



Par Geneviève Folzer et Mathieu Abboud,
avocats au barreau de Luxembourg, inscrits au
barreau de Strasbourg

Cybersurveillance des salariés et règles de preuve devant les Prud'hommes

Bon sens et bonne foi sont les repères les plus fiables lorsque les employeurs comme les employés s'observent sur la périlleuse question de leur connaissance réciproque. Notons que si dans le présent article il sera principalement question du contrôle des salariés, ces derniers ne sont pas en reste et s'interrogent bien souvent sur l'emploi du temps et les activités de leur employeur. N'ont-ils pas, à ce propos, une certaine légitimité ? La réciprocité n'a-t-elle aucune place ?

Le contexte actuel

L'employeur, propriétaire des moyens de production et de communication, cherche à établir avec son employé une relation de confiance. Cette relation de confiance requiert, comme de toute autre relation contractuelle, que les obligations réciproques des parties soient remplies de bonne foi et sans malice. Ainsi, l'employeur peut attendre de son employé qu'il se comporte loyalement.

Dans ce contexte, l'employeur peut-être tenté de lever le voile qui subsiste entre lui et son employé dans son activité quotidienne. Ce voile tissé de la distance entre le bureau du « PDG » et le poste de travail du salarié était auparavant opaque. Les nouvelles technologies permettent de le lever chaque jour un peu plus. Il y eut tout d'abord le contremaître puis, la carte d'accès, le téléphone et les autocommutateurs, les factures détaillées. Aujourd'hui, s'ajoutent Internet, la messagerie électronique, la biométrie, la cryptographie, la signature électronique, la certification et peut-être un jour le contrôle individuel par puce intradermique ceci, sans parler des potentialités du génie génétique.

Cet inventaire à la Prévert n'est ni catastrophiste, ni irréaliste mais relate l'accroissement des moyens de communication et ceux, corrélatifs, de surveillance. Même si les risques d'atteintes disproportionnées aux libertés individuelles existent, l'activité de traitement de données à caractère personnel des salariés par l'employeur est encadrée.

L'encadrement de la mise en œuvre et de l'exploitation d'un traitement de données à caractère personnel des salariés par l'employeur

Avant toute action, l'employeur doit remplir certaines exigences qui sont autant de pré requis et de conditions indispensables.

► Les pré requis dans la gestion de l'entreprise

> le besoin de l'entreprise est source de légitimité

Dans sa gestion courante, l'employeur doit définir ses besoins. Dans le jargon de la protection des données, seul ce qui est nécessaire au responsable du traitement et conforme à son intérêt légitime est légal.

Selon l'article 7 f) de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, l'employeur, en tant que responsable de traitement, ne peut agir que si cela est « *nécessaire à la réalisation de l'intérêt légitime poursuivi (...), à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée (le salarié)* ».

Pour respecter ces prescriptions, l'employeur doit, tout d'abord, définir quelles sont les fonctions existantes dans l'entreprise exigeant, pour leur accomplissement, la collecte et le traitement de données à caractère personnel de ses salariés. Pour exemple, la fonction paye dans l'entreprise exigera que soient traitées un certain nombre de ces données (identité, état civil, heures prestées ...). Il devra encore lister les lieux où sont traitées des données, à caractère personnel, de manière inhérente (p.ex fichiers log) à son système informatique, sans qu'il en soit besoin autrement que pour le fonctionnement dudit système, ceci afin de prendre en charge le contrôle de l'accès et de garantir la confidentialité.

Ainsi, pour chaque fonction importante, l'employeur aura un intérêt légitime à traiter des données concernant ses employés. En particulier, la protection des biens de l'entreprise mais également, la protection des secrets industriels sont des fonctions se rattachant aisément à l'intérêt légitime de l'employeur. Toutefois, face à l'intérêt légitime de l'employeur se dresse celui, non moins légitime, du droit des salariés au respect de leurs libertés fondamentales.

Il s'agit là, d'une balance d'intérêts qui penchera, selon les circonstances, tantôt d'un côté tantôt de l'autre. Vouloir décrire, a priori, l'ensemble des situations qui se présenteront sur le terrain est vain. Toutefois, il est possible d'ouvrir des pistes de réflexion au management des entreprises .

> La proportionnalité de la mesure de surveillance est le corollaire du besoin

L'article L120-2 du code du travail dispose que : *« 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. »*

Afin de respecter cette disposition, l'employeur doit se poser la question suivante : Ai-je besoin de données (image, son, données informatisées...) à caractère personnel, c'est-à-dire, permettant l'identification directe ou indirecte de l'un ou l'autre de mes salariés. Au contraire, des données anonymes ou rendues anonymes, ne sont-elles pas suffisantes ?

Cette question taraude bien des employeurs à l'heure de la navigation sur Internet et des possibilités de collecte de données de connexion. On peut apporter un début de réponse à cette question en proposant une analogie avec la route, lieu où les camions remplacent les paquets d'informations.

Les systèmes de vidéosurveillance mis en place, sur autoroute, afin de gérer les flux de circulation n'ont pas besoin de permettre la lecture des plaques d'immatriculation. Il suffit qu'ils permettent de visualiser un accident exigeant une intervention ou encore qu'ils permettent de mesurer un débit horaire des véhicules. Ici, aucun traitement de données à caractère personnel n'est nécessaire car le traitement de données anonymes suffit à réaliser pleinement la finalité du système. N'en est-il pas, dans une certaine mesure, de même de la gestion des flux informatisés dans un réseau interne ou externe ? Sinon, quels sont les besoins réels en données à caractère personnel ? Il semble, à ce propos, que le contrôle anonyme des flux de connexion, la limitation d'accès de certains sites, l'information des salariés sur un usage extra-professionnel modéré et encadré peut, le plus souvent, suffire pour garantir de saines pratiques de navigation dans l'entreprise.

Le choix de telles mesures présente plusieurs avantages pour le management d'une entreprise. Tout d'abord, cela évite des discussions complexes en son sein. Ensuite, l'entreprise se préserve d'un travail long et fastidieux de définition et de mise en œuvre d'une chaîne de responsabilité et de confidentialité qui, si elle se brise au mauvais moment, peut entraîner des conséquences lourdes sur le plan social. Enfin, elle évite la génération d'un coût administratif et financier (déclaration CNIL, conseils technologiques et juridiques).

> Le principe de proportionnalité dans la loi : une soumission de l'ensemble des écrits dans l'entreprise

Selon l'article L 122-35 du code du travail, le règlement intérieur ne peut apporter aux droits et libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nécessité de la tâche à accomplir, ni proportionnées au but recherché. L'atteinte à la vie privée devra, par ailleurs rester, lorsqu'elle est nécessaire, la plus limitée et la plus courte possible. La combinaison des articles 122-35 du code du travail et 122-39 du même code étend le principe de proportionnalité aux « *notes de service ou tout autre document qui portent prescriptions générales et permanentes (...)* ».

Mais ne peut-on pas, quelle que soit la situation, traiter des données concernant des salariés dès lors que ceux-ci y auraient préalablement consenti en offrant un blanc-seing lors de la conclusion du contrat de travail ? Ne se conforme-t-on pas ainsi à l'article 7 a) de la directive 95/46/CE (op. cit.) ? L'article 2 de la directive 95/46/CE nous offre un élément de réponse en définissant le consentement de la façon suivante : « *toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement.* ».

Vu le rapport de force existant lors de la signature du contrat de travail, on peut s'interroger sur l'existence même d'un consentement libre, tel que défini dans la directive. Tout au moins, la condition relative à la qualité de l'information du salarié et exigée par la directive 95/46/CE, ne semble pas réunie par la signature d'une clause au contrat de travail qui couvrirait tout traitement futur de données du salarié.

