

DONNEES PERSONNELLES

Citation : Nicolas Ivaldi et Pascaline Vincent, Caprioli & Associés, Données personnelles, www.caprioli-avocats.com

Première publication: septembre 2005.

Cybersurveillance des salariés et chartes informatiques

Nicolas IVALDI, Avocat au Barreau de Nice et **Pascaline VINCENT**, Juriste Caprioli & Associés, Société d'avocats

[www. caprioli-avocats.com](http://www.caprioli-avocats.com)

contact@caprioli-avocats.com

Plan

I/ UN CADRE JURIDIQUE PROTECTEUR DU SALARIE

A) Les formalités à respecter

B) Droits fondamentaux et contrôle du juge

II/ UN REEQUILIBRAGE CONVENTIONNEL AVEC LA CHARTE INFORMATIQUE

A) La démarche juridique d'adoption d'une charte

B) L'efficacité de la charte

Notes

Les réseaux Internet et Intranet ont ouvert l'Entreprise au monde numérique. Pour autant, émergent de ces moyens de communication de nouveaux risques pour l'employeur. Le risque majeur encouru par l'entreprise du fait de ces nouveaux moyens est l'atteinte à son patrimoine informationnel. Ses fichiers confidentiels, son savoir-faire ou ses secrets de fabrique qui ne sont pas protégés par un droit de propriétés intellectuelles peuvent faire l'objet d'une intrusion venant de l'extérieur, voire même d'une divulgation privée ou d'une diffusion publique par l'un des salariés. Dès lors, aux risques économiques et informatiques encourus par l'entreprise notamment par la divulgation d'informations confidentielles et de la propagation de virus informatiques s'ajoute le risque juridique de voir se distendre le lien de subordination qui le lie à son salarié.

Aujourd'hui, l'Employeur n'a plus seulement à craindre ses concurrents. Il doit aussi se préoccuper de ses salariés et notamment, de l'utilisation que ceux-ci font du poste informatique qu'il met à sa disposition [1]. En effet, si l'outil informatique et les connexions afférentes sont destinés strictement à l'exécution de son contrat de travail, ils peuvent également être utilisés par le salarié à des fins personnelles. La mise en place de mesures de

sécurité technique, juridique et organisationnelle au sein de l'entreprise répond dès lors à un besoin de protection. Le problème se cristallise à la frontière ténue entre le droit et l'abus de ce droit. Il appartient à l'employeur de trouver cette limite et de se prémunir en conséquence contre les éventuels abus de son salarié.

La solution apparaissait simple jusqu'alors. Il suffisait de surveiller l'activité de celui-ci dans le cadre de l'exécution de son contrat de travail. On a installé des systèmes de vidéosurveillance et des pointeuses à l'entrée et à la sortie du lieu de travail. La cybersurveillance n'est autre que l'expression moderne du lien de subordination qui préside à la relation de travail et du pouvoir disciplinaire de l'employeur qui la régule. Cependant, on ne saurait nouer les pieds et les poings du salarié avec ce lien. La subordination n'est pas l'aliénation. L'entreprise est devenue un véritable lieu de vie. En démontrant la revalorisation du dialogue social [2] et l'adaptation des règles aux besoins de proximité de l'entreprise et des salariés qui l'animent.

Le salarié ne quitte plus ses droits fondamentaux dès qu'il revêt son habit de travail. A ce titre, l'entreprise ne saurait s'y soustraire. La protection du salarié est d'autant plus justifiée dans l'ère numérique que des données " identifiantes " le concernant peuvent figurer sur des sites de présentation de son entreprise. La Commission Nationale Informatique et Liberté (CNIL) opère en garde-fou, tant en amont avec la déclaration de fichiers de données personnelles informatisées qu'en aval avec les garanties et les droits dont elle assure la protection. C'est aussi dans cette logique que la réglementation tant textuelle que jurisprudentielle de la cybersurveillance a été bâtie. Cependant, la protection qu'offre ce régime légal à l'employeur apparaît obsolète face à la protection qu'offre la loi au salarié (I). C'est donc dans un souci d'équilibre qu'il convient d'envisager le régime conventionnel, parallèle à ce régime légal, des chartes informatiques (II), pour faire valoir les intérêts de l'entreprise à côtés de ceux du salarié et trouver, qui sait ? cette fameuse frontière entre le droit et l'abus du droit d'utiliser l'outil professionnel à des fins personnelles.

I/ UN CADRE JURIDIQUE PROTECTEUR DU SALARIE

Le régime légal de la cybersurveillance n'offre que peu de marge de manœuvre à l'employeur soucieux de la productivité de sa structure et de la rentabilité de ses éléments en ce qu'il est rigoureusement encadré de formalités en amont (A) et son salarié, protégé en aval par le respect de la vie privée et le contrôle du juge (B).

A) Les formalités à respecter

La cybersurveillance n'a de spécifique que les moyens mis en œuvre pour l'exercer. Elle ne bénéficie pas d'un régime légal dérogatoire. En effet, surveiller l'activité d'un salarié signifie contrôler la bonne exécution du contrat de travail. " Cybersurveiller " l'activité d'un salarié, c'est contrôler l'utilisation que les salariés font de leur outil informatique, et conserver le cas échéant, des informations, identifiantes ou pas. Si ce dispositif doit se justifier par un motif légitime de l'Entreprise et avoir une finalité autre que le strict contrôle de l'activité des salariés [3], il peut également donner lieu à une intrusion dans la vie privée du salarié, intrusion d'autant plus vraisemblable depuis l'émergence des réseaux informatiques. C'est pourquoi sa mise en place au sein de l'entreprise doit remplir des conditions de forme rigoureuses de déclaration (1°) et d'information (2°).

1°) La déclaration du système de cybersurveillance

Un dispositif de cybersurveillance n'est autre qu'un traitement automatisé des données personnelles, comme tel, relevant de la loi Informatique et Liberté du 6 janvier 1978 [4]. Ce texte impose la déclaration préalable auprès de la CNIL de tout traitement automatisé d'informations nominatives, entendues tant comme des données personnelles que professionnelles, qui permettent l'identification directe ou indirecte d'une personne. Cette déclaration est facilitée depuis l'ouverture du service de déclaration en ligne sur le site Internet de la CNIL. L'employeur doit y préciser la finalité des données collectées ainsi que leur durée de conservation qui ne doit pas être excessive. L'absence de déclaration rend non seulement le traitement illégal et l'employeur passible de sanctions pénales [5] et de dommages et intérêts dans le cadre d'une action en responsabilité civile [6], mais également les sanctions fondées sur un tel traitement sont nulles. Jusqu'alors, la sanction de l'inobservation des prescriptions légales de déclaration était soumise à la preuve d'un préjudice subi par les salariés [7]. Aujourd'hui, ce n'est plus le cas. La chambre sociale de la cour de cassation a jugé en effet le 6 avril 2004 [8] que le non-respect par un salarié du système de badge à l'entrée et à la sortie du lieu de travail [9] qui a été installé en contravention des formalités légales (déclaration à la CNIL) rendait le licenciement sans cause réelle et sérieuse. Cette nouvelle sanction répond aux intérêts du salarié mais participe du régime défavorable de la cybersurveillance pour l'employeur.

2°) L'information du salarié et des organes représentatifs du personnel

La modification apportée par la loi du 6 août 2004 [10] renforce l'importance du consentement de la personne concernée par le traitement en général sauf pour les cas où il existe une obligation légale incombant au responsable du traitement. Et tel est le cas en l'espèce. En effet, l'obligation de consentement trouve un corollaire édulcoré en droit du travail dans l'information préalable et obligatoire du salarié pour la collecte et l'utilisation de ses données personnelles.

Force est de constater qu'il n'est nullement question de consentement. Aux termes de l'article L. 121-8 du Code du Travail, "aucune information concernant personnellement un salarié ou un candidat à l'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". La protection formelle du salarié est certes rigoureuse mais assez malléable pour que l'employeur ne pêche pas. La question est dès lors de savoir comment satisfaire à cette obligation d'information préalable et comment la prouver. Outre la clause dans le contrat de travail ou la diffusion d'une note de service, l'insertion d'une mention relative à la mise en place d'un système de cybersurveillance dans le règlement intérieur apparaît suffisante, celui-ci faisant l'objet d'un affichage et d'une remise en main propre aux nouveaux salariés.

Cependant, une telle insertion n'a d'intérêt et n'offre un gain de temps et de preuve que pour les entreprises de plus de 20 salariés pour lesquelles l'adoption d'un règlement intérieur est obligatoire [11]. L'entrée en vigueur d'un règlement intérieur requiert de lourdes formalités [12].

Cette obligation formelle se double de la consultation préalable du comité d'entreprise. En effet, les organes représentatifs du personnel doivent être consultés non seulement, préalablement à la mise en place d'un système de traitement de données [13] mais également préalablement à "tout projet important d'introduction de nouvelles technologies, lorsque

celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail du personnel [14]." La validité de la mise en place d'un dispositif de cybersurveillance l'exige. Aussi, faute de respecter ces lourdes prescriptions, l'Employeur ne pourra-t-il fonder une sanction disciplinaire sur un manquement de son salarié audit traitement automatisé. L'employeur prévoyant n'aura pas à craindre ce régime légal sous réserve qu'il respecte en outre les droits et libertés fondamentaux du salarié.

B) Droits fondamentaux et contrôle du juge

Les droits et libertés fondamentales du salarié sont à prendre en considération avant la mise en place d'un système de cybersurveillance (1°). Cependant, elles n'interviennent qu'en aval de celle-ci sous l'action des juges (2°).

1°) Le respect de la vie privée au travail

Le principe de proportionnalité qui préside à l'instauration d'une restriction à la liberté du salarié fait figure de garde-fou dans la jurisprudence. Non limités aux dispositions de l'article 9 du Code civil protégeant la vie privée, de l'article 9 du Nouveau Code de procédure civile et de l'article L. 120-2 du Code du Travail consacrant cette proportion [15], les juges peuvent également recourir à l'article 8 de la Convention européenne de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales [16] pour parer les intrusions de l'Employeur dans la vie privée de son salarié.

En effet, il existe une part irréductible de vie privée sur le lieu de travail [17] auquel aucun système de cybersurveillance ne saurait porter atteinte [18]. C'est l'apport du désormais célèbre arrêt Nikon [19]. L'employeur ne peut pas contrôler les courriers électroniques de son salarié même s'il lui avait expressément interdit d'utiliser l'outil informatique à des fins personnelles. Le secret des correspondances privées est absolu. Cet absolutisme est d'autant plus préjudiciable que la Cour de Cassation considère dans cet arrêt le courrier électronique comme une correspondance privée sans même dissocier les mails personnels des mails professionnels.

Aussi, en réaction, les entreprises ont-elles pris la contre-allée : certaines ont renoncé à exercer quelconque contrôle sur les correspondances, d'autres ont interdit toute utilisation personnelle de l'outil professionnel privilégiant ainsi la faute objective du salarié, d'autres encore, prenant le principe de l'arrêt Nikon a contrario, ont présumé que comme elles ne pouvaient plus contrôler les mails personnels de leurs salariés, tout courrier électronique reçu ou émis depuis une boîte professionnelle était présumé de manière irréfragable comme étant un mail professionnel [20]. Cette solution est un artifice douteux. Pour autant, elle démontre l'impasse dans laquelle se trouvent les employeurs face à l'utilisation personnelle du matériel informatique. L'issue serait-elle le recours à la " proportion raisonnable " que propose la CNIL [21] quant à l'utilisation des outils professionnels par le salarié ? Cette notion floue ne deviendra efficace que si le Juge fait application de l'obligation de loyauté et de la bonne foi dans la relation du travail. La difficulté sera soulevée dès lors au niveau de la preuve de l'utilisation déraisonnable du salarié des moyens de l'entreprise qui sera soumise non seulement à l'appréciation souveraine du juge mais également à son éventuelle irrecevabilité.

2°) La recevabilité de la preuve informatique

Le problème se pose au regard de la responsabilité encourue par l'employeur en cas de faute préjudiciable ou de délit commis par le salarié [22] dans l'utilisation de son outil professionnel [23]. Plus précisément, il s'agit ici du problème de l'admissibilité et de la recevabilité de la preuve. En effet, l'employeur ne peut se prévaloir d'une preuve obtenue en contravention des droits et libertés fondamentaux de son salarié, et notamment en violation du secret des correspondances privées pour fonder une sanction disciplinaire car cette preuve est illicite au vu de la jurisprudence [24]. Dès lors, faut-il penser que la seule preuve que l'employeur peut produire au soutien de sa sanction doit provenir exclusivement de l'extérieur ? Cette solution est envisageable [25] mais elle revient à promouvoir sinon la délation ou le recours intempestif à un agent assermenté [26], du moins la délégation du pouvoir de direction de l'employeur. En effet, le pouvoir de contrôle de l'utilisation que font les salariés de leur poste informatique peut être exercé dans ce strict cadre par l'administrateur du réseau de l'entreprise [27]. Cette délégation garantit outre les droits et libertés fondamentaux du salarié, la validité de la preuve mais n'offre hélas que peu de garantie d'impartialité, sauf à définir les règles déontologiques ou de conduite et à définir son rôle dans le cadre d'une charte informatique.

