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

3. Die Cyber-Überwachung am Arbeitsplatz

Veröffentlicht mit der finanziellen Unterstützung der Europäischen Kommission

ABSCHNITT 0
ZUR ORIENTIERUNG

3.00

Plan des Titels.

3.01

Anwendbare Texte.

> Französische Texte.

C. trav., not. art. L. 1121-1, L. 1221-6, L. 2323-13, L. 2323-32 — C. pén., not. art. 226-15, 226-24 et 432-9 — L. n° 78-17, 6 janv. 1978, relative à l'informatique et aux libertés — L. n° 2004-801, 6 août 2004, relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978.

3.03

Auswahlbibliographie.

> Berichte und Leitfaden.

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

> Werke.

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-Malmaison, 2001 ; *Droit du travail – Droit vivant,* 15e éd., Éd. Liaisons, août 2006.

> Kolloquium.

Mardi de l'ADIJ (C. Baudoin), « Droit du travail et nouvelles technologies : actualités législatives et jurisprudentielles », compte-rendu J.-B. Auroux, *RLDI* n° 14, mars 2006, p. 83 ; compte-rendu L. Teyssandier, *Lexbase* N5659AKS

> Artikel.

Sonderausgabe der Zeitschrift *Dr. social,* « Le droit du travail à l'épreuve des NTIC », Januar 2002.

KAPITEL

31. Kontrolle des Arbeitgebers über die Arbeitsmittel

ABSCHNITT 0
ZUR ORIENTIERUNG

31.00

Plan des Kapitels.

Abschnitt 1 Überwachungsmöglichkeiten des Arbeitgebers

Abschnitt 2 Loyalitätspflicht des Arbeitnehmers

Abschnitt 3 Verantwortlichkeiten

31.01

Anwendbare Texte.

> Französische Texte.

* s. Nr. 03.01.

L. n° 2004-575, 21 juin 2004, pour la confiance dans l'économie numérique — L. n° 82-689, 4 août 1982, relative aux libertés des travailleurs dans l'entreprise, *JO* 6 août, 2518.

31.02

Relevante Rechtssprechung.

> Bezüglich der allgemeinen Loyalitätspflicht des Arbeitnehmers.

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

* s. Nr. 31.21.

> Zu der Verwendung von Passwörtern am PC-Arbeitsplatz

• **Soc. 6 févr. 2001,** n° 98-46.345, Sté Laboratoires pharmaceutiques Dentoria c/Mme Bardagiet et a., *Bull. civ.* V, n° 43 ; *JCP G* 25 juill. 2001, n° 30, p. 1514, note C. Puigelier ; *RTD civ.* oct.-déc. 2001, n° 4, 880-882, note J. Mestre et B. Fages — aufgehoben durch **CA Toulouse, 4e ch. soc., 23 oct. 1998.**

• **Soc. 18 oct. 2006,** n° 04-48.025, Jérémy L… c/Sté Techni-Soft, *Bull. civ.,* n° 308 ; *CCE* janv. 2007, note E. Caprioli, p. 40 s. — bestätigt durch **CA Rennes, ch. soc., 21 oct. 2004.**

* s. Nr. 31.24, auch Nr. 33.22 und 35.21.

> Zu der missbräuchlichen Verwendung der Arbeitsmittel.

• **Soc. 10 oct. 2007,** n° 06-03.007, Claude G… c/Assoc. Ogec Emmanuel d'Alzon — bestätigt durch **CA Montpellier, ch. soc., 17 mai 2006,** Claude G… c/Assoc. Ogec Emmanuel d'Alzon, http://www.legalis.net/jurisprudence-decision.php3?id_article=2066 (Besuch pornographischer Websites).

• Für das (bestätigte) Urteil in erster Instanz s. **Cons. prud'h. Montpellier, 26 sept. 2005,** Claude G… c/Assoc. Ogec Emmanuel d'Alzon.

* s. Nr. 31.23, auch Nr. 32.24.

• **Soc. 14 mars 2000,** n° 1270, n° 98-42.090, M. Dujardin c/Sté Instinet France *Bull. civ.* V, n° 101 ; *Gaz. Pal.* 28 oct. 2000, n° 302, p. 34, note J. Berenguer-Guillon et L. Guignot ; *JCP G* 7 févr. 2001, n° 6, p. 325, note C. Puigelier ; *LPA* 11 juill. 2000, n° 137, p. 5, note G. Picca et A. Sauret — bestätigt durch **CA Paris, 18e ch., sect. A, 16 févr. 1998,** n° 020563.

• Für das (teilweise aufgehobene) Urteil in erster Instanz s. **Cons. prud'h. Paris, 2e ch., sect. Encadrement, 13 déc. 1995.**

* s. Nr. 31.22, auch Nr. 32,11 und 30.23.

• **Soc. 11 mars 1998,** n° 96-40.147, NPB, *RJS* 4/1998, n° 415 — bestätigt durch **CA Paris, 21e ch., sect. C, 7 nov. 1995.**

* s. Nr. 31.12, auch Nr. 32.24 (missbräuchliche Nutzung des Telefons).

• **CA Aix-en-Provence, 1re ch. A, 25 nov. 2003,** n° 2003/798.

* s. Nr. 31.21.

> Bezüglich der Verantwortlichkeit des Arbeitgebers.

• **Ass. plén. 19 mai 1988,** n° 87-82.654, Cie d'assurance « La Cité », *Bull. civ.,* n° 5 ; *RTD civ.* 1989, 89, obs. P. Jourdain — bestätigt durch **CA Lyon, 24 mars 1987.**

* s. Nr. 31.32.

• **Civ. 2e, 19 juin 2003,** n° 00-22.626, AGV Vie et a. c/ Cts X… et a., *Bull. civ*. II, n° 202 ; *D.* 2003, 1808 — aufgehoben

durch **CA Lyon, 6e ch. civ., 18 oct. 2000.**

* s. Nr. 31.23.

• CA Aix-en-Provence, 2e ch., 13 mars 2006, SA Lucent Technologies c/ SA Lycos France, M. Nicolas B… — bestätigt durch **TGI Marseille, 11 juin 2003,** RG n° 01/390.

* s. Nr. 31.33.

31.03

Auswahlbibliographie.

> Berichte und Leitfaden.

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

> Artikel.

J.-B. Auroux, « Les mardis de l'ADIJ : droit du travail et nouvelles technologies : actualités législative et jurisprudentielle », *RLDI* mars 2006 n° 14, p. 83 ; v. aussi compte-rendu 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 août-15 sept. 2005, p. 52 s. — G. Haas et O. de Tissot, « Des restrictions inacceptables à la liberté d'action des syndicats », *Expertises* avr. 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* janv. 2007, n° 23, p. 69 s. — A. Saint Martin, « Contrôle des messages électroniques du salarié et mesures d'instruction in futurum », *RLDI* juin 2007, n° 28 ; « Une présomption de professionnalité des messages électroniques du salarié ? », *RLDI* mai 2007, n° 27 — Étudiants du Master 2 de droit du multimédia et de l'informatique de l'Université de Paris II dirigé par le professeur J. Huet, « Le blog : nouvelle arme des salariés », *RLDI* n° 27, mai 2007, p. 90 s.

31.04

Grundsätzliche Fragen.

• Unter welchen Bedingungen kann der Arbeitgeber die Nutzungsbedingungen des Internetzugangs in seinem Unternehmen eingrenzen?

* s. Nr. 31.12.

• Inwiefern ist der Arbeitnehmer bei der Nutzung des Internets am Arbeitsplatz verantwortlich?

* s. Nr. 31.21.

• Kann der Arbeitgeber für die Verbreitung rechtswidriger Inhalte durch einen Arbeitnehmer zur Verantwortung gezogen werden?

* s. Nr. 31.32.

31.09

Der Internetzugang ist ein Arbeitsmittel. Der Internetzugang, insbesondere die E-Mailbox, ist zu einem ebenso wichtigen Arbeitsmittel wie das Telefon geworden. In der Tat wird er bei der Ausübung der beruflichen Tätigkeit der meisten Arbeitnehmer immer nützlicher, ja sogar unverzichtbar.

Nun verfügt der Arbeitgeber bei diesem Arbeitsmittel jedoch über technische Kontrollmöglichkeiten, die es ihm erlauben, die E-Mails seines Arbeitnehmers abzufangen und Kenntnis über die Empfänger dieser Nachrichten, den Betreff der Nachricht, die Art und den Inhalt der Dateianhänge, besuchte Websites und Foren, an denen er teilnimmt, zu erlangen. Er kann zum Beispiel herausfinden, ob seine Angestellten das Internet zu beruflichen oder privaten Zwecken nutzen, wie viel Zeit sie im Internet verbringen und wann sie surfen. Wie bei den Telefon-Selbstwählanlagen[1] kann die automatische Speicherung von E-Mail-Adressen und Websites ermöglichen, ein Profil des Arbeitnehmers zu erstellen und somit Informationen über sein Privatleben zu sammeln (Zugehörigkeit zu einer Gewerkschaft oder politischen Gruppierung, Interesse für Pornographie, revisionistische Ansichten, usw.) Diese Möglichkeiten erlauben die Überwachung der Arbeitnehmer, die Verfolgung ihrer „Spuren" mittels der per Internet versandten oder erhaltenen Daten, was von der französischen Datenschutzbehörde – der Nationalen Kommission für Information und Rechte

[1] Siehe auch Cnil, 5e Rapport d'activité, p. 109 und 15e Rapport d'activité, p. 74, Doc. fr.

(*Commission nationale de l'information et des libertés* – Cnil) bereits in ihrem Bericht von 2001 über die Cyber-Überwachung der Arbeitnehmer durch die Arbeitgeber kritisiert wurde[2] .

Dies wirft unvermeidbar die Frage nach dem Schutz der Grundfreiheiten des Arbeitnehmers – zu diesem Thema hat die Cnil eine Reihe von Empfehlungen über die Cyber-Überwachung in Untenehmen abgegeben – und die nicht weniger schwierige Frage nach den Grenzen der Rechte des Arbeitnehmers auf.

ABSCHNITT 1
ÜBERWACHUNGSMÖGLICHKEITEN DES ARBEITGEBERS

31.11

Duldung der privaten Nutzung der Arbeitsmittel. Der Internetzugang und die E-Mailbox, ein Telefonanschluss sind Mittel, die dem Arbeitnehmer zur Verfügung gestellt werden, damit er seine Arbeit ausführen kann. Auch wenn die Benutzung dieser Mittel – zum Beispiel des Telefons - zu privaten Zwecken geduldet wird, ist doch alles eine Frage des Ausmaßes. Was würde man sagen, wenn von 100 ausgetauschten E-Mails pro Tag 75 % der privaten Kommunikation dienten? Ob es sich um private E-Mails oder das Surfen im Internet zu privaten Zwecken handelt, erleidet der Arbeitgeber in der Tat Verluste durch die Verkürzung der Arbeitszeit sowie durch die damit verbundenen Ausgaben, insbesondere die Verbindungskosten. So soll eine Umfrage ergeben haben, dass 20 bis 50 % der am Arbeitsplatz im Internet verbrachten Zeit nichts mit der Arbeit zu tun hat.

31.12

Regelung der Nutzungsbedingungen der Arbeitsmittel. In diesem Zusammenhang scheint es legitim, dass sich ein Arbeitgeber vergewissert, dass seine Arbeitnehmer die ihnen zur Verfügung gestellten Arbeitsmittel nicht missbräuchlich verwenden. Er muss dabei jedoch mit absoluter Transparenz und "verhältnismäßig" [3].vorgehen. Im Sinne der von der Cnil aufgestellten Prinzipen und der Empfehlungen des *Forum des droits sur internet* (Forum der Rechte des Internets) [4] geht es darum, das richtige Gleichgewicht zwischen den Kontrollbefugnissen des Arbeitgebers und dem Schutz der Grundfreiheiten des Arbeitnehmers zu suchen.

In ihrem am 18. Dezember 2003 geänderten Bericht „*La Cybersurveillance sur les lieux de travail"* (Cyber-Überwachung am Arbeitsplatz) beobachtet die Cnil, dass wenn ein allgemeines und absolutes Verbot jeglicher Nutzung des Internets durch Arbeitnehmer zu anderen Zwecken als beruflichen in einer Informations- und Kommunikationsgesellschaft nicht realistisch erscheint und darüber hinaus hinsichtlich der anzuwendenden Texte unverhältnismäßig erscheint, eine vernünftige Nutzung, durch die die Zugangsbedingungen ins Internet zu beruflichen Zwecken nicht beeinträchtigt wird und die Arbeitsleistung nicht mindert allgemein und gesellschaftlich in den meisten Untenehmen oder Behörden gestattet ist. Trotzdem ist die Cnil der Meinung, dass diese gestattete Nutzung der Arbeitsmittel Computer und Internet durch einen Arbeitnehmer zu privaten Zwecken Bedingungen oder Beschränkungen unterliegen kann, die durch den Arbeitgeber festgelegt werden. So empfiehlt die Cnil zusätzlich zu einer Firewall die Verwendung von Filtern für nicht zugelassene Websites sowie einer nachträglichen globalen Kontrolle der Internet-Verbindungsdaten (z. B. auf Unternehmens- bzw. Behördenebene oder Abteilungsebene) ohne, dass es zu einer individuellen Kontrolle der von einem bestimmten Arbeitnehmer besuchten Websites kommt. In anderen Worten, der Arbeitgeber ist berechtigt, die Bedingungen der privaten Nutzung des Internets und der E-Mailbox zu regeln. Er

---

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

[3] Soc. 11 mars 1998, n° 1375, *RJS* 4/1998, n° 415.

[4] FDI, *Relations du travail et internet,* rapp. du FDI, 17 sept. 2002, http://www.foruminternet.org/recommandations/lire.phtml?id=394.

kann den Zugang zu sittenwidrigen Websites (mit pornographische oder pädophilen Inhalten, Anstachelung zum Rassismus, usw.) oder das Herunterladen von Programmen, die Teilnahme an Foren oder Chats und das Einloggen in private E-Mailboxen wegen des Risikos der Verbreitung von Viren verbieten. Wenn eine solche Kontrolle jedoch detailliert für jeden einzelnen Computerarbeitsplatz durch den Arbeitgeber durchgeführt wird, unterliegt diese Maßnahme der Erklärungspflicht bei der Cnil.

ABSCHNITT 2
LOYALITÄTSPFLICHT DES ARBEITNEHMERS

31.21

Allgemeine Loyalitätspflicht. Nachdem die Richter in einer ersten Zeit zugunsten der Arbeitnehmer entschieden, erinnern sie immer öfter daran, dass der Arbeitgeber ein legitimes Recht hat, vom Arbeitnehmer zu erwarten, dass er seinen Arbeitsvertrag unter Einhaltung der allgemeinen Loyalitätspflicht ausübt.[5]

Ein Urteil des Berufungsgerichts (*cour d'appel*) von Aix-en-Provence vom 25. November 2003[6] hebt in diesem Zusammenhang hervor, dass die Gesamtheit der nationalen oder internationalen Texte zum Schutz des Privatlebens der Arbeitnehmer an ihrem Arbeitsplatz keine Zone schaffen darf, in der Fehler des Arbeitnehmers gegenüber seinem eigenen Arbeitgeber oder Dritten immun oder straffrei bleiben.

31.22

Spielen am Arbeitsplatz. Der Kassationsgerichtshof (*Cour de cassation*) stellt in einem Urteil vom 14. März 2000 fest[7], dass spielen am Arbeitsplatz "illegal" ist[8]. Dabei wurde einem Arbeitgeber Recht gegeben, der seinen Arbeitnehmer wegen groben Verstoßes *(faute grave)* entlassen hatte, weil er während seiner Arbeitszeit und mit den Arbeitsmitteln des Unternehmens mit Dritten gespielt hatte (dabei ging es u.a. um Sportwetten).

31.23

Pornographische Websites. Ebenso kann der Besuch pornographischer Websites durch einen Arbeitnehmer von seinem Arbeitsplatz aus und während seiner Arbeitszeit zur Entlassung führen, wie es ein Urteil vom 10. Oktober 2007[9] der Sozialkammer des Kassationsgerichtshofs (*chambre sociale de la Cour de cassation*) zeigt (Ablehnung des Rechtsmittels durch CA Montpellier, 17. Mai 2006).

31.24

Sicherheitsmaßnahmen. Die Cnil erinnert, dass der dem Arbeitnehmer zur Verfügung gestellte PC durch ein Passwort oder Login geschützt werden kann, aber dass diese Sicherheitsmaßnahme dafür bestimmt ist, einen Missbrauch durch Dritte zu verhindern und nicht dazu dient, den Firmencomputer zum Privatcomputer zu machen. In diesem Zusammenhang muss der Arbeitnehmer, der als einziger das Passwort kennt, auf Anfrage des Arbeitgebers die materiellen Voraussetzungen in den vorigen Stand zurückversetzen und die Informationen mitteilen, über die er verfügt und die nötig sind, um das Geschäft des

---

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

[6] CA Aix-en-Provence, 1re ch. A, 25 nov. 2003, no 2003/798.

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

[8] F. Lemaître, « Jouer sur le lieu de travail est illégal, estiment les juges », Zeitungsartikel in *Le Monde* vom 28. März 2000.

[9] Soc. 10 oct. 2007, no 06-43.816, Ablehnung des Rechtsmittels CA Montpellier, 17 mai 2006, v. http://www.legalis.net/jurisprudence-decision.php3?id_article=2065.

Unternehmens weiterzuführen.[10].

Ebenso ist der Kassationsgerichthof bei der Verwendung von kryptologischen Mitteln der Meinung, dass ein Arbeitnehmer, der ohne Erlaubnis seines Arbeitgebers den Zugang zu den Daten auf seinem PC willentlich verschlüsselt, einen groben Verstoß *(faute grave)* begeht[11].

ABSCHNITT 3
VERANTWORTLICHKEITEN

31.31

Verantwortlichkeit des Arbeitnehmers in der Ausübung seiner Meinungsfreiheit. Der Arbeitnehmer hat das Recht, seine Meinung innerhalb und außerhalb seines Unternehmens zu äußern, wie es das Gesetz vom 4. August 1982 erinnert, das ihm ein Recht auf direkte und kollektive Äußerung über den Inhalt, die Ausübungsbedingungen und die Organisation der Arbeit zuerkennt (über die allgemeinen Prinzipien für den Respekt des Privatlebens des Arbeitnehmers s. Nr. 34.00 f).

Die Rechtssprechung erinnert jedoch daran, dass sich aus diesem Prinzip die Verantwortung jener ergibt, die es anwenden. Auch wenn es richtig ist, dass die sich aus dem Arbeitsvertrag ergebende untergeordnete Stellung, nicht zur Folge hat, dem Arbeitnehmer seine zu seiner Person gehörenden Grundrechte abzuerkennen, insbesondere seine Rechte auf Meinungs- und Gewissensfreiheit und freie Meinungsäußerung, so legt ihm doch die loyale Ausführung des Arbeitsvertrags die Verpflichtung zur Diskretion sowohl gegenüber Dritten als auch gegenüber anderen Arbeitnehmern seines Unternehmens auf[12]. So muss ein Arbeitnehmer, der von seinem Recht auf freie Meinungsäußerung Gebrauch macht, dies auf eine Art tun, die nicht zu einem Missbrauch dieses Rechts führt, wie bei der Verleumdung oder der üblen Nachrede.

Diese Rechtsprechung ermöglicht es die Nutzungsbedingungen von elektronischen Möglichkeiten des Abreagierens abzugrenzen[13] die immer üblicher werden, entweder im Rahmen von Foren, die zu diesem Zweck vom Arbeitgeber eingerichtet werden oder im Rahmen von Websites oder Foren, die auf Initiative eines Arbeitnehmers oder einer Gruppe von Arbeitnehmern eingerichtet werden.

Darüber hinaus muss präzisiert werden, dass der Grundsatz der Diskretion ebenso für Arbeitnehmervertreter gilt (zu den Grenzen der gewerkschaftlichen Kommunikationsfreiheit s. Nr. 37.14).

31.32

Verantwortlichkeit des Arbeitgebers bei gewissen Vergehen von Arbeitnehmern. Artikel 1384 Absatz 5 des französischen Zivilgesetzbuchs (*Code civil*) legt ein Prinzip der Haftung des Arbeitgebers für Fehler, die einer seiner Arbeitnehmer im Rahmen seiner beruflichen Tätigkeit begangen hat, fest. Man nennt dies die Haftung des Geschäftsherrn für den durch seine Erfüllungsgehilfen verursachten Schaden („*la responsabilité du commetant du fait de des préposés*").

Die Verbindung zwischen dem Fehler des Arbeitnehmers und seiner beruflichen Funktion wird von der Rechtssprechung in Abhängigkeit des rechtlichen Zusammenhangs zwischen dem Fehler und der Ausübung seines Arbeitsvertrags bewertet. Dieser Zusammenhang wird im Allgemeinen als gegeben angesehen, wenn der Fehler von dem Arbeitnehmer während der Arbeitszeit, am Arbeitsplatz, mit den vom Arbeitgeber zur Verfügung gestellten Mittel, durch die Durchführung der Anweisungen des Arbeitgebers oder auch mit der Absicht, für den Arbeitgeber zu handeln, begangen wird. Die Rechtssprechung nimmt die Haftung des

---

[10] Soc. 6 févr. 2001, n° 98-46.345, *Bull. civ.* V, n° 43 ; *JCP G* 25 juill. 2001, n° 30, p. 1514, note C. Puigelier ; *RTD civ.* oct.-déc. 2001, n° 4, p. 880-882, note J. Mestre et B. Fages.

[11] Soc. 18 oct. 2006, *CCE* janv. 2007, note E. Caprioli, p. 40 s.

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

[13] Artikel von M.-J. Gros et L. Lamprière, « J'irai cracher sur ma boîte », kostenpflichtige Archive der Zeitung Libération.

Arbeitgebers auch für einen in seinem Auftrag von einem seiner Arbeitnehmer außerhalb der Arbeitszeit und des Arbeitsplatzes begangenen Fehler an, ob dieser mit privaten Mitteln begangen wurde, oder nicht, wenn diese Tätigkeit als im Zusammenhang mit seiner beruflichen Tätigkeit stehend angesehen werden kann. Wenn die frühere Rechtssprechung sich weigerte, den Arbeitgeber für einen mit einem Arbeitsmittel verursachten Schaden haftbar zu machen, wenn der Schaden außerhalb des Arbeitsplatzes und der Arbeitszeit verursacht wurde, so ist die Abgrenzung nun unklarer geworden und viele Urteile sehen den Zusammenhang des verursachten Schadens mit der beruflichen Funktion allein schon durch die Benutzung einer Sache oder eines Arbeitsmittels wie z.B. eines Blogs oder eines Forums.

Der Arbeitgeber ist selbstverständlich nicht haftbar, wenn der Fehler nicht in Verbindung mit der ausgeübten Funktion steht und kein Zusammenhang dazu besteht.

Wenn es möglich ist, einen Zusammenhang zwischen dem Fehler und der ausgeübten Funktion herzustellen, kann sich der Arbeitgeber von der Haftung befreien, wenn er drei vom Kassationsgerichtshof festgelegte kumulative Bedingungen beweist[14] : der Arbeitnehmer hat außerhalb seiner beruflichen Funktion, ohne Erlaubnis und mit einem Ziel gehandelt, das außerhalb seines Zuständigkeitsbereichs liegt. Auf der Grundlage dieser drei genannten Bedingungen hat das Berufungsgericht von Aix-en-Provence einen Arbeitgeber wegen der schuldhaften Nutzung des Internets durch einen seiner Arbeitnehmer verurteilt. In dem vorliegenden Fall hatte der Arbeitnehmer auf eigene Initiative eine private Website ins Internet gestellt, in der ein anderes Unternehmen kritisiert wurde. Bei dieser Gelegenheit haben die Richter daran erinnert, dass es Aufgabe des Arbeitgebers ist, die verantwortungsvolle Nutzung der unternehmenseigenen Arbeitsmittel durch die Arbeitnehmer zu kontrollieren. Sie waren der Meinung, dass der Arbeitnehmer 1. im Rahmen seiner beruflichen Funktion gehandelt hatte, denn er hatte innerhalb seiner beruflichen Funktion die Gelegenheit und die Mittel, vor allem die elektronischen Mittel, eine Straftat zu begehen, 2. mit Erlaubnis des Arbeitgebers gehandelt hatte, der in einer internen Notiz erklärt hatte, die persönliche und rechtmäßige Nutzung des Internets zu dulden, 3. nicht mit einer Absicht gehandelt hatte, die außerhalb seines Zuständigkeitsbereichs liegt, weil die Betriebsordnung es ihm erlaubte, den Internetzugang auch außerhalb seiner Arbeitszeiten zu nutzen[15].

Eine ebenso strenge Entscheidung sprach der Kassationsgerichtshof im Fall einer Versicherungsvertreterin aus, die während ihrer Arbeitszeit und an ihrem Arbeitsplatz mit den elektronischen Arbeitsmitteln mehrere Hinterziehungen begangen hatte: Die Erfüllungsgehilfin hatte während der Arbeitszeit und am Arbeitsplatz bei Tätigkeiten gehandelt, für die sie eingestellt worden war, mit den Arbeitsmitteln, die ihr zur Verfügung gestellt worden waren, was ausschloss dass sie diese Hinterziehungen außerhalb ihrer beruflichen Funktion begangen hatte.

Schließlich hat das Berufungsgericht von Paris die Schuld einem Arbeitgeber zugewiesen, der seine Arbeitnehmer ohne Kontrolle im Internet surfen ließ (Multimediadateien, Spiele, pornographische Websites, usw.), die in keinem Zusammenhang mit ihrer beruflichen Tätigkeit standen. In diesem Fall ging es um einen Rechtsstreit zwischen dem Arbeitgeber und seinem Dienstleister für Datensicherung und Virenschutz. Während die Richter in erster Instanz der Meinung waren, dass das Vorhandensein eines Virus (beim Kunden) der Beweis dafür ist dass der Lieferant (der Dienstleister) den Virenschutz nicht korrekt ausgeführt hat, berücksichtigte das Berufungsgericht, dass der Kunde, indem er seine Arbeitnehmer auf solche Websites gehen ließ, aus eigener Schuld den Schutz, zu dem sich der Lieferant verpflichtet hatte, unwirksam machte, so dass das Versagen des Virenschutzes nicht als rechtmäßiger Grund für die Auflösung

---

[14] Ass. plén. 19 mai 1988, n° 87-82.654, *RTD civ.* 1989, 89, obs. P. Jourdain.

[15] TGI Marseille, 1re ch. civ., 11 juin 2003, Escota c/Lucent Technologies, http://www.juriscom.net ; bestätigt durch CA Aix-en-Provence, 13 mars 2006, pourvoi n° 2006/170.

der Verträge angegeben werden kann[16].Es wurde jedoch auch geurteilt, dass aus der alleinigen Tatsache, dass ein Arbeitnehmer einen privaten Online-Blog führt, noch kein Angriff auf den Ruf seines Arbeitgebers abgeleitet werden kann (Cons. prud'h., 30. März 2007, s. Nr. 125.28).

Diese Rechtssprechungen zeigen, wie nützlich es ist, in der Betriebsordnung oder als Anhang zu dieser, die Bedingungen festzulegen, unter denen die Arbeitnehmer die Informatik und den Internetzugang nutzen dürfen, die ihnen zur Ausübung ihrer beruflichen Tätigkeit zur Verfügung gestellt werden.

KAPITEL

32. Das Prinzip der Transparenz

ABSCHNITT 0
ZUR ORIENTIERUNG

32.00

Plan des Kapitels.

Abschnitt 1 Verpflichtung zur Information

Abschnitt 2 Konsequenzen im Fall der fehlenden Transparenz

32.01

Anwendbare Texte.

> Französische Texte.

* s. Nr. 03.01.

32.02

Relevante Rechtssprechung.

> Zu der Verpflichtung zur Information der Arbeitnehmer.

• **Soc. 22 mai 1995,** n° 93-44.078, *Bull. civ.* V, n° 164 ; *Rev. soc. Francis Lefebvre* 1995, n° 7, p. 489, note Y. Chauvy — bestätigt durch **CA Douai, 30 juin 1993.**

* s. Nr. 32.11, auch Nr. 30.23.

> Zu der Verpflichtung zur Information und Konsultation des Betriebsrats.

• **Soc. 7 juin 2006,** n° 04-43.866, Girouard c/Continent France, *Bull. civ.* V, n° 206 ; *D.* 2006, 1704 — bestätigt durch **CA Bourges ch. soc., 24 oct. 2003.**

* s. Nr. 32.12 und auch Nr. 30.24.

> Ablehnung der Beweismittel wegen fehlender Information der Arbeitnehmer.

• **Soc. 6 juin 2007,** n° 05-43.996, sté Eliophot c/M. X — bestätigt durch **CA Aix-en-Provence, 18e ch., 7 juin 2005.**

• **Soc. 2, 20 nov. 1991,** n° 88-43.120, *Bull. civ.* V, n° 519 ; *D.* 13 févr. 1992, n° 7, 73, note Y. Chauvy — aufgehoben durch **CA Colmar, ch. soc., 17 déc. 1987.**

* s. Nr. 32.11 und 32.22, auch Nr. 30.23.

• **CA Paris, 31 mai 1995,** *Juris-Data* n° 024755 ; *RLDI* mai 2007, n° 27, comm. A. Saint Martin.

* s. Nr. 32.23.

> Ablehnung der Beweismittel wegen Verstoßes gegen die Regeln der Cnil.

• **CA Paris, 7 mars 1997,** *Gaz. Pal.* 21 janv. 1999.

siehe auch **CA Paris, 31 mai 1995** (o.g.).

* s. Nr. 32.23.

> Zulassung von Aufstellungen von Telefonverbindungen als Beweismittel.

• **Soc. 29 janv. 2008,** n° 06-45.279, Touati c/sté Canon France, *JS Lamy* 2008, n° 228, comm. J.-E. Tourreil ; *Gaz. Pal.* 24 avr. 2008, n° 115, p. 39, note L. Boncourt — bestätigt durch **CA Versailles, 11e ch., 5 sept. 2006.**

* s. Nr. 32.23.

> Zulassung des Beweismittels.

• **Soc. 11 mars 1998,** n° 96-40.147, Pisani c/sté Pisani, *Sem. soc. Lamy* 28 mai 2001, n° 1030 — bstätigt durch **CA Paris, 21e ch., 7 nov. 1995.**

* s. Nr. 32.24.

• **CA Montpellier, 17 mai 2006,** n° 05/01954, Claude G… c/Assoc. Ogec Emmanuel d'Alzon, http://www.legalis.net/jurisprudence-decision.php3?id_article=2066 — bestätigt durch **Soc. 10 oct. 2007,** n° 06-03.007, Claude G… c/Assoc. Ogec Emmanuel d'Alzon.

• Für das (bestätigte) Urteil in erster Instanz s. **Cons. prud'h. Montpellier, 26 sept. 2005,** Claude G… c/Assoc. Ogec Emmanuel d'Alzon.

* s. Nr. 32.24, auch Nr. 31.23.

• Siehe auch **Soc. 10 oct. 2007,** Claude G… c/Assoc. Ogec Emmanuel d'Alzon (o.g.)

* s. Nr. 32.24.

• **CA Aix-en-Provence, 18e ch., 4 janv. 1994**, Perez c/Beli Intermarchés, *Dr. soc.* 1995, 332 ; S. Darmaisin, « L'ordinateur, l'employeur et le salarié », *Dr. soc.* 2000, p. 580 ; *Juris-Data* n° 041281 — aufgehoben durch **Cons; pud'h. Nice,**

sect. comm., 10 déc. 1990.

* s. Nr. 32.25.

• **Soc. 14 mars 2000,** n° 1270, n° 98-42.090, *Bull. civ.* V, n° 101 ; *Gaz. Pal.* 28 oct. 2000, n° 302, p. 34, note J. Berenguer-Guillon et L. Guignot ; *JCP G* 7 févr. 2001, n° 6, p. 325, note C. Puigelier — bestätigt durch **CA Paris, 18e ch., sect. A, 16 févr. 1998,** n° 020563.

Für das (teilweise aufgehobene) Urteil in erster Instanz s. **Cons. prud'h. Paris, 2e ch., sect. Encadrement, 13 déc. 1995**.

* s. Nr. 32.11 und 32.24, auch Nr. 30.23 und 31.22.

> Zu der Rechtswirkung von Chartas.

• **Soc. 21 déc. 2006,** n° 05-41.165, J.-H. Pettre c/sté Ad 2 One SA — bestätigt durch **CA Versailles, 5e ch., sect. B, 25 nov. 2004.**

* s. Nr. 32.15.

> Zu der Zulassung der Beweismittel im Bereich des Strafrechts

• **Crim. 6 avr. 1994,** n° 93-82.717, *Bull. crim.,* n° 136 — bestätigt durch **CA Bordeaux, 3e ch., 13 mai 1993.**

• **Crim. 23 juill. 1992,** n° 92-82.721, *Bull. crim.,* n° 274 — bestätigt durch **CA Caen, ch. acc., 8 avr. 1992.**

• **Crim. 31 mai 2005,** n° 04-85.469 — bestätigt duch **CA Montpellier, ch. corr., 6 mai 2004.**

* s. Nr. 32.26, auch Nr. 30.26 und 30.23.

32.04

Grundsätzliche Fragen.

• Unter welchen Bedingungen ist die Erhebung und Verarbeitung personenbezogener Daten zulässig?

* s. Nr. 32.11 und 32.12.

• Welche rechtlichen Konsequenzen zieht die Missachtung der Verpflichtung zur Information der Arbeitnehmer nach sich?

* s. Nr. 32.22.

ABSCHNITT 1
VERPFLICHTUNG ZUR INFORMATION

32.11

Verpflichtung zur Information der Arbeitnehmer. Das französische Arbeitsgesetzbuch (*Code du travail*) sieht ausdrücklich vor, dass keine Information, die einen Arbeitnehmer (oder einen Bewerber um eine Stelle) persönlich betrifft durch ein Instrument erfasst werden darf, über das der Arbeitnehmer (oder der Bewerber um eine Stelle) nicht zuvor informiert worden war. (Code du travail Art. L. 1221-9 [früher Art. L. 121-8]). Die französische Datenschutzbehörde *Commission nationale de l'informatique et des libertés* (Cnil) erinnert ebenfalls daran, dass die betroffenen Arbeitnehmer immer einzeln über den Einsatz von Kontrollvorrichtungen, die Modalitäten ihres Zugangsrecht zu den Daten und den Zweck der Kontrollmaßnahmen informiert werden müssen.

An diese Regel hat der Kassationsgerichtshof mehrmals erinnert: Auch wenn der Arbeitgeber das Recht hat, die Tätigkeit seines Personals während der Arbeitszeit zu kontrollieren und zu überwachen, so darf er doch keine Kontrollinstrumente einsetzen, über die er die Arbeitnehmer nicht zuvor in Kenntnis gesetzt hat.[17] Oder auch: Der Arbeitgeber hat das Recht, die Tätigkeit seiner Angestellten während der Arbeitszeit zu kontrollieren und zu überwachen, die heimliche Überwachung ist jedoch ausgeschlossen[18] .

Man kann also feststellen, dass weniger der Einsatz von Instrumenten zur Kontrolle und Überwachung der Arbeitnehmer als die Tatsache, dabei ohne das Wissen der Arbeitnehmer vorzugehen, verurteilt wird. Es ist also vernünftig, im Rahmen einer Betriebsordnung oder eines Verhaltenskodex oder auch einer „Charta", die Bedingungen zur Nutzung des Internetzugangs und insbesondere der E-Mailbox festzulegen und sich in den Arbeitsverträgen darauf zu beziehen.

---

[17] Soc. 20 nov. 1991, n° 88-43.120, *Bull. civ.* V, n° 519 ; *D.* 13 févr. 1992, n° 7, 73, note Y. Chauvy : es handelte sich um eine versteckte Kamera — Soc. 22 mai 1995, n° 93-44.078, *Bull. civ.* V, n° 164 ; *Rev. soc. Francis Lefebvre* 1995, n° 7, p. 489, note Y. Chauvy : es handelte sich um die Beschattung eines Arbeitnehmers durch einen Privatdetektiv.

[18] Soc. 14 mars 2000, n° 1270, n° 98-42.090, *Bull. civ.* V, n° 101 : es handelte sich um ein System zum Abhören von Telefongesprächen.

An diese Nutzungsbedingungen kann außerdem bei der Vergabe eines Zugangscodes oder auf gewissen Bildschirmseiten oder auch bei der Verteilung von Dienstanweisungen erinnert werden. Die Cnil unterstützt diese Initiative, sofern diese "Charta" oder "Verhaltenskodex" das Ziel hat, eine vollständige Information der Nutzer zu gewährleisten, die Angestellten oder öffentlichen Bediensteten für die Sicherheitsanforderungen zu sensibilisieren und ihre Aufmerksamkeit auf gewisse Komponenten zu lenken, die dem allgemeinen Interesse des Unternehmens oder der Behörde schaden könnten.[19].

32.12

Verpflichtung zur Information und Konsultation des Betriebsrats. Wenn es einen Betriebsrat gibt, ist der Arbeitgeber ebenfalls verpflichtet, diesen zu informieren, bevor automatisierte Verarbeitungsprozesse für die Personalverwaltung eingesetzt werden und jedes Mal wenn eine Änderung daran vorgenommen wird. (Code du travail, Art. L. 2323-32 ; früher L. 432-2-1)[20]. Der Betriebsrat muss ebenfalls vor jeder bedeutenden Einführung einer neuen Technologie konsultiert werden, wenn diese Auswirkungen auf die Beschäftigung, die Qualifikation, die Bezahlung, die Ausbildung oder die Arbeitsbedingungen der Beschäftigten haben können. (Code du travail, Art. L. 2323-13; früher L. 432-2, Absatz 1). Schließlich muss der Arbeitgeber den Betriebsrat vor der Entscheidung, in dem Unternehmen Maßnahmen oder Techniken einzusetzen, die eine Kontrolle der Tätigkeit der Arbeitnehmer ermöglichen, informieren und konsultieren. (Code du travail, Art. L. 2323-32) Die Information des Betriebsrats muss präzise sein und auf schriftlichem Weg erfolgen (Code du travail, Art. L. 2323-4, früher L. 431-5, Absatz 2). Die Stellungnahme des Betriebsrats hat jedoch einen rein beratenden Charakter und ist für den Arbeitgeber nicht bindend.

Der Internetanschluss, die Schaffung eines Intranets, die Einführung eines elektronischen Nachrichtenübermittlungssystems sind eindeutig neue Technologien und Techniken, die eine Kontrolle der Tätigkeit der Arbeitnehmer im Sinne der oben genannten Artikel ermöglichen. Allgemein wird man festhalten, dass der Arbeitgeber den Betriebsrat informieren und konsultieren muss (Code du travail, Art. L 1221-9, früher L. 121-8) oder im öffentlichen Dienst das *comité technique paritaire* (paritätischer technischer Ausschuss) oder jegliche gleichwertige Instanz, bevor ein Verarbeitungssystem oder Vorgänge eingesetzt werden, die eine „Verfolgung" der Tätigkeiten der Arbeitnehmer ermöglichen, zum Beispiel indem sie den Zugang zum Computerarbeitsplatz eines abwesenden Arbeitnehmers ermöglichen.

Die Akte für die Erklärung bei der Cnil muss die Informationen enthalten, dass und wann die Personalvertretung konsultiert wurde.

Der Kassationsgerichtshof hatte die Gelegenheit, das Fehlen der Konsultierung des Betriebsrats unter Anwendung des Artikels L. 432-2-1 (heute Art. L. 2323-32) des Arbeitsgesetzbuchs zu verurteilen, obwohl nicht ernsthaft behauptet werden konnte, dass die Arbeitnehmer nichts von den installierten Kameras wussten, da diese schon lange im Gebrauch waren und Schilder auf ihre Anwesenheit hinwiesen[21].

32.13

„Internetcharta" und Arbeitsgesetzbuch. Der Arbeitgeber kann von den Arbeitnehmern ein Dokument, das die Nutzungsbedingungen der elektronischen Arbeitsmittel im Unternehmen festlegt, unterzeichnen lassen. Ein solches Dokument kann als Anhang dem Arbeitsvertrag beigefügt werden.

Wenn der Text Leistungsanordnungen (*injonctions de faire*), Verbote oder Disziplinarstrafen vorsieht, stellt er eine Ergänzung zur Betriebsordnung dar. In diesem Fall unterliegt der Text schwerwiegenderen Veröffentlichungs- und

---

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

[20] Im öffentlichen Dienst muss der Arbeitgeber das *comité technique* (technischer Ausschuss) oder jede andere dem Betriebsrat entsprechende Institution konsultieren: siehe L. n° 84-16, 11 janv. 1984 ; L. n° 84-53, 26 janv. 1984 und L. n° 86-33, 9 janv. 1986.

[21] Soc. 7 juin 2006, n° 04-43.866, Girouard c/Continent France, *Bull. civ.* V, n° 206 ; *D.* 2006, 1704.

Informationsbedingungen: Er muss dann dem Betriebsrat zur Konsultation und Information vorgelegt werden, der Arbeitsinspektion mitgeteilt werden, bei dem *Conseil des prud'hommes* (erstinstanzliches Arbeitsgericht) hinterlegt werden und in einem Aushang veröffentlicht werden. Dieses Dokument ermöglicht eine Aufstellung der internen Regeln bezüglich der Sicherheit und der Berufsethik im Zusammenhang mit der Nutzung der Informatik und der Netzwerke. Die Aufstellung eines solchen Verhaltenscodex hat mehrere Vorteile: er kann nicht nur eventuellen Rechtsstreitigkeiten zwischen dem Arbeitgeber und den Arbeitnehmern vorbeugen, sondern erfüllt darüber hinaus die Informationspflicht bezüglich der im Unternehmen eingesetzten Systeme zur Kontrolle der Arbeitnehmer sowohl gegenüber den Arbeitnehmern als auch gegenüber den Instanzen der Personalvertretung.

32.14

Internetcharta und Cnil. Laut Cnil muss das angenommene Dokument die technischen Potentialitäten der Arbeitsmittel und die wirklich eingesetzten Verwendungsmöglichkeiten präzisieren, insbesondere bezüglich der Nachverfolgung von Spuren. Genauer gesagt müssen in einer solchen Charta die Modalitäten der eingesetzten Kontrolle, die vom Arbeitgeber verwendeten Speichersysteme sowie die Dauer der Speicherung genannt werden.

In ihrem im März 2001 veröffentlichten Forschungsbericht und ihrer öffentlichen Konsultation zum Thema *La cybersurveillance des employés dans l'entreprise (*Cyber-Überwachung der Beschäftigten in Unternehmen) sowie in ihrem am 18. Dezember 2003 geänderten Bericht mit dem Titel *La cybersurveillance sur les lieux de travail* (Cyber-Überwachung am Arbeitsplatz) hat die französische Datenschutzbehörde Cnil vor Fehlformen und Missbrauch gewarnt, auf die sie oft bei Chartas zur Nutzung der Informatik gestoßen ist. Das Ungleichgewicht zwischen Arbeitgeber und Arbeitnehmer kommt laut der Datenschutzbehörde bei der Unterzeichnung eines solchen Dokuments oft klar zum Ausdruck. Sie unterstützt jedoch die Initiative der Schaffung einer solchen "Charta", sofern sie sich zum Ziel setzt, eine vollständige Information der Nutzer zu gewährleisten, die Angestellten für die Sicherheitsanforderungen zu sensibilisieren, ihre Aufmerksamkeit auf gewisse Komponenten zu lenken, die dem allgemeinen Interesse des Unternehmens schaden könnten.

32.15

„Chartas" und Rechtsstatus. Ein Urteil der Sozialkammer des Kassationsgerichtshofs spricht den Chartas zur Nutzung der Informatik eine Rechtswirkung zu und ordnet sie neben der Betriebsordnung als Dokument ein, das gegenüber den Arbeitnehmern geltend gemacht werden kann. In dem Fall wurde das Verhalten eines Arbeitnehmers, der ohne legitimes Motiv versucht hatte, sich mit dem Passwort eines anderen Arbeitnehmers auf den PC des Geschäftsführers einzuloggen, als im Widerspruch zu der Respektpflicht der in diesem Unternehmen geltenden Informatikcharta stehend verurteilt. Ein solches Verhalten stellte einen groben Verstoß *(faute grave)* dar und machte seinen Verbleib im Unternehmen während der Kündigungsfrist unmöglich.[22].

ABSCHNITT 2
KONSEQUENZEN IM FALL DER FEHLENDEN TRANSPARENZ

32.21

Verletzung der Privatsphäre. Das Arbeitsgesetzbuch (*Code du travail*) legt fest, dass der Arbeitgeber für das Erheben und die Verarbeitung personenbezogener Daten der Arbeitnehmer ohne deren Wissen aufgrund der Nichterfüllung seiner allgemeinen Verpflichtung zur Transparenz haftbar gemacht werden kann. So könnte ein Kontrollsystem der E-Mailbox des Arbeitnehmers oder auch ein

[22] Soc. 21 déc. 2006 n° 05-41.165, NPB, J.-H. Pettre c/sté Ad 2 One SA : Ablehnung des Rechtsmittels CA Versailles, 5e ch. B, 25 nov. 2004 ; *Gaz. Pal.*, 07 août 2007, n° 219, p. 22.

Instrument zur Nachverfolgung der Websites, die ein Arbeitnehmer besucht hat, als Verletzung seiner Privatsphäre angesehen werden, wenn der Betriebsrat (oder im öffentlichen Dienst das *comité technique paritaire* - der paritätische technische Ausschuss - oder jegliche gleichwertige Instanz) und die Arbeitnehmer nicht unter den zuvor genannten Bedingungen darüber informiert waren.

Ebenso wird eine Vorrichtung, die ohne das Wissen der Arbeitnehmer so angebracht wird, dass beabsichtigt ist, dass die nicht gesehen wird (z.B. Kameras) oder die das Kommen und Gehen der Arbeitnehmer kontrollieren soll, als Verletzung der Privatsphäre der Arbeitnehmer angesehen.

Die Rechtssprechung hat die rechtlichen Konturen für die Einsetzung von Instrumenten zur Überwachung der Arbeitnehmer umrissen, insbesondere indem sie sich auf die Zulassung oder Ablehnung von Beweismitteln stützt, die aus Systemen der Cyber-Überwachung stammen.

32.22

Ablehnung der Beweismittel wegen fehlender Information der Arbeitnehmer. Der Arbeitgeber kann sich nicht auf Beweismittel berufen, die aus Kontrollmaßnahmen stammen, über die die Arbeitnehmer nicht zuvor in Kenntnis gesetzt worden waren. Solche Beweise würden aus den rechtlichen Debatten ausgeschlossen und eventuell auf der Grundlage dieser Beweise gegen die Arbeitnehmer vollzogene Sanktionen könnten annulliert werden.

Der Kassationsgerichtshof hat ab 1991 klargestellt, dass, auch wenn der Arbeitgeber das Recht hat, die Tätigkeit seiner Angestellten während der Arbeitszeit zu kontrollieren und zu überwachen, jegliche Aufzeichnung von Bildern oder Gesprächen, aus welchem Grund auch immer sie gemacht wurde, ein rechtswidriges Beweismittel darstellt, wenn die Aufzeichnung ohne das Wissen der Arbeitnehmer erfolgte.[23]. In diesem Fall ging es um die Entlassung einer Verkäuferin wegen eines groben Verstoßes *(faute grave)*, die sich auf eine mit Hilfe einer in der Kasse der betroffenen Person versteckten Kamera erfolgten Aufzeichnung stützte.

In jüngerer Zeit hat der Kassationsgerichtshof mit einem Urteil vom 6. Juni 2007 ein Urteil des Berufungsgerichts bestätigt, das den privaten Charakter einer E-Mail eines Arbeitnehmers an seinen Kollegen berücksichtigte und daraus ableitete, dass dieses Element der Privatsphäre der betroffenen Person keinen Kündigungsgrund darstellen könne.[24].

32.23

Ablehnung der Beweismittel wegen Verstoßes gegen die Regeln der Cnil. Die Richter haben einen durch ein ordnungsgemäß bei der Cnil erklärtes Namensverarbeitungsprogramm erbrachten Beweis in der Erwägung, dass die betreffende Information in keinem Zusammenhang mit dem Zweck des Verarbeitungsprogramms steht, abgelehnt[25]. So durfte z.B. ein den Arbeitnehmern zur Verfügung gestelltes Computersystem zur Ticketreservierung nicht ohne das Wissen der Arbeitnehmer zur Kontrolle ihrer Arbeitszeit verwendet werden.

Ebenso urteilte das Berufungsgericht von Paris am 7. März 1997, dass die Vorlage einer Aufstellung der Telefonverbindungen eines Arbeitnehmers, die mittels einer Telefon-Selbstwählanlage erstellt wurde, vor Gericht rechtswidrig sei, da in jedem Fall, die Verpflichtung der vorherigen Erklärung laut Artikel 6 des Gesetzes vom 6. Januar 1978 von dem Unternehmen nicht eingehalten worden sei und diese Aufstellung zu keinem anderen Zweck aufbewahrt werden dürfe, als dafür, der Arbeitnehmerin die Kosten für ihre Privatgespräche eventuell in Rechnung zu stellen[26].

Es muss jedoch auch auf das Urteil des Kassationsgerichtshofs vom 29. Januar 2008 hingewiesen werden, der zugelassen hat, dass die vom Arbeitgeber vorgelegten Aufstellungen über Telefonverbindungen die Entlassung eines

---

[23] Soc. 20 nov. 1991, n° 88-43.120, *Bull. civ.* V, n° 519.

[24] Soc. 6 juin 2007, n° 05-43.996, NPB, sté Eliophot c/M. X… : Ablehnung des Rechtsmittels CA Aix-en-Provence, 18e ch., 7 juin 2005.

[25] CA Paris, 31 mai 1995, *Juris-Data* n° 024755 ; *RLDI* mai 2007, n° 27, comm. A. Saint Martin.

[26] CA Paris, 7 mars 1997, *Gaz. Pal.* 21 janv. 1999, p. 30.

Arbeitnehmers wegen missbräuchlicher Nutzung seines Geschäftstelefons rechtfertigen können[27]. Diese Aufstellungen zeigten, dass der Arbeitnehmer von seinem Geschäftstelefon aus zwischen Juli 2002 und Januar 2003 mit einer Verbindungsdauer von insgesamt 63 Stunden bei Partnervermittlungsdiensten angerufen hatte. Der Arbeitnehmer hat vergeblich versucht, sich mit der Argumentation, dass er nicht zuvor von der Kontrollmaßnahme informiert worden war, auf die Rechtswidrigkeit des erbrachten Beweismittels zu berufen. Der Hohe Gerichtshof war jedoch der Ansicht, dass die einfache Überprüfung der von einer Telefon-Selbstwählanlage erstellten Aufstellung der Gesprächsdauer, der Gebühren und der von jedem Telefon aus gewählten Telefonnummern nicht deshalb einen rechtswidrigen Überwachungsvorgang darstellt, weil die Arbeitnehmer nicht zuvor darüber informiert worden waren. Man muss jedoch feststellen, dass die Frage nach der Konformität der Erhebung personenbezogener Daten der Arbeitnehmer mittels Telefonaufstellungen mit dem Gesetz vom 6. Januar 1978 bezüglich des Schutzes von Personen im Hinblick auf die Verarbeitung persönlicher Daten (*loi informatique et libertés*) in diesem Fall nicht gestellt wurde.

32.24

Zulassung der Beweismittel. Die Richter waren der Ansicht, dass der Arbeitgeber sich auf Aufzeichnungen von Telefongesprächen seines Arbeitnehmers stützen konnte, die zeigten, dass sich dieser während seiner Arbeitszeit mit Glücksspielen mit Dritten beschäftigt hatte (Wetten über den Ausgang der Präsidentschaftswahl, Fußballergebnisse), da dieser zuvor davon in Kenntnis gesetzt worden war, dass er aufgezeichnet würde[28]. Sie haben bekräftigt, dass der Arbeitgeber das Recht hat, die Tätigkeit seiner Angestellten während der Arbeitszeit zu kontrollieren und zu überwachen, und dass nur die Verwendung heimlicher Überwachungsverfahren rechtswidrig ist[29]. In dem vorliegenden Fall ist zu beachten, dass es sich um eine Börsengesellschaft handelte, deren Berufsordnung die Aufzeichnung der über das Telefon vollzogenen Kaufanweisungen erlaubt.

Ebenso hat ein Urteil vom 11. März 1998 der Sozialkammer des Kassationsgerichtshofs gelten lassen, dass die Aufstellungen von Telefonverbindungen des Geschäftstelefons eines Arbeitnehmers, die der Arbeitgeber zur Bezahlung von *France Télécom* erhalten hat, kein rechtswidriges Beweismittel darstellen[30]. Oder auch in jüngerer Zeit ein Urteil des Berufungsgerichts von Montpellier vom 17. Mai 2006, das gelten ließ, dass der Arbeitgeber rechtsmäßig über die bei einem Einsatz des für die Wartung des Computersystems seiner Firma zuständigen Unternehmens, das von einem Arbeitnehmer für die Beseitigung eines Virus von seinem Firmencomputer um Hilfe gebeten worden war, entdeckten Tatsachen informiert worden war[31]. Die Richter waren der Ansicht, dass die Entlassung wegen groben Verstoßes *(faute grave)* gerechtfertigt war, da der Arbeitnehmer, indem er mehrmals auf pornographische Websites ging, gegen seine Verpflichtungen als Lehrer und Erzieher, die mit seiner Funktion verbundene Würde zu wahren und den reinen Charakter der Einrichtung zu erhalten, die in dem kollektiven Arbeitsvertrag der Lehrer der Sekundarstufe an Privatschulen festgeschrieben ist, verstoßen hatte. Die Sozialkammer des Kassationsgerichtshofs hat in einem Urteil vom 10. Oktober

---

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

28 F. Lemaître, « Jouer sur le lieu de travail est illégal, estiment les juges », Zeitungsartikel in *Le Monde* vom 28. März 2000.

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

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

31 CA Montpellier, 17 mai 2006, nº 05/01954, Claude G… c/Assoc. Ogec Emmanuel d'Alzon, v. http://www.legalis.net/jurisprudence-decision.php3?id_article=2066

2007 diese Auslegung bestätigt[32].

32.25

Die Richter fordern auf jeden Fall eine gute Qualität der Beweise. So stellte ein Urteil vom 4. Januar 1994 des Berufungsgerichts von Aix-en-Provence klar, dass das vorgelegte Beweisdokument sowohl was das Datum als auch den Inhalt angeht, ausreichende Garantien für die Authentizität, die Unparteilichkeit und die Aufrichtigkeit erbringen muss[33].

(Für umfassendere Ausführungen über die Schwierigkeit, den Beweis zu erbringen siehe Nr. 141.31.)

32.26

Im Bereich des Strafrechts. Der Kassationsgerichtshof hat auch daran erinnert, dass keine rechtliche Bestimmung den Strafrichtern erlaubt, von den Parteien erbrachte Beweismittel aus dem alleinigen Grund abzuweisen, dass sie auf rechtswidrige oder unlautere Weise erhalten wurden, es steht ihnen nur zu, den Wert ihrer Aussagekraft zu beurteilen[34]. Oder auch, dass kein für Strafverfahren relevanter Text dem Kläger verbietet, zur Unterstützung seiner Klage Beweise zur Belastung der angeklagten Personen zu erbringen, es obliegt den Strafgerichtsbarkeiten, deren Wert hinsichtlich der Regeln bezüglich der Beweisführung der Straftaten zu beurteilen[35].

So kann man als Beispiel den Fall von Aufzeichnungen der Tätigkeiten in einer Apotheke mit Publikumsverkehr schildern, mit einer Kamera, die auf Veranlassung des Apothekers eingerichtet wurde, aufgrund derer ein Vertrauensmissbrauch eines Angestellten zum Schaden des Apothekers aufgedeckt werden konnte. Oder auch den Fall eines wegen gemeinschaftlichen Diebstahls angeklagten Arbeitnehmers auf der Grundlage der Aufzeichnungen eines Videoüberwachungssystems, das zwei Personen zeigte, die mehrere Gegenstände mitnahmen, durch das Toilettenfenster nach draußen gaben und in ein in der Nähe dieses Fensters stehendes Fahrzeug brachten [36].

Man muss jedoch anmerken, dass der Kassationsgerichtshof mindestens zwei Mal bestätigt hat, dass es nicht möglich ist, auf polizeiliche Provokation zurückzugreifen, um den Beweis einer Straftat zu erbringen (Crim. 7. Feb. 2007[37] — Crim. 4. Juni 2008[38] — Ausführungen siehe Nr. 143.12).

---

[32] Soc. 10 oct. 2007, n° 06-03.007 ; Ablehnung des Rechtsmittels CA Montpellier, 17 mai 2006, v. http://www.legalis.net/jurisprudence-decision.php3?id_article=2065.

[33] CA Aix-en-Provence, 4 janv. 1994, *Dr. soc.* 1995, 332. ; S. Darmaisin, « L'ordinateur, l'employeur et le salarié », *Dr. soc.* 2000, p. 580.

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

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

[36] Crim. 31 mai 2005, n° 04-85.469.

[37] Crim. 7 févr. 2007, n° 06-87.753, *Bull. crim.,* n° 37 ; cass. CA Paris, 26 sept. 2006 (Überweisung an CA Versailles) ; siehe auch « Une procédure fondée sur une provocation à commettre une infraction, même commise à l'étranger, doit être annulée » (Ein Verfahren, das sich auf eine Provokation stützt, eine Straftat zu gehen, muss annulliert werden, auch wenn sie im Ausland begangen wurde), *AJ pénal* 2007, n° 5, mai, juri. p. 233.

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

KAPITEL

33. Das Prinzip der Verhältnismäßigkeit

ABSCHNITT 0
ZUR ORIENTIERUNG

33.00

Plan des Kapitels.

33.01

Anwendbare Texte.

> Französische Texte.

Gesetzestexte.

* s. Nr. 3.01.

Stellungnahmen und Empfehlungen.

Cnil, document d'orientation vom 10. Nov. 2005 für die Einführung von Whistleblowing-Systemen in Konformität mit dem Gesetz vom 6. Januar 1978 (geändert im August 2004) – Cnil, délib. n° 2005-305, vom 8. Dez. 2005, über eine *autorisation unique* (Rahmenbeschluss) für die Verarbeitung personenbezogener Daten im Rahmen von Whistleblowing-Systemen – Cnil, délib. n° 2006-067, vom 16. März 2006, zur Annahme einer *norme simplifiée* (vereinfachte Erklärungsformalitäten bei Konformität mit der Norm) bezüglich der von öffentlichen oder privaten Institutionen eingeführten automatischen Verarbeitungssysteme personenbezogener Daten, die zur Geolokalisierung der von ihren Arbeitnehmern genutzten Fahrzeugen dienen (norme simplifiée n° 51), *JO* n° 1003, 3 mai. - der dem damaligen Arbeitsminister *ministre délégué à l'Emploi, au Travail et à l'Insertion professionnelle des jeunes*, am 7. März 2007 vorgelegte Bericht, *Charte d'éthique, alerte professionnelle et droit du travail français :* état des lieux et perspectives, auf http://lesrapports.ladocumentationfrancaise.fr/BRP/074000335/0000.pdf l.

33.02

Relevante Rechtssprechung.

> Prinzip des Verbots des Abhörens von Telefongesprächen am Arbeitsplatz.

• **Soc. 7 nov.1995,** n° 92-44.498, NPB, Sté polyclinique Volney c/M. Bordeau — bestätigt durch **CA Rennes, 5e ch., 29 sept. 1992**.

• **Soc. 3 févr. 1999,** n° 97-40.495, NPB, Sté Locamion c/Belgacem ben Mariem — bestätigt durch **CA Lyon, ch. soc. coll. B, 5 déc. 1996**.

• **Soc. 30 mars 1999,** n° 97-40.850, NPB — bestätigt durch **CA Lyon, ch. soc. coll. B, 8 nov. 1996**.

• **Soc. 18 nov.1998,** n° 96-43.902, Sté Cegeor, SARL c/Mme I. NPB — bestätigt durch **CA Lyon, ch. soc., 5 juin 1996**.

* s. Nr. 33.13.

> Zu dem Prinzip der Unverletzbarkeit des Briefgeheimnisses.

• **TGI Paris, 12e ch., 1er juin 2007,** Oddo et Cie c/Trinh Nghia T… et Trung T…, http://www.legalis.net/breves-article.php3?id_article=2178.

* s. Nr. 33.20.

> Zu der Einsichtnahme in die E-Mailbox des Arbeitnehmers und die von ihm erstellten Dateien.

• **Soc. 2 oct. 2001, arrêt Nikon,** n° 99-42.942, *Bull. civ.* V, n° 291 ; *D.* 8 nov. 2001, n° 39, jur., comm. 3148-3153 ; *Sem. soc. Lamy* 15 oct. 2001, n° 1046 ; *JCP E et A* 29 nov. 2001, n° 48, p. 1918-1922, note C. Puigelier ; *JCP G* n° 2, 9 janv. 2002, doctr., I, 102, p. 63-69, note M. Bourrié-Quenillet et F. Rodhain ; *RTD civ.* janv.-mars 2002, n° 1, 72-73, note J. Hauser ; *RJPF* janv. 2002, n° 1, p. 10-11, note B. Bossu ; *RJS* n° 12/01, déc. 2001, chron. p. 940-946, note F. Favennec-Hery ; *Gaz. Pal.* 16 mai 2002, n° 136, p. 47, note H. Vray ; *LPA* 10 déc. 2001, n° 245, p. 6, note G. Picca — aufgehoben durch **CA Paris, 18e ch.,**

sect. A, 22 sept. 1999.

* s. Nr. 33.21.

• **Soc. 18 oct. 2006,** n° 04-48.025, NPB, Jérémy L. F… c/Techni-Soft : *Bull. civ.* V, 18 oct. 2006 comm. 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 avr. 2008, n° 85, p. 7, note X. Daverat et S. Tournaux — bestätigt durch **CA Rennes, ch. soc., 21 oct. 2004,** *Gaz. Pal.* 18 janv. 2007, n° 18, p. 37, note S. Hadjali et C. Fagot ; *LPA* 28 avr. 2008, n° 85, p. 7, note X. Daverat.

• **CA Toulouse, 4e ch. soc., 6 févr. 2003,** aff. n° 02-02519.

* s. Nr. 33.22, 33.21 und auch Nr. 31.24.

• **Soc. 17 mai 2005,** n° 03-40.017, NPB, Philippe K… c/Sté Cathnet-Science, *Juris-Data* n° 028449 ; *CCE* juill.-août 2005, p. 34 s., comm. A. Lepage ; *Gaz. Pal.* 20 oct. 2005, n° 293, p. 36, note S. Hadjali ; *LPA* 23 avr. 2007, n° 81, p. 6, note S. Tournaux — aufgehoben durch **CA Paris, 22e ch., sect. A, 6 nov. 2002**.

• **CA Besançon, ch. soc., 21 sept. 2004,** RG n° 2003-1807, SNC General Electric Energy Products France c/Girardot et a., *RJS* 4/2005, n° 342.

• **Soc. 23 mai 2007,** n° 05-17.818, Datacep c/Hansart, NPB, *Bull. civ.* V ; *D.* 2007, AJ 1590, note A. Fabre ; *Gaz. Pal.* 18 mars 2008, n° 78, p. 20 ; *LPA* 28 avr. 2008, n° 85, p. 7, note X. Daverat et S. Tournaux — aufgehoben durch **CA Douai, 1re ch., sect. 2, 18 mai 2005**.

* s. Nr. 33.23.

• **CA Versailles, 2 avr. 2003,** aff. n° 02-00293 et **CA Besançon, ch. soc., 21 sept. 2004,** RG n° 2003-1807**,** SNC General Electric Energy Products France c/Girardot a., *RJS* 4/05, n° 342.

* s. Nr. 33.21.

> Zu dem gerechtfertigten und verhältnismäßigen Charakter einer Kontrollvorrichtung.

• **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.* 1er févr. 2003, n° 32, p. 23, note C.-E. Brault : zum Thema Geolokalisierung — aufgehoben durch **CA Nancy, ch. soc., 23 févr. 2000**.

* s. Nr. 33.31.

• **TGI Paris, 19 avr. 2005,** *CCE* oct. 2005, comm. 164, p. 46.

* s. Nr. 33.11.

• **TGI Paris, 1re ch., 19 avr. 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.

* s. Nr. 33.11.

> Zu der anzunehmenden privaten oder beruflichen Natur einer Nachricht oder einer Datei.

• **Soc. 18 oct. 2006,** n° 04-48.025, NPB, Jérémy L. F… c/Techni-Soft (o.g.) — bestätigt durch **CA Rennes, ch. soc., 21 oct. 2004** (o.g.).

• **CA Bordeaux, ch. soc., sect. A, 8 févr. 2005,** n° 04/02449.

* s. Nr. 33.22.

> Zu den Whistleblowing-Systemen.

• **TGI Libourne, ord. réf., 15 sept. 2005,** RG n° 05/00143, Comité d'établissement BSN Glasspack, Synd. CGT du personnel de BSN Glasspack c/SAS BSN-Glasspack, v. chron. F. Naftalski, *Lamy Dr. informatique et réseaux* 2005 : retrait.

• **TGI Nanterre, ord. réf., 27 déc. 2006 :** Aussetzung des Systems.

• ***CONTRA:*** für den Erhalt des Systems, **TGI Lyon, ch. urg., 19 sept. 2006**, Union départementale CGT du Rhône, synd. CGT Bayer Cropscience c/Bayer Cropscience.

• **TGI Nanterre, ord. réf., 1er avr. 2005,** CE ING Bank c/ING Bank France.

* s. Nr. 33.32.

33.03

Auswahlbibliographie.

> Leitfaden.

Cnil, *Guide pratique pour les employeurs* — Mitteilung der CNIL bezüglich des Einsatzes von Instrumenten zur Erkennung von digitalen Fingerabdrücken mit Speicherunge in einer Datenbank, siehe http://www.cnil.fr/index.php?id=2363&news[uid]=508&cHash=0a2ef80a3e.

> Artikel.

G. Haas et L. Goutorbe, « Cybersurveillance : l'employeur doit être prudent en matière de collecte de preuve », *Expertises* août-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

Grundsätzliche Fragen

• Wie lassen sich das Recht des Arbeitgebers, die Arbeitsmittel zu kontrollieren und der Respekt der Privatsphäre des Arbeitnehmers vereinbaren?

* s. Nr. 33.11

• Unter welchen Bedingungen darf man auf die personenbezogenen Daten eines Arbeitnehmers zugreifen?

* s. Nr. 33.20 f.

• Nach welchen Kriterien wird über die Erlaubnis einer biometrischen Zugangskontrolle zum Arbeitplatz entschieden?

* s. Nr. 33.30, auch Nr. 28.00 f.

ABSCHNITT 1
EIN GERECHTFERTIGTES INSTRUMENT

33.11

Ein "gerechtfertigtes" Kontrollinstrument. Das Gesetz vom 31. Dezember 1992 hat ein Prinzip der Verhältnismäßigkeit eingeführt, das nun Bestandteil von Artikel L. 1121-1 des französischen Arbeitsgesetzbuchs (*Code du travail*) ist: Niemand darf die Rechte von Personen und ihre individuellen und kollektiven Freiheiten einschränken, wenn diese Einschränkungen weder durch die Art der zu erfüllenden Aufgabe gerechtfertigt sind noch im Verhältnis zu dem angestrebten Ziel stehen (früher Art. L. 120-2).

Daran hat das *tribunal de grande instance* (Zivilgericht der ersten Instanz) von Paris in seiner Entscheidung vom 19. April 2005[39], bezüglich eines biometrischen Instruments, gegen dessen Einführung der Betriebsrat und die Gewerkschaft *Sud-Rail* geklagt hatten, erinnert. Betriebsrat und Gewerkschaft waren der Ansicht, dass das System zur Erkennung von digitalen Fingerabdrücken zur Verwaltung und Überwachung der Anwesenheitszeiten der Arbeitnehmer an den verschiedenen Arbeitsorten die individuellen Freiheitsrechte der Arbeitnehmer verletze.

Der Arbeitgeber darf nur angesichts eines verdächtigen Verhaltens seines Arbeitnehmers eine derartige Kontrolle ausüben: ungewöhnliche lange Verbindungszeiten oder auch ungewöhnlich große Downloads (z.B. von Spielen oder pornographischen Bildern) könnten z.B. Indizien darstellen, die eine Überwachungs- und Abhörmaßnahme rechtfertigen würden. Man muss jedoch beachten, dass solche Überprüfungen als „Störung" angesehen werden könnten, wenn es sich um einen „geschützten" Arbeitnehmer handelt (Gewerkschaftsvertreter, Personalvertreter, Betriebsratsmitglied, usw.).

33.12

Rechtlicher Rahmen der Telefon-Selbstwählanlagen. In einer ersten Empfehlung vom 18. September 1984 hat die französische Datenschutzbehörde Cnil klargestellt, dass der Arbeitgeber weder Telefongespräche aufzeichnen, noch die kompletten von seinen Arbeitnehmern gewählten Telefonnummern speichern darf (sondern nur die ersten vier Ziffern, aus denen hervorgeht, in welches Land oder welche Region der Arbeitnehmer angerufen hat.[40]).

In der Zwischenzeit hat die Cnil mit ihrem Beschluss vom 20. Dezember 1994 ein *norme simplifée* genanntes Verfahren entwickelt (vereinfachte Erklärungsformalitäten bei Konformität mit der Norm), das den rechtlichen Rahmen für die Verwendung von Telefon-Selbstwählanlagen bildet. Der Beschluss

---

[39] TGI Paris, 1re ch., 19 avr. 2005, CE Effia Services, Synd. Sud Rail c/Effia Services, *CCE* oct. 2005, p. 46 s.

[40] Cnil, recomm. no 84-31, 18 sept. 1984, bezüglich der Verwendung von Telefon-Selbstwählanlagen am Arbeitsplatz, *3e 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.

erlaubt die Speicherung der von den Geschäftstelefonen der Arbeitnehmer aus gewählten Telefonnummern. Die Cnil hat klar festgelegt, dass die Nutzung der Telefonleitung für Privatgespräche der Arbeitnehmer erlaubt ist, der Arbeitgeber jedoch von den betreffenden Arbeitnehmern die Rückerstattung der Kosten für Privatgespräche fordern kann. Auch wenn der Arbeitgeber über die Möglichkeit verfügt, die von den Arbeitnehmern von ihrem Geschäftstelefon aus gewählten Nummern zu speichern, dürfen diese Nummern jedoch auf keinen Fall vollständig den anderen Arbeitnehmern offen gelegt werden. Außerdem darf der Arbeitgeber diese Nummern nicht länger als sechs Monate speichern. Abschließend erinnert die Cnil daran, dass die Personalvertreter vor der Einführung einer solchen Telefon-Selbstwählanlage konsultiert werden müssen.

33.13

Bedingungen für die Abhörung von Telefongesprächen der Arbeitnehmer. Das Abhören von Telefongesprächen ist durch das Gesetz vom 17. Juli 1970 rechtlich geregelt. Es wurde ergänzt durch das Gesetz vom 10. Juli 1991, das die Tragweite des Prinzips des Verbots des Abhörens von Telefongesprächen erweitert und so in das Strafgesetzbuch (*Code pénal*) einen Artikel 226-15 Absatz 2 einführt, der den Tatbestand inkriminiert, über Telefonleitungen abgegebene, übertragene oder erhaltene Nachrichten vorsätzlich abzuhören, umzuleiten, zu verwenden oder offen zu legen oder Geräte zu installieren, die für Abhörzwecke geschaffen sind (ein Jahr Gefängnisstrafe und 45000 € Geldstrafe).

Mit den gleichen Strafen wird der Tatbestand bestraft, Nachrichten – ob sie an ihr Ziel gelangt sind oder nicht – vorsätzlich zu öffnen, zu unterschlagen, zu verzögern oder zurückzusenden und ihren Inhalt unberechtigt zur Kenntnis zu nehmen (Code pénal, Art. 226-15, Absatz 1).

Artikel 432-9 des Strafgesetzbuchs inkriminiert ebenfalls den Tatbestand für einen Träger der öffentlichen Gewalt oder eine Person, die im Auftrag des öffentlichen Dienstes arbeitet, außerhalb der vom Gesetz vorgesehenen Fälle das Abhören oder das Umleiten von über Telefonleitungen abgegebenen, übertragenen oder erhaltenen Nachrichten, die Verwendung oder die Offenlegung ihres Inhalts anzuordnen, zu begehen oder zu erleichtern (drei Jahre Gefängnisstrafe, 45000 € Geldstrafe).

Außerdem unterlegt das Strafgesetzbuch die Verwendung von Geräten zur Abhörzwecken der Auflage einer von einer speziell zu diesem Zweck durch Artikel R.226-2 des Strafgesetzbuchs eingesetzten Kommission, deren Vorsitz das *secétariat général de la Défense nationale* (Generalsekretariat für nationale Verteidigung) innehat, ausgestellten Erlaubnis.

Bei der Anwendung dieses Verbots auf Arbeitgeber blieben Zweifel zurück. Die Cnil hat den Arbeitgebern erlaubt, Telefongespräche ihrer Arbeitnehmer abzuhören, unter der Bedingung, dass der Zweck der Abhöreinrichtung genau angegeben wird, dass die Arbeitnehmer vor der Inbetriebnahme des Geräts über das Abhören, die möglichen Konsequenzen aus dem Abhören der Gespräche und über die Zeiträume, während derer ihre Gespräche abgehört werden können, informiert werden. Außerdem ist vorgesehen, dass den Arbeitnehmern für alle Gespräche, die keinen direkten Zusammenhang mit dem Zweck der Abhörung haben, Telefonleitungen zur Verfügung stehen, die nicht an das Abhörgerät angeschlossen sind. Schließlich wird klargestellt, dass wenn das Abhören zum Zweck der Qualitätskontrolle des Telefongesprächs geschieht, die Arbeitnehmer kurzfristig von dem Ergebnis des abgehörten Gesprächs informiert werden müssen. Wenn die Analyse durchgeführt wurde, müssen die aufgezeichneten Gespräche anschließend innerhalb einer Frist zwischen zwei Wochen und einem Monat gelöscht werden. Auf der anderen Seite müssen auch die Kunden am anderen Ende der Telefonleitung über den Mitschnitt des Telefongesprächs informiert werden.

Die Rechtssprechung hat einige Prinzipien im Bereicht des Abhörens von Telefongesprächen bestätigt. So wurde die Nutzung des Geschäftstelefons zu Privatzwecken in vielen Fällen als grober Verstoß (*faute grave*) gewertet[41]. Andere

[41] Soc. 7 nov. 1995, n° 92-44.498, NPB, sté polyclinique Volney c/M. Bordeau ; v.

Urteile haben jedoch anerkannt, dass eine solche Nutzung, auch wenn sie keinen groben Verstoß (*faute grave*) darstellt, doch einen „reellen und ernsthaften" Kündigungsgrund (*cause réelle et sérieuse*) darstellen kann[42]. Die Rechtssprechung war jedoch auch der Ansicht, dass die aus diesem Grund ausgesprochenen Kündigungen ungerechtfertigt waren, wenn sie in keinem Verhältnis zu dem beanstandeten Verhalten standen[43].

Man kann also festhalten, dass die einzigen zugelassenen Ausnahmen, die dem Arbeitgeber das Abhören von Telefongesprächen erlauben, Telefonmarketing, Versandhandel und die Telefonzentrale betreffen. Wenn keine anerkannte und verhältnismäßige Notwendigkeit besteht, sollte eine Alternativlösung gesucht werden, zum Beispiel anstatt alle Gespräche mit der Kundschaft aufzuzeichnen, um für den Fall eines Rechtsstreits Beweismaterial zu sammeln, den Kunden um eine schriftliche Bestätigung, z.B. per E-Mail, zu bitten[44].

ABSCHNITT 2
BEDINGUNGEN FÜR DEN ZUGANG ZU PERSONENBEZOGENEN DATEN DER ARBEITNEHMER

33.21

Prinzip der Unverletzbarkeit des Briefgeheimnisses Jegliche Verletzung dieses Prinzips stellt den von Artikel 226-15 des französischen Strafgesetzbuchs (*Code pénal*) gemeinten und geahndeten Straftatbestand dar: Der Tatbestand, an Dritte adressierte Nachrichten – ob sie an ihr Ziel gelangt sind oder nicht – vorsätzlich zu öffnen, zu unterschlagen, zu verzögern oder fehlzuleiten oder ihren Inhalt unberechtigt zur Kenntnis zu nehmen, wird mit einer Gefängnisstrafe von einem Jahr und einer Geldstrafe von 45000 € geahndet. Mit derselben Strafe wird der Tatbestand, über Telefonleitungen abgegebene, übertragene oder erhaltene Nachrichten vorsätzlich abzuhören, umzuleiten, zu verwenden oder offen zu legen oder Geräte zu installieren, die für Abhörzwecke geschaffen sind, geahndet[45].

Mehrere Rechtsentscheidungen erinnern daran, dass es dem Arbeitgeber verboten ist, sich Kenntnis über den Inhalt der von seinen Arbeitnehmern versandten und erhaltenen persönlichen Nachrichten zu verschaffen. Das Urteil des Kassationsgerichtshofs vom 2. Oktober 2001 (*arrêt Nikon*[46]) stellt ausdrücklich klar, dass der Arbeitnehmer selbst am Arbeitsplatz und während der Arbeitszeit das Recht auf den Respekt seiner Privatsphäre hat; dass dies insbesondere das Briefgeheimnis einschließt; dass sich der Arbeitgeber daher nicht ohne dieses grundlegende Freiheitsrecht zu verletzen, Kenntnis über den Inhalt von

---

http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007286836.

[42] Soc. 3 févr. 1999, n° 97-40.495, NPB, sté Locamion c/Belgacem ben Mariem, http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007394923.

[43] Soc. 30 mars 1999, n° 97-40850 ; Soc. 18 nov. 1998, n° 96-43902, NPB, sté Cégéor c/Mme I. Maulet, v. http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007399898.

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

[45] Dieser Artikel stammt aus folgender Verordnung: ordonnance n° 2000-916, 19 sept. 2000, art. 3, *JO* 22 sept. 2000, en vigueur le 1er janvier 2002.

[46] Soc. 2 oct. 2001, n° 99-42.942, Nikon France c/M. Onof, aufgehoben durch CA Paris, 22 mars 1999 (Überweisung an CA Paris in anderer Besetzung), *D.* 2001, 3148, note P.-Y. Gautier ; *D.* 2002, somm. 2296, note C. Caron ; *CCE* 2001, comm. 120 et obs. ; *Dr. soc.* nov. 2001, p. 915, note J.-E. Ray — siehe auch die Debatte zu dem Urteil Nikon France, n° 99-42.942, *Bull. civ.* V, n° 291 ; *Sem. soc. Lamy* 15 oct. 2001, n° 1046, http://www.legifrance.gouv.fr/WAspad/UnDocument?base=CASS&nod=CXCXAX2001X10X05X00291X000 ; *Gaz. Pal.*, 16 mai 2002, n° 136, p. 47, note H. Vray ; *LPA*, 10 déc. 2001, n° 245, p. 6, note G. Picca.

persönlichen Nachrichten verschaffen darf, die der Arbeitnehmer mit einem Computer versandt und empfangen hat, der ihm für seine Arbeit zur Verfügung gestellt worden war und dies selbst in dem Fall gilt, in dem der Arbeitgeber eine über die berufliche Tätigkeit hinausgehende Nutzung des Computers verboten hat. Im vorliegenden Fall hatte der Arbeitgeber entdeckt, dass sein Angestellter während seiner Arbeitszeit und von dem Computer aus, den ihm das Unternehmen, bei dem er angestellt war, zur Verfügung gestellt hatte, eine parallele berufliche Tätigkeit ausübte. Laut den Richtern waren die aus der E-Mailbox des Arbeitnehmers gewonnenen Beweismittel auf rechtswidrige Weise erbracht worden und wurden deshalb von der Verhandlung ausgeschlossen.

In jüngerer Zeit hat der Kassationsgerichtshof ein Urteil des Berufungsgerichts bestätigt, das den privaten Charakter einer E-Mail eines Arbeitnehmers an seinen Kollegen hervorhob und daraus ableitete, dass dieses Element der Privatsphäre der betroffenen Person keinen Kündigungsgrund darstellen könne.[47].

Das Prinzip der Unverletzbarkeit des Briefgeheimnisses gilt auch für die Arbeitnehmer, wie es das *tribunal de grande instance* (Zivilgericht der ersten Instanz) von Paris in seiner Entscheidung (TGI Paris, 1. Juni 2007[48]) zeigte, bei der ein ehemaliger Informatikberater eines Unternehmens verurteilt wurde, der nach dem Verlassen des Unternehmens die Passwörter behalten hatte, die ihm den Zugang zu den E-Mailboxen des Geschäftsführers und des Leiters der Personanlabteilung ermöglichten. In dem vorliegenden Fall hatten die beiden Führungskräfte bemerkt, dass sie elektronisch überwacht wurden. Bei der bei dem Berater durchgeführten Durchsuchung konnten Verbindungen zu den betroffenen E-Mailboxen nachgewiesen werden. Er gab an, die Passwörter an seinen Bruder weitergegeben zu haben, einen ehemaligen Angestellten des Unternehmens, der nun für den Konkurrenten arbeitete, damit dieser einen möglichen Kauf des Unternehmens *Oddo* durch seinen Arbeitgeber überwachen konnte. Wie die Richter erinnert haben, stellt bereits die Tatsache, unter Verwendung deren Passwörter Einblick in die E-Mails von Dritten zu nehmen, einen betrügerischen Zugriff auf ein Computersystem und eine Verletzung des Briefgeheimnisses laut Artikel 226-15 des Strafgesetzbuchs dar.

33.22

Anzunehmende berufliche Natur von Nachrichten. Laut Cnil muss im Allgemeinen angenommen werden, dass eine mit einem Computer am Arbeitsplatz, der dem Arbeitnehmer von seinem Unternehmen oder der Behörde zur Verfügung gestellt wurde, versandte oder empfangene Nachricht beruflicher Art ist, außer eine offensichtliche Angabe in der Betreffzeile oder in dem Namen des Verzeichnisses, unter der sie von ihrem Empfänger gespeichert wird, verleiht ihr den Status einer Privatkorrespondenz, die durch das Briefgeheimnis geschützt ist[49].

Dieser Argumentation folgten die Richter des Berufungsgerichts von Bordeaux bei der Zulassung der von dem Arbeitgeber erbrachten Beweismittel. Sie haben klargestellt, dass die Ordner und Dateien auf dem Geschäftscomputer der Arbeitnehmer oder auch die Dokumente an ihrem Arbeitplatz beruflicher Art sind, wenn sie nicht ausdrücklich als persönlich gekennzeichnet sind. Daraus folgt, dass der Arbeitgeber ein rechtmäßiges Zugriffsrecht auf diese beruflichen Ordner, Dateien oder Dokumente hat, ohne dass die Anwesenheit des betroffenen Arbeitnehmers während der Einsichtnahme erforderlich ist. Folglich darf der Arbeitgeber auf die Computer der Arbeitnehmer zugreifen. Der Arbeitgeber hatte also völlig legitim Zugang zu dem Computer seiner Angestellten. Mangels einer durch die Angestellte erfolgte besonderen Kennzeichnung der E-Mails, die sie von ihrem Geschäftscomputer aus versandt hat, hat der Arbeitgeber das Recht, diese als Beweismittel vor Gericht zu verwenden. Folglich wird die Existenz dieser E-Mails anerkannt und die Tatsachen sind bewiesen (CA Bordeaux, ch. soc., sect.

---

[47] Soc. 6 juin 2007, n° 05-43.996, NPB, sté Eliophot c/M. X…. : Ablehnung des Rechtsmittels CA Aix-en-Provence, 18e ch., 7 juin 2005.

[48] TGI Paris, 1er juin 2007, Oddo et Cie c/Trinh Nghia T… et Trung T…, einsehbar über die Website legalis.net : http://www.legalis.net/jurisprudence-decision.php3?id_article=2179.

[49] Cnil, Guide pratique pour les employeurs.

A, 8 févr. 2005[50]).

Aus dieser Logik ergibt sich im Umkehrschluss, dass der Arbeitgeber im Prinzip eine Nachricht, sobald diese als privat gekennzeichnet ist, nicht öffnen darf, um ihren Inhalt zu lesen.

Andere Urteile erinnern jedoch daran, dass das Prinzip der Unverletzbarkeit des Briefgeheimnissen unter allen Umständen anwendbar ist, auch wenn der Betreff der Nachricht nicht eindeutig ist und dass es Aufgabe des Arbeitgebers ist, die Elemente zu überprüfen, die der Nachricht einen offensichtlich persönlichen Charakter verleihen (dies wäre der Fall bei einer Nachricht, in deren Betreffzeile es um Urlaub geht und die in einem Ordner mit der Bezeichnung "persönlich" abgelegt ist)[51].

Um diese Regel auszuschalten, greifen die Arbeitgeber auf verschiedene Mittel zurück, insbesondere auf die Aufnahme spezieller Bestimmungen in die Charta zur Benutzung der Informatik. Als Beispiel kann das Urteil des *Conseil des prud'hommes* (erstinstanzliches Arbeitsgericht) von Nanterre vom 15. September 2005 geschildert werden. Im vorliegenden Fall war ein Arbeitnehmer, der einem Konkurrenzunternehmen viele Nachrichten hatte zukommen lassen, wegen groben Verstoßes *(faute grave)* entlassen worden. Die Richter argumentierten, dass obwohl die Nachricht mit dem Vermerk *message strictement privé et confidentiel* („streng private und vertrauliche Nachricht") versehen war, dem Antrag des Klägers auf eine Kündigung „aus reellem und ernsthaften Grund" (*cause réelle et sérieuse*) nicht stattgegeben wird, weil die in diesem Unternehmen gültige Charta für die Nutzung der Kommunikationsmittel, die die Betriebsordnung ergänzt, genau festlegte, dass Nachrichten mit privatem Charakter mit dem Vermerk „*PRV*" versehen sein müssen. Aus diesem Grund hatte der Arbeitgeber die absolute Freiheit, alle Nachrichten, die nicht mit diesem Vermerk versehen worden waren, einzusehen.

33.23

Zugriff auf persönliche Dateien in Anwesenheit des Arbeitnehmers. Das Berufungsgericht von Besançon hat geurteilt, dass die Verletzung des Briefgeheimnisses nicht geltend gemacht werden konnte, da der Arbeitgeber nicht direkt auf die betreffenden (pornographischen) Dateien zugegriffen hatte, sondern sie von einem vom *Conseil des prud'hommes* beauftragten gerichtlichen Sachverständigen in Anwesenheit der Parteien oder ihrer Berater geöffnet und eingesehen wurden (CA Besançon, 24. sept. 2004[52]). Der Kassationsgerichtshof hat bestätigt, dass der Arbeitgeber Zugang zu den persönlichen Dateien eines Arbeitnehmers haben darf. In dem vorliegenden Fall hatte der Arbeitgeber erotische Fotografien in der Schreibtischschublade des Arbeitnehmers entdeckt und daraufhin beschlossen, die Computerfestplatte dieses Arbeitnehmers zu untersuchen. In einer „*perso*" genannten Datei befanden sich eine Reihe von Dokumenten, die nichts mit der beruflichen Tätigkeit des Arbeitnehmers zu tun hatten. Laut Kassationsgerichtshof darf der Arbeitgeber die von dem Arbeitnehmer als persönlich gekennzeichneten Dateien, die sich auf der Festplatte des Computers befinden, der ihm für seine Arbeit zur Verfügung gestellt worden war, nur in Anwesenheit des Arbeitnehmers öffnen oder wenn er ordnungsgemäß einberufen worden war, außer es liegt ein besonderes Ereignis oder Risiko vor (Soc. 17 mai 2005[53]). In einem jüngeren Urteil hat der Hohe Gerichtshof präzisiert, dass bei den Verzeichnissen und Dateien, die ein Arbeitnehmer mit dem Computer erstellt, die ihm sein Arbeitgeber für die Ausübung seiner beruflichen Tätigkeit zur Verfügung gestellt hat, außer wenn der Arbeitnehmer sie als

---

[50] CA Bordeaux, ch. soc., sect. A, 8 févr. 2005, n° 04/02449.

[51] CA Toulouse, 4e ch. soc., 6 févr. 2003, aff. n° 02-02519.

[52] CA Besançon, ch. soc., 21 sept. 2004, RG n° 2003-1807, SNC General Electric Energy Products France c/Girardot et a., *RJS* 4/2005, n° 342.

[53] Soc. 17 mai 2005, n° 03-40.017, NPB, Philippe X. c/Cabinet-Science, *Juris-Data* n° 2005-028449 ; *CCE* juill.-août 2005, p. 34 s., comm. A. Lepage ; siehe auch G. Haas et L. Goutorbe, « Cybersurveillance : l'employeur doit être prudent en matière de collecte de preuve », Expertises août-sept. 2005, p. 304 ; *Gaz. Pal.*, 20 oct. 2005, n° 293, p. 36, note S. Hadjali ; *LPA* 23 avr. 2007, n° 81, p. 6, note S. Tournaux

persönlich kennzeichnet, davon ausgegangen werden kann, dass sie beruflicher Art sind und der Arbeitgeber somit auch in Abwesenheit des Arbeitnehmers auf sie zugreifen darf (Soc. 18 oct. 2006[54]).

In derselben Logik hat das Berufungsgericht von Versailles die von einem Arbeitgeber als Beweismittel erbrachten Nachrichten abgewiesen, die zeigten, dass sein Arbeitnehmer ein Konkurrenzunternehmen gründete, da die Nachrichten dem Notebook des Arbeitnehmers entnommen wurden, ohne seiner vorherigen Bitte nachgekommen zu sein, ihm seine persönlichen Dateien zurückzugeben (CA Versailles, 2 avr. 2003[55]).

33.23

SMS als Beweismittel. Der Kassationsgerichtshof musste über die Zulässigkeit von SMS als Beweismittel in einem Fall entscheiden, in dem eine wegen groben Verstoßes *(faute grave)* entlassene Arbeitnehmerin ihre Kündigung anfocht, indem sie die sexuelle Belästigung geltend machte, deren Opfer sie war. Diese durch SMS bewiesene Tatsache war vom Berufungsgericht zugelassen worden. Der Arbeitgeber legte eine Nichtigkeitsklage vor dem Kassationsgerichtshof ein, da er die Zulässigkeit der erbrachten Beweismittel anfocht (ohne das Wissen des Autors rekonstruierte und von einem Gerichtsdiener transkribierte telefonische Nachrichten und eine von der Arbeitnehmerin ohne das Wissen des Arbeitgebers auf einer Mikrokassette mitgeschnittene Unterhaltung). Der Kassationsgerichtshof vertrat die Auffassung, dass die Aufzeichnung eines privaten Telefongesprächs ohne das Wissen des Urhebers der Äußerungen zwar in der Tat eine unlautere Vorgehensweise ist, die einen auf diese Weise erlangten Beweis vor Gericht unzulässig macht, dies jedoch nicht für die Verwendung von SMS durch den Empfänger gilt, da der Absender einer SMS nicht in Unkenntnis darüber sein kann, dass SMS im Telefon des Empfängers gespeichert werden. Mit den SMS konnte also die sexuelle Belästigung, über die die Arbeitnehmerin klagte, nachgewiesen werden (Soc. 23 mai 2007[56]).

ABSCHNITT 3
EIN HEIKLES INSTRUMENT

33.30

Biometrische Zugangskontrolle. Bei den biometrischen Vorrichtungen zur Zugangskontrolle am Arbeitsplatz oder von Informatiksystemen lässt sich eine bedeutende Entwicklung beobachten (siehe Nr. 28.20 f.)

Ihre Verwendung unterliegt einer von der Cnil ausgestellten Genehmigung. In einem am 28. Dezember 2007 veröffentlichten Leitfaden[57], erläutert die Cnil ihre wichtigsten Beurteilungskriterien sowie die Risiken, denen sich die Unternehmen aussetzen, die auf solche Techniken zurückgreifen, und die Rechte der Arbeitnehmer (siehe Nr. 28.21 f.).

Das wichtigste ist, dass die Vorrichtung die Reaktion auf einen starken Sicherheitszwang ist. Außerdem muss der Zweck der Vorrichtung auf die Zugangskontrolle zu einem genau festgelegten Bereich für eine festgelegte Anzahl von Personen begrenzt sein (1. Kriterium). Wegen der mit ihrem Einsatz einhergehenden Risiken für den Schutz personenbezogener Daten muss die

---

[54] Soc. 18 oct. 2006, n° 04-48.025, Jérémy L. F… c/Techni-Soft, *Bull. civ.* V, 18 oct. 2006, comm. J.-E. Ray, 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 ; *Gaz. Pal.* 18 janv. 2007, n° 18, p. 37, note S. Hadjali et C. Fagot ; *LPA* 28 avr. 2008, n° 85, p. 7, note X. Daverat.

[55] CA Versailles, 2 avr. 2003, aff. n° 02-00293.

[56] Soc. 23 mai 2007, n° 05-17.818, NPB, *Bull. civ.* V ; *D.* 2007, AJ 1590, note A. Fabre ; *Gaz. Pal.* 18 mars 2008, n° 78, p. 20 ; *LPA* 28 avr. 2008, n° 85, p. 7, note X. Daverat et S. Tournaux.

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

Vorrichtung verhältnismäßig, d.h. an den beabsichtigten Zweck angepasst sein (2. Kriterium). Es müssen Maßnahmen ergriffen werden, um zu garantieren, dass die Authentifizierung und/oder Identifizierung nicht zur Offenlegung der Daten führt (3. Kriterium). Schließlich müssen die betroffenen Personen informiert werden (4. Kriterium).

So hat die Cnil am 13. September 2007 die Einführung einer automatischen Verarbeitung personenbezogener Daten genehmigt, die auf einer Stimmerkennung beruht[58]. Diese Vorrichtung, die es ermöglicht, automatisch Passwörter zum Zugang zu dem Computersystem des Unternehmens zu generieren und zurückzusetzen, beruht auf der Erkennung des Stimmabdrucks der Arbeitnehmer.

Am 8. November 2008 hat die Cnil durch fünf Beschlüsse (Nr. 2007-335 bis Nr. 2007-339)[59], die Einführung mehrerer Vorrichtungen genehmigt, die auf der Erkennung des Adermusters am Finger beruhen und zur Zugangskontrolle zu Räumen oder Computersystemen dienen.

33.31

Geolokalisierung. Immer mehr Unternehmen verwenden Geolokalisierungsgeräte, die über die Lokalisierung der verwendeten Arbeitsmittel, insbesondere der Dienstfahrzeuge, die geographische Ortung ihrer Arbeitnehmer zu einem bestimmten Zeitpunkt oder fortlaufend ermöglichen. Diese Geräte beruhen hauptsächlich auf der Nutzung der GSM/GPS-Technologie, die zu jedem Zeitpunkt die Ortung eines mit einem solchen System ausgestatteten Fahrzeugs ermöglicht. Durch die Verarbeitung der Ergebnisse dieser Geräte können Daten wie die Nutzungsdauer des Fahrzeugs, die zurückgelegte Kilometerzahl und die Fahrtgeschwindigkeiten gesammelt werden.

Die Cnil vertritt die Ansicht, dass diese permanente Überwachung der von einem Arbeitnehmer zurückgelegten Wege unverhältnismäßig ist, wenn die von ihm zu erfüllende Aufgabe nicht der Fahrweg als solcher ist, sondern die Erfüllung einer anderen Leistung, die selbst überprüft werden kann[60]. So entschied der Kassationsgerichtshof in einem Urteil vom 26. November 2002[61], dass eine von dem Arbeitgeber organisierte Beschattung zur Kontrolle und Überwachung der Tätigkeit eines Arbeitnehmers ein rechtswidriges Beweismittel darstellt, ganz gleich, ob der Arbeitnehmer über diese Kontrolle informiert worden war oder nicht[62]. So hat die Cnil mit einer Konsultierung der betroffenen Personen (vor allem in Ministerien, gewerkschaftlichen und beruflichen Organisationen) und der Integratoren von Geolokalisierungsdiensten begonnen, um die Nutzungsbedingungen dieser Geräte sinnvoll festzulegen[63].

Diese Reflektion hat zu der Annahme von zwei Beschlüssen (Nr. 2006-066 und Nr. 2006-067) am 16. März 2006 geführt, die je eine Empfehlung und eine *norme simplifiée* (vereinfachte Erklärungsformalitäten bei Konformität mit der Norm) bezüglich der von öffentlichen oder privaten Institutionen eingeführten automatischen Verarbeitungssysteme personenbezogener Daten, die zur Geolokalisierung der von ihren Arbeitnehmern genutzten Fahrzeugen dienten, aufstellten[64]. Angesichts des sehr in die Privatsphäre eingreifenden Charakters der Geräte zur Geolokalisierung stellt die Cnil eine Liste der Zwecke auf, zu denen ihr die Verwendung eines solchen Geräts legitim und somit zulässig erscheint:

---

[58] Cnil, délib. n° 2007-248, 13 sept. 2007, http://www.wk-rh.fr/mybdd/upload/bdd_80/Cnil-D2007-248.pdf.

[59] Cnil, délib. n°s 2007-335 à 2007-339, 8 nov. 2007, http://www.wk-rh.fr/mybdd/upload/bdd_80/Cnil-D2007-335-339.pdf.

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

[61] Soc. 26 nov. 2002, n° 00-42.401, *Bull. civ.* V, n° 352 ; *RTD civ.* 2003, 58.

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

[63] Cnil, communiqué 29 sept. 2005.

[64] Cnil, délib. n° 2006-067, 16 mars 2006, zur Annahme einer *norme simplifiée* (vereinfachte Erklärungsformalitäten bei Konformität mit der Norm) bezüglich der von öffentlichen oder privaten Institutionen eingeführten automatischen Verarbeitungssysteme personenbezogener Daten, die zur Geolokalisierung der von ihren Arbeitnehmern genutzten Fahrzeugen dienen (norme simplifiée n° 51), *JO* n° 1003, 3 mai.

Sicherheit oder Sicherung der Arbeitnehmer oder der Ware, bessere Mittelvergabe, Nachverfolgung und Fakturierung einer Transportdienstleistung von Personen oder Waren oder einer im direkten Zusammenhang mit der Benutzung des Fahrzeugs stehenden Dienstleistung, Nachverfolgung der Arbeitszeit. Andererseits gibt die Datenschutzbehörde an, dass die Verwendung eines solchen Geräts nicht zu einer permanenten Überwachung des betroffenen Arbeitnehmers führen darf. Sie sieht eine bedeutende Erleichterung der behördlichen Formalitäten für die Unternehmen vor, die sich an die vorgesehenen Bedingungen halten, vor allem was die Art der erhobenen Daten und die Dauer ihrer Speicherung anbelangt (*norme simplifiée* Nr. 51). Dafür stellt die Cnil in diesem Beschluss eine Liste der Zwecke auf, die die Sammlung von Daten durch ein solches Verfahren unbedingt erfüllen muss. Die Cnil schränkt auch die Daten ein, die durch die Verwendung eines Geolokalisierungsgeräts verarbeitet werden dürfen. Sie stellt auch eine Liste zur Einschränkung der Empfänger dieser Daten auf.

Schließlich stellt die Cnil klar, dass die für die Datenverarbeitung verantwortlichen Personen, die ein Geolokalisierungsgerät einführen wollen, unbedingt vor der Einführung dieses Geräts die Instanzen, die das Personal vertreten, informieren und konsultieren müssen. Diese Informationspflicht gilt auch hinsichtlich der von der Überwachung durch das Gerät betroffenen Arbeitnehmer. Auf der anderen Seite müssen sich die für die Datenverarbeitung verantwortlichen Personen vergewissern, dass alle notwendigen Sicherheitsmaßnahmen ergriffen wurden.

33.32

Whistleblowing-Systeme. Das amerikanische Gesetz *Sarbanes-Oxley Act* (Juli 2002) gebietet den Unternehmen, deren Wertpapiere an US-Börsen gehandelt werden und ihren ausländischen Tochterunternehmen die Einrichtung eines Whistleblowing-Systems, das die Weitergabe eines im Unternehmen begangenen Verstoßes an Stellen in- oder außerhalb des Unternehmens ermöglichen soll (im Deutschen wird ebenfalls der anglo-amerikanische Begriff *Whistleblowing* verwendet, der mit „in die Pfeife blasen", „Alarm schlagen" übersetzt werden kann. In Frankreich wird das Whistleblowing als *alerte professionnelle* oder auch *alerte éthique*, also „Berufsalarm" oder „ethischer Alarm" bezeichnet).

In Frankreich sind diese Whistleblowing-Systeme nicht gesetzlich geregelt, aber womöglich gibt es bald ein entsprechendes Gesetz, das von einem am 7. März 2007 an den damaligen französischen Arbeitsminister übergebenen Bericht befürwortet wird.[65] In der Tat befürwortet dieser Bericht (*Charte d'éthique, alerte professionnelle et droit du travail français : état des lieux et perspectives)* mehrere Wege zur Stärkung der rechtlichen Sicherheit der Ethikcharta und zur rechtlichen Regelung eines Whistleblowing-Systems. Er schlägt unter anderem vor, in das französische Arbeitsgesetzbuch (*Code du travail*) spezielle Bestimmungen aufzunehmen, die es den Unternehmen ermöglichen, Systeme einzusetzen, die die Möglichkeit bieten, nicht nur Verstöße gegen rechtliche oder reglementarische Bestimmungen und Angriffe auf die Personenrechte und die Gesundheit der Arbeitgeber weiterzugeben, sondern auch Verstöße gegen ethische oder berufliche Regeln. Diese neue gesetzliche Regelung hätte hauptsächlich die Ziele, das Whistleblowing zu definieren, die rechtlichen Instrumente zur Einrichtung des Systems zu bestimmen, die Organisationsregeln, die das gewählte rechtliche Instrument beinhalten muss, festzulegen und den Whistleblower zu schützen.

Momentan ist es die Cnil, die die Bedingungen zur Umsetzung dieser Systeme eingrenzt, welche sie als Systeme definiert, die den Arbeitnehmern einer öffentlichen oder privaten Institution zur Verfügung gestellt werden, um sie zu ermuntern, zusätzlich zu den üblichen Warnmöglichkeiten im Falle eines Problems, ihrem Arbeitgeber Verhaltensweisen zu melden, von denen sie der Meinung sind, dass sie gegen die anzuwendenden Regeln verstoßen und um die Überprüfung der so erhaltenen Warnung innerhalb der betroffenen Institution zu organisieren.

---

[65] Siehe den Bericht („Charte d'éthique, alerte professionnelle et droit du travail français : état des lieux et perspectives, auf
http://lesrapports.ladocumentationfrancaise.fr/BRP/074000335/0000.pdf l.

Zunächst hatte die Cnil sich im Mai 2005 geweigert[66], die Einführung solcher Systeme zu genehmigen, mit der Begründung, sie wären unverhältnismäßig im Bezug auf die verfolgten Ziele und auf die Risiken von verleumderischen Denunzierungen und einer Stigmatisierung der Arbeitnehmer, die durch das Whistleblowing gemeldet werden. Sie hat auch betont, dass die von einer Meldung betroffenen Arbeitnehmer per se nicht vom Beginn der Sammlung von Daten an, die ihre berufliche oder staatsbürgerliche Integrität in Frage stellen, informiert würden und somit nicht die Mittel hätten, sich dieser sie betreffenden Datenverarbeitung zu widersetzen. Die Art und Weise der Erhebung und der Verarbeitung dieser Daten, von denen einige Tatsachen betreffen könnten, die einen Straftatbestand begründen könnten, kann somit als unlauter qualifiziert werden. Diese Position brachte die französischen Tochterunternehmen von amerikanischen Unternehmen in Schwierigkeiten, die verpflichtet sind, die widersprüchlichen Bestimmungen des französischen Datenschutzgesetzes *loi informatique et libertés* und des amerikanischen *Sarbanes-Oxley act* einzuhalten.

Deshalb hat die Cnil ihre Position revidiert. Zunächst hat sie sich an die *Securities and Exchange Commission (SEC)* angenähert, um Garantien zu finden, die sowohl mit dem französischen Datenschutzgesetz *loi informatique et libertés* als auch mit dem amerikanischen *Sarbanes-Oxley act* vereinbar sind und hat am 10. November 2005 ein *document d'orientation* (Orientierungsdokument) veröffentlicht, um die Bedingungen genau festzulegen, unter denen die Einführung eines Whistleblowing-Systems möglich ist[67] . Anschließend hat sie am 8. Dezember 2005 eine Entscheidung über eine *autorisation unique* (Rahmenbeschluss) angenommen, die die Bedingungen festlegt, die eingehalten werden müssen, um von den vereinfachten Formalitäten profitieren zu können[68] . Im Wesentlichen hat sie das Prinzip des Whistleblowing zugelassen, aber dabei sein Anwendungsgebiet auf genau festgelegte Bereiche beschränkt (Buchhaltung, Finanz- und Bankensektor und Korruptionsbekämpfung). Darüber hinaus sieht sie vor, dass ein solches System die Ergreifung von Vorsichtsmaßnahmen erfordert, um die betreffenden Daten zu sammeln, zu verarbeiten und außerhalb der Europäischen Union zu übertragen. Parallel dazu wurden die Rechte der Arbeitnehmer auf Information, Zugang und Richtigstellung geändert.

Die Artikel-29-Datenschutzgruppe (siehe Nr. 15.18) hat ebenfalls am 1. Februar 2006 eine Stellungnahme über die Whistleblowing-Systeme im Banken- und Buchhaltungssektor, im Bereich der internen Rechnungslegungskontrolle, der Wirtschaftsprüfung und der Bekämpfung von Korruption und Finanzkriminalität angenommen[69] . Sie gibt im Wesentlichen die Prinzipien des von der Cnil im November und Dezember 2005 erstellten *document d'orientation* (Orientierungsdokument) und der *autorisation unique* (Rahmenbeschluss) wider.

Am Rande dieser Vorschriften muss wegen der Flut der Klagen zur Aussetzung der Whistleblowing-Systeme die Rechtssprechung berücksichtigt werden. So hat der für Entscheidungen über den Eilantrag zuständige Richter des erstinstanzlichen Zivilgerichts von Libourne (Gironde) per Verordnung vom 15. September 2005[70], das französische Tochterunternehmen eines

---

[66] Cnil, délib. n° 2005-110, 26 mai 2005, bezüglich eines Antrags von "Mc Donald's France" zur Genehmigung der Einführung eines Whistleblowing-Systems,
http://www.cnil.fr/index.php?id=1833&delib[uid]=73&cHash=ed7a84e6a7 — und Cnil, délib. n° 2005-111, 26 mai 2005, bezüglich eines Antrags von der "Compagnie européenne d'accumulateurs" zur Genehmigung der Einführung eines Whistleblowing-Systems,
http://www.cnil.fr/index.php?id=1834&delib[uid]=74&cHash=89a931a002.

