L'utilisation de la messagerie électronique dans l'entreprise. Aspects juridiques et managériaux en France et aux Etats-Unis.

Martine Bourrie-Quenillet, Florence Rodhain

Informatique - L'UTILISATION DE LA MESSAGERIE ÉLECTRONIQUE DANS L'ENTREPRISE Aspects juridiques et managériaux en France et aux États-Unis - Etude par Martine BOURRIÉ-QUENILLET par Florence RODHAIN

Document: La Semaine Juridique Edition Générale n° 2, 9 Janvier 2002, doctr. 102

La Semaine Juridique Edition Générale n° 2, 9 Janvier 2002, doctr. 102

L'UTILISATION DE LA MESSAGERIE ÉLECTRONIQUE DANS L'ENTREPRISE - . - Aspects juