Les Cahiers de droit

Preuve et surveillance des salariés : regard français

Bernard Bossu et Alexandre Barège

Volume 54, numéro 2-3, juin–septembre 2013

URI : https://id.erudit.org/iderudit/1017614ar
DOI : https://doi.org/10.7202/1017614ar

Aller au sommaire du numéro

Éditeur(s)

Faculté de droit de l'Université Laval

ISSN

0007-974X (imprimé)
1918-8218 (numérique)

Découvrir la revue

Citer cet article

Bossu, B. & Barège, A. (2013). Preuve et surveillance des salariés : regard français. *Les Cahiers de droit*, *54*(2-3), 277–302. https://doi.org/10.7202/1017614ar

Résumé de l'article

Avec le développement des technologies de l'information et de la communication, les techniques de surveillance des salariés se sont multipliées. L'évolution s'est principalement traduite par un contrôle moins visible, la caméra et les badges électroniques ayant progressivement remplacé le contremaître. En outre, l'outil informatique a largement pénétré les entreprises. Ces situations soulèvent des interrogations majeures : faut-il notamment poser des limites aux contrôles que peuvent exercer les employeurs sur les salariés ? Il convient d'abord de rappeler qu'il est légitime pour un employeur de surveiller l'activité de ses travailleurs. Par le contrat de travail, le salarié se soumet au pouvoir de direction du chef d'entreprise. La difficulté réside en réalité dans la possibilité de porter atteinte à certains espaces de vie personnelle. C'est notamment la vie privée qui risque d'être malmenée, le salarié pouvant être filmé ou écouté à son insu. Le contrat de travail ne peut légitimer de telles situations : la liberté étant inhérente à la condition d'Homme, on ne peut y renoncer moyennant rémunération. De plus, ces nouveaux procédés de preuve sont peu compatibles avec la loyauté contractuelle qui doit présider aux relations de travail.

Preuve et surveillance des salariés : regard français

Bernard Bossu* et Alexandre Barège**

Avec le développement des technologies de l'information et de la communication, les techniques de surveillance des salariés se sont multipliées. L'évolution s'est principalement traduite par un contrôle moins visible, la caméra et les badges électroniques ayant progressivement remplacé le contremaître. En outre, l'outil informatique a largement pénétré les entreprises. Ces situations soulèvent des interrogations majeures : faut-il notamment poser des limites aux contrôles que peuvent exercer les employeurs sur les salariés ? Il convient d'abord de rappeler qu'il est légitime pour un employeur de surveiller l'activité de ses travailleurs. Par le contrat de travail, le salarié se soumet au pouvoir de direction du chef d'entreprise. La difficulté réside en réalité dans la possibilité de porter atteinte à certains espaces de vie personnelle. C'est notamment la vie privée qui risque d'être malmenée, le salarié pouvant être filmé ou écouté à son insu. Le contrat de travail ne peut légitimer de telles situations : la liberté étant inhérente à la condition d'Homme, on ne peut y renoncer moyennant rémunération. De plus, ces nouveaux procédés de preuve sont peu compatibles avec la loyauté contractuelle qui doit présider aux relations de travail.

With the growth of Information and Communications Technologies, the number of techniques used to monitor wage-earners has increased.

* Doyen, Faculté de droit, Université de Lille 2 ; directeur, Équipe de recherche en droit social (LEREDS) du Centre de recherche Droits et perspectives du droit (CRDP).

** Maître de conférences, Université de Lille 2 ; directeur, Institut des Sciences du travail (Université Lille 2).

***Les Cahiers de Droit*, vol. 54, n^os^ 2-3, juin-septembre 2013, p. 277-302**

Over time, less visible controlling methods, such as video cameras and electronic badges, have gradually replaced overseers. In addition, electronic devices have been widely adopted by companies. These developments raise major questions. For example, should limits be set on the controls exercised by employers over their workers ? First, it is important to note that employers have legitimate grounds for monitoring the activity of their workforce. By signing a job contract, wage-earners submit to the authority of the head of the company. The difficulty, however, lies in the possibility of encroachment into certain spheres of employees' personal lives. Their privacy, in particular, is under threat, since they may be filmed or have their conversations monitored without their knowledge. A job contract cannot legitimize such a situation ; freedom is inherent in the human condition and cannot be waived for monetary consideration. Moreover, these new processes for adducing evidence are hard to reconcile with the contractual loyalty that governs labour relations.

Pages

1 Le respect de la loyauté contractuelle 280
1.1 L'absence de dispositif spécifique de surveillance 282
1.2 La présence d'un dispositif spécifique de surveillance 285
1.2.1 L'information 285
1.2.2 La proportionnalité 289
2 Le respect de la vie privée 292
2.1 Le principe 292
2.2 Les limites 298
Conclusion 302

Avec la banalisation des technologies de l'information et de la communication, les rapports entre la vie privée et le travail ont été profondément bouleversés. Beaucoup de salariés sont aujourd'hui joignables et donc dérangeables partout et à tout moment, dans un total mépris pour la vie privée. À l'inverse, certains travailleurs n'hésitent pas à passer de longues heures sur leur lieu de travail à surfer sur Internet ou à rédiger du courrier personnel. Selon une étude réalisée de 2006 à 2010 par le cabinet Olféo,

le temps moyen d'utilisation d'Internet pour chaque salarié ayant accès à Internet à l'occasion de son travail est de 35 minutes par jour pour des raisons professionnelles et 59 minutes pour des raisons non professionnelles[1]. Par ailleurs, des milliers d'internautes exposent aussi régulièrement leur vie personnelle par des textes, photos et vidéos, partout sur la planète. Les réseaux sociaux, et en tout premier lieu Facebook, permettent d'échanger librement sur le directeur des ressources humaines ou sur la nouvelle collègue de travail avec beaucoup d'amis qui nous veulent forcément du bien ! Pourtant, par hasard sans doute, les propos échangés se retrouvent sur le bureau de l'employeur …

Ce constat renouvelle la problématique des contrôles que peuvent exercer les employeurs sur les salariés. Bien évidemment, il est légitime pour un employeur de surveiller la prestation de travail de ses salariés. En vertu de son pouvoir de direction, l'employeur a non seulement le droit de donner des ordres ou des instructions, mais aussi d'en contrôler l'exécution. Ce droit se présente même parfois comme un devoir, l'employeur étant tenu de veiller au respect des règles d'hygiène et de sécurité[2]. Cependant, ces contrôles, pour légitimes qu'ils soient, doivent être exercés dans le respect de la personne humaine. Or l'ordre technologique est peu respectueux des droits des personnes : le salarié « est surveillé par la machine, à la limite par lui-même, par tous et par personne[3] ». Soucieuse de protéger la personne au travail, la jurisprudence a posé deux limites au pouvoir de contrôle et de surveillance exercé par l'employeur sur ses salariés pour s'arroger des preuves. La première limite a pour fondement l'obligation de loyauté ; l'autre prend sa source dans la vie privée au travail. Le principe de loyauté, qui innerve l'ensemble des relations de travail, condamne toute ruse aboutissant à piéger l'adversaire[4]. En conséquence, le salarié doit être informé des techniques de surveillance mises en place dans l'entreprise. L'employeur ne peut pas non plus recourir à des artifices ou à des stratagèmes pour placer le salarié dans une situation qui pourrait ultérieurement lui être imputée à faute[5]. Ainsi, des faits résultant d'une provocation de l'employeur ne peuvent servir de cause réelle et sérieuse[6].

1. Yves Lasfargue, « Panorama de l'utilisation des TIC par les salariés dans leur travail », dans Tristan Klein et Daniel Ratier (dir.), *L'impact des TIC sur les conditions de travail*, Paris, La Documentation française, 2012, p. 67, à la page 77.
2. Philippe Waquet, *L'entreprise et les libertés du salarié. Du salarié-citoyen au citoyen-salarié*, Paris, Éditions Liaisons, 2003, p. 163.
3. Gérard Lyon-Caen, *Les libertés publiques et l'emploi. Rapport pour le ministre du Travail, de l'Emploi et de la Formation*, Paris, La Documentation française, 1992, p. 138.
4. Philippe Waquet, « Halte aux stratagèmes », *Semaine Sociale Lamy* 2008.5, 6.
5. Jacques Duplat, « Surveillance des salariés et vie privée », R.J.S. 2003.104, 105.
6. Soc. 16 janv. 1991, *Bull. civ.* V, nº 15.

S'agissant de la vie privée au travail, on pourrait assurément s'interroger sur son existence puisque le salarié doit normalement se consacrer dans l'entreprise à l'exercice de son activité professionnelle. Cela étant, on ne peut pas ignorer que l'entreprise n'est pas seulement le lieu d'exécution de la prestation de travail : c'est aussi un lieu de vie au sein duquel peuvent être accomplis des actes ne relevant pas de la sphère professionnelle[7]. C'est pourquoi la Cour de cassation s'efforce de soustraire au regard de l'employeur ce qui peut légitimement être regardé comme relevant de la vie privée. Le 2 octobre 2001, après avoir proclamé le principe d'une vie privée au travail, la Cour de cassation a décidé qu'un salarié peut prétendre, au temps et au lieu du travail, au secret des correspondances dès lors que celles-ci sont identifiées comme personnelles[8]. En définitive, la considération de la personne au travail implique un contrôle exercé loyalement (1) mais aussi le respect de la vie privée du salarié (2).

1 Le respect de la loyauté contractuelle

L'administration de la preuve doit s'effectuer conformément au principe de loyauté, ce qui exclut, sous couvert de rassembler des éléments de preuve, les ruses, machinations ou stratagèmes de nature à tromper une personne[9]. Le principe de loyauté dans l'administration de la preuve a été consacré par l'Assemblée plénière de la Cour de cassation le 7 janvier 2011. Pour juger irrecevable « l'enregistrement d'une communication téléphonique réalisé à l'insu de l'auteur des propos », l'Assemblée plénière a visé l'article 9 du Code de procédure civile, l'article 6 § 1 de la *Convention de sauvegarde des droits de l'homme et des libertés fondamentales*[10] et « le principe de loyauté dans l'administration de la preuve[11] ». L'article 9 du Code de procédure civile, qui prévoit qu'« il incombe à chaque partie de prouver conformément à la loi les faits nécessaires au succès de sa prétention », pose un principe de légalité : on ne doit pas commettre une infraction pour rapporter la preuve d'un fait[12]. En vertu de ce texte, la preuve

7. Soc. 8 juill. 2009, D. 2009.2393, note Loiseau.
8. Soc. 2 oct. 2001, *Dr. Soc.* 2001.915, note Ray, D. 2001.3148, note Gauthier.
9. Frédéric Debove, François Falletti et Thomas Janville, *Précis de droit pénal et de procédure pénale*, 4e éd., Paris, Presses universitaires de France, 2011, p. 650.
10. *Convention de sauvegarde des droits de l'homme et des libertés fondamentales*, 4 novembre 1950, S.T.E. no 5.
11. Ass. plén. 7 janv. 2011, *R.T.D. civ.* 2011.127, obs. Fages, *R.T.D. civ.* 2011.383, obs. Thery, J.C.P. éd. E. 2011.1053, note Malaurie-Vignal.
12. Anne Leborgne, « L'impact de la loyauté sur la manifestation de la vérité ou le double visage d'un grand principe », *R.T.D. civ.* 1996.535, 546.

légalement admissible est celle obtenue de façon loyale[13]. La référence à l'article 6 § 1 de la *Convention de sauvegarde des droits de l'homme et des libertés fondamentales*, qui affirme le droit à un procès équitable, s'analyse aussi comme une manifestation du principe de loyauté. Ce rapprochement s'explique par le fait que le principe d'égalité des armes, qui est une des composantes du procès équitable, interdit le comportement déloyal d'un plaideur[14].

En matière pénale, l'action des agents de l'autorité (magistrats, policiers, gendarmes) est étroitement subordonnée au principe de loyauté[15]. En revanche, les parties privées y échappent largement[16]. Il résulte en effet d'une jurisprudence constante « qu'aucune disposition légale ne permet aux juges répressifs d'écarter les moyens de preuve produits par les parties au seul motif qu'ils auraient été obtenus de façon illicite ou déloyale ; […] il leur appartient seulement […] d'en apprécier la valeur probante après les avoir soumis à la discussion contradictoire[17] ». Est ainsi recevable, pour la Chambre criminelle, l'enregistrement vidéo montrant un préparateur en pharmacie en train de prendre de l'argent dans la caisse[18]. Au contraire, en matière civile, la Chambre sociale de la Cour de cassation considère qu'un principe de loyauté gouverne la recherche de la preuve et qu'en conséquence les procédés visant à surprendre l'adversaire doivent être bannis. Tous les coups ne sont pas permis, même s'il s'agit de faire surgir la vérité[19]. S'appuyant sur l'article 9 du Code de procédure civile, la Chambre sociale de la Cour de cassation a affirmé ceci dans un arrêt de principe en date du 20 novembre 1991 : « Si un employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps du travail, tout enregistrement, quels qu'en soient les motifs, d'images ou de paroles à leur insu constitue un mode de preuve illicite[20]. » Plus récemment, dans un arrêt

13. Yves Chauvy, « Contrôle du travail par filature du salarié : un procédé de preuve illicite », R.J.S. 1995.489, 490 ; Bernard Bossu, « Nouvelles technologies et surveillance du salarié », R.J.S. 2001.663, 664.
14. Civ. 2e, 7 oct. 2004, D. 2005.122, note Bonfils.
15. F. Debove, F. Falletti et T. Janville, préc., note 9, p. 652 ; Serge Guinchard et Jacques Buisson, *Procédure pénale*, 7e éd., Paris, LexisNexis, 2011, nos 570 et suiv.
16. F. Debove, F. Falletti et T. Javille, préc., note 9, p. 652 ; S. Guinchard et J. Buisson, préc., note 15, no 575.
17. Crim. 11 juin 2002, *Bull. crim.*, no 131 ; Crim. 27 janv. 2010, *Bull. crim.*, no 16. Voir aussi : Crim. 7 mars 2012, *Bull. crim.*, no 64 ; Françoise Favennec-Héry, « Vie professionnelle, vie personnelle du salarié et droit probatoire », *Dr. soc.* 2004.48.
18. Crim. 6 avr. 1994, *Bull. crim.*, no 136. Voir aussi : Crim. 23 juill. 1992, *Bull. crim.*, no 274 ; Crim. 23 juill. 1992, *R.T.D. civ.* 1993.101, obs. Hauser.
19. Laurent Aynès, « L'obligation de loyauté », *Arch. philo. dr.* 2000.195, 202.
20. Soc. 20 nov. 1991, *Bull. civ.* V, no 519, R.J.S. 1992.1, *Dr. soc.*, 1992.28, rapp. Waquet, D. 1992.73, note Chauvy.

du 23 mai 2012, la Chambre sociale a réaffirmé ce principe de loyauté en s'appuyant, comme l'Assemblée plénière de la Cour de cassation, sur « les articles 9 du Code de procédure civile, 6 § 1 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales et le principe de loyauté dans l'administration de la preuve[21] ». La loyauté suppose que l'employeur mette en place une surveillance connue du personnel : les procédés clandestins de surveillance ne sont pas admissibles. En pratique, deux situations peuvent se rencontrer. En premier lieu, pour prouver le comportement fautif d'un salarié, l'employeur n'est pas tenu de mettre en place un dispositif spécifique de surveillance et, si le procédé utilisé n'est pas déloyal, la preuve est valablement reconnue. En second lieu, si l'employeur décide de mettre en place un dispositif spécifique de surveillance, il doit respecter des conditions d'ordre procédural pour échapper au grief de clandestinité[22]. Ainsi, parce qu'il ne peut pas surprendre le salarié, il devra informer celui-ci du dispositif de contrôle utilisé.

1.1 L'absence de dispositif spécifique de surveillance

Pour contrôler l'activité de ses salariés, l'employeur n'est pas obligé de mettre en place un dispositif spécifique de surveillance. Comme le précise la Cour de cassation dans son arrêt rendu le 26 avril 2006, « [l]a simple surveillance d'un salarié faite sur les lieux du travail par son supérieur hiérarchique, même en l'absence d'information préalable du salarié, ne constitue pas en soi un mode de preuve illicite[23] ». Il résulte de cette décision que la simple surveillance d'un salarié, c'est-à-dire celle résultant d'une observation directe du salarié par son supérieur hiérarchique, sans recours à un procédé technique de contrôle de l'activité, est licite. L'employeur tire en effet de son pouvoir de direction le droit de contrôler et de surveiller l'activité de ses salariés. Pour mesurer la portée exacte de cette décision, deux précisions doivent être apportées. L'arrêt parle tout d'abord de la surveillance par un supérieur hiérarchique : il n'évoque pas la question d'un contrôle qui serait opéré par un collègue de travail de même niveau hiérarchique ou par un observateur extérieur à l'entreprise. Dans ce dernier cas, la jurisprudence se montre plutôt réservée. Ainsi, une société ne peut recruter à l'insu du personnel un vigile pour contrôler l'utilisation par les salariés des distributeurs de boissons et de sandwiches[24]. Un employeur

21. Soc. 23 mai 2012, J.C.P. S. 2012.1371, note Bossu.
22. Alexandre Barège et Bernard Bossu, « L'ordinateur et la vie privée du salarié », J.C.P. S. 2007.1451 ; F. Favennec-Héry, préc., note 17, 52.
23. Soc. 26 avr. 2006, J.C.P. S. 2006.1444, note Corrignan-Carsin.
24. Soc. 15 mai 2001, *Bull. civ.* V, nº 168, R.J.S. 2001.830. Voir toutefois Soc. 4 juill. 2012, nº 11-14241, inédit.

ne peut pas non plus avoir recours au service d'un détective privé au temps et au lieu du travail sans une information préalable du salarié[25]. L'arrêt du 26 avril 2006[26] parle par ailleurs d'une surveillance effectuée par un supérieur hiérarchique sur les lieux du travail. Et ce qui est possible à l'intérieur de l'entreprise ne l'est pas forcément à l'extérieur. Ainsi, même si le salarié exerce sa prestation de travail en dehors des locaux de l'entreprise, l'employeur ne peut pas recourir à un détective privé. Dans un arrêt de principe en date du 26 novembre 2002, la Cour de cassation affirme qu'« une filature organisée par l'employeur pour contrôler et surveiller l'activité d'un salarié constitue un moyen de preuve illicite dès lors qu'elle implique nécessairement une atteinte à la vie privée de ce dernier, insusceptible d'être justifiée, eu égard à son caractère disproportionné, par les intérêts légitimes de l'employeur[27] ». Dans une autre affaire, l'employeur voulait démontrer qu'un salarié travaillait pendant son temps de travail dans le restaurant tenu par son épouse. Pour prouver un tel comportement, il a demandé à plusieurs salariés de l'entreprise de se rendre dans le restaurant, de prendre des photographies et d'établir un rapport. Pour la Cour de cassation, il s'agit « [d']un dispositif de surveillance clandestin et à ce titre déloyal[28] », car les salariés mandatés par l'employeur s'étaient présentés comme de simples clients, sans révéler leurs qualités et le but de leur visite.

Au-delà de la surveillance directe par le supérieur hiérarchique, la preuve est également valablement recueillie, même sans information préalable du salarié, si elle ne se traduit pas par l'organisation d'un dispositif particulier, mais résulte de la seule utilisation de techniques connues et légitimes[29]. Il en va ainsi des relevés de communications téléphoniques adressées par la société France Télécom pour le règlement des communications correspondant au poste d'un salarié. L'absence d'information préalable du salarié ne rend pas illicite le procédé de surveillance[30].

Qu'en est-il du constat d'huissier ? Peut-on utiliser un tel procédé pour faire constater la faute disciplinaire d'un salarié ? Pour la Cour de cassation, « si un constat d'huissier ne constitue pas un procédé clandestin de surveillance nécessitant l'information préalable du salarié, en revanche il est interdit à cet officier ministériel d'avoir recours à un stratagème pour

25. Soc. 23 nov. 2005, *Dr. soc.* 2006.277, note Mouly.
26. Soc. 26 avr. 2006, préc., note 23.
27. Soc. 26 nov. 2002, *Dr. soc.* 2003.225, note Savatier.
28. Soc. 18 mars 2008, 1re esp., J.C.P. S. 2008.1396, note Bossu, *Dr. Soc.* 2008.610, note Radé.
29. Bernard Teyssié, « La preuve en droit du travail », dans Catherine Puigelier (dir.), *La preuve*, Paris, Economica, 2004, p. 73, à la page 78.
30. Soc. 15 mai 2001, préc., note 24.

recueillir une preuve[31] ». La solution est conforme à l'article 1er de l'*Ordonnance nº 45-2592 du 2 novembre 1945 relative au statut des huissiers*[32]. Selon ce texte, les huissiers peuvent être commis par justice pour effectuer des constatations purement matérielles, exclusives de tout avis sur les conséquences de fait ou de droit qui peuvent en résulter ; ils peuvent également procéder à des constatations de même nature à la requête de particuliers ; dans l'un et l'autre cas, ces constatations n'ont que la valeur de simples renseignements. Puisque le constat d'huissier ne constitue pas en lui-même un procédé clandestin de surveillance, l'employeur n'a pas à informer les salariés avant d'y avoir recours. En revanche, les pouvoirs de l'huissier sont strictement encadrés : il doit se borner à constater objectivement les faits sans avoir recours à un stratagème pour confondre le salarié. Ainsi, l'huissier ne peut faire usage d'une fausse identité pour obtenir des renseignements défavorables au salarié[33]. De même, un huissier ne peut pas organiser « un montage en faisant effectuer, dans les différentes boutiques et par des tiers qu'il y avait dépêchés, des achats en espèces puis en procédant, après la fermeture du magasin et hors la présence de la salariée, à un contrôle des caisses et du registre des ventes[34] ».

Pour en terminer avec l'absence de dispositif spécifique de surveillance, il convient de s'interroger sur la licéité des autocommutateurs téléphoniques. Ce procédé permet d'enregistrer les numéros appelés, mais aussi la date, l'heure et le coût à partir de chacun des postes téléphoniques. L'employeur, qui met en place un autocommutateur téléphonique, doit-il en informer les salariés ? La Cour de cassation répond par la négative au motif que « la simple vérification des relevés de la durée, du coût et des numéros des appels téléphoniques passés à partir de chaque poste édités au moyen de l'autocommutateur téléphonique de l'entreprise ne constitue pas un procédé de surveillance illicite pour n'avoir pas été préalablement porté à la connaissance du salarié[35] ». L'affirmation surprend, car il s'agit bien d'un dispositif technique[36]. La Commission nationale informatique et libertés

31. Soc. 18 mars 2008, 2e esp., préc., note 28.
32. *Ordonnance nº 45-2592 du 2 novembre 1945 relative au statut des huissiers*, J.O. 3 nov. 1945, p. 7163.
33. Soc. 5 juill. 1995, R.J.S. 1995.1110.
34. Soc. 18 mars 2008, préc., note 31.
35. Soc. 29 janv. 2008, 2e esp., J.C.P. S. 2008.1396, note Bossu.
36. F. Favennec-Héry, préc., note 17, 52. De façon aussi curieuse, la Cour de cassation considère que « le fait pour une banque de mettre en place un système d'exploitation intégrant un mode de traçage permettant d'identifier les consultants des comptes ne peut être assimilé […] au recours à une preuve illicite, le travail effectué par utilisation de l'informatique ne pouvant avoir pour effet de conférer l'anonymat aux tâches différentes effectuées par les salariés » : Soc. 18 juill. 2000, R.J.S. 2000.1068.

(CNIL) recommande d'ailleurs de déclarer ce système et de procéder à l'information des salariés et à la consultation du comité d'entreprise[37].

Reste maintenant à envisager la procédure à suivre lorsque l'employeur décide de mettre en place un dispositif technique de surveillance et qu'il est analysé comme tel par la jurisprudence.

1.2 La présence d'un dispositif spécifique de surveillance

En présence d'un dispositif spécifique de surveillance, la loyauté est posée de manière prescriptive par l'article 6 de la loi du 6 janvier 1978[38]. En conséquence lorsqu'un employeur envisage d'avoir recours à un dispositif spécifique de surveillance, quel qu'il soit (vidéosurveillance, géolocalisation, badges, enregistrement des conversations téléphoniques, etc.), il est tenu de respecter certaines modalités procédurales.

1.2.1 L'information

L'employeur doit tout d'abord informer la collectivité de travail sur la technique de contrôle utilisée. Conformément aux dispositions de l'article L. 2323-32 alinéa 3 du Code du travail, le comité d'entreprise doit être informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés[39]. À défaut, il faut considérer que l'élément de preuve obtenu à l'aide du dispositif de surveillance l'a été par un moyen illicite, ce qui le rend irrecevable[40].

C'est ensuite le salarié qui doit être informé sur les techniques de surveillance utilisées. Un arrêt a posé en principe que, « si l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail, tout enregistrement, quels qu'en soient les motifs, d'images ou de paroles à leur insu constitue un mode de preuve illicite[41] ». L'obligation de transparence ainsi imposée par la jurisprudence a ensuite fait l'objet d'une consécration législative. Selon l'article L. 1222-4 du Code du travail,

37. CNIL, délib. nº 2005-19, 3 févr. 2005, J.O. 1 mars 2005, nº 50.
38. *Loi nº 78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés*, J.O. 7 janv. 1978, p. 227.
39. On peut également s'interroger sur la nécessité de consulter préalablement le comité d'hygiène, de sécurité et des conditions de travail au titre des problèmes généraux intéressant les conditions de travail. Voir Soc. 4 juill. 2012, nº 11-19678, inédit ; Soc. 28 nov. 2007, *Bull. civ.* V, nº 201.
40. Soc. 31 janv. 2001, J.C.P. E. 2001.1145, note Puigelier, R.J.S. 2001.405 ; Soc. 15 mai 2001, préc., note 24.
41. Soc. 20 nov. 1991, préc., note 20.

« aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance ». Mais puisqu'il s'agit d'informer les salariés des moyens destinés à assurer leur surveillance, aucune obligation ne peut peser sur l'employeur lorsque le dispositif de surveillance n'a pas pour objectif de contrôler l'activité des salariés. Ainsi, dans un arrêt du 31 janvier 2001, la Chambre sociale de la Cour de cassation a considéré que l'information du salarié n'est pas requise lorsque le dispositif de surveillance a été mis en place au sein de locaux dans lesquels les salariés ne travaillent pas[42]. En l'espèce, un employeur avait installé un système de vidéosurveillance dans des locaux auxquels les salariés n'avaient normalement pas accès. Ce dispositif de surveillance avait permis de mettre en évidence qu'un salarié de l'entreprise s'était livré à un vol de marchandises après être entré sans autorisation dans les locaux. Ce dernier soutenait alors que la vidéo ne lui était pas opposable puisque le dispositif n'avait pas été porté à sa connaissance, pas plus qu'à celle du comité d'entreprise. Cela importait peu selon la Cour de cassation puisqu'il n'avait pas à pénétrer dans les locaux. *A contrario*, dès lors que le système permet la surveillance du salarié, ce dernier doit être informé de son existence, peu important que le dispositif n'ait pas été mis en place par l'employeur mais par une société cliente. Ainsi, dans un arrêt du 10 janvier 2012, après avoir rappelé que « l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail », la Cour de cassation a précisé qu'« il ne peut être autorisé à utiliser comme mode de preuve les enregistrements d'un système de vidéosurveillance installé sur le site d'une société cliente permettant le contrôle de leur activité dont les intéressés n'ont pas été préalablement informés de l'existence[43] ». L'arrêt concernait une entreprise proposant des prestations de nettoyage. Un salarié a été affecté sur le site d'une entreprise cliente. Celle-ci avait mis en place un système de vidéosurveillance qui a permis de mettre en évidence que le salarié ne respectait les horaires de travail qu'il prétendait avoir réalisés. Pour en établir la démonstration, l'employeur a obtenu, sur le fondement de l'article 145 du Code de procédure civile, qu'un huissier soit désigné aux fins de visionner les vidéos et d'établir un relevé des heures d'arrivée et de départ du salarié. Contestant la licéité de la preuve, le salarié en demandait le rejet. Pour la Cour de cassation, puisque le salarié n'avait pas été informé de l'existence du dispositif, la

42. Soc. 31 janv. 2001, préc., note 40. Dans le même sens, Voir également Soc. 19 avr. 2005, *Bull. civ.* V, nº 141, J.C.P. S. 2005.1032, note Cesaro, J.C.P. E. 2005.1394, obs. Béal et Devaux ; Soc. 19 janv. 2010, R.J.S. 2010.307.

43. Soc. 10 janv. 2012, J.C.P. S. 2012.1122, note Loiseau, R.D.T. 2012.223, note Gardin, R.J.S. 2012.182.

preuve n'était pas recevable. Le fait que le système de surveillance soit mis en place par un tiers à la relation de travail, en l'espèce une entreprise cliente, est sans incidence.

Enfin, au terme des dispositions légales, tout traitement automatisé de données à caractère personnel doit être déclaré à la CNIL, voire, dans certains cas spécifiques, faire l'objet d'une autorisation de la part de l'autorité administrative indépendante[44]. Les entreprises sont dispensées de l'obligation préalable de déclaration lorsqu'elles ont désigné un « correspondant à la protection des données à caractère personnel[45] ». Sous cette réserve, puisqu'il s'agit d'un traitement automatisé de données à caractère personnel, tout dispositif spécifique de contrôle de l'activité des salariés doit être déclaré à la CNIL, voire de façon plus exceptionnelle faire l'objet d'une autorisation.

On l'aura compris, l'employeur doit informer les salariés, individuellement et collectivement, lorsqu'il entend avoir recours à un dispositif spécifique de surveillance. Mais doit-il les informer de la finalité du dispositif ? Et peut-il utiliser le dispositif à d'autres fins que celles ayant donné lieu à information ?

Un premier élément de réponse peut être trouvé dans un arrêt du 7 juin 2006. Dans cette affaire, l'employeur avait apporté la preuve des faits reprochés au salarié grâce à un système de vidéosurveillance. Le salarié contestait la recevabilité de ce mode de preuve, car le comité d'entreprise n'avait pas été informé ni consulté. De son côté, l'employeur faisait valoir que le dispositif de contrôle était valable et n'avait pas à être porté à la connaissance des salariés, car il avait pour objectif de surveiller la clientèle, principalement pour limiter les vols dans l'entreprise. Pour la Cour de cassation, les enregistrements constituaient un moyen de preuve illicite, car « le système de vidéo surveillance de la clientèle mis en place par l'employeur était également utilisé par celui-ci pour contrôler ses salariés sans information et consultation préalable du comité d'entreprise[46] ». Il faut donc comprendre que les juges ne se limitent pas à la finalité du dispositif affichée par l'employeur. Au contraire, ils se livrent à un strict contrôle de la

44. *Loi n° 78-17 du 6 janv. 1978 relative à l'informatique, aux fichiers et aux libertés*, préc., note 38, art. 23 et suiv. À propos des situations conduisant à l'obligation d'obtenir une autorisation préalablement à la mise en place du dispositif : *id.*, art. 25.

45. *Id.*, art. 22. Lorsqu'un transfert de données à caractère personnel à destination d'un État non membre de la Communauté européenne est envisagé, la désignation d'un correspondant à la protection des données à caractère personnel ne dispense pas l'entreprise de son obligation de déclaration.

46. Soc. 7 juin 2006, *Bull. civ.* V, n° 206, *Juris-Data n° 033904*, J.C.P. S. 2006.1614, note Corrignan-Carsin.

finalité du système mis en place par l'employeur. S'il apparaît que l'une des finalités du dispositif est le contrôle de l'activité des salariés, l'employeur doit informer les salariés et la CNIL de son existence. À défaut, le système ne peut être utilisé pour prouver les agissements fautifs d'un salarié.

La solution a été confirmée dans un arrêt du 3 novembre 2011 relatif à un système de géolocalisation que l'employeur avait mis en place. Il soutenait alors que le dispositif devait permettre de réaliser une étude *a posteriori* des déplacements effectués par les commerciaux itinérants de son entreprise ainsi que d'analyser le temps nécessaire aux déplacements pour optimiser les visites effectuées. Pourtant, sans en informer les salariés, l'employeur utilisait également le dispositif afin de contrôler le temps de travail des salariés. Dans cette affaire, la Cour de cassation a confirmé l'impossibilité de détourner un dispositif de contrôle de l'activité des salariés de sa finalité en posant en principe qu'« un système de géolocalisation ne peut être utilisé par l'employeur pour d'autres finalités que celles qui ont été déclarées auprès de la Commission nationale de l'informatique et des libertés, et portées à la connaissance des salariés[47] ».

Une solution identique se retrouve encore dans l'arrêt du 10 janvier 2012 envisagé précédemment qui concernait un système de vidéosurveillance mis en place par une entreprise cliente de l'employeur au sein de laquelle un salarié était affecté pour effectuer des prestations de nettoyage[48]. En l'espèce, les salariés avaient été informés de l'existence d'un dispositif ayant pour seul but de surveiller les portes d'accès des locaux pour renforcer la sécurité. Pour considérer que la preuve résultant du système technique était inopposable aux salariés en raison de son caractère illicite, la Cour de cassation a relevé que les salariés n'avaient pas été informés du fait que le dispositif permettait de contrôler leurs heures d'arrivée et de départ sur le lieu de travail. L'employeur ne doit donc pas se contenter d'informer les salariés de l'existence du dispositif. Il doit également les informer de sa finalité et le système ne pourra aucunement être utilisé à d'autres fins.

Sur ce point, la Chambre sociale de la Cour de cassation rejoint la position de la CNIL. En application de l'article 6 de la loi du 6 août 2004, aux termes duquel les données à caractère personnel « sont collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées

47. Soc. 3 nov. 2011, J.C.P. E. 2011.1926, note Corrignan-Carsin, J.C.P. S. 2012.1054, note Loiseau, R.D.T. 2012.156, note Bossu et Morgenroth. Voir aussi : Christophe Radé, « À propos de la géolocalisation des salariés : la CNIL et la Cour de cassation à l'unisson », *Hebdo édition sociale* 2011.N8765BSG ; Philippe Flores, « La géolocalisation et le contrôle de la durée du travail : l'état des cartes », *Semaine Sociale Lamy* 2011.7.

48. Soc. 10 janv. 2012, préc., note 43.

ultérieurement de manière incompatible avec ces finalités[49] », l'autorité administrative indépendante considère que, si un système de vidéosurveillance est mis en place pour lutter contre le vol, il ne peut conduire à placer les salariés sous la surveillance constante de l'employeur[50]. En outre, elle estime que la simple apposition d'un autocollant comportant le dessin d'une caméra et le mot « vidéo » est « notoirement insuffisante » pour satisfaire à l'obligation d'information des salariés sur l'existence et les caractéristiques du système[51]. En matière de géolocalisation, la CNIL considère également que l'information doit à la fois porter sur le dispositif mis en place et sur sa finalité[52]. Le même raisonnement doit être appliqué à l'ensemble des dispositifs spécifiques de surveillance.

En conclusion, il apparaît donc que, préalablement à la mise en place ou à l'utilisation d'un dispositif spécifique de surveillance, l'employeur doit informer le comité d'entreprise, les salariés individuellement et la CNIL de sa mise en place ou de son existence. Il doit également les informer de la finalité du dispositif. Toute preuve résultant d'un dispositif utilisé sans information préalable ou à d'autres fins que celles ayant donné lieu à information est déloyale et donc illicite.

1.2.2 La proportionnalité

On l'aura compris, outre la déclaration, voire l'autorisation requise auprès de la CNIL, lorsque la mise en place d'un dispositif spécifique de surveillance est envisagée, l'information collective et individuelle des salariés est essentielle. Pour autant, elle ne peut justifier à elle seule l'existence du dispositif. Pour être acceptable, la surveillance doit respecter une juste mesure entre le contrôle de l'activité des salariés justifié par la préservation des intérêts de l'entreprise et la considération de la personne au travail qui s'accommode difficilement d'une exposition à une surveillance continue. Certes, l'entreprise est avant tout un lieu consacré au travail, mais elle est aussi un lieu de vie dans lequel chacun doit pouvoir se comporter sans

49. *Loi nº 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*, J.O. 7 août 2004, p. 14063.
50. CNIL, délib. nº 2009-201, 16 avr. 2009, J.C.P. S. 2009, act. 480. Voir également CNIL, déc. nº 2011-036, 16 déc. 2011, J.C.P. S. 2012, act. 95.
51. CNIL, délib. nº 2010-112, 22 avr. 2010, J.C.P. S. 2010, act. 281 ; Grégoire Loiseau, « Droits de la personnalité », *Légipresse* 2011.63, 67 et 68 ; Soc. 10 janv. 2012, préc., note 43, note Loiseau.
52. CNIL, délib. nº 2006-066, 16 mars 2006, J.O. 3 mai 2006, nº 62 ; Soc. 3 nov. 2011, préc., note 47, note Loiseau.

être soumis à un regard permanent[53]. Dès lors, l'exercice de la surveillance implique le respect d'un principe de proportionnalité. Celui-ci est au cœur de l'article L. 1121-1 du Code du travail : « Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché. » Or, toute surveillance apporte une restriction aux droits et aux libertés. Sont par exemple menacées la liberté d'expression lorsque le salarié est écouté ou filmé, la liberté d'aller et venir lorsque le salarié est géolocalisé. Plus généralement, les dispositifs de surveillance sont susceptibles de restreindre la vie privée des salariés. En effet, depuis l'affaire *Nikon* du 2 octobre 2001, il est acquis que la vie professionnelle n'est pas exclusive de toute vie privée. Selon la Cour de cassation, le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée[54]. Puisque tout dispositif spécifique de surveillance est susceptible d'apporter des restrictions aux droits et libertés des salariés, celles-ci doivent être justifiées par la nature de la tâche à accomplir et proportionnées au but recherché[55].

En premier lieu, la restriction apportée aux droits et libertés par le dispositif de surveillance doit être justifiée par la nature de la tâche à accomplir. Par hypothèse, on peut penser que cette condition sera toujours remplie puisque l'employeur tire de son pouvoir de direction le droit de surveiller l'activité des salariés[56].

En second lieu, la restriction aux droits et libertés doit être proportionnée au but recherché. Autrement dit, il faut vérifier que la mesure prise n'excède pas ce qui est strictement nécessaire pour atteindre l'objectif recherché. On doit notamment s'assurer que le même objectif ne peut pas être atteint avec un moyen moins attentatoire aux droits ou aux libertés du salarié[57]. Ainsi, dans l'arrêt du 3 novembre 2011 relatif à la géolocalisation envisagé précédemment, la Chambre sociale de la Cour de cassation a considéré qu'il n'était pas possible d'installer un dispositif de géolocalisation dans le véhicule d'un salarié disposant d'une liberté dans l'organisation

53. Soc. 10 janv. 2012, préc., note 43, note Loiseau ; Soc. 2 févr. 2011, J.C.P. S. 2011.1313, note Bossu.
54. Soc. 2 oct. 2001, *Bull. civ.* V, nº 291, J.C.P. E. 2001.1918, note Puigelier, J.C.P. G. 2002.I.102, note Bourrié-Quenillet ; Rodhain, *R.T.D. civ.* 2002.72, note Hauser, R.J.P.F. 2002.10, note Bossu, R.J.S. 2001.940, note Favennec-Héry.
55. C. trav., art. L. 1121-1 ; Philippe Waquet, « Vie privée, vie professionnelle et vie personnelle », *Dr. soc.* 2010.14, 16 ; B. Bossu, préc., note 13, 666.
56. A. Barège et B. Bossu, préc., note 22.
57. B. Bossu, préc., note 13, 666 ; Bernard Bossu, « Droits de l'Homme et pouvoirs du chef d'entreprise : vers un nouvel équilibre », *Dr. soc.* 1994.747, 752 ; A. Barège et B. Bossu, préc., note 22 ; P. Waquet, préc., note 55.

de ses déplacements. Selon la haute juridiction, « l'utilisation d'un système de géolocalisation pour assurer le contrôle de la durée du travail, laquelle n'est licite que lorsque ce contrôle ne peut pas être fait par un autre moyen, n'est pas justifiée lorsque le salarié dispose d'une liberté dans l'organisation de son travail[58] ». De la même façon, la vidéosurveillance n'est admissible que si elle représente le seul moyen possible, compte tenu de la nature du travail effectué, pour atteindre l'objectif recherché. La CNIL adopte la même analyse. À titre d'illustration, dans une délibération en date du 22 avril 2010, elle a considéré que la mise en place d'un dispositif de vidéosurveillance permettant un contrôle général et permanent des salariés porte atteinte aux droits et libertés des salariés et notamment à leur vie privée. Pour l'autorité administrative indépendante, une telle atteinte n'était pas proportionnée au but recherché, à savoir la sécurité du personnel[59].

Plus récemment, par une décision du 16 décembre 2011, la CNIL a mis en demeure une société de modifier le dispositif de vidéosurveillance que celle-ci utilisait pour se livrer à une surveillance permanente de salariés. Alors que la société avait déclaré installer le dispositif pour assurer la sécurité des salariés et lutter contre le vol, l'autorité administrative a constaté que le dispositif comportait une caméra par salarié, chacune étant équipée d'un microphone permettant une écoute sonore. Pour la CNIL, un tel système était manifestement excessif[60].

Reste néanmoins à préciser que, de façon exceptionnelle, la présence d'un système de surveillance fonctionnant en permanence peut être justifiée par des prescriptions réglementaires. Il en est ainsi, par exemple, dans un casino. Dès lors, il suffit que le personnel ait été « avisé de la présence de caméras de vidéosurveillance fonctionnant en permanence conformément aux prescriptions réglementaires en la matière[61] » pour que les enregistrements d'images constituent un moyen de preuve licite.

À ce stade du raisonnement, il apparaît que le pouvoir de contrôle et de surveillance de l'employeur doit respecter le principe de loyauté. Une seconde limite a également été affirmée par la Cour de cassation. Elle trouve sa source dans la vie privée au travail.

58. Soc. 3 nov. 2011, préc., note 47 ; Alain Chirez et Patricia Boughanmi-Papi, « Vidéosurveillance, droit à l'image et vie privée des salariés », *B.S. Francis Lefebvre* 1994.569, 572 ; Soc. 2 févr. 2011, préc., note 53, note Bossu.
59. CNIL, délib. nº 2010-112, préc., note 51 ; Voir également : CNIL, délib. nº 2009-201, préc., note 50.
60. CNIL, déc. nº 2011-036, préc., note 50.
61. Soc. 2 févr. 2011, préc., note 53, *Gaz. Pal.* 2011.113.35, note Walle.

2 Le respect de la vie privée

Le contrôle par l'employeur de l'activité de ses salariés ne doit pas se traduire par une remise en cause de leur vie privée. Or, avec la multiplication des techniques de surveillance, les risques d'atteinte à ce droit fondamental se sont multipliés. C'est pourquoi la Cour de cassation a affirmé avec force dans la célèbre affaire *Nikon* en date du 2 octobre 2001 que le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée. Mais ce principe du respect de la vie privée, y compris sur le lieu de travail, ne dispense pas le salarié de respecter ses obligations professionnelles. Le temps de travail doit être consacré à l'activité professionnelle et non à la découverte de « sites érotiques » sur Internet[62]. L'intérêt de l'entreprise commande d'apporter des limites au respect de la vie privée.

2.1 Le principe

La nécessité de protéger la vie privée du salarié s'est imposée progressivement en droit du travail. C'est d'abord l'existence d'une vie privée en dehors du temps et du lieu de travail qui sera proclamée. Ainsi, un prêtre-ouvrier est libre de ne pas révéler sa qualité d'ecclésiastique lors de son embauche[63]. À partir de 1997, la Cour de cassation va donner une nouvelle impulsion à sa jurisprudence en affirmant qu'un fait tiré de la vie personnelle ne peut révéler une faute du salarié, et un licenciement fondé sur ce fait n'est donc pas en principe possible[64].

Le développement des technologies de l'information et de la communication a permis à la Cour de cassation d'affirmer que la vie privée des travailleurs ne s'arrête pas aux portes de l'entreprise. Comme nous l'avons vu précédemment, elle a décidé dans l'affaire *Nikon* en date du 2 octobre 2001 que le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée[65]. Cette décision va être le point de départ d'une construction jurisprudentielle encore non achevée sur la « fouille » par l'employeur du contenu de l'ordinateur utilisé par son salarié. Quel bilan peut-on faire de la jurisprudence douze ans après l'affaire *Nikon* ? L'employeur peut-il lire un courriel rédigé par un salarié ? Est-il possible de prendre connaissance du contenu d'un fichier figurant

62. Soc. 2 oct. 2001, *Dr. soc.* 2001.920, note Ray, J.C.P. E. 2001.1918, note Puigelier, R.J.S. 2001.940, note Favennec-Héry.
63. Soc. 17 oct. 1973, J.C.P. G. 1974.II.17698, note Saint-Jours, *Dr. soc.* 1974.290, note Savatier.
64. Soc. 16 déc. 1997, *Bull. civ.* V, nº 441, J.C.P. G. 1998.II.10101, note Escande-Varniol.
65. Soc. 2 oct. 2001, préc., note 54 et 62.

sur le disque dur de l'ordinateur de l'entreprise ? Peut-on contrôler les sites Internet visités par les salariés ? Toutes ces interrogations soulèvent une même difficulté : que recouvre exactement la notion de vie privée ?

S'agissant des documents ou fichiers figurant sur le disque dur de l'ordinateur, la Cour de cassation pose en principe depuis le 18 octobre 2006 que « les dossiers et fichiers crées par un salarié grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumés, sauf si le salarié les identifie comme étant personnels, avoir un caractère professionnel de sorte que l'employeur peut y avoir accès hors sa présence[66] ». C'est donc le salarié qui détermine l'étendue de sa sphère d'intimité : dès lors qu'il n'a pas clairement identifié le document ou le fichier par la mention « Personnel », l'employeur peut y accéder librement. La solution, qui a le mérite de sauvegarder le pouvoir de direction du chef d'entreprise, s'explique par le fait que l'ordinateur doit être utilisé à des fins professionnelles[67]. Par ailleurs, l'absence d'un salarié pourrait paralyser le bon fonctionnement de l'entreprise si le contenu de l'ordinateur était purement et simplement analysé comme un espace de vie privée. On songe notamment à l'impossibilité d'accéder au dossier contenant les commandes des salariés[68].

Une difficulté peut survenir dans l'hypothèse où le fichier n'est pas clairement identifié par la mention « Personnel ». Dans ce cas, le titrage retenu ne doit laisser aucun doute sur le caractère personnel du dossier. La Cour de cassation a précisé que la mention des initiales du salarié[69] ou de son prénom ne confère pas au fichier un caractère personnel[70]. L'employeur peut également accéder librement à un fichier intitulé « Mes documents »[71]. Une autre solution était difficilement concevable, car la mention « Mes documents » est souvent générée automatiquement par les logiciels informatiques. Cette analyse est justifiée, car elle vise à éviter une instrumentalisation par le salarié de la jurisprudence de la Cour de cassation[72].

Que se passe-t-il dans l'hypothèse où le fichier est formellement identifié comme personnel ? Depuis un arrêt du 17 mai 2005, la Cour de cassation

66. Soc. 18 oct. 2006, J.C.P. S. 2006.1946, note Frouin.
67. A. Barège et B. Bossu, préc., note 22, nº 13.
68. *Id.*, nº 15.
69. Soc. 21 oct. 2009, J.C.P. S. 2010.1026, note Bossu.
70. Soc. 8 déc. 2009, R.J.S. 2010.144.
71. Soc. 10 mai 2012, nº 11-13884, J.C.P. S. 2012.1331, note Bossu.
72. De la même façon, renommer le disque dur lui-même « Personnel » ne peut suffire à conférer un caractère personnel à l'intégralité des données qu'il contient : voir Soc., 4 juill. 2012, nº 11-12502, J.C.P. S. 2012.1331, note B. Bossu.

décide que, « sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou de celui-ci dûment appelé[73] ». Cette exigence de la présence du salarié a été aussi affirmée par la Cour de cassation à l'occasion de l'ouverture de l'armoire individuelle du salarié[74]. La présence du salarié s'explique par l'atteinte qui est portée à sa vie privée mais aussi par le principe du contradictoire : il est contraire aux droits de la défense de fouiller l'ordinateur du salarié en son absence[75]. De façon plus générale, la Cour de cassation considère que, sauf circonstances exceptionnelles, l'employeur ne peut procéder à la fouille des effets personnels des salariés, « qu'avec leur accord et à la condition de les avoir avertis de leur droit de s'y opposer et d'exiger la présence d'un témoin[76] ». Ainsi, même si un salarié est soupçonné de vol, l'employeur ne peut ouvrir les sacs appartenant aux salariés en dehors des conditions précitées.

L'employeur peut-il également s'intéresser aux courriers électroniques de ses salariés ? Dès lors que ne figure pas la mention « Personnel » sur le courrier, l'employeur peut en prendre librement connaissance. Dans l'hypothèse où le courrier comporte une telle précision, la Cour de cassation a d'abord considéré que l'employeur ne pouvait prendre connaissance du message émis ou reçu même en présence du salarié. Cette solution, très rigoureuse pour l'entreprise, était fondée sur le secret des correspondances. Depuis 2009, la Cour de cassation a décidé d'unifier les règles gouvernant l'ouverture des courriels et des fichiers informatiques. Elle affirme désormais que, « sauf risque ou événement particulier, l'employeur ne peut ouvrir les messages identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé[77] ».

Dès lors que l'employeur a pris connaissance d'un courriel émis ou reçu par le salarié, peut-il se prévaloir de son contenu ? En principe, lorsque les messages échangés relèvent de la sphère privée, l'employeur ne peut les utiliser à l'encontre du salarié. Reste qu'en pratique il peut être difficile de savoir si les messages litigieux relèvent de la sphère privée ou professionnelle. Progressivement, en fonction des cas qui lui sont soumis, la Cour de cassation apporte des éléments de réponse. C'est d'abord la question des

73. Soc. 17 mai 2005, *Dr. soc.* 2005.789, note Ray, J.C.P. S. 2005.1031, note Favennec-Héry.
74. Soc. 11 déc. 2001, *Dr. soc.* 2002.352, note Savatier.
75. A. Barège et B. Bossu, préc., note 22, nº 21 ; Philippe Waquet, « Retour sur l'arrêt Nikon », *Semaine Sociale Lamy* 2002.1090.5.
76. Soc. 11 févr. 2009, J.C.P. S. 2009.1212, note Barège et Bossu.
77. Soc. 17 juin 2009, *Petites affiches* 2010.94.12, note Adam.

messages figurant dans la messagerie professionnelle du salarié qui a été tranchée par la Cour de cassation. Il apparaît que, même si l'employeur a connaissance du message, il ne peut s'en prévaloir que si le courrier est « en rapport avec l'activité professionnelle du salarié ». Pour établir un tel rapport, on s'appuie principalement sur le contenu du courrier. Ainsi, dans un arrêt du 2 février 2011, la Cour de cassation a considéré que le courrier envoyé via la messagerie professionnelle par un salarié à une collègue (également sa compagne) et qui comportait des propos irrespectueux à l'égard de son supérieur hiérarchique « était en rapport avec l'activité professionnelle du salarié[78] ». Au contraire, l'employeur ne peut se prévaloir de messages d'ordre privé échangés par le salarié avec une collègue de l'entreprise[79]. Il en va ainsi de courriers à caractère érotique entre deux salariés d'une même entreprise[80]. En pratique, le critère du « contenu du courrier » pour déterminer le caractère privé ou professionnel de la correspondance peut être source d'insécurité juridique. On sait bien que les propos tenus entretiennent souvent un lien, même ténu, avec la vie professionnelle. Qui plus est, beaucoup de correspondances contiennent souvent un mélange de propos relevant de la vie privée et d'autres de la vie professionnelle[81]. Dans ce dernier cas, même si la mise en œuvre risque de s'avérer délicate, la Cour de cassation semble admettre, dans un arrêt en date du 18 octobre 2011, que l'on puisse se prévaloir du courrier en retirant les passages d'ordre privé. En l'espèce, pour démontrer le caractère injustifié des demandes formulées par un salarié, l'employeur a produit divers courriels qui ont été écartés des débats. La Cour de cassation approuve cette mise à l'écart, car « la cour d'appel, qui a relevé qu'il était constant que le contenu des courriels produits était d'ordre privé s'agissant de la correspondance amoureuse du salarié, en a justement déduit que sa production intégrale en justice ne pouvait être justifiée par la nécessité pour l'employeur de démontrer la volonté de l'intéressé de démissionner ou la réalité de ses horaires de travail[82] ». La Cour de cassation semble donc rejeter uniquement la production intégrale en justice du contenu des courriers. L'arrêt n'exclut finalement pas que l'employeur puisse remettre au juge des courriers expurgés des passages d'ordre privé.

Au-delà des courriers figurant sur la messagerie professionnelle, la Cour de cassation a été également amenée à se prononcer le 26 janvier 2012

78. Soc. 2 févr. 2011, J.C.P. S. 2011.1274, note Martinon.
79. Soc. 5 juill. 2011, J.C.P. S. 2011.1501, note Bossu.
80. *Id.*
81. Jean-Emmanuel Ray, « Actualités des technologies de l'information et de la communication », *Dr. soc.* 2011.933.
82. Soc. 18 oct. 2011, J.C.P. S. 2012.1041, note Bossu.

sur l'utilisation par l'employeur d'un courrier figurant dans la messagerie personnelle. En l'espèce, depuis sa messagerie personnelle, en dehors du temps et du lieu de travail, un cadre avait envoyé sur la messagerie personnelle d'un collègue un courriel dans lequel il dénigrait sa supérieure hiérarchique. Le destinataire a alors transféré le message à un autre collègue et ce dernier l'a porté à la connaissance de la direction des ressources humaines de l'entreprise. Pour la Cour de cassation, « l'envoi du courriel litigieux par le salarié, de sa messagerie personnelle et en dehors du temps et du lieu de travail, à l'adresse électronique personnelle d'un collègue de travail, ce qui conférait à ce message un caractère purement privé, ne constituait pas un manquement à son obligation de loyauté envers son employeur[83] ». Une difficulté demeure encore aujourd'hui : l'employeur peut-il se prévaloir du contenu d'un courriel envoyé depuis sa messagerie personnelle mais au temps et au lieu du travail ?