[67] Von der Cnil am 10. November 2005 angenommenes Orientierungsdokument zur Einführung von Whistleblowing-Systemen in Konformität mit dem im August 2004 geänderten französischen Datenschutzgesetz vom 6. Januar 1978 (*loi informatique et libertés*):
http://www.cnil.fr/fileadmin/documents/La_CNIL/actualite/CNIL-docori-10112005.pdf.

[68] Cnil, délib. n° 2005-305, 8 déc. 2005, über eine *autorisation unique* (Rahmenbeschluss) für die Verarbeitung personenbezogener Daten im Rahmen von Whistleblowing-Systemen,
http://www.cnil.fr/index.php?id=1969.

[69] Artikel-29-Datenschutzgruppe, Stellungnahme 1. Februar 2006,
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_de.pdf.

[70] TGI Libourne, 15 sept. 2005, BSN Glasspack, zitiert in « Alertes éthiques : quelles orientations

amerikanischen Unternehmens angewiesen, sein Whistleblowing-System zurückzunehmen, mit der Begründung, dass diese Maßnahme aufgrund des möglichen Schadens für die individuellen Freiheitsrechte der Arbeitnehmer geboten ist, die Opfer von anonymen Denunzierungen auf der Grundlage eines privaten Systems werden könnten, das sich jeglicher Kontrolle entzieht, ohne dass das Unternehmensinteresse ein solches System ernsthaft rechtfertigen könnte. Per Verordnung vom 27. Dezember 2006 des für Entscheidungen über den Eilantrag zuständigen Richters des erstinstanzlichen Zivilgerichts Nanterre wurde auch die Verteilung eines Fragebogens mit dem Titel „*business ethics*" gestoppt, den die Arbeitnehmer verpflichtend ausfüllen mussten und dabei unter anderem dazu verpflichtet waren anzugeben, ob ein Mitglied ihrer Familie ein bedeutendes Interesse an einem anderen Unternehmen hat, das in Konkurrenz zu ihrem Unternehmen steht oder auch, ob eine persönliche oder familiäre Beziehung sie davon abbringen könne, im absoluten Interesse ihres Unternehmens zu handeln[71]. Der für Entscheidungen über den Eilantrag zuständige Richter war der Meinung, dass dieses Whistleblowing-System nicht mit dem Beschluss der Cnil vom 8. Dezember 2005 vereinbar sei, insbesondere insofern, als die Cnil klarstellt, dass nur solche Whistleblowing-Systeme von einer *autorisation unique* (Rahmenbeschluss) profitieren können, die nicht verpflichtender Art sind.

Man muss jedoch auch mit gerichtlichen Entscheidungen rechnen, die Whistleblowing-Systeme für gültig erklären wie das Urteil vom 19. September 2006 vom erstinstanzlichen Zivilgericht von Lyon, in dem argumentiert wurde, dass auch wenn die Antragsteller anfänglich das eingerichtete Whistleblowing-System zur Sprache gebracht und kritisiert hatten, doch festgestellt werden muss, dass der überarbeitete Text, indem er ein freiwilliges Mittel darstellt, das nur Interessen erfüllen kann, deren Legitimität bewiesen ist (Bereich der Buchhaltung, Rechnungslegungskontrolle und Korruptionsbekämpfung), indem die Identität der meldenden Person vertraulich behandelt wird und indem die angezeigte Person ein Zugangsrecht zu den Informationen und ein Recht auf Richtigstellung hat, mit dem Beschluss der Cnil vom 8. Dezember 2005 konform ist[72]. Bereits im April 2005 war der für Entscheidungen über den Eilantrag zuständige Richter von Nanterre der Meinung, dass das dem Betriebsrat vorgelegte Dokument, mit dem ein Whistleblowing-System eingeführt wurde, im Stadium des Eilantrags und der Beweislage kein Problem darzustellen schien, weder der Interpretation noch der Verletzung der Rechte der Arbeitnehmer, da es sich um ein freiwilliges Verfahren handelte, aus dem sich keine Sanktionen oder Konsequenzen jeglicher Art ergeben [73].

Manche sind der Meinung, dass diese juristischen Präzedenzfälle genügen, um den für Whistleblowing-Systeme anwendbaren Rahmen festzulegen. Die Autoren des Berichts vom März 2007 stellen ihrerseits fest, dass man zu einer Zeit, in der viele das legitime Bedürfnis nach einer größeren Rechtssicherheit haben, im Bereich des Whistleblowing eine gerichtliche Konstruktion, die von ihrer Natur her langsam und konfliktgeladen ist, besser vermeiden sollte.

Die Rechtssprechung im Bereich der Whistleblowing-Systeme führt unbestritten noch zu Diskussionen.

---

suite aux décisions de la CNIL ? », *RLDI* 2005/11, n° 318, obs. F. Naftalkski ; *CCE* déc. 2005, A. Lepage, comm. 191, p. 37 et A. Caprioli, comm. 194, p. 44.

[71] TGI Nanterre, 27 déc. 2006, Comité central d'entreprise Dupont de Nemours c/SAS Dupont de Nemours, n° 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. réf., 1er avr. 2005, CE ING Bank c/ING Bank France, unveröffentlicht

KAPITEL

34. Allgemeine Prinzipien für den Respekt der Privatsphäre des Arbeitnehmers

ABSCHNITT 0
ZUR ORIENTIERUNG

34.00

Plan des Kapitels.

Abschnitt 1 Rechte des Arbeitnehmers

Abschnitt 2 Relevanz und Zweck der Datenverarbeitung

Abschnitt 3 Schutzmaßnahmen

34.01

Anwendbare Texte.

> Französische Texte.

Gesetzestexte.

C. trav., art. L. 1121-1 et L. 1134-1 s.

Stellungnahmen und Empfehlungen.

Cnil, délib. n° 2002-001, vom 8. Januar 2002, bezüglich der automatischen Verarbeitung namensbezogener Informationen am Arbeitplatz für die Verwaltung von Zugangskontrollen zu Räumlichkeiten, Arbeitszeiten und Kantinen – Cnil, délib. n° 2007-368, 11 déc. 2007, Stellungnahme zu einem Entwurf eines Erlasses (*projet de décret)* des *Conseil d'État* zur Änderung des Erlasses *décret* n° 2005-1726 vom 30. Dezember 2005 bezüglich der elektronischen Pässe.

34.02

Relevante Rechtssprechung.

> Zum Informationsrecht des Arbeitnehmers.

• **Soc. 6 avr. 2004,** n° 01-45.227, Sté Allied signal industrial Fibers c/M. Pacheco NPB, *Bull. civ.* V, n° 103 ; *Gaz. Pal.* 20 juill. 2004, n° 202, p. 31, note J. Bérenguer-Guillon et L. Maurel-Guignot — bestätigt durch **CA Nancy, ch. soc., 25 juin 2001,** M. Pacheco c/Sté Allied signal industrial Fibers, *Juris-Data* n° 145997 ; *Dr. ouvrier* 2002, n° 652.

Für das (bestätigte) Urteil in erster Instanz s. **Cons. prud'h. Longwy, 3 déc. 1999.**

* s. Nr. 34.10, auch Nr. 14.24.

> Über den Zugang zu den Daten der jährlichen Beurteilung

• **Soc. 23 oct. 2001,** n° 99-44.215, NPB, CANSSM c/Mme Vicheney, siehe http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007628680 — bestätigt durch **CA Paris, 18e ch., sect. A, 1er juin 1999.**

* s. Nr. 34.12.

> Zu der Beurteilung der Relevanz der Daten.

• **Civ. 1re, 29 mai 1984,** n° 82-12.232, CEMU c/Mme D… et a., *Bull. civ.* I, n° 176 — bestätigt durch **CA Rouen, 3e ch., 17 déc. 1981**.

* s. Nr. 34.21.

34.03

> Bericht:

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

> Artikel.

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

34.04

Grundsätzliche Fragen

• Welche Rechte hat der Arbeitnehmer bezüglich der ihn betreffenden personenbezogenen Daten?

* s. Nr. 34.10 f.

• Welchen Verpflichtungen unterliegt der Arbeitgeber?

* s. Nr. 34.21 f.

ABSCHNITT 1
RECHTE DES ARBEITNEHMERS

34.10
Recht auf Information. S. Nr. 12.30 f. und 32.11 f.

34.11
Recht auf Zugang, Richtigstellung und Vernichtung. Jeder Arbeitnehmer hat wie jede natürliche Person das Recht darauf, sich alle ihn betreffenden Informationen einer Datei mitteilen zu lassen und die falschen Angaben richtig stellen oder löschen zu lasen. Außerdem hat er das Recht, sich der Aufnahme in eine Datei zu widersetzen, aber nur aus legitimen Motiven, über die der Arbeitgeber zu entscheiden hat. Er kann sich nicht der Erhebung von Daten entziehen, die für die Einhaltung einer gesetzlichen Verpflichtung wie zum Beispiel für die obligatorischen Erklärungen der Sozialabgaben notwendig sind. Er kann sich jedoch weigern, dass der Betriebsrat die ihn betreffenden Informationen erhält. Er muss jedoch klar und deutlich über die sich für ihn ergebenden Konsequenzen informiert werden (z.B. Ausschluss vom Vorteil reduzierter Tarife). Wenn die Daten bereits übermittelt wurden, muss der Betriebsrat informiert werden, um gemäß dem Antrag des Arbeitnehmers die Daten zu vernichten. Diese Verpflichtung lastet nicht nur auf dem Arbeitgeber, sondern auch auf dem Betriebsrat oder jeglicher anderer Institution im öffentlichen Sektor, die für die Verarbeitung von Computerdateien mit personenbezogenen Daten der Arbeitnehmer zuständig sind Diese Angaben müssen obligatorisch auf dem Fragebogen zur Erhebung der personenbezogenen Daten der Arbeitnehmer vermerkt sein. Ansonsten ist die französische Datenschutzbehörde Cnil der Ansicht, dass der Aushang einer Information in den Geschäftsräumen oder die Verteilung eines Informationsdokuments an die Arbeitnehmer angemessene Informationsmaßnahmen darstellen können[74] (über die Rechte der betroffenen Personen s. Nr. 12.41 f.).

34.12
Zugang zu den Daten der jährlichen Beurteilung. In Folge von mehreren Klagen gegen einen Arbeitgeber, der sich weigerte, seinen leitenden Angestellten ihre Beurteilung und ihr Karrierepotential mitzuteilen, hat die Cnil in ihrer Plenarsitzung vom 8. März 2007 die Meinung vertreten, dass diese Art von Daten den betroffenen Arbeitnehmern mitgeteilt werden muss, sobald die Daten bei einer Entscheidung über eine Gehaltserhöhung, Beförderung oder Versetzung berücksichtigt worden sind. Gemäß Artikel 39 des im August 2004 modifizierten Gesetzes vom 6. Januar 1978 kann der Arbeitnehmer eine Kopie des Dokuments, das diese Daten enthält, verlangen.

Ein Urteil des Kassationsgerichtshofs vom 23. Oktober 2001 hatte bereits geurteilt, dass die Tatsache, einem Arbeitnehmer die Mitteilung eines Beurteilungsdokuments zu verweigern, obwohl er darum gebeten hatte, eines der Elemente darstellt, die ein diskriminierendes Verhalten gegenüber diesem Arbeitnehmer kennzeichnen können[75].

ABSCHNITT 2
RELEVANZ UND ZWECK DER DATENVERARBEITUNG

34.21
Relevanz der Daten. Die personenbezogenen Daten müssen in Bezug auf den

---

[74] V. Cnil, Guide pratique pour les employeurs, p. 30.
[75] Soc. 23 oct. 2001, nº 99-44.215, NPB, CANSSM c/Mme Vicheney, v. http://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000007628680.

beabsichtigten Zweck angemessen, relevant und nicht überzogen sein. Die Erhebung von Informationen über die Gesundheit oder die Angehörigen des Arbeitnehmers stehen im Widerspruch zu diesem Prinzip. Die Speicherung der Sozialversicherungsnummer wird bei Dateien im Zusammenhang mit dem Lohn bzw. Gehalt und der Personalverwaltung genehmigt, um die Erstellung der Gehalts- bzw. Lohnzettel und der verschiedenen obligatorischen Erklärungen der Sozialabgaben zu ermöglichen (Décr. n° 91-1404, 27 déc. 1991 — CSS, art. R. 115-1 et R. 115-2) sowie für die Führung der Lohnsparkonten (C. trav. art. L. 3341-6). Auch wenn die Kopie des Steuerbescheids eines Arbeitnehmers an den Betriebsrat weitergegeben werden darf, um diesem die Berechnung des von diesem Arbeitnehmer zu entrichtenden Beitrags zu ermöglichen, gilt dies wegen des privaten Charakters der darin enthaltenen Informationen nicht für die Steuererklärung[76].

34.22

Legitimer Verwendungszweck. Die Erfassung personenbezogener Daten muss einen festgelegten und legitimen Verwendungszweck haben.

So wäre ein Gerät zur Videoüberwachung, das an einem Ort angebracht ist, an dem die Intimsphäre der Arbeitnehmer verletzt werden könnte (z.B. in der Dusche) oder das einen Arbeitnehmer oder eine Personengruppe einer ununterbrochenen Überwachung aussetzen würde, rechtswidrig. Darüber hinaus muss der angekündigte Verwendungszweck eingehalten werden.

Ein Lesegerät für den Firmenausweis darf nicht die Überwachung der Wege der Arbeitnehmer ermöglichen und auch nicht Auskunft über Details ihrer Bestellungen in der Firmenkantine geben. In ihrem Beschluss Nr. 02-001 vom 8. Januar 2002 hat die Cnil eine Reihe von Empfehlungen abgegeben, um solche Zweckentfremdungen zu vermeiden[77].

34.23

Keine überzogenen Kommentare in den Personalakten. Die Cnil hat am 11. Dezember 2007 ein französisches Unternehmen wegen subjektiver Kommentare in der Datei zur Verwaltung der Arbeitnehmer zur Zahlung einer Geldstrafe von 40 000 € verurteilt [78]. In ihrem Beschluss stellt sie klar, dass auch wenn es zulässig ist, dass Verarbeitungsprogramme für personenbezogene Daten Kommentarzonen enthalten, in denen Verwaltungsinformationen wie Gesprächszusammenfassungen oder Angaben zur Weiterverfolgung einer Akte erfasst werden können, diese Angaben in Bezug auf den beabsichtigten Zweck angemessen, relevant und nicht überzogen sein müssen. Die Verletzung dieser Verpflichtung kann die Anwendung von Artikel 226-18 des französischen Strafgesetzbuchs (*Code pénal*) nach sich ziehen. In dem vorliegenden Fall handelte es sich um bei diesem Unternehmen angestellte Personen, die ihre Arbeit nicht zur Zufriedenheit ausgeführt hatten.

ABSCHNITT 3
SCHUTZMAßNAHMEN

34.31

Aufbewahrungsdauer der Daten. Dieser Zeitraum muss für jede Datei und in Abhängigkeit ihres Verwendungszwecks genau festgelegt werden (zum Beispiel von einigen Tagen bis maximal einen Monat für Aufzeichnungen aus

---

[76] Civ. 1re, 29 mai 1984, n° 82-12.232, *Bull. civ.* I, n° 176.

[77] Cnil, délib. n° 02-001, vom 8. Januar 2002, (norme simplifiée 42) bezüglich der automatischen Verarbeitung namensbezogener Informationen am Arbeitplatz für die Verwaltung von Zugangskontrollen zu Räumlichkeiten, Arbeitszeiten und Kantinen, http://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000017653507

[78] Cnil, délib. n° 2007-368, 11 déc. 2007, Stellungnahme zu einem Entwurf eines Erlasses (*projet de décret)* des *Conseil d'État* zur Änderung des Erlasses *décret* n° 2005-1726 vom 30. Dezember 2005 bezüglich der elektronischen Pässe.

Videoüberwachungen). Eine zeitlich unbegrenzte Aufbewahrung ist ausgeschlossen.

Wenn es um Verbindungsdaten geht (s. Nr. 27.00 f.) muss der Arbeitgeber so genau wie möglich den Zeitraum angeben, über den die Verbindungsdaten, die die Identifizierung des Geräts oder des Nutzers ermöglichen, aufbewahrt oder gespeichert werden. Die Cnil empfiehlt dafür die Aufstellung einer jährlichen Bilanz: Die Sicherheitsmaßnahmen, die dazu führen, Spuren der Tätigkeiten der Nutzer oder des Gebrauchs, den sie von den Informations- und Kommunikationstechnologien machen, zu speichern oder die auf den Einsatz der automatisierten Verarbeitung von direkt oder indirekt namesbezogenen Informationen beruhen, sollten anlässlich der Diskussion der dem Betriebsrat oder dem *comité technique paritaire* (paritätischer technischer Ausschuss) oder jeder anderen gleichwertigen Instanz vorgelegten Sozialbilanz Gegenstand einer jährlichen Datenschutzbilanz sein[79].

34.32

Regelung der Bevollmächtigungen. Der Arbeitgeber hat die Verpflichtung, eine Sicherheitspolitik festzulegen, um die Vertraulichkeit der Daten zu gewährleisten (Gesetz vom 6. Januar 1978, Art. 34). Gewisse Daten dürfen nur von gewissen Personen eingesehen werden, vorbehaltlich der Befugnis, sie an berechtigte Dritte zu übermitteln (Arbeitinspektion, Finanzamt, usw.) Ebenso dürfen die von einem Gerät zur Videoüberwachung aufgezeichneten Bilder nur von den ordnungsgemäß zu diesem Zweck bevollmächtigten Personen im Rahmen ihrer Zuständigkeiten angesehen werden (weitere Ausführungen zur Videoüberwachung s. Nr. 30.00 f.).

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

KAPITEL

35. Spezielle Regelungen für Netzwerkadministratoren

ABSCHNITT 0
ZUR ORIENTIERUNG

35.00

Plan des Kapitels.

Abschnitt 1 Prinzip: Berufsgeheimnis

Abschnitt 2 Ausnahme: im Falle eines Risikos einer Sicherheitsbedrohung für das Unternehmen

35.01

Anwendbare Texte.

> Französische Texte. S. Nr. 3.01.

35.02

Relevante Rechtssprechung.

> Zugriff auf die Dokumente des Arbeitnehmers.

• **Soc. 6 févr. 2001,** n° 98-46.345, Sté Laboratoires pharmaceutiques Dentoria c/Mme Bardagiet et a., *Bull. civ.* V, n° 43 ; *JCP G* 25 juill. 2001, n° 30, p. 1514, note C. Puigelier ; *RTD civ.* oct.-déc. 2001, n° 4, 880-882, note J. Mestre et B. Fages — aufgehoben durch **CA Toulouse, 4e ch. soc., 23 oct. 1998.**

• **Soc. 18 mars 2003,** n° 01-41.343, NPB, UMS c/Mme C…, *Gaz. Pal.* 25 sept. 2003, n° 268, p. 37, note L. Maurel-Guignot — aufgehoben durch **CA St Denis de la Réunion, ch. soc., 28 nov. 2000**.

* s. Nr. 35.21, auch Nr. 31.24 und 33.22.

> Gerechtfertigte Maßnahmen im Falle einer Sicherheitsbedrohung.

• **CA Paris, 11e ch., sect. A, 17 déc. 2001,** n° 2000-07565, F. M…, H. H… et V. R… c/Min. Public et A. T…, *Gaz. Pal.* 8 mai 2002, p. 31, comm. S. Le Guillas.

* s. Nr. 35.21.

35.04

Grundsätzliche Fragen

• Welche Verpflichtungen und Verantwortlichkeiten haben die Netzwerkadministratoren?

* s. Nr. 35.12.

Wo liegen die Grenzen ihres Interventionsbefugnisses?

* s. Nr. 35.21.

ABSCHNITT 1
PRINZIP: BERUFSGEHEIMNIS

35.11

Überwachungsmöglichkeiten aus der Ferne. Die Frage nach der Verletzung des Briefgeheimnisses nimmt im Fall der Netzwerkadministratoren eine besondere Dimension an. Diese sind dafür zuständig, sich von dem reibungslosen Funktionieren und der Sicherheit der Systeme und Netze im Unternehmen zu überzeugen. Durch ihre Aufgabe haben sie Zugang zu Informationen, die die Nutzer der Systeme und Netze betreffen (E-Mailboxen, Internet-Verbindungsdaten, Logdateien, usw.). Sie haben normalerweise die technischen Möglichkeiten, die PC-Arbeitsplätze aus der Ferne zu überwachen, z.B. um die Fernwartung der Software zu gewährleisten, oder allgemeiner, um die Kontrolle über den PC-Arbeitsplatz anstelle des Nutzers zu übernehmen.

35.12

Einhaltung der Verpflichtungen zur Transparenz und Verhältnismäßigkeit. Die Arbeitnehmer und die Personalvertretungsorgane müssen im Sinne der Verpflichtung des Arbeitgebers zur Transparenz (zu diesem Prinzip siehe Nr.

32.00 f.) von den Interventionsbedingungen der Netzwerkadministratoren in Kenntnis gesetzt werden. Die Interventionen müssen strengen Bedingungen unterliegen (vorherige Information des Nutzers und Intervention mit seinem vorherigen Einverständnis, nötigenfalls per E-Mail) und auf das reibungslose Funktionieren der Anwendungen beschränkt sein.

Die Überwachung muss auch im Einklang mit dem Prinzip der Verhältnismäßigkeit sein (zu diesem Prinzip s. Nr. 32.00 f.) und das Zweckprinzip des französischen Datenschutzgesetzes *loi informatique et libertés* einhalten.

