas informaciones deben tener un vínculo directo y necesario con el empleo propuesto o con la evaluación de las aptitudes profesionales. El candadito debe responder de buena fe a todas estas solicitudes de información » (Cód. trab., art. L. 1221-6).

La Cnil considera por su parte que, excepto los casos particulares justificados por la naturaleza de un puesto vacante o unas reglas vigentes en el país extranjero concernido por el puesto, las preguntas siguientes van en contra de las

prescripciones legales: fecha de entrada en Francia, fecha de naturalización, modalidades para adquirir la nacionalidad francesa, nacionalidad de origen, números matrícula o de afiliación a la seguridad social, detalle de la situación militar, dirección anterior, informaciones sobre el entrono familiar (cónyuge sobre todo), estado de salud (sobre todo tamaño, peso), estatuto de propietario o de inquilino, vida asociativa, domiciliación bancaria, préstamos suscritos.

Por otro lado, podrá considerarse recogida fraudulenta, desleal o prohibida (L. 6 ene. 1978, art. 6), el uso de anuncios para crear un fichero de candidaturas o incluso recabar información entre el entorno profesional del candidato a espaldas de este último.

Por último, está prohibido recoger y conservar datos que, directa o indirectamente, muestren los orígenes raciales o las opiniones políticas, filosóficas o religiosas o la pertenencia sindical, las informaciones relativas a la vida sexual de las personas (L. 6 ene. 1978, art. 6). La única derogación, a reserva del acuerdo expreso de los interesados, se refiere a la especificidad de un puesto vacante.

SECCIÓN 2
DERECHOS DEL CANDIDATO

36.21

Derecho de información de los candidatos. Los candidatos, como todas las personas de las que se recaban datos personales, tienen derecho de información (i) del carácter obligatorio o facultativo de las respuestas; (ii) de las consecuencias para con ellos de la omisión de respuesta; (iii) de las personas físicas o morales destinatarias de las informaciones; (iv) de la existencia de un derecho de acceso y de rectificación (L. 6 ene. 1978, art. 32). Por otro lado, tienen derecho a oponerse, por razones legítimas, a que estas informaciones nominales sean objeto de tratamiento (L. 6 ene. 1978, art. 38).

El candidato también debe ser informado de la identidad del responsable del tratamiento y de la finalidad del tratamiento al que están destinados estos datos (Dir. n° 95-46, 24 oct. 1995, art. 10). A este respecto, la Cnil propone dos recomendaciones:

(i) « (que) las personas encargadas del reclutamiento tomen todas las disposiciones necesarias para informar al candidato, en un plazo de tiempo razonable, del resultado de su candidatura, de la duración de conservación de las informaciones así como de la posibilidad de solicitar la restitución o la destrucción de estas informaciones";

(ii) « (que) la personas, cuyos datos estén registrados en un fichero de candidatos potenciales utilizado en el marco de una actividad por acercamiento directo sean informados sobre las disposiciones del artículo 27 de la ley del 6 de enero de 1978, como muy tarde en el momento del primer contrato. Cuando la identidad del empleador no haya sido precisada en la oferta de trabajo, habrá que recabar previamente el acuerdo del candidato antes de transmitir las informaciones nominales a este trabajador. En el caso de recogida de informaciones a través de conexiones a distancia, la Cnil recomienda que el candidato al empleo sea informado de la forma, personal o no, en la que las informaciones que relativas a su persona serán difundidas en línea o trasmitidas a los empleadores. El candidato también debe ser previamente informado de cualquier cesión de informaciones a otros organismos encargados de reclutar y poder oponerse a ello".

La Cnil recuerda también que "las informaciones recogidas sólo pueden ser utilizadas para la propuesta de empleo, sin ninguna otra finalidad, sobre todo de prospección comercial».

Por último, el candidato debe ser expresamente informado "previamente a su uso, de los métodos y técnicas de ayuda al reclutamiento utilizados para con él » (Cód. trab., art. L. 1221-8; anc. L. 121-7). A este respecto, la Cnil recomienda que « la información relativa a los métodos de ayuda al reclutamiento utilizadas se entreguen previamente por escrito a título individual o colectivo".