II/ UN REEQUILIBRAGE CONVENTIONNEL AVEC LA CHARTE INFORMATIQUE

Les chartes informatiques font figure de remède ultime pour les employeurs acculés au régime légal protecteur du salarié. Pour autant, elles ne sont pas la panacée. La pratique a démontré que l'efficacité de la charte était subordonnée au respect de conditions [28]. L'adoption d'une telle charte doit suivre un cheminement en plusieurs phases (A) pour développer les effets escomptés (B).

A) La démarche juridique d'adoption d'une charte

La démarche juridique se déroule en trois phases : cadrage, analyse et rédaction, négociation et mise en œuvre. L'employeur doit, dans un premier temps, prendre en compte l'environnement juridique existant dans l'entreprise. Cet environnement est constitué de la politique de sécurité [29], du règlement intérieur, des notes de services et des recommandations diverses telles que syndicales. Les moyens mis à la disposition du salarié ainsi que les dispositifs de surveillance déjà établis dans l'entreprise doivent ensuite faire l'objet d'un inventaire. Les objectifs poursuivis par ces dispositifs ainsi que ceux à mettre en place doivent être clairement définis.

En effet, comme vu précédemment, la cybersurveillance ne doit pas avoir pour seul but de contrôler l'activité des salariés. Elle doit également répondre à un souci de sécurité de systèmes d'information de l'entreprise et à la défense de son patrimoine informationnel. Les contraintes mises en place par la charte et les intérêts protégés par elle doivent se balancer pour respecter le principe de proportionnalité. A cet égard, il conviendra d'informer et d'impliquer les divers départements de l'entreprise. Aussi le rédacteur devra-t-il s'imprégner des compétences de ces différents acteurs pour respecter les conditions de validité de la charte. Une fois le calendrier établi, la phase rédactionnelle pourra débiter [30].

A ce titre, il convient de rappeler la consultation obligatoire du comité d'entreprise pour l'installation de nouvelles technologies au sein de l'entreprise, ayant des conséquences sur l'emploi [31]. La charte devra comprendre outre les moyens mis en place par l'employeur pour contrôler l'activité des salariés (traçabilité, contrôle d'accès, utilisation de certificats électroniques, processus d'horodatage, statut de l'administrateur-réseau...), les infractions répréhensibles comme telles avec les sanctions correspondantes ainsi que les moyens de preuves. Cependant, la charte ne pourra prévoir tous les cas d'infractions au règlement. Aussi doit-elle laisser une marge de manœuvre à l'employeur, pour adapter les sanctions conformément aux stipulations de la charte et au règlement intérieur de l'entreprise.

B) L'efficacité de la charte

L'arrêt Nikon a montré les limites des interdictions faites au salarié relativement à l'utilisation de l'outil informatique. Elles tiennent à la précision de la rédaction et à son opposabilité. L'employeur de Nikon France avait pourtant interdit l'utilisation personnelle de l'ordinateur, il n'avait pas respecté les principes fondamentaux qui président aux restrictions dans le domaine social. Si la liberté contractuelle permet de se prémunir contre les rouages judiciaires, elle doit néanmoins respecter la Loi et les textes qui l'entourent au risque de ne pouvoir être appliquée. Elle doit aussi être opposable aux salariés. Les juges exigent la preuve que les salariés ont pris effectivement connaissance du contenu de la charte [32]. Cette charte peut être envoyée par courrier électronique ou par Intranet depuis que ce moyen a été reconnu comme un moyen de communication dans l'entreprise [33]. L'employeur n'aura pas de problème à prouver que le courrier envoyé est professionnel. Le problème demeure quant à la faute et à la détermination de la sanction, même si elle est prévue dans la charte. Le point d'orgue de la question se cristallise sur la personne compétente à administrer les réseaux de l'entreprise. Son rôle sera essentiel. La charte devra contenir en outre des dispositions relatives aux données à conserver notamment celles permettant l'identification d'un délinquant ou d'un individu fautif au sens de l'employeur. Ce dernier a intérêt à encadrer ces nouveaux usages pour mieux circonscrire les risques juridiques et assurer la sécurité juridique des échanges qu'il a sous sa responsabilité et pour lesquels il fournit les moyens d'exécution. Dans l'idéal, la solution consistera à adopter une approche transversale aux services de l'entreprise et globale de la problématique, c'est à dire en s'appuyant sur des mesures juridiques, techniques et organisationnelles.