Ici encore, tout est une question de mesure et de pratiques professionnelles raisonnables. On peut, en tout cas, retenir que « l'abdication » du salarié de façon définitive et permanente à travers son contrat de travail n'est pas une couverture satisfaisante pour l'employeur.

► **Les conditions formelles dans la mise en place du traitement de données des salariés dans l'entreprise**

Sans prétendre avoir abordé toutes les questions de fonds (celles relatives au respect du principe de finalité mériteraient de plus amples développements), viennent s'ajouter celles plus prosaïquement procédurales. La gestion de ces contraintes se superpose dans le temps à celles vues ci-avant. La prise en compte des salariés se traduit dans la Loi par une obligation d'information et de déclaration.

> **L'obligation d'informer le salarié**

L'article L 121-8 du code du travail a le mérite d'être clair en disposant que :

« *Aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à un emploi.* »

Notons que la lettre de cet article est parfaitement conforme avec la directive 95/46/CE. Le champ d'application de cette dernière englobe toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés. Celui de la loi 78-17 informatique et libertés se limite aux traitements automatisés d'informations nominatives et cette petite divergence mériterait, dans la législation en cours d'adoption, d'être clarifiée.

> **L'obligation d'informer, de consulter le comité d'entreprise et le délégué du personnel**

L'obligation d'informer et de consulter le comité d'entreprise est un préalable à la mise en place de nouvelles technologies au sein de l'entreprise pouvant avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail du personnel (article L 432-2 du code du travail). Toute technologie introduite afin de traiter des données à caractère personnel des salariés semble susceptible d'avoir de telles conséquences, en particulier sur les conditions de travail.

L'article 432-2 poursuit : « *Lorsque l'employeur envisage de mettre en oeuvre des mutations technologiques importantes et rapides, il doit établir un plan d'adaptation. Ce plan est transmis, pour information et consultation, au comité d'entreprise en même temps que les autres éléments d'information relatifs à l'introduction de nouvelles technologies. En outre, le comité d'entreprise est régulièrement informé et périodiquement consulté sur la mise en oeuvre de ce plan.* »

Par ailleurs et indépendamment de l'emploi d'une nouvelle technologie, le comité d'entreprise devra être informé (article L 432-2-1 code du travail) « *préalablement à leur utilisation, sur les méthodes ou techniques d'aide au recrutement des candidats à un emploi ainsi que sur toute modification de ceux-ci. Il est aussi informé, préalablement à leur introduction dans l'entreprise, sur les traitements automatisés de gestion du personnel et sur toute modification de ceux-ci. Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en oeuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés.* ». Notons qu'en cas de carence de comité d'entreprise et par application de l'article 431-3 du code du travail, le délégué du personnel y sera substitué.

> **L'obligation de notifier à la CNIL**

L'article 16 de la loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés impose de façon générale une obligation de notification préalable à la mise en oeuvre de tout traitement automatisé à la CNIL, précisant toutefois que la mise en oeuvre peut avoir lieu dès réception du récépissé de notification. Les informations à fournir sont précisées à l'article 19 de la loi 78-17. Le cas échéant, la notification pourra prendre la forme d'une déclaration simplifiée de conformité conformément à l'article 17 de la loi 78-17.

► **L'utilisation des données traitées devant les tribunaux : permanence des principes**

Ce qui est vrai au moment de la collecte et du traitement des données le reste devant les tribunaux. Bonne foi et loyauté sont les principes qui devraient guider le Conseil de Prud'hommes dans l'admission de la preuve. Nous aborderons brièvement, sans prétention à l'exhaustivité, quelques jurisprudences marquantes qui viennent à l'appui de ces dires quelque soit le mode de surveillance (vidéosurveillance, e-mail ...). Pour de plus amples précisions et un survol plus large on recommandera, entre autres, la visite du site de la CNIL mais également de celui du forum des droits de l'Internet qui comprennent, l'un un dossier fort enrichissant et l'autre, un répertoire de jurisprudence.