36.22
Derecho de acceso y de rectificación. Un candidato puede ejercer el derecho de acceso y de rectificación del que se beneficia cada persona sobre los datos que a ella se refieran, ya se trate de datos recogidos directamente de su persona o ante terceros o incluso de los datos procedentes de los métodos y técnicas de ayuda al reclutamiento. Así puede obtener la información relativa a su persona y exigir su rectificación en caso de que no sea exacta (L. 6 ene. 1978, art. 39). La Cnil recomienda pues que "todo candidato sea claramente informado de las modalidades de ejercicio del derecho de acceso y pueda obtener si lo solicita todas las informaciones relativas a su persona, incluidos los resultados de los análisis y de las pruebas o evaluaciones profesionales que haya hecho». Recomienda también que « la comunicación de las informaciones recogidas en la ficha del candidato se efectúe por escrito, pues la comunicación de los resultados e las pruebas o evaluaciones debe hacerse con los medios apropiados de acuerdo con la naturaleza de la herramienta utilizada.

SECCIÓN 3
MEDIDAS PARA PROTEGER AL CANDIDATO

36.31
Duración de conservación de los datos. Excepto autorización de la Cnil, los datos personales no pueden conservarse más allá de la duración indicada en la declaración del tratamiento (L. 6 ene. 1978, art. 36). La Cnil recomienda a este respecto que el candidato « sea informado de la duración durante la cual serán conservadas las informaciones relativas a su personas y del derecho que tiene de solicitar, en cualquier momento, su supresión. En todo caso, la duración de conservación de las informaciones no debería exceder dos años después del primer contacto con la persona en cuestión". Esta medida es la que se preconiza para cualquier candidato, sea cual sea el resultado del procedimiento de reclutamiento.

36.32
Seguridad y confidencialidad de los datos. El responsable del tratamiento automatizado de los datos relativos a los candidatos debe comprometerse ante los candidatos a tomar todas las medidas de seguridad y confidencialidad necesarias (L. 6 ene. 1978, art. 34). Las terceras partes en el procedimiento de reclutamiento no pueden pues tener acceso directa o indirectamente a los datos.

36.33
Perfiles automáticos. El candidato tiene derecho a ser informado del razonamiento utilizado en el tratamiento automatizado de ayuda a la selección de candidaturas (L. 6 ene. 1978, art. 22). Ahora bien, ninguna decisión de selección de candidatura que implique una apreciación sobre un comportamiento humano puede tener como único fundamento un tratamiento informatizado que presente una definición del perfil o de la personalidad del candidato (L. 6 ene. 1978, art. 10). Del mismo modo, la Cnil pide que se prohíban "las herramientas de evaluación automatizadas a distancia que excluyan cualquier apreciación humana».

36.34
Herramientas estadísticas de medición de las discriminaciones. La Cnil recomienda no recoger datos relativos al origen racial o étnico de los trabajadores o de los candidatos a un empleo y de no analizar la consonancia del apellido o del nombre. Por el contrario, pueden recoger y tratar datos como el apellido del candidato al empleo o del trabajador, su nombre, su nacionalidad, su nacionalidad de origen, su lugar de nacimiento, la nacionalidad o el lugar de nacimiento de sus padres, su dirección.

Por otro lado, la Cnil considera que el rechazo de una candidatura a un empleo o a un ascenso puede ser el resultado de la consideración simultánea de varios criterios no discriminatorios, por ejemplo una experiencia profesional. El factor discriminante puede pues resultar del análisis estadístico cruzado de estos

distintos criterios. Del mismo modo, cuando los cuestionarios contienen datos que permiten identificar a la persona de manera indirecta, la Cnil recomienda que el acceso al contenido se limite únicamente a las personas especialmente encargadas del estudio, que "los resultados sean presentados en forma de estadísticas autorizadas" de manera que se garantice el anonimato y que los cuestionarios sean destruidos una vez explotadas las respuestas. Cuando los cuestionarios integran un dato de identificación, la Cnil preconiza que se recurra a otros identificantes que los utilizados en el marco de la gestión de los recursos humanos (como el número de seguridad social sobre todo), la grabación de las respuestas en un fichero diferente de los ficheros de gestión de los recursos humanos así como el uso de un procedimiento de anonimización que prevea el borrado "no sólo de la identidad del candidato a un empleo, sino también su dirección, sus datos telefónicos y electrónicos, su fotografía, y cualquier otro dato que permita identificarle"

A este respecto, conviene sin embargo señalar la adopción por la Comisión de las leyes de la Asamblea nacional[84], de una enmienda al proyecto de ley relativo a control de la inmigración, la integración y el asilo. Esta enmienda, del 12 de septiembre de 2007, se inspira en las observaciones y recomendaciones[85] de la Cnil en materia de medidas de la diversidad. Pretenden proponer la modificación de la ley informática y libertadles para facilitar las búsquedas en materia de mediciones de la diversidad de los orígenes, de la discriminación y de la integración, al tiempo que mejoran la protección de los datos y el carácter científico de las encuestas. El texto sugiere sobre todo que los datos que muestren directa o indirectamente los orígenes raciales o étnicos de las personas puedan recabarse para las necesidades de estudio cuya finalidad sea "medir la diversidad de los orígenes de las personas, de la discriminación y de la integración", pero que estos tratamientos sean sometidos a la autorización de la Cnil y que las personas implicadas conserven su derecho de opción a este tratamiento.

[84] Informe de la Commission des lois, http://www.assemblee-nationale.fr/13/informes/r0160.asp.
[85] Cnil, recomend., 5 jul. 2005, para medir la diversidad de los orígenes en la lucha contra las discriminaciones, v. http://www.cnil.fr/index.php?id=1844.

CAPÍTULO

37. Reglas específicas para las organizaciones sindicales

SECCIÓN 0
ÍNDICE

37.00

Índice del capítulo.

37.01

Textos vigentes.

> Textos franceses. Ver s^{s} n^{o} 3.01: Cód. trab., art. L. 2142-6 — L. n^{o} 82-689, 4 ago. 1982, relativa a las libertades de los trabajadores en la empresa — L. n^{o} 2004-391, 4 may. 2004 relativa a la formación profesional permanente y al diálogo social, *JO* n^{o} 105, 5 may., 7983 — L. n^{o} 2008-67, 21 ene. 2008, que ratifica la disposición judicial n^{o} 2007-329 del 12 mar. 2007 relativa al Código de trabajo (parte legislativa), *JO* n^{o} 0018, 22 ene., 1122.

37.02

Jurisprudencia de referencia.

> Libertad de utilización de la mensajería y de Intranet según las condiciones del acuerdo de empresa

• **Soc. 25 ene. 2005,** n^{o} 02-30.946, Fédération des services CFDT et a. c/Sté Clear Channel France *Bull. civ.* V, n^{o} 19; *LPA* 8 mar. 2005, n^{o} 47, p. 3, nota A. Sauret et G. PicTA — confirmación del TA **París, sala 14ª, Sección B, 31 may. 2002**.

• **Soc. 22 ene. 2008,** n^{o} 06-40.514, M. M. c/Crédit industriel et commercial, *RDT* 2008, p. 324; *Sem. soc. Lamy* n^{o} 1339, 2008 — confirmación del TA **París, sala 18ª, Sección D, 29 nov. 2005**.

• **Crim. 10 may. 2005,** n^{o} 04-84705, *Bull. crim.,* n^{o} 144.

* Ver s^{s} n^{o} 37.11.

> Sobre la libertad de expresión sindical

• **CAA de Nancy, sala 3^{e}, 2 ago. 2007,** cne de Lons le Saunier c/Elisabeth M…, *RLDI* 2007, n^{o} 31 — anulación del **TA Besançon, sala 1ª 19 dic. 2006,** Elisabeh M… c/Ville de Lons-Le-Saunier, RG n^{o} 0400718.

* Ver s^{s} n^{o} 37.12.

• **Soc. 5 mar. 2008,** n^{o} 06-18.907, sté TNS Secodip c/féd. CGT des stés d'études, *Gaz. Pal.* 26 abr. 2008, n^{o} 117, http://www.courdecasación.fr/jurisprudence_publications_documentation_2/actualite_jurisprudence_21/chambre_sociale_576/arrets_577/br_arret_11274.html — sentencia del TA **París, sala 18ªciv., 15 jun. 2006,** Féd. CGT des stés d'études c/TNS Secodip, y después remitido al TA París.