Notes

[1] Rapport " Relation du travail et internet ", 17 septembre 2002, Forum des droits sur l'Internet.

[2] Loi n°2004-391 du 4 mai 2004, J.O. n°105 du 5 mai 2004 relative à la formation professionnelle tout au long de la vie et au dialogue social. La loi renforce la légitimité des accords par l'extension du principe majoritaire et l'autonomie des accords d'entreprises par rapport aux accords supérieurs par l'instauration d'un régime dérogatoire. La remise en cause du principe de faveur est balancée par l'instauration d'un droit d'opposition au profit des organes représentatifs du personnel pour contrecarrer un accord collectif qui contreviendrait aux intérêts des salariés qu'ils défendent.

[3] La cybersurveillance ne peut avoir pour seul but de contrôler l'activité professionnelle des salariés. Le recours à un système de contrôle doit être justifié par un intérêt légitime autre, tel qu'assurer la sécurité des salariés et du système d'information.

- [4] Loi n°78-17 du 6 janvier 1978, Informatique et Libertés (JO 7 janvier 1978)
- [5] A titre d'exemple, les articles 226-16 à 226-24 du Code pénal et l'article 42 de la loi prévoient jusqu'à 5 ans d'emprisonnement et 300.000 € d'amende. L'article 226-1 du code pénal dispose : "Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements automatisés d'informations nominatives sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de trois ans d'emprisonnement et de 45.000 euros d'amende".
- [6] Cass. Soc. , 7 mai 1995 : Gaz. Pal. 1996, somm. , p.2, note A. Mole-Lexis, n°91-44-919
- [7] Cass. soc. 7 juin 1995 , Bull. civ., V, n°184 ; Comm. Com. Electr. Juin 2004, n°79, p. 41, note Agathe Lepage
- [8] Cass. Soc. 6 avril 2004, n°944, www.courdecassation.fr, Droit et Patrimoine, note Eric A. Caprioli, n°133-janvier 2005, p.103.
- [9] Les traitements automatisés d'informations à caractère personnel mis en œuvre sur les lieux de travail pour la gestion des contrôles d'accès aux locaux font l'objet d'une réglementation rigoureuse (Norme simplifiée n°42, Délibération de la CNIL n°02-001 du 8 janvier 2002, disponible sur www.cnil.fr).
- [10] Loi n°2004-801 du 6 août 2004, J.O. 7 août 2004, portant transposition de la Directive 95/46/CE 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 (JOCE du 23 novembre 1995, L.281/31) et modifiant la Loi informatique et liberté du 6 janvier 1978 (ancien chapitre IV, nouvel article 5).
- [11] Article L. 122-33 du Code du Travail.
- [12] L'entrée en vigueur de règlement intérieur doit faire l'objet d'une consultation du comité d'entreprise ou des délégués du personnel, d'une communication à l'inspecteur du travail et d'un dépôt au secrétariat-greffe du conseil des prud'hommes (article L. 122-36 du Code du Travail).
- [13] Article L. 432-2-1 alinéa 2 et 3 du Code du Travail : " [Le comité d'entreprise] est aussi informé et consulté, préalablement à la décision de mise en œuvre de 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 œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés. "
- [14] Article L. 432-2 du Code du Travail.
- [15] Article L. 120-2 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. "
- [16] "1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sécurité publique, au bien-être économique du pays [...] ou à la protection des droits et des libertés d'autrui."
- [17] La Cour européenne des Droits de l'Homme a posé le principe qu'il y avait atteinte à la vie privée même lorsque l'atteinte avait eu lieu sur le lieu de travail. (Arrêt Niemietz c/ Allemagne, 23 novembre 1992, Numéro de requête 00013710/88 disponible sur <http://www.echr.coe.int/Fr/Judgments.htm>).
- [18] Cette constatation découle d'une prise en compte européenne de la mutation de la relation de travail sous l'ère numérique. Le groupe européen des commissaires à la protection des données a adopté le 29 mai 2002 un avis sur la " surveillance des communications électroniques " sur le lieu de travail, disponible sur www.europa.eu.int/comm/privacy.
- [19] Cass. soc. 2 oct.2001, Sté Nikon France SA/M. Onof, n°99-42.942 : D. 2001, p. 3148,

note P.-Y Gautier, D. 2002. somm. Comm. p.2296, note C. Caron. - G. Lyon-Caen, Débat autour de l'arrêt Nikon France : sem. Soc. Lamy, 15 oct. 2001, n°1046, p.8 et obs. A. Mole, p.12 - M. Hautefort, Le secret des correspondances professionnelles s'applique aux e-mails émis ou reçus sur un poste professionnel : Juris. Soc. lamy, 18 oct. 2001, n°88, p.7- A. Lepage, La bataille du mail : Comm. com. electr. Nov.2001, comm. 120 - D. Forest, Vers une " ambassade virtuelle " en terre patronale ? ; Expertises, n°254, déc. 2001, p.424.