Parmi les contentieux les plus fréquents, il convient d'apporter quelques précisions sur le contrôle par l'employeur des sites Internet visités par ses salariés. Pour la Cour de cassation, « les connexions établies par un salarié sur des sites Internet pendant son temps de travail grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumées avoir un caractère professionnel, de sorte que l'employeur peut les rechercher aux fins de les identifier, hors de sa présence[84] ». Pour comprendre le raisonnement suivi par la Cour de cassation, il convient de noter que le salarié ne peut se prévaloir du secret des correspondances, car la consultation ne suppose ni expéditeur ni destinataire. Dans un arrêt du 9 février 2010, un salarié avait tenté de placer le débat sur le terrain de la protection accordée par la jurisprudence au fichier personnel[85]. Le salarié prétendait que cette protection devait être étendue aux sites inscrits sur la liste des « favoris » de l'ordinateur. L'argumentation est rejetée par la Cour de cassation au motif qu'une telle inscription ne permet pas d'affirmer que la consultation a été identifiée par le salarié comme personnelle. La solution est commandée par le bon sens : la liste des sites « favoris » a simplement pour objectif de rendre plus rapide l'accès à des fichiers d'utilisation fréquente ; on ne peut pas en déduire que la consultation est faite à titre personnel.

Un contentieux commence également à émerger quant aux propos tenus par des salariés sur les réseaux sociaux. Comme l'a affirmé il y a quelques années un certain Barack Obama : « Attention à ce que vous allez

83. Soc. 26 janv. 2012, nº 11-10189, inédit.
84. Soc. 9 févr. 2010, J.C.P. S. 2010.1243, note Bossu.
85. *Id.*

poster sur Facebook ! Tout cela pourra se retourner contre vous tôt ou tard[86]. » La prévision s'est révélée exacte : le recruteur n'hésite pas à utiliser les réseaux sociaux pour obtenir des informations sur le candidat à un emploi[87] et les licenciements pour avoir critiqué l'entreprise sur Facebook se multiplient. Ces situations soulèvent une interrogation majeure : est-ce que les propos tenus sur Facebook relèvent de la vie privée et plus particulièrement du secret des correspondances[88] ? En l'absence d'arrêt de la Cour de cassation, il est difficile d'apporter une réponse certaine à cette question. Toutefois, les premières décisions des juges du fond montrent que, en fonction des paramétrages effectués par son utilisateur, un réseau social peut constituer soit un espace privé, soit un espace public. Pour comprendre le raisonnement, il convient de rappeler que, sur Facebook, chaque titulaire d'un compte dispose d'une page généralement qualifiée de mur ou de profil, c'est-à-dire une page personnelle sur laquelle il peut publier des photos ou des commentaires. Lors de l'ouverture du compte, son titulaire doit régler des paramètres de confidentialité. S'il décide de laisser son mur ouvert, c'est forcément un espace public puisque tout le monde peut y accéder librement. C'est également public s'il suffit d'être inscrit sur Facebook pour avoir accès au mur : une conversation avec des milliers de personnes ôte aux échanges leur caractère de correspondance privée[89]. Le titulaire du compte Facebook peut aussi autoriser ses seuls amis à avoir accès aux informations publiées. Dans une telle hypothèse, on pourrait parler d'une conversation d'ordre privé, encore qu'il soit difficile de savoir si le destinataire des propos a limité l'accès à son propre mur[90]. Enfin, le titulaire du compte peut laisser ouvert son profil aux « amis de ses amis ». Dans une telle situation, il est difficile de retenir la notion de vie privée, car on ne connaît jamais tous les amis de ses amis et ils peuvent

86. « Barak Obama conseille aux jeunes de faire attention à Facebook », 20 décembre 2011, [En ligne], [cyrilleemery.wordpress.com/2011/12/20/barak-obama-conseille-aux-jeunes-de-faire-attention-a-facebook/] (14 juin 2013 ; la traduction est de nous).
87. Yan Gauchard, « Un internaute piégé par ses traces sur la Toile », *Le Monde*, 18 janvier 2009. Dans cet article, l'ancien président de la CNIL, Alex Turk, rapporte que, « [l]ors d'un entretien d'embauche, un jeune homme s'est vu présenter une photo de ses fesses ». Quelques mois plus tôt, dans une soirée arrosée, avec des copains de la faculté de droit, il avait montré ses fesses. Un de ses copains a pris la photo et l'a balancée sur le réseau social. C'était amusant. La suite de l'histoire est beaucoup moins drôle : le candidat n'a pas eu l'emploi.
88. Jean-Emmanuel Ray, « Facebook, le salarié et l'employeur », *Dr. soc.* 2011.128 ; Jean-Emmanuel Ray, « Facebook m'a licencié », *Semaine Sociale Lamy* 2010.1470.103 ; Pierre-Yves Verkindt, « Les "amis" de nos "amis"… », J.C.P. S. 2010, act. 550.
89. *Id.*
90. Besançon, 15 nov. 2011, *Comm. com. électr.* 2012.4.44, note Caprioli ; Reims, 9 juin 2010, *Juris-Data n° 013284.*

être fort nombreux[91]. Le conseil de prud'hommes de Boulogne-Billancourt a ainsi admis le licenciement pour faute grave de salariés suite à des propos tenus sur Facebook[92] qui mettaient en cause la supérieure hiérarchique. Les juges du fond ont relevé que le mur était accessible aux amis des amis et qu'en conséquence les propos tenus ne relevaient pas de la vie privée.

La nécessité de sauvegarder la vie privée du salarié ne doit pas déboucher sur une remise en cause du bon fonctionnement de l'entreprise. En conséquence, la protection de la vie privée connaît forcément des limites.

2.2 Les limites

On l'aura compris, par principe, lorsque les messages ou les fichiers informatiques d'un salarié relève de la sphère privée, l'employeur ne peut les utiliser à l'encontre du salarié. Plus généralement, la Cour de cassation a consacré une immunité disciplinaire pour les faits relevant de la vie personnelle du salarié[93]. Ainsi, lorsqu'un fait commis par un salarié relève de sa vie personnelle ou de sa vie privée, il ne peut lui être imputé à faute. La solution s'explique aisément : si un fait relève de la vie personnelle du salarié, il échappe au champ contractuel et, à ce titre, ne peut justifier une sanction disciplinaire. Le propos doit néanmoins être nuancé. L'immunité disciplinaire connaît en effet certaines limites qui sont commandées par l'indispensable conciliation des intérêts de l'entreprise avec les droits et libertés de la personne. La solution est désormais bien établie : « un motif tiré de la vie personnelle du salarié ne peut, en principe, justifier un licenciement disciplinaire, sauf s'il constitue un manquement de l'intéressé à une obligation découlant de son contrat de travail[94] ».

En premier lieu, l'obligation de loyauté constitue une limite à la liberté du salarié d'agir comme il l'entend dans sa vie personnelle. Des actes de déloyauté à l'égard de l'employeur peuvent être constitutifs d'une faute et justifier un licenciement disciplinaire même s'ils ont été commis dans le cadre de la vie personnelle[95]. Ainsi, le salarié qui utiliserait en dehors du temps et du lieu de travail le fichier « Clients » de l'entreprise pour se livrer à des actes de démarchage à l'occasion de la création d'une société

91. Rouen, 15 nov. 2011, nº 11/01827.
92. Cons. prud. Boulogne-Billancourt, 19 nov. 2010, R.J.S. 2011.5.
93. Soc. 16 déc. 1997, préc., note 64.
94. Soc. 3 mai 2011, *Bull. civ.* V, nº 105, *Juris-Data nº 007705*, J.C.P. S. 2011.1312, note Corrignan-Carsin, J.C.P. G. 2011.764, note Mouly, D. 2011.1357, D. 2011.1568, note Loiseau.
95. Soc. 15 avr. 1996, R.J.S. 1996.792 ; Soc. 6 févr. 2001, *Dr. soc.* 2001.439, obs. Gauriau ; Soc. 18 mars 2003, *Dr. soc.* 2003.770, obs. Savatier ; Soc. 25 févr. 2003, *Bull. civ.* V, nº 66, *Juris-Data nº 017934*, *Dr. soc.* 2003.625, obs. Savatier.

concurrente adopterait assurément un comportement déloyal qui justifierait son licenciement.