Por la sentencia emitida (revocada) en 1ª instancia, v**. TGI Bobigny, 11 ene. 2005,** TNS Secodip c/Fédération CGT des Sociétés d'Etudes.

• **TA París, sala 18ª C, 15 jun. 2006,** Féd. CGT des stés d'études c/TNS Secodip, (prec.).

* Ver s^{s} n^{o} 37.14.

37.04

Preguntas principales.

• ¿Los sindicatos pueden contar con un sitio Internet especialmente previsto para ellos?

* Ver s^{s} n^{o} 37.11.

• ¿Cuáles son las condiciones de uso de un sitio así?

* Ver s^{s} n^{os} 37.13 s.

• ¿Qué garantías tienen los trabajadores de que los datos personales son utilizados por los sindicatos?

* Ver s^{s} n^{os} 37.21 s.

SECCIÓN 1
CONDICIONES DE USO DE INTERNET Y DE INTRANET

37.11

Un acuerdo de empresa obligatorio. En el Código de trabajo está previsto que "un acuerdo de empresa puede autorizar que se pongan a disposición las publicaciones y panfletos de naturaleza sindical, ya sea en un sitio sindical creado en el Intranet de la empresa, ya sea por difusión sobre la mensajería electrónica de la empresa. En este último caso, la difusión debe ser compatible con las exigencias de buen funcionamiento de la red informática de la empresa y no debe obstaculizar la realización del trabajo. El acuerdo de empresa define las modalidades de uso o de este modo de difusión, precisando sobre todo las condiciones de acceso de las organizaciones sindicales y las reglas técnicas destinadas a conservar la libertad de elección de los trabajadores de aceptar o de rechazar un mensaje» (Cód. trab., art. L. 2142-6 — L. n° 2004-391, 4 may. 2004 — L. n° 2008-67, 21 ene. 2008).

Las organizaciones sindicales pueden pues acceder a Intranet, sobre todo para crear un blog sindical accesible a todos dentro de la empresa, y a la mensajería de la empresa con la condición no obstante de haber negociado y concluido previamente un acuerdo de empresa.

A falta de acuerdo de empresa, la jurisprudencia se pronuncia por la prohibición de la difusión – lo que confirma la sentencia del 25 de enero de 2005[86] pronunciada por el Tribunal de Casación. En este caso, el sindicato había enviado a la dirección electrónica profesional de todos los trabajadores un correo electrónico sindical. No había ni acuerdo de empresa, ni siquiera autorización del empleador.

Por otro lado, en presencia de un acuerdo de empresa, el Tribunal de Casación lo aplica estrictamente. En una sentencia del 22 de enero de 2008 considera que el acuerdo de empresa subordinaba la facultad de uso de la mensajería electrónica para la publicación de informaciones sindicales a la existencia de un vínculo entre el contenido y la situación social existente en la empresa, y que tal no era el caso en cuestión (Soc. 22 ene. 2008[87]).

No obstante, observamos que el texto no se refiere al acceso a estos medios informáticos por las instancias representativas del personal, sobre todo el comité de empresa o incluso los delegados de personal.

37.12

El derecho sindical es una libertad fundamental. Esta regla, enunciada por el tribunal administrativo de Besançon, el 19 de diciembre de 2006, precisa que nadie puede aportar "restricciones que no estuvieran justificadas por la naturaleza de la tarea por hacer y que no estén en proporción con el objetivo buscado[88]. Consideró que el alcalde del ayuntamiento de Lons-Le-Saunier no podía sancionar a uno de sus trabajadores, adjunto administrativo de los servicios de la ciudad y responsable sindical, que había hecho un llamamiento a manifestarse utilizando las mensajerías Intranet e Internet de la ciudad y rechazó el argumento del alcalde que pretendía hacer valer que esta empleada no había cumplido con sus obligaciones profesionales al no respetar la prohibición de utilizar la mensajería con fines personales.