[20] Aux termes de la décision rendue par la chambre criminelle de la Cour de Cassation le 16 janvier 1992, le courrier mentionnant les noms du salarié et de l'entreprise est un courrier professionnel. Le courrier personnel a contrario doit être identifiable comme tel dès réception. L'objet du mail fait figure de critère unique pour l'employeur qui se voit contraint de l'interpréter pour faire valoir son droit de contrôle sur les courriers professionnels. Hélas ! La part de subjectivité qui demeure dans cette appréciation joue souvent en sa défaveur (en ce sens, voir : CA Toulouse, 6 février 2003, RJS 11/2003, n°154 et le mail " mon neurone est en vacances ")

[21] Rapport CNIL, 28 mars 2001, disponible sur www.cnil.fr

[22] D. Serio et C. Manara, Traçabilité et responsabilité dans les relations de travail, p. 220, Traçabilité et Responsabilité, Economica, 2003, disponible sur le site www.caprioli-avocats.com.

[23] C'est sur le fondement de l'article 1384 alinéa 5 du Code civil relatif à la responsabilité du commettant du fait de son préposé que la société Lucent Technologies a été reconnue responsable de la création et de l'exploitation d'un site à contenus diffamatoires par un de ses salariés depuis son poste professionnel (TGI Marseille, 11 juin 2003). La société peut se retourner contre son salarié et agir au pénal pour détournement et abus de confiance comme cela a été admis par la chambre criminelle de la Cour de cassation le 19 mai 2004 dans le cadre d'une exploitation d'un site à caractère pornographique depuis l'ordinateur professionnel (D. pénal, 2004, n°9, com. n°129, p.20).

[24] C. Beguin, La licéité de la preuve en Droit du Travail : l'Employeur peut-il produire en justice les éléments recueillis grâce à la Cybersurveillance ? Petites Affiches, n°115, 9 juin 2004 p.315.

[25] Cass. soc. 2 juin 2004, Marc X c/ Spot Image, www.legalis.net : en l'espèce, c'est le destinataire du courriel litigieux qui a averti l'employeur. La preuve a été admise car elle ne violait pas le secret des correspondances.

[26] C'est dans le cadre d'une procédure sur requête fondée sur l'article 145 du Nouveau Code de Procédure Civile que le président du TGI compétent nommera un huissier et un expert pour, notamment, faire des recherches sur le poste informatique du salarié.

[27] F. Bitan, Messagerie électronique de l'entreprise : le pouvoir de contrôle de l'employeur à l'épreuve du secret des correspondances, Comm. com. electr. Juin 2004, p.12.

[28] Eric A. Caprioli, Cybersurveillance des salariés : du droit à la pratique des chartes informatiques, Petites Affiches, n°195, 29 sept. 2004 ; même auteur en matières de collectivités publiques, La mise en place d'une charte informatique et communications électroniques, La gazette des communes, 1er mars 2004, disponible sur le site www.caprioli-avocats.com/doc.

[29] Le guide pour l'élaboration d'une Politique de sécurité interne de la Direction centrale de la sécurité des systèmes d'information (DCSSI/SGDN) et la norme ISO 17799 peuvent être adaptés aux besoins de l'entreprise dans le cadre d'une élaboration de sa politique de sécurité. Voir Eric A. Caprioli, Cybersurveillance des salariés : du droit à la pratique des chartes " informatiques ", Petites Affiches, n°195, 29 sept. 2004.

[30] Pour un modèle de charte, v. Lionel Bocherberg et Sebastien Cornuau, Internet et vie privée au bureau, Paris, Delams Express, 2001.

[31] v. note 12.

[32] TGI Paris, 2 novembre 2000, RJS, 2/01, n°166.

[33] Loi n°2004-391 du 7 mai 2004 sur le dialogue social a inséré des dispositions dans le code du travail relatives à l'Intranet et aux possibilités offertes aux syndicats et aux organes représentatifs du personnel de recourir à cette voie de diffusion, voir note n°2.