Die französische Datenschutzbehörde Cnil hat daran erinnert, dass jegliche Nutzung dieser technischen Möglichkeiten auf eigene Initiative der Netzwerkadministratoren oder auf Anweisung eines Vorgesetzten, z.B. zu Überwachungszwecken, weder mit dem Prinzip der Verhältnismäßigkeit noch mit dem Zweckprinzip des französischen Datenschutzgesetzes konform ist[80].

35.13

Verpflichtung der besonderen Vertraulichkeit Die Netzwerkadministratoren unterliegen dem Berufsgeheimnis und allgemeiner der Verpflichtung der beruflichen Diskretion, die es ihnen verbietet, die Informationen, über die sie im Rahmen der Ausübung ihrer Funktion Kenntnis erhalten haben, offen zu legen.

An diese Regel erinnert die Cnil in ihrem Bericht über die *Cybersurveillance sur les lieux de travail* (Cyber-Überwachung am Arbeitsplatz) (Feb. 2004): Die Netzwerk- und Systemadministratoren, die im Allgemeinen dem Berufsgeheimnis oder einer Verpflichtung zur beruflichen Diskretion unterliegen, dürfen keine Informationen, über die sie ihm Rahmen der Ausübung ihrer Funktion Kenntnis erhalten haben, offen legen, insbesondere dann nicht, wenn diese dem Briefgeheimnis unterliegen oder im Zusammenhang mit dem Privatleben des Benutzers stehen und weder das reibungslose technische Funktionieren der Anwendungen, ihre Sicherheit, noch das Unternehmensinteresse gefährden. Sie stellt außerdem klar, dass die Netzwerkadministratoren nicht gezwungen werden können, diese Informationen offen zu legen, außer im Falle einer rechtlichen Bestimmung in diesem Sinne.

Schließlich weist das *Forum des droits sur l'internet* (Forum der Rechte des Internets) seinerseits darauf hin, dass der Netzwerkadministrator darauf achten sollte, niemandem innerhalb des Unternehmens, seine Vorgesetzten und Kollegen eingeschlossen, die persönlichen Informationen über einen Arbeitnehmer, von denen er im Rahmen seiner Funktion Kenntnis erhalten hat, offen zu legen.

Deshalb müssen Sicherheitsmaßnahmen ergriffen werden, um die Vertraulichkeit der Informationen, auf die die Netzwerkadministratoren bei der Ausübung ihrer beruflichen Funktion Zugriff haben, zu gewährleisten. An diese Verpflichtung zur Vertraulichkeit sollte im Arbeitsvertrag, ja sogar in der Betriebsordnung oder der Informatikcharta erinnert werden.

ABSCHNITT 2
AUSNAHME: IM FALLE EINES RISIKOS EINER SICHERHEITSBEDROHUNG FÜR DAS UNTERNEHMEN

35.21

Gerechtfertigte Maßnahmen im Falle einer Sicherheitsbedrohung. Im Falle des Risikos einer Sicherheitsbedrohung für das Unternehmens oder die Behörde stoßen diese Regelungen jedoch an eine Grenze. In diesem Zusammenhang hat das Berufungsgericht von Paris in einem Urteil vom 17. Dezember 2001 klargestellt, dass die Besorgnis um die Sicherheit des Netzwerkes es rechtfertigte, dass die System- und Netzwerkadministratoren von ihren Positionen und den technischen Möglichkeiten, die ihnen zur Verfügung standen Gebrauch machten, um die Untersuchungen durchzuführen und die Maßnahmen zu ergreifen, die die Sicherheit erforderte - in der gleichen Art und Weise, wie auch die Post auf ein verdächtiges Paket oder einen verdächtigen Brief reagieren muss. Die

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

Offenlegung des Inhalts der Nachrichten und insbesondere der letzten Nachricht, die den unterschwelligen Konflikt im Labor betraf, geschah jedoch nicht aus diesem Zweck[81].

Ebenso muss auch der Arbeitgeber auf die in dem Computer seines Arbeitnehmers gespeicherten Dokumente zugreifen können, wenn dieser abwesend ist (vor allem im Fall von Urlaub oder Krankheit)[82]. Demzufolge hat der Kassationsgerichtshof am 18. März 2003 geurteilt, dass der Arbeitnehmer verpflichtet ist, sein Passwort oder die sich in seinem Besitz befindlichen Dateien mitzuteilen, wenn der reibungslose Ablauf des Unternehmens von den Daten abhängt, die dieser Arbeitnehmers besitzt[83].

---

[81] CA Paris, 11e ch., sect. A, 17 déc. 2001, F. M..., H. H... et V. R... c/Min. public et A. T..., *Gaz. Pal.* 8 mai 2002, p. 31, comm. S. Le Guillas ;
http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=240.

[82] Soc. 6 févr. 2001, no 98-46.345, NPB, *Bull. civ.* V, no 43 ; *JCP G* 2001, no 30, p. 1514, note C. Puigelier ; *RTD civ.* oct.-déc. 2001, no 4, 880-882, note J. Mestre et B. Fages ; *Gaz. Pal.* 20 mars 2001, no 79, p. 9.

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

KAPITEL

36. Spezielle Regelungen für Einstellungsverfahren

ABSCHNITT 0
ZUR ORIENTIERUNG

36.00

Plan des Kapitels.

36.01

Anwendbare Texte.

> Französische Texte.

Gesetzestext.

C. trav., art. L. 1221-6 et L 1221-8.

Stellungnahmen und Beschlüsse.

Cnil, délib. n° 02-017, vom 21. März 2002, zur Annahme der Empfehlung bezüglich der Erhebung und der Verarbeitung namensbezogener Informationen bei Einstellungsverfahren (hebt auf und ersetzt: Cnil, recomm. 85-44, 15 oct. 1985).

Cnil, recomm. vom 5. Juli 2005 zum Ermessen der Vielfältigkeit der Herkünfte im Kampf gegen Diskriminierung

> EU-Text.

* s. Nr. 1.01: Richtlinie 95/46/EG, 24. Okt. 1995, Art. 10.

36.04

Grundsätzliche Fragen

• Welche Rechte hat der Bewerber bei einem Einstellungsverfahren?

* s. Nr. 36.21 f.

• Welche Garantien werden ihm gewährleistet?

* s. Nr. 36.31 f.

ABSCHNITT 1
ANWENDUNGSBEDINGUNGEN

36.11

Formalitäten der Deklarierung. Die für die Einstellung zuständigen Personen müssen Systeme zur automatischen Verarbeitung von namensbezogenen Informationen vor deren Inbetriebnahme bei der französischen Datenschutzbehörde Cnil deklarieren (Gesetz vom 6. Januar 1978, Art. 22). Jeder Verstoß gegen diese Vorschrift zieht strafrechtliche Konsequenzen nach sich (Code pénal, Art. 226-24).

36.12

Ein auf das Einstellungsverfahren beschränkter Verwendungszweck. Das französische Arbeitsgesetzbuch (*Code du travail*) legt fest, dass die von einem Bewerber für eine Stelle auf welche Art auch immer erfragten Informationen keinen anderen Verwendungszweck haben dürfen als die Beurteilung seiner Eignung, die angebotene Stelle zu besetzen oder seiner beruflichen Fähigkeiten. Die Informationen müssen einen direkten und notwendigen Zusammenhang mit der angebotenen Stelle oder der Beurteilung der beruflichen Fähigkeiten aufweisen. Der Bewerber ist verpflichtet, die Fragen nach bestem Wissen und Gewissen zu beantworten (Code du travail art. L. 1221-6).

Die Cnil ist ihrerseits der Meinung, dass abgesehen von Sonderfällen, die durch die Art einer zu besetzenden Stelle oder die in einem von dieser Stelle betroffenen anderen Land geltenden Vorschriften gerechtfertigt sind, folgende Fragen die gesetzlichen Vorschriften verletzen: Datum der Einreise nach Frankreich, Datum der Einbürgerung, Umstände des Erwerbs der französischen Staatsbürgerschaft, ursprüngliche Staatsangehörigkeit, die Registrierungs- oder Mitgliedsnummer der Sozialversicherung, Einzelheiten militärischen Stellung, vorherige Anschrift, Informationen bezüglich des familiären Umfelds (insbesondere des Partners), Gesundheitszustand (insbesondere Gewicht, Größe), Wohnsituation als Eigentümer oder Mieter, Mitgliedschaft in Vereinen, Bankensitz, aufgenommene Darlehen.

Darüber hinaus könnte die Verwendung von Annoncen zur Erstellung einer Bewerberdatei oder auch die Sammlung von Informationen im beruflichen Umfeld eines Bewerbers ohne sein Wissen eine betrügerische, unlautere oder verbotene Erhebung darstellen (Gesetz vom 6. Januar 1978, Art. 6).

Schließlich sind die Erhebung und die Aufbewahrung von Daten verboten, aus denen sich direkt oder indirekt die Rasse oder ethnische Herkunft, politische, philosophische oder religiöse Ansichten, Gewerkschaftszugehörigkeiten oder Informationen bezüglich der Gesundheit oder der sexuellen Orientierung ableiten lassen (Gesetz vom 6. Januar 1978, Art. 6). Die einzige Ausnahme, unter dem Vorbehalt des ausdrücklichen Einverständnisses der Betroffenen, betrifft die Besonderheit einer zu vergebenden Stelle.

ABSCHNITT 2
RECHTE DES BEWERBERS

36.21

Das Recht des Bewerbers auf Information. Bewerber auf eine Stelle haben wie alle Personen, von denen personenbezogene Daten erhoben werden, das Recht auf Information über 1. den verpflichtenden oder freiwilligen Charakter der Auskünfte; 2. die sich für sie im Falle einer fehlenden Auskunft ergebenden Konsequenzen; 3. die natürlichen oder juristischen Personen, die diese Informationen erhalten; 4. die Existenz eines Rechts auf Zugang und Richtigstellung (Gesetz vom 6. Januar 1978, Art. 32). Darüber hinaus haben sie einen legitimen Anspruch darauf, sich der Verarbeitung der sie betreffenden namensbezogenen Daten zu widersetzen (Gesetz vom 6. Januar 1978, Art. 38).

Außerdem muss der Bewerber über die Personalien der für die Datenverarbeitung zuständigen Person und über den Verwendungszweck, für den die Daten bestimmt sind, informiert werden (Richtlinie 95/46/EG vom 24. Oktober 1995, Art. 10). In diesem Zusammenhang gibt die Cnil zwei Empfehlungen:

1. dass die mit der Einstellung beauftragten Personen alle notwendigen Vorkehrungen ergreifen, um den Bewerber innerhalb eines vernünftigen Zeitraums über den Ausgang seiner Bewerbung, über die Aufbewahrungsdauer der ihn betreffenden Informationen sowie über seine Möglichkeit, die Rückgabe oder die Vernichtung dieser Informationen zu verlangen, zu informieren.

2. dass die Personen, deren Daten in eine Bewerberdatei aufgenommen wird, die im Rahmen der Direktansprache (*Direct Search*) von Kandidaten verwendet wird, spätestens bei der ersten Kontaktaufnahme über die Bestimmungen des Art. 27 des Gesetzes vom 6. Januar 1978 informiert werden. Falls die Identität des Arbeitgebers nicht bei der Stellenausschreibung bekannt gegeben wurde, muss das Einverständnis des Bewerbers vor der Weiterleitung namensbezogener Informationen an diesen Arbeitgeber eingeholt werden. Im Falle der Erhebung namensbezogener Daten über Fernverbindungen empfiehlt die Cnil, den Bewerber darüber zu informieren, in welcher Form (namensbezogen oder nicht) die ihn betreffenden Informationen möglicherweise online übertragen oder an den Arbeitgeber weitergeleitet werden. Auch muss der Bewerber vor jeder möglichen Abtretung seiner Informationen an andere für Rekrutierung zuständige Institutionen informiert werden und die Möglichkeit haben, sich dem zu widersetzen.

Die Cnil erinnert auch daran, dass die erhobenen Informationen zu keinem anderen Zweck verwendet werden dürfen als für die Besetzung der freien Stelle. Jeglicher andere Verwendungszweck, insbesondere die kommerzielle Werbung, ist ausgeschlossen.

Schließlich muss der Bewerber ausdrücklich über die bei ihm verwendeten Hilfsmethoden und –techniken für die Kandidatenauswahl informiert werden, bevor diese eingesetzt werden (Code du travail, art. L. 1221-8, früher L. 121-7). In diesem Zusammenhang empfiehlt die Cnil, dass die Information bezüglich der verwendeten Methoden zur Hilfe bei der Kandidatenauswahl vorab schriftlich vermittelt wird, entweder einzeln oder kollektiv.

36.22

Recht auf Zugang und Richtigstellung. Ein Bewerber kann das Recht auf Zugang und Richtigstellung, das jede Person hat, bei den ihn betreffenden Daten ausüben, ganz gleich ob es sich um Daten handelt, die direkt von ihm oder über Dritte erhoben wurden oder um Daten aus Hilfsmethoden und –techniken für die Kandidatenauswahl. Er kann so die ihn betreffenden Informationen mitgeteilt bekommen und im Falle von Unstimmigkeiten deren Richtigstellung fordern (Gesetz vom 6. Januar 1978, Art. 39). Daher empfiehlt die Cnil, dass jeder Bewerber klar und deutlich über die Modalitäten der Ausübung des Zugangsrechts informiert wird und auf Anfrage alle ihn betreffenden Informationen erhalten kann, einschließlich der Ergebnisse von Analysen und Tests oder möglicherweise durchgeführten beruflichen Evaluierungsmaßnahmen. Sie empfiehlt außerdem, dass die Mitteilung der in der Bewerberdatei enthaltenen Informationen auf dem schriftlichen Wege geschieht, die Mitteilung der Ergebnisse von Tests oder Evaluierungen sollte auf einem angemessenen Weg hinsichtlich der Art des verwendeten Mittels geschehen.

ABSCHNITT 3
MAßNAHMEN ZUM SCHUTZ DES BEWERBERS

36.31

Aufbewahrungsdauer der Daten. Vorbehaltlich einer Genehmigung durch die Cnil dürfen personenbezogene Daten nicht länger aufbewahrt werden, als in der Erklärung der Verarbeitung angegeben wurde (Gesetz vom 6. Januar 1978, Art. 36). Die Cnil empfiehlt in diesem Zusammenhang, dass der Bewerber über den Zeitraum, über den die ihn betreffenden Informationen aufbewahrt werden und über sein Recht, jederzeit die Vernichtung der Daten zu fordern, informiert wird. In jedem Fall sollte die Aufbewahrungsdauer der Informationen nicht länger als zwei Jahre nach dem letzten Kontakt mit der betreffenden Person betragen. Diese Maßnahme wird für jeden Bewerber empfohlen, ganz gleich ob das Bewerbungsverfahren erfolgreich ausgegangen ist oder nicht.

36.32

Sicherheit und Vertraulichkeit der Daten. Der für die automatische Verarbeitung der die Bewerber um eine Stelle betreffenden Daten Verantwortliche muss sich gegenüber den Bewerbern verpflichten, alle Sicherheits- und Vertraulichkeitsmaßnahmen zu ergreifen (Gesetz vom 6. Januar 1978, Art. 34). Dritte in einem Bewerbungsverfahren dürfen also weder direkt noch indirekt Zugang zu den Daten haben.

36.33

Automatisch erstellte Profile. Der Bewerber hat das Recht darauf, über die in automatischen Datenverarbeitungsprogrammen zur Unterstützung bei der Kandidatenauswahl verwendeten Argumentationen informiert zu werden (Gesetz vom 6. Januar 1978, Art. 22). Keine Entscheidung über eine Bewerbung, die eine Einschätzung über das Verhalten der Person mit einschließt, kann jedoch als einzige Grundlage ein Computerprogramm haben, das ein Profil des Bewerbers erstellt oder seine Persönlichkeit definiert (Gesetz vom 6. Januar 1978, Art. 10). Daher empfiehlt die Cnil eine Ächtung der Instrumente zur automatischen

Bewertung aus der Ferne, die jegliche menschliche Einschätzung ausschließen.

36.34

Statistische Mittel zur Erfassung von Diskriminierungen. Die Cnil empfiehlt, keine Daten zu erheben, die im Zusammenhang mit der Rasse oder der ethnischen Herkunft der Arbeitnehmer oder der Bewerber um eine Stelle stehen und keine Analyse des Klangs ihres Vor- oder Nachnamens vorzunehmen. Folgende Daten des Bewerbers oder des Arbeitnehmers dürfen jedoch erhoben und verarbeitet werden: Vorname, Nachname, Staatsangehörigkeit, ursprüngliche Staatsangehörigkeit, Geburtsort, Staatsangehörigkeit oder Geburtsort der Eltern, seine Anschrift.

Darüber hinaus ist die Cnil der Meinung, dass die Ablehnung eines Bewerbers für eine freie Stelle oder eine Beförderung das Ergebnis der gleichzeitigen Berücksichtigung mehrerer nicht diskriminierender Kriterien, wie z.B. der Berufserfahrung sein kann. Der diskriminierende Faktor kann sich also aus der statistischen Kreuzanalyse dieser verschiedenen Kriterien ergeben. Deshalb empfiehlt die Cnil, wenn die Erhebungsbögen Daten enthalten, die die indirekte Identifizierung der befragten Person ermöglichen, dass der Zugang zu den Inhalten nur auf die Personen begrenzt sein sollte, die speziell für die Auswertung zuständig sind, dass die Ergebnisse in einer zugelassenen statistischen Form erstellt werden, um die Anonymität zu gewährleisten und dass die Erhebungsbögen vernichtet werden, sobald die Antworten ausgewertet wurden. Wenn die Erhebungsbögen ein Identifizierungszeichen beinhalten, empfiehlt die Cnil, auf ein anderes zurückzugreifen als jenes, das im Rahmen der Personalverwaltung verwendet wird (wie z.B. die Sozialversicherungsnummer), die Antworten in einer anderen Datei zu speichern als die Dateien zur Personalverwaltung und ein Anonymisierungsverfahren zu verwenden, das nicht nur die Löschung der Identität eines Bewerbers, sondern auch seiner Anschrift, seiner Telefonnummer und E-Mail-Adresse, seiner Fotografie und aller anderer Daten vorsieht, die seine Identifizierung ermöglichen können.

In diesem Zusammenhang muss jedoch auf einen von dem Rechtsausschuss der Nationalversammlung (*Commission des lois de l'Assemblée nationale*) angenommenen Änderungsantrag des Gesetzesentwurfs zur Kontrolle der Immigration, zur Integration und zum Thema Asyl hingewiesen werden[84]. Dieser Änderungsantrag vom 12. September 2007 lehnt sich an die Beobachtungen und Empfehlungen der Cnil zum Thema Ermessen der Vielfältigkeit an[85] . Sie beabsichtigen, eine Gesetzesänderung des französischen Datenschutzgesetzes *loi informatique et libertés* vorzuschlagen, um die Untersuchungen im Bereich Ermessen der Vielfältigkeit der Herkünfte, der Diskriminierung und der Integration zu erleichtern und dabei den Datenschutz und den wissenschaftlichen Charakter der Untersuchungen zu verbessern. Der Text legt insbesondere nahe, dass die Daten, die direkt oder indirekt die Rasse oder die ethnische Herkunft der Personen erkennen lassen, zu Studienzwecken erfasst werden können, deren Verwendungszweck in dem Ermessen der Vielfältigkeit der Herkünfte der Personen, der Diskriminierung und der Integration liegt, aber dass diese Datenverarbeitungen einer Genehmigung durch die Cnil unterliegen und dass die betroffenen Personen das Recht beibehalten, sich dieser Verarbeitung zu widersetzen.

[84] Rapp. de la Commission des lois, http://www.assemblee-nationale.fr/13/rapports/r0160.asp.

[85] Cnil, Empfehlung vom 5. Juli 2005, zum Ermessen der Vielfältigkeit der Herkünfte im Kampf gegen Diskriminierung, siehe http://www.cnil.fr/index.php?id=1844.

KAPITEL

37. Spezielle Regelungen für Gewerkschaften

ABSCHNITT 0
ZUR ORIENTIERUNG

37.00

Plan des Kapitels.

37.01

Anwendbare Texte.

> Französische Texte. S. Nr. 3.01: C. trav., art. L. 2142-6 — L. n° 82-689, 4 août 1982, relative aux libertés des travailleurs dans l'entreprise — L. n° 2004-391, 4 mai 2004 relative à la formation professionnelle tout au long de la vie et au dialogue social, *JO* n° 105, 5 mai, 7983 — L. n° 2008-67, 21 janv. 2008, ratifiant l'ordonnance n° 2007-329 du 12 mars 2007 relative au Code du travail (partie législative), *JO* n° 0018, 22 janv., 1122.

37.02

Relevante Rechtssprechung.

> Freie Nutzung der E-Mailbox und des Intranets unter der Bedingung einer Betriebsvereinbarung

• **Soc. 25 janv. 2005,** n° 02-30.946, Fédération des services CFDT et a. c/Sté Clear Channel France *Bull. civ.* V, n° 19 ; *LPA* 8 mars 2005, n° 47, p. 3, note A. Sauret et G. Picca — bestätigt durch **CA Paris, 14e ch., sect. B, 31 mai 2002**.

• **Soc. 22 janv. 2008,** n° 06-40.514, M. M. c/Crédit industriel et commercial, *RDT* 2008, p. 324 ; *Sem. soc. Lamy* n° 1339, 2008 — bestätigt durch **CA Paris, 18e ch., sect. D, 29 nov. 2005**.