> **loyauté des relations contractuelles, loyauté de la preuve**

Comme vu précédemment, on ne surveille pas son salarié sans l'en informer. En effet, surveiller revient à récolter des données relatives au salarié concerné. Par un arrêt important du 20 novembre 1991, la Chambre sociale de la Cour de Cassation a rappelé cette règle et a écarté une preuve par vidéosurveillance rapportée à l'insu du salarié. La Cour considère, en l'absence d'information de la salariée, que le mode de preuve était illicite. Dans cette espèce, une caméra avait été dissimulée ...et l'arrêt ayant considéré le licenciement régulier fut cassé. Dans le même esprit, la bonne foi dans les relations contractuelles empêche d'utiliser un système de réservation pour contrôler et blâmer des employés (Cour de Paris, 31 mai 1995 s'agissant du système SOCRATES de la SNCF).

Notons qu'à travers la jurisprudence et au-delà du problème de la loyauté de la preuve se pose souvent la question de sa qualité. La preuve informatique est-elle fiable ? Certainement non si les disques durs versés par les parties n'ont pas été mis sous scellés. Certainement non si les documents (image, films) sont équivoques. S'ajoute à cette question celle de l'existence ou non d'une notification régulière à la CNIL.

Certains pourraient, se pensant plus malins que d'autres, pérorer devant leur employeur. Bien mal leur en prendrait ! En effet, si la loyauté est exigée de l'employeur, elle l'est aussi de l'employé qui ne peut lui

reprocher de l'avoir surpris la main dans le sac ...dans un hangar vidéosurveillé dans lequel il n'avait rien à faire (Cassation Sociale, 31 janvier 2001).

Encore pour exemple, le Conseil de Prud'hommes de Montbéliard , dans un jugement du 19 septembre 2000, a considéré régulier le licenciement d'une salariée qui avait envoyé pendant ses heures de bureau des mails personnels contenant des informations sur l'entreprise. Mais était-ce encore, vu leur contenu des mails personnels ? Comme nous le verrons plus bas rien n'est moins sûr. En toute hypothèse, versant elle-même à la barre les e-mails litigieux, la salariée n'a certainement pas été très habile dans cette affaire !

> **Le e-mail : correspondance protégée par le secret des correspondances et le droit à la vie privée**

La chambre sociale, dans son arrêt du 2 octobre 2001, Société Nikon France c/ Monsieur O., a confirmé ce qui semblait déjà acquis, à savoir la protection du e-mail professionnel par le secret des correspondances et le droit à la vie privée .

Ainsi, la Cour de Cassation, s'appuyant sur l'article 8 de la convention européenne des droits de l'homme, l'article 9 du code civil et l'article 120-1 du code du travail et par un Attendu désormais célèbre explique : *« que le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur »* .

Cette décision est conforme à la directive 2002/58/CE , au principe de neutralité technologique auquel elle est attachée et à son article 5 intitulé « Confidentialité des communications » qui dispose de la façon suivante : *« (...) En particulier, ils (les Etats membres) interdisent à toute autre personne que les utilisateurs (salariés) d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs concernés (...) »*.

Toutefois, l'employeur peut se demander si cette décision est source de loyauté. N'a-t-il décidément pas le droit de contrôler les activités de ses salariés ? Une chose est certaine, un règlement intérieur, un contrat, une charte d'utilisateur interdisant formellement l'utilisation des moyens informatiques et en particulier du e-mail professionnel à des fins privées semble vouée à l'inefficacité. En effet, à quoi sert-il d'interdire sans pouvoir contrôler l'ensemble des correspondances échangées? L'utilisation à des fins personnelles doit être tolérée, comme l'est celle du téléphone, sans perturbation, ni du service, ni des réseaux. Mais comment distinguer ce qui est personnel de ce qui est professionnel ? Quelles solutions apporter à ce qui ressemble à une impasse ?