En second lieu, la théorie de l'abus de droit permet de sanctionner l'utilisation contestable par un salarié de ses droits fondamentaux. La vie personnelle ne saurait justifier toutes les dérives. Toute la difficulté est en réalité de savoir où commence l'abus. Pour en cerner les frontières, on peut notamment s'intéresser à l'utilisation de l'outil informatique professionnel à des fins personnelles. Si une telle pratique doit probablement être tolérée, encore faut-il qu'elle reste raisonnable. La CNIL estime d'ailleurs que « l'utilisation de la messagerie électronique […] pour envoyer ou recevoir, dans des proportions raisonnables, un message à caractère personnel correspond à un usage généralement et socialement admis[96] ». De la même façon, la Cour de cassation considère que « la seule conservation sur son poste informatique de trois fichiers contenant des photos à caractère pornographique sans caractère délictueux ne constitue pas, en l'absence de constatation d'un usage abusif affectant son travail, un manquement du salarié aux obligations résultant de son contrat susceptible de justifier son licenciement[97] ». Reste qu'en cas d'abus manifeste une sanction disciplinaire est néanmoins envisageable. À titre d'illustration, dans un arrêt du 2 mai 2004, la Chambre sociale de la Cour de cassation a relevé que « le fait pour un salarié d'utiliser la messagerie électronique que l'employeur met à sa disposition pour émettre, dans des conditions permettant d'identifier l'employeur, un courrier contenant des propos antisémites est nécessairement constitutif d'une faute grave[98] ». De la même façon, le fait pour un salarié de négliger ses fonctions en passant le plus clair de son temps de travail à se connecter à des sites à caractère pornographique et zoophile et d'avoir mis en ligne le numéro de son téléphone mobile professionnel sur de tels sites faisant ainsi courir un risque tangible à l'image de l'entreprise constituent une faute grave[99]. La même solution s'est imposée en présence d'un salarié qui avait utilisé le matériel de l'entreprise pour imprimer des photos pédo-pornographiques, celles-ci ayant été découvertes dans son logement de fonction, alors même que ses fonctions le conduisaient à être en contact permanent avec des mineurs[100]. Dans un arrêt du 18 mars 2009, la haute juridiction a encore considéré qu'un salarié pouvait être licencié

96. Commission nationale de l'informatique et des libertés, *La cybersurveillance sur les lieux de travail*, Paris, La Documentation française, 2004, p. 25.
97. Soc. 8 déc. 2009, R.D.T. 2010.235, note Leroy, R.J.S. 2010, nº 236. Voir également Soc. 10 mai 2012, nº 11-11060, inédit.
98. Soc. 2 juin 2004, *Bull. civ.* V, nº 152, *Dr. et pat.* 2005.139.109, obs. Caprioli.
99. Soc. 23 nov. 2011, nº 10-30833, inédit.
100. Soc. 8 nov. 2011, nº 10-23593, inédit.

pour faute, car il avait usé de la connexion Internet de l'entreprise à des fins non professionnelles pour une durée d'environ 41 heures sur un mois[101]. Une solution identique a également été retenue dans un arrêt du 10 mai 2012 à propos d'un salarié qui avait, pendant plus de six mois, utilisé de manière répétée pendant les heures de service les ordinateurs que son employeur avait mis à sa disposition pour l'exécution de sa prestation de travail en se connectant pendant les heures de service, au vu et au su du personnel, à des sites pornographiques sur Internet[102].

En définitive, pour caractériser l'abus, il apparaît que les juges font preuve d'un grand pragmatisme. Une appréciation souveraine de la situation factuelle leur permet de déterminer si l'abus est caractérisé ou si tel n'est pas le cas. Sont susceptibles d'être pris en compte les agissements du salarié, ses fonctions, ses responsabilités, le contenu des messages, le temps de connexion, l'activité de l'entreprise Sans transformer l'entreprise en un lieu d'interdiction, les juges permettent ainsi à l'employeur d'écarter ceux qui la mettent réellement en péril.

Par ailleurs, même si le fait commis par le salarié relève de sa vie personnelle, il peut constituer une cause non fautive de licenciement. Le principe a été posé par l'arrêt *Léger* en date du 20 novembre 1991 : « si, en principe, il ne peut être procédé au licenciement d'un salarié pour une cause tirée de sa vie privée, il en est autrement lorsque le comportement de l'intéressé, compte tenu de ses fonctions et de la finalité propre de l'entreprise, a créé un trouble caractérisé au sein de cette dernière[103] ». Ainsi, alors qu'un fait tiré de la vie personnelle ne peut en principe justifier le licenciement d'un salarié, celui-ci redevient possible si le fait cause un trouble objectif à l'intérêt de l'entreprise. Mais le licenciement ne peut aucunement relever du domaine disciplinaire[104].

La notion de trouble objectif est d'origine prétorienne. Elle implique, en premier lieu, que le trouble ne soit pas subjectif ; ce n'est pas le sentiment personnel de l'employeur qui est pris en considération, mais il faut des éléments précis et vérifiables. En second lieu, le trouble doit être suffisamment caractérisé au regard de la finalité de l'entreprise et des fonctions

101. Soc. 18 mars 2009, *Juris-Data nº 048024*, *Expertises* 2009.230, note Lecardonnel.
102. Soc. 10 mai 2012, nº 10-28585, inédit ; Voir également : Soc. 4 juill. 2012, nº 11-12502, inédit ; Soc. 21 sept. 2011, nº 10-14869, inédit ; Soc. 9 févr. 2010, nº 08-44632, inédit ; Soc. 16 mai 2007, nº 05-43455, inédit.
103. Soc. 20 nov. 1991, *Bull. civ.* V, nº 512, *Juris-Data nº 003219*.
104. Ch. mixte, 18 mai 2007, *Bull. civ*., nº 5, *Juris-Data nº 038898*, J.C.P. S. 2007.1538, note Barège et Bossu, D. 2007.2137, note Mouly ; Soc. 9 mars 2011, *Bull. civ*. V, nº 69, *Juris-Data nº 003089*, J.C.P. S. 2011.1230, note Mouly.

occupées dans l'entreprise par le salarié[105]. À titre d'illustration, la Cour de cassation a retenu l'existence d'un « trouble caractérisé et certain » justifiant le licenciement d'un salarié dans un contexte où la publicité donnée à la condamnation pénale de ce dernier avait désorganisé le service dans lequel il travaillait, l'employeur ayant en outre été contraint d'intervenir à de multiples reprises auprès du personnel pour prévenir la propagation de rumeurs sur le sujet. De surcroît, certains salariés du service en cause, amenés à côtoyer la mère de la victime, elle-même salariée de l'entreprise et travaillant sur le site, avaient exprimé une forte émotion et une cellule psychologique avait dû être mise en place[106]. De la même façon, justifient le licenciement en raison du trouble causé à la bonne marche de l'entreprise les agissements d'un salarié, lequel avait été mis en garde à vue puis condamné en raison de violences commises à l'encontre de son amie dans un appartement que lui louait son employeur, ce dernier ayant dû reloger en urgence la famille de la victime, également locataire de l'employeur[107].

Avec le développement de l'outil Internet au travail, les litiges liés à la pornographie se sont multipliés. Dès lors, un employeur pourrait-il invoquer un trouble objectif si un membre du personnel d'encadrement visualisait sur son propre ordinateur ou sur sa tablette personnelle un film pornographique durant une pause ? De façon certaine, le salarié étant en pause et la pornographie n'ayant rien d'illicite, aucune faute ne semble pouvoir être opposée au salarié dans une telle hypothèse. La simple visualisation d'un « film pour adulte » au travail est-elle alors suffisante pour caractériser un trouble objectif ? À une époque où les plus hauts dirigeants de ce monde ne cachent plus être adeptes du libertinage, où les kiosques affichent des revues érotiques et où des films, même passés à la télévision, comportent des images sexuelles, on peut en douter[108]. Mais si la visualisation de la vidéo conduit certaines salariées placées sous la responsabilité de ce membre du personnel d'encadrement à ne plus vouloir travailler avec lui, ou que l'une d'elles est victime d'un trouble psychologique, l'employeur pourrait potentiellement invoquer les agissements du salarié pour le licencier en raison du trouble objectif apporté aux intérêts de l'entreprise.

105. Philippe Waquet, « Le "trouble objectif dans l'entreprise" : une notion à redéfinir », R.D.T. 2006.304 et suiv. Voir également : Philippe Waquet, « Trouble objectif : le retour à la case "départ" », *Semaine Sociale Lamy* 2007.1310.5 ; Soc. 6 juin 2007, *Juris-Data n° 039445*, J.C.P. S. 2007.1716 ; Ch. mixte, 18 mai 2007, préc., note 104.
106. Soc. 26 sept. 2012, n° 11-11247, inédit.
107. Soc. 14 sept. 2010, n° 09-65675, inédit.
108. P. Waquet, « Trouble objectif : le retour à la case "départ" », préc., note 105 ; J.-E. Ray, préc., note 81.

Conclusion

À l'issue de cette étude, il apparaît que les technologies de l'information et de la communication ont profondément renouvelé la problématique de la vie privée du travailleur. Ce dernier n'hésite plus à faire pénétrer celle-ci au sein de l'entreprise en réclamant des espaces de vie personnelle. L'entreprise n'est pas en reste : il est aujourd'hui banal de correspondre avec le salarié en dehors du temps et du lieu de travail. La distinction entre vie privée et vie professionnelle est-elle encore d'actualité ?