• **Crim. 10 mai 2005,** n° 04-84705, *Bull. crim.,* n° 144.

* s. Nr. 37.11.

> Freie gewerkschaftliche Betätigung.

• **CAA de Nancy, 3e ch., 2 août 2007,** cne de Lons le Saunier c/Elisabeth M…, *RLDI* 2007, n° 31 — Nichtigerklärung von **TA Besançon, 1re ch., 19 déc. 2006,** Elisabeh M… c/Ville de Lons-Le-Saunier, RG n° 0400718.

* s. Nr. 37.12.

• **Soc. 5 mars 2008,** n° 06-18.907, sté TNS Secodip c/féd. CGT des stés d'études, *Gaz. Pal.* 26 avr. 2008, n° 117, http://www.courdecassation.fr/jurisprudence_publications_documentation_2/actualite_jurisprudence_21/chambre_sociale_576/arrets_577/br_arret_11274.html — aufgehoben durch **CA Paris, 18e ch. civ., 15 juin 2006,** Féd. CGT des stés d'études c/TNS Secodip, dann Überweisung an CA Paris.

Für das (bestätigte) Urteil in erster Instanz s. **TGI Bobigny, 11 janv. 2005,** TNS Secodip c/Fédération CGT des Sociétés d'Etudes.

• **CA Paris, 18e ch. C, 15 juin 2006,** Féd. CGT des stés d'études c/TNS Secodip, (o.g.).

* s. Nr. 37.14.

37.04

Grundsätzliche Fragen.

• Können Gewerkschaften eine dedizierte Website haben?

* s. Nr. 37.11.

• Unter welchen Bedingungen kann eine solche Website in Betrieb genommen werden?

* s. Nr. 37.13 f.

• Welche Garantien werden den Arbeitnehmern geboten, deren personenbezogene Daten von den Gewerkschaften verwendet werden?

* s. Nr. 37.21 f.

ABSCHNITT 1
NUTZUNGSBEDINGUNGEN DES INTERNETS UND INTRANETS

37.11

Eine Betriebsvereinbarung ist Pflicht. Das französische Arbeitsgesetzbuch (*Code du travail*) sieht vor, dass eine Betriebsvereinbarung die Bereitstellung von Gewerkschaftsveröffentlichungen und –trakten entweder auf einer Website der Gewerkschaft im Intranet des Unternehmens oder durch Verteilung über die Unternehmens-E-Mail genehmigen kann. Im letzteren Fall muss diese Verteilung mit den Anforderungen eines reibungslosen Funktionierens des Informatiknetzes des Unternehmens vereinbar sein und darf die Ausführung der Arbeit nicht beeinträchtigen. Die Betriebsvereinbarung legt die Modalitäten dieser Bereitstellung oder die Art und Weise der Verteilung fest und präzisiert insbesondere die Zugangsbedingungen für die gewerkschaftlichen Organisationen und die technischen Regelungen, die den Arbeitnehmern die freie Wahl lassen, eine Nachricht entgegenzunehmen oder abzulehnen (Code du travail, Art. L. 2142-6 — Gesetz Nr. 2004-391 vom 4. Mai 2004 — Gesetz Nr. 2008-67 vom 21. Januar 2008).

Gewerkschaftliche Organisationen können also Zugang zum Intranet, z.B. um einen gewerkschaftlichen Blog einzurichten, der für alle Mitarbeiter des Unternehmens zugängig ist und zu dem E-Mail-Programm des Unternehmens bekommen, jedoch unter der Bedingung, dass sie zuvor eine Betriebsvereinbarung verhandelt und abgeschlossen haben.

Wenn keine Betriebsvereinbarung abgeschlossen wurde, spricht sich die Rechtssprechung für ein Verbot der Verteilung aus, dies bestätigt das Urteil des Kassationsgerichtshof vom 25. Januar 2005[86] . In dem vorliegenden Fall hatte die Gewerkschaft an die geschäftliche E-Mail-Adresse aller Arbeitnehmer eines Unternehmens eine gewerkschaftliche Nachricht versandt. Es gab dafür weder eine Betriebsvereinbarung, noch eine Genehmigung des Arbeitgebers.

Außerdem legt der Kassationsgerichtshof eine bestehende Betriebsvereinbarung sehr streng aus. In einem Urteil vom 22. Januar 2008 beobachtet er, dass die Betriebsvereinbarung die Möglichkeit der Nutzung der Unternehmens-E-Mail zur Veröffentlichung von gewerkschaftlichen Informationen von dem Bestehen eines Zusammenhangs mit der bestehenden sozialen Lage in dem Unternehmen machte, was in dem vorliegenden Fall nicht gegeben war (Soc. 22 janv. 2008[87]).

Man kann jedoch beobachten, dass der Text nicht den Zugang zu diesen informationstechnologischen Mitteln durch die Personalvertretungen wie die Betriebsräte oder die Personalvertreter betrifft.

37.12

Das Gewerkschaftsrecht ist eine Grundfreiheit. Diese von dem Verwaltungsgericht (*tribunal admisitratif*) von Besançon am 19. Dezember 2006 aufgestellte Regel stellt klar, dass niemand Einschränkungen dieses Rechts vornehmen kann, die weder durch die Natur der zu erfüllenden Aufgabe gerechtfertigt sind noch in Verhältnis zu dem angestrebten Ziel stehen[88]. Es argumentierte, dass der Bürgermeister der Gemeinde Lons-Le-Saunier eine seiner Arbeitnehmerinnen, stellvertretende Verwalterin der städtischen Dienste und Gewerkschaftsvertreterin, die über die Mitteilungsfunktionen des städtischen Intranets und Internet zu einer Demonstration aufgerufen hatte, keinen Verweis erteilen durfte und wies das Argument des Bürgermeisters ab, der einen Verstoß der Arbeitnehmerin gegen ihre beruflichen Verpflichtungen geltend machen wollte, weil sie das Verbot der privaten Nutzung des E-Mail-Programms nicht einhielt.

Nach einer anderen Analyse des Inhalts der strittigen Mail durch das Verwaltungsberufungsgericht (*cour administrative d'appel*) von Nancy entschied

---

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

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

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

dieses am 2. August 2007[89], dass es sich um eine Nachricht mit politischem Charakter handelte. Unter diesen Bedingungen urteilte es, dass der Bürgermeister von Lons-le-Saunier seine gewerkschaftlich tätige Arbeitnehmerin rechtmäßig bestraft hatte, insofern als eine Dienstnotiz vom 18. November 2003 dem Personal die Nutzung des Internets zu politischen Zwecken untersagte.

37.13

Respekt des Zweckprinzips. Der Verwendungszweck der Datenverarbeitung muss streng eingehalten werden. Wenn eine Betriebsvereinbarung die Verteilung gewerkschaftlicher Informationen per E-Mail genehmigt, so dürfen die E-Mail-Adressen der Arbeitnehmer zu nichts anderem als zur Verteilung von Veröffentlichungen und Trakten mit gewerkschaftlichem Charakter genutzt werden.

37.14

Respekt der Rechte Dritter. Über die Frage nach den Grenzen der gewerkschaftlichen Kommunikationsfreiheit von einer unternehmensexternen Website aus urteilte die Sozialkammer des Kassationsgerichtshofs am 5. März 2008[90].

In dem vorliegenden Fall hatte eine Gewerkschaft auf ihrer Website einige vertrauliche Informationen über ein Unternehmen veröffentlicht: zwei Gutachten eines Wirtschaftsprüfungsbüros über die Rechnungslegung des Unternehmens sowie mehrere Protokolle von Vertragsverhandlungen, von Betriebsratssitzungen und von den von Personalvertretern gestellten Fragen. Das Unternehmen war der Ansicht, dass es durch diese Veröffentlichungen geschädigt würde und rief das erstinstanzliche Zivilgericht (*tribunal de grande instance*) von Bobigny an, um die Löschung dieser Rubriken einzufordern.

Die erstinstanzlichen Richter gaben dieser Klage statt und argumentierten, dass vier Rubriken mit vertraulichen Informationen nicht an Dritte und Konkurrenten weitergegeben werde dürfen und dass die Verpflichtung zur Diskretion und Vertraulichkeit auch für Gewerkschaften gilt, die die Arbeitnehmer in einem Unternehmen vertreten (TGI Bobigny, 11 janv. 2005[91]).

Diese Entscheidung wurde vom Berufungsgericht (*cour d'appel*), mit seinem Urteil vom 15. Juni 2006 aufgehoben, indem es berücksichtigte, dass eine Gewerkschaft den gleichen Spielraum wie jeder Bürger hat, eine Website zu erstellen, um sein Recht auf direkte und kollektive Meinungsäußerung auszuüben, dass die Ausübung dieses Rechts keiner Einschränkung unterliegt und dass keine gesetzliche Verpflichtung oder Vertraulichkeitsverpflichtung auf den Gewerkschaftsmitgliedern lastet wie die Verpflichtung laut Artikel L. 432-7, Absatz 2 des französischen Arbeitsgesetzbuchs (*Code du travail*) für die Betriebsratsmitglieder oder Gewerkschaftsvertreter, auch wenn Personenidentität bestehen kann[92].

Der in Kassationsbeschwerde angerufene Kassationsgerichtshof hat seinerseits das Urteil des Berufungsgerichtshof aufgehoben, denn auch wenn eine Gewerkschaft das Recht hat, der Öffentlichkeit Informationen frei über eine Internet-Website mitzuteilen, so kann diese Freiheit insofern beschränkt werden, als es nötig ist, um zu vermeiden, dass die Offenlegung vertraulicher

---

[89] CAA Nancy, 3e ch., 2 août 2007, cne de Lons le Saunier c/Elisabeth M…, *RLDI* 2007, no 31.

[90] Soc. 5 mars 2008, no 06-18.907, sté TNS Secodip c/féd. CGT des stés d'études : cass. arrêt CA Paris, 15 juin 2006 (renvoi devant la CA Paris), http://www.courdecassation.fr/jurisprudence_publications_documentation_2/actualite_jurisprudence_21/chambre_sociale_576/arrets_577/arret_no_11275.html ; http://www.legalis.net/jurisprudence-decision.php3?id_article=2227 ; Gaz. *Pal.* 26 avr. 2008, no 117.

[91] TGI Bobigny, 11 janv. 2005, TNS Secodip c/Féd. CGT des stés d'études, *Gaz. Pal.* 20 juill. 2005, no 101, p. 45-46 ; *Expertises* avr. 2005, p. 156 — für eine kritische Analyse dieser Entscheidung siehe G. Haas et O. de Tissot, « Des restrictions inacceptables à la liberté d'action des syndicats », Expertises avr. 2005, S. 145.

92 CA Paris, 18e ch. C, 15 juin 2006, Féd. CGT des stés d'études c/TNS Secodip, http://www.courdecassation.fr/jurisprudence_publications_documentation_2/actualite_jurisprudence_21/chambre_sociale_576/arrets_577/br_arret_11274.html.

Informationen die Rechte Dritter verletzt. Der Hohe Gerichtshof stützte sich dabei auf Artikel 10-2 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), der ausdrücklich vorsieht, dass die freie Meinungsäußerung gewissen gesetzlich vorgesehenen Bedingungen und Einschränkungen unterstellt werden darf, die nötige Maßnahmen zum Schutz der Rechte oder des Ansehens Dritter darstellen. Außerdem hat er sich auf das Gesetz für das Vertrauen in die elektronische Wirtschaft (*loi pour la confiance dans l'économie numérique*) gestützt, das vorsieht, dass die Ausübung der Kommunikationsfreiheit auf elektronischem Weg in dem erforderlichen Maße eingeschränkt werden kann, insbesondere im Rahmen des Respekts der Freiheit und des Eigentums Dritter.

Zuvor hatte die Strafrechtskammer (*chambre criminelle*) des Kassationsgerichtshofs ebenfalls die auf der Website einer Gewerkschaft veröffentlichten Informationen wegen des ehrenrührigen Infragestellens eines Direktors des Unternehmens in Worten, die als über das in einem solchen Rahmen zulässige Maß hinausgehend, beurteilt wurden, geahndet (Crim. 10 mai 2005[93]).

ABSCHNITT 2
REGELUNGEN ZUM SCHUTZ DES ARBEITNEHMERS

37.21

Einspruchsrecht der Arbeitnehmer. Die Arbeitnehmer müssen ihr Einspruchsrecht gegen den Versand jeglicher gewerkschaftlicher Nachricht auf ihre geschäftliche E-Mail-Adresse ausüben können. Zu diesem Zweck müssen sie zuvor über die abgeschlossene Betriebsvereinbarung und die Modalitäten zur Wahrnehmung ihres Einspruchrechts informiert werden. Sie müssen dieses Recht jederzeit wahrnehmen können und deshalb müssen sie in jeder Nachricht an dieses Recht erinnert werden. Darüber hinaus empfiehlt die Cnil, kenntlich zu machen, dass es sich um eine gewerkschaftliche Nachricht handelt, um die größtmögliche Transparenz bezüglich der Herkunft und der Art der Nachricht zu fördern.

37.22

Gewährleistung der Vertraulichkeit. Der E-Mail-Verkehr zwischen den Arbeitnehmern und den gewerkschaftlichen Organisationen ist vertraulich. Aus diesem Grund ist die Cnil der Ansicht, dass der Arbeitgeber über die so erstellten Verteilerlisten keine Kontrolle ausüben können sollte, um jegliche Möglichkeit einer zweckentfremdeten Verwendung zu vermeiden. Denn solche Nachrichten können durch die Entscheidung eines Arbeitnehmers für oder gegen den Empfang gewerkschaftlicher Nachrichten seine positive Einstellung zu einer gewerkschaftlichen Organisation, ja sogar seine Mitgliedschaft bei einer bestimmten Gewerkschaft preisgeben[94].

[93] Crim. 10 mai 2005, n° 04-84.705, *Bull. crim.,* n° 144.
[94] Cnil, Guide pratique pour les employeurs, p. 28.

KAPITEL

38. Im Ausland geltende Regelungen und Gebräuche

ABSCHNITT 0
ZUR ORIENTIERUNG

38.00

Plan des Kapitels.

38.04

Grundsätzliche Frage.

• Wie gehen die internationalen Instanzen und die Rechtsvorschriften der anderen Länder mit der Frage der Technologien am Arbeitsplatz um?

ABSCHNITT 1
AUF EU-EBENE

38.11

Der Europäische Gerichtshof für Menschenrechte. Das Prinzip des Schutzes des Privatlebens des Arbeitnehmers an seinem Arbeitsplatz wurde wiederholt von dem Europäischen Gerichtshof für Menschenrechte bestätigt[95]: "Jedermann hat Anspruch auf Achtung seines Privat- und Familienlebens, seiner Wohnung und seines Briefverkehrs" (EMRK, Art. 8). Auch wenn nicht immer auf dieselbe Art ausgelegt, so findet man doch insgesamt der Sinn und der Wortlaut der Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK) wieder. Das Anliegen ist immer dasselbe: Die Suche nach einem Kompromiss zwischen dem Recht des Arbeitgebers, die Tätigkeit seiner Arbeitnehmer zu kontrollieren und dem Schutz ihrer Privatsphäre. Mehrere Texte formalisieren auf EU-Ebene und international die Verpflichtung der vorherigen Information des Arbeitnehmers.

38.12

Empfehlung Nr. R (89) 2. Die Empfehlung Nr. R (89) 2 des Ministerkomitees des Europarats an die Mitgliedstaaten über den Schutz personenbezogener Daten im Arbeitsverhältnis vom 18. Januar 1989 legt fest:

„3. Information und Konsultierung der Arbeitnehmer:

3.1. In Übereinstimmung mit den nationalen Rechtsvorschriften und Praktiken und gegebenenfalls mit einem kollektiven Arbeitsvertrag sollten die Arbeitgeber ihre Arbeitnehmer oder deren Vertreter informieren oder konsultieren, bevor sie ein automatisiertes System zur Erhebung und Verwendung personenbezogener Daten der Arbeitnehmer einführen oder ändern. Dieses Prinzip gilt auch für die Einführung oder die Änderung von technischen Verfahren zur Kontrolle des Kommens und Gehens oder der Produktivität der Arbeitnehmer.

3.2. Das Einverständnis der Arbeitnehmer oder ihrer Vertreter sollte vor der Einführung oder Änderung solcher Systeme oder Verfahren eingeholt werden, wenn sich durch den in Paragraph 3.1. erwähnten Vorgang der Konsultierung eine mögliche Verletzung der Privatsphäre oder der Menschenwürde der Arbeitnehmer herausstellt, außer wenn andere angemessene Garantien durch die nationalen Rechtsvorschriften oder Praktiken vorgesehen sind."

---

[95] EGMR, 16. Dezember 1992, Fall Niemietz/Deutschland, Nr. 00013710/88, Serie A, Nr. 251 B, § 29, JDI 1993, S. 755, Bem. E. Decaux und P. Tavernier; D. 1993, Zusf. 386, Bem. J.-F. Renucci.

38.13

Sammlung praktischer Richtlinien für den Schutz von Beschäftigtendaten des Internationalen Arbeitsamtes vom 7. Oktober 1996.

Dieses Dokument sieht insbesondere vor: „Personenbezogene Daten, die im Zusammenhang mit technischen oder organisatorischen Maßnahmen zur Gewährleistung der Sicherheit und des einwandfreien Funktionierens automatischer Informationssysteme erhoben werden, sollten nicht verwendet werden, um das Verhalten von Arbeitnehmern zu kontrollieren“ (Punkt 5.4).

Diese Sammlung sieht jedoch auch vor, dass eine elektronische Überwachung unter gewissen Bedingungen eingesetzt werden darf: einerseits dürfen die bei dieser Gelegenheit erhobenen Daten nicht die einzige Grundlage zur Beurteilung des Arbeitnehmers darstellen, andererseits, wenn Arbeitnehmer überwacht werden, sollten Sie vorab über die Gründe der Überwachung, den Zeitplan, die eingesetzten Methoden und Techniken und die Daten, die erhoben werden sollen, informiert werden (Punkt 6 der Sammlung). So wird angegeben, dass eine ständige Überwachung nur zulässig sein kann, wenn sie aus Gründen der Gesundheit und Sicherheit oder zum Schutze des Eigentums des Unternehmens erforderlich ist. Außerdem wird angegeben, dass eine heimliche Überwachung nur zulässig sein kann, wenn sie in mit den nationalen Rechtsvorschriften vereinbar ist oder „wenn der begründete Verdacht strafbarer Handlungen oder anderer ernsthafter Verfehlungen besteht“, zu denen es angebracht ist, die sexuelle Belästigung zu zählen.

38.14

Arbeitsdokument vom 29. Mai 2002 der Artikel-29-Datenschutzgruppe.

Es soll hier auch auf das am 29. Mai 2002 von der Artikel-29-Datenschutzgruppe angenommene Arbeitsdokument hingewiesen werden (s. Nr. 15.18). Dieses “Arbeitsdokument zur Überwachung der elektronischen Kommunikation von Beschäftigten” [96], scheint weitgehend von den Arbeiten und Reflektionen der französischen Datenschutzbehörde Cnil inspiriert zu sein.

ABSCHNITT 2
NATIONALE BESONDERHEITEN

38.21

USA. Mit der heiklen Problematik der Cyber-Überwachung wird in den USA nicht gleich umgegangen wie in Frankreich. Die US-amerikanischen Arbeitgeber bekommen oft das Recht auf den Zugang zu dem E-Mail-Verkehr ihrer Arbeitnehmer zugesprochen. In der Tat zeigen die neuesten Umfragen [97], dass 46,5 % der Unternehmen den Inhalt der E-Mails ihrer Arbeitnehmer prüfen und speichern. Auch wenn das Briefgeheimnis durch den *Electronic Communications Privacy Act of 1986*[98] (18 USC §§ 2510 f.), geschützt wird, so darf der Arbeitgeber doch das Informatik-Netzwerk des Unternehmens unter Überwachung stellen, was ihm konkret das Recht gibt, völlig legal die Telefongespräche seiner Arbeitnehmer abzuhören oder ihre E-Mails einzusehen, auch wenn diese Ausnahmen nur möglich sind, wenn die geschäftlichen Bedürfnisse sie erfordern und unter dem Vorbehalt, dass der Arbeitnehmer zuvor über diese Überwachung informiert worden war.

38.22

Großbritannien. Die für den Schutz der personenbezogenen Daten zuständige Obrigkeit *Information Commissioner* hat einen Kodex über den Schutz der personenbezogenen Daten und die Praktiken im Arbeitsverhältnis veröffentlicht [99].

---

[96] Artikel-29-Datenschutzgruppe, Arbeitsdokument vom 29. Mai 2002 http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp55_de.pdf

[97] Durch das “ePolicy Institute” durchgeführte Umfrage: http://www.epolicyinstitute.com/survey/survey.pdf.

[98] http://cpsr.org/issues/privacy/ecpa86/.

[99] *The Employment Practices Data Protection Code,*

Dieser grenzt die Bedingungen ein, unter denen der Arbeitgeber seine Arbeitnehmer überwachen kann. Dieser Kodex, der sich auf die Bestimmungen des *Data Protection Act of 1998* (Kapitel 29)[100] stützt, macht die Überwachung der Arbeitnehmer von zwei Prinzipien abhängig: Transparenz und Verhältnismäßigkeit. So muss der Arbeitgeber seine Arbeitnehmer nicht nur über die eingesetzten Überwachungsmaßnahmen informieren, sondern auch alle personenbezogenen Informationen herausfiltern, die in Anbetracht der zwischen ihnen bestehenden beruflichen Beziehung unnötig oder überzogen sind.

http://www.informationcommissioner.gov.uk/eventual.aspx?id=437.

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