Il y a donc des e-mails personnels et d'autres professionnels. Tous sont soumis au secret des correspondances. Pour les distinguer, l'employeur peut demander que chaque e-mail personnel se signale comme tel dans son intitulé. Il peut également demander au salarié de créer un « folder » dédié aux correspondances personnelles. Ces solutions devraient offrir à l'employeur qui consulte des correspondances dites « professionnelles » la protection de l'excuse de bonne foi de l'article 226-15 du code pénal (notons que les autorités publiques conformément aux articles 226-13 et 432-9 du code pénal n'en bénéficient pas).

Une solution plus restrictive de la liberté de l'employeur mais garantissant un risque encore moindre consiste à demander que soit expédiée une copie de chaque correspondance professionnelle à un autre membre de la société qui sera dédié à cette fonction. A ce propos, le choix de l'administrateur réseau, comme destinataire, n'est peut-être pas le meilleur. En effet, si un administrateur réseau doit avoir accès à l'ensemble des terminaux, s'il doit pouvoir prendre possession de terminaux pour garantir le fonctionnement et la sécurité du réseau, sa tâche ne lui permet pas en principe de prendre connaissance de données de contenu (sites visités, contenu des mails...). Dès lors, mieux vaut lui éviter d'être

réciplendaire de copies de e-mail pour éviter toute confusion des genres. Cette dernière remarque appelle les entreprises à réfléchir à la création de la fonction de chargé de la protection des données.

En conclusion, les principes de nécessité et de proportionnalité dictent à l'employeur qu'il lui est interdit d'interdire, mais la loyauté des relations contractuelles ainsi que les besoins de fonctionnement des entreprises, lui permettent de réguler et d'accéder aux données appropriées. Aujourd'hui, la question du traitement des données des salariés, mais plus largement, celle du traitement des données dans l'entreprise à des fins aussi variées que le marketing, la phase contractuelle, la relation au travail appelle de leur part une prise de conscience et une gestion intégrée au processus décisionnel.

Strasbourg, le 17 janvier 2003

Geneviève Folzer et Mathieu Abboud
Avocats au barreau de Luxembourg, inscrits au barreau de Strasbourg
geneviefolzer@wanadoo.fr
mathieuabboud@aol.com

Pour en savoir plus

1° dossier thématique « travail » sur le site de la CNIL <http://www.cnil.fr/thematic/index.htm>

2° Recommandation du Forum des Droits sur l'Internet : « Relations du travail et Internet »
<http://www.foruminternet.org/recommandations/lire.phtml?id=394>

3° Peines avec sursis pour détournement de courriers électroniques au travail
<http://www.foruminternet.org/actualites/lire.phtml?id=237>

4° Le rôle de l'administrateur réseau dans la cybersurveillance par Me Martine Ricouart-Maillet, Caroline Requillart, <http://www.juriscom.net/pro/2/priv20020408.htm>

5° Courrier électronique : les suites de la décision de la Cour de Cassation du 9 octobre 2001 par Olivier Iteanu, avocat <http://www.journaldunet.com/juridique/juridique011009.shtml>

6° avis du groupe de l'article 29 de la directive 95/46/CE n°8/2001 sur le traitement des données à caractère personnel dans le contexte professionnel
http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48en.pdf.

7° Document de travail du groupe de l'article 29 de la directive 95/46/CE concernant la surveillance des communications électroniques sur le lieu de travail
http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp55_fr.pdf

8° Recommandation (89) 2 du Conseil de l'Europe sur la protection des données à caractère personnel utilisées à des fins d'emploi <http://cm.coe.int/ta/rec/1989/f89r2.htm>

9° Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données *Journal officiel* n° L 281 du 23/11/1995 p. 0031 - 0050
http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=FR&numdoc=31995L0046&model=guichett

10° Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) *Journal officiel*

n° L 201 du 31/07/2002 p. 0037 - 0047

http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=FR&numdoc=32002L0058&model=guichett

11° textes légaux dont loi 78-17 informatique et libertés <http://www.cnil.fr/textes/index.htm>