Pero al proceder a un análisis diferente del contenido del correo electrónico en litigio, el Tribunal administrativo de Apelación de Nancy estimó, en su decisión del 2 ago. 2007[89], i.e. que se trataba de un mensaje de naturaleza política. En estas condiciones, consideró que el alcalde de Lons-le-Saunier había dictado

---

[86] Soc. 25 ene. 2005, n° 02-30.946, *Bull. civ.* V, n° 19.

[87] Soc. 22 ene. 2008, n° 06-40.514, *Sem. soc. Lamy* n° 1339, 2008.

[88] TA Besançon, sala 1ª 19 dic. 2006, Elisabeh M… c/Ville de Lons-Le-Saunier, v. http://www.legalis.net/jurisprudence-decision.php3?id_article=1818.

[89] CAA Nancy, 3e ch., 2 ago. 2007, cne de Lons le Saunier c/Elisabeth M…, *RLDI* 2007, n° 31.

legalmente una sanción contra su trabajador sindicalista en la medida en que una nota de servicio del 18 de noviembre de 2003 prohibía al personal el uso de Internet con fines políticos. .

37.13

Respeto del principio de finalidad. La finalidad de trato debe ser estrictamente respetada. Así, si el acuerdo de empresa autoriza la difusión de informaciones sindicales por vía electrónica, las direcciones de mensajería electrónica de los trabajadores no pueden utilizarse solamente para difundir publicaciones y panfletos de naturaleza sindical.

37.14

Respeto de los derechos de los demás. La cuestión de los límites que se ponen a la libertad de comunicación sindical a partir de un sitio exterior a la empresa quedó zanjada por la cámara social del Tribunal de Casación el 5 de marzo de 2008[90].

En este caso, un sindicato había publicado en su sitio algunas informaciones confidenciales de la empresa: dos dictámenes de un gabinete de expertos contables sobre las cuentas de la empresa, varias actas de las negociaciones contractuales, de las reuniones del comité de empresa y algunas preguntas presentadas por los delegados de personal. La empresa, considerando que esta difusión la perjudicaba, se dirigió al Tribunal de gran instancia de Bobigny para obtener que se suprimieran estos documentos.

Los jueces de primera instancia dieron la razón a la demanda, considerando que los cuatro documentos contenían informaciones confidenciales no tenían que ponerse al alcance de terceros y de la competencia y que la obligación de discreción y de confidencialidad del trabajador se imponía también a los "sindicatos que representan a los trabajadores en el seno de una empresa» (TGI Bobigny, 11 ene. 2005[91]).

Este análisis fue invalidado por el Tribunal de Apelación, en su sentencia del 15 de junio de 2006 quien retuvo que "como cualquier ciudadano, un sindicato tiene margen para crear un sitio Internet para ejercer su derecho de expresión directa y colectiva, que no se podría presentar restricción alguna al ejercicio de este derecho y que ninguna obligación legal o de confidencialidad pesa sobre los miembros del sindicato, excepto la que pesa en virtud del artículo L. 432-7, párrafo 2 del Código de trabajo sobre los miembros del comité de empresa o representantes sindicales, aun cuando pueda haber identidad de personas entre ellos»[92].

El Tribunal de Casación, ante el recurso presentado, censuró a su vez al Tribunal de Apelación pues "si un sindicato tiene derecho a comunicar libremente las informaciones al público en un sitio Internet, esta libertad puede estar limitada en la medida en que sea necesario para evitar que la divulgación de informaciones confidenciales sea un atentado contra los derechos de terceros". La Alta jurisdicción se basó en el artículo 10-2 de la Convención Europea para la protección de los derechos humanos y de las libertades fundamentales (CESDH) que prevé expresamente que la libertad de expresión puede estar sometida a ciertas condiciones y restricciones previstas por la ley, que son medidas

---

[90] Soc. 5 mar. 2008, nº 06-18.907, sté TNS Secodip c/féd. CGT des stés d'études: casación arrêt TA París, 15 jun. 2006 (renvoi devant la TA París), http://www.courdecasación.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 abr. 2008, nº 117.

[91] TGI Bobigny, 11 ene. 2005, TNS Secodip c/Féd. CGT des stés d'études, *Gaz. Pal.* 20 jul. 2005, nº 101, p. 45-46; *Expertises* abr. 2005, p. 156 — para un análisis crítico de esta decisión, v. G. Haas et O. de Tissot, « Des restrictions inacceptables à la liberté d'action des syndicats », *Expertises* abr. 2005, p. 145.

[92] TA París, sala 18ª C, 15 jun. 2006, Féd. CGT des stés d'études c/TNS Secodip, http://www.courdecasación.fr/jurisprudence_publications_documentation_2/actualite_jurisprudence_21/chambre_sociale_576/arrets_577/br_arret_11274.html.

necesarias para proteger los derechos de terceros así como su reputación. También se basó en la ley para la confianza en la economía digital, que prevé que el ejercicio de la libertad de comunicación por vía electrónica puede limitarse en la medida necesaria, sobre todo el marco del respeto de la libertad y de la propiedad de terceros.

Con anterioridad, la cámara criminal del Tribunal de Casación también sancionó los propósitos publicados en el sitio de un sindicato al cuestionarse de manera injuriosa a un director de la empresa, en unos términos considerados como "que superaban el temple admisible en un marco semejante» (Crim. 10 may. 2005[93]).

SECCIÓN 2
REGLAS PARA PROTEGER AL TRABAJADOR

37.21

Derecho de oposición de los trabajadores. Los trabajadores deben poder ejercer su derecho de opción al envío de cualquier mensaje sindical en su mensajería profesional. A tal efecto deben ser informados previamente del acuerdo concluido y de las modalidades del ejercicio de su derecho de oposición. Deben poder ejercer este derecho en cualquier momento y, a este respecto, este derecho les debe ser recordado en cada mensaje. Por otro lado, la Cnil preconiza prever la indicación del carácter sindical del mensaje para favorecer así una mayor transparencia en cuanto al origen y a la naturaleza del mensaje.

37.22

Garantía de confidencialidad. Los intercambios electrónicos entre los trabajadores y las organizaciones sindicales son confidenciales. A este respecto, la Cnil considera que "para evitar cualquier posibilidad de uso no conforme, el trabajador no debería poder ejercer control alguno en las listas de difusión así creadas. En efecto, estas son susceptibles de revelar la opinión favorable de un trabajador con respecto a una organización, incluso su pertenencia a un sindicato determinado, sobre la base de una decisión tomada por este trabajador en cuanto a su aceptación o rechazo de recibir mensajes con carácter sindical »[94].

---

[93] Crim. 10 may. 2005, nº 04-84.705, *Bull. crim.,* nº 144.

[94] Cnil, *Guide pratique pour les employeurs,* p. 28.

CAPÍTULO

38. Reglas y usos vigentes en el extranjero

SECCIÓN 0
ÍNDICE

38.00

Índice del capítulo.

SECCIÓN 1
A NIVEL EUROPEO

38.11

Tribunal europeo de Derecho Humanos. El principio de protección de la vida privada del trabajador en su lugar de trabajo ha sido declarado en varias ocasiones por el Tribunal europeo de derechos humanos[95]: « Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia» (Conv. EDH, art. 8). Aunque no siempre se comprenda de la misma manera, el mismo espíritu se refleja en la carta del Convenio Europeo para la protección de los derechos humanos y las libertades fundamentales (CESDH). La preocupación es siempre la misma: la búsqueda de un compromiso entre el poder de control del empleador sobre la actividad de sus trabajadores y el respeto de su vida privada. Varios textos formalizan, a nivel europeo e internacional, la obligación de información previa del trabajador.

38.12

Recomendación n° R (89). La recomendación n° R (89) del Comité de ministros del Consejo de Europa a los Estados miembros sobre protección de datos personales utilizados a efectos de empleo de 18 de enero de 1989 « 3. Información y consulta de los trabajadores

3.1. De conformidad con la legislación y la práctica nacionales y, llegado el caso, los convenios colectivos, los empleadores deberían informar o consultar a sus trabajadores o a los representantes de estos últimos antes de introducir o modificar sistemas automatizados para recoger y utilizar datos personales sobre los trabajadores. Este principio también se aplica a la introducción o modificación de procesos técnicos destinados a controlar los movimientos o la productividad de los trabajadores.

3.2. Debería buscarse el acuerdo de los trabajadores o de sus representantes antes de introducir o modificar tales sistemas o procesos cuando el procedimiento de consulta mencionado en el párrafo 3.1. revela la posibilidad de un atentado

---

[95] Not. CEDH, 16 dic. 1992, caso Niemietz c/Allemagne, req. n° 00013710/88, A-251 B § 29, *JDI* 1993, p. 755, obs. E. Decaux et P. Tavernier; *D.* 1993, somm. 386, obs. J.-F. Renucci.

contra la vida privada y la dignidad humana de los trabajadores, a menos que haya otras garantías previstas en la legislación o la práctica nacionales».

38.13
Repertorio de recomendaciones prácticas sobre la protección de datos personales de los trabajadores de la Organización Mundial del Trabajo con fecha de 7 de octubre de 1996. Este documento prevé sobre todo que: "Los datos personales reunidos en función de disposiciones técnicas o de organización que tengan por objeto garantizar la seguridad y el buen funcionamiento de los sistemas automatizados de información no deberían servir para controlar el comportamiento de los trabajadores" (punto 5.4)

Ahora bien, este repertorio prevé que puede recurrirse a la vigilancia electrónica en ciertas condiciones: por un lado, los datos recabados no deben ser la única fuente de evaluación del trabajador; por otro lado, si se utilizan medidas de vigilancia, los trabajadores deberían ser informados de antemano de las razones que las motivan, de las horas en las que se aplican, de los métodos y técnicas utilizados y de los datos que serán recabados (punto 6 del repertorio). Se indica pues que la vigilancia continua sólo debería permitirse si lo requieren la salud, la seguridad y la protección de los bienes de la empresa. También se indica que el secreto en materia de vigilancia sólo debería permitirse cuando se realice de conformidad con la legislación nacional o si existen sospechas suficientes de actividad delictiva u otras infracciones graves, apartado en el que hay que incluir también el acoso sexual.

38.14
Dictamen del 29 may. 2002 del G 29. También hay que mencionar el dictamen presentado el 29 de mayo de 2002 por el G 29 (v. s^{s} n^{o} 15.18). Este dictamen, dedicado a la "vigilancia de las comunicaciones electrónicas en el lugar de trabajo[96]," parece ampliamente inspirado de los trabajos y reflexiones de la Commission nationale de l'informatique et des libertés (Cnil).

SECCIÓN 2
PARTICULARIDADES NACIONALES

38.21
Estados Unidos. El tema delicado de la cibervigilancia no se ve de la misma manera en Estados Unidos, donde al empleador se le suele reconocer el derecho de conocer la mensajería de sus trabajadores. Los últimos sondeos[97] indican en efecto que el 46,5 % de las empresas examinan y almacenan el contenido de los correos electrónicos de sus trabajadores. En efecto, si el secreto de correspondencia está protegido por el *Electronic Communications Privacy Act of 1986*[98] (18 USC §§ 2510 s.), el empleador puede vigilar la red de la empresa lo que, concretamente, le da derecho a escuchar legalmente las conversaciones telefónicas de sus trabajadores, o consultar sus correos electrónicos, incluso si las derogaciones sólo se dan en caso de necesidad para la empresa y a reserva de que el trabajador haya sido previamente avisado de que está vigilado.

38.22
Reino Unido. La autoridad que se encarga de la protección de los datos personales, el *Information Commissioner*, publicó un código de protección de los datos personales y de las prácticas relativas al empleo[99]. Este marca las condiciones en las que el empleador puede vigilar a sus trabajadores. Basándose

---

[96] G 29, dictamen, 29 may. 2002,
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_fr.pdf
[97] Sondeo realizado por el ePolicy 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.

en las disposiciones del *Data Protection Act of 1998* (c. 29)[100] este código "subordina" la vigilancia de los trabajadores en el lugar de trabajo a dos principios: la transparencia y la proporcionalidad. Del mismo modo, el empleador tiene no sólo que prevenir a los trabajadores de las medidas de vigilancia vigentes, sino que también debe eliminar todas las informaciones personales "inútiles o excesivas" teniendo en cuenta la relación de trabajo que les une.

[100] http://www.opsi.gov.uk/Acts/Acts1998/ukpga_19980029_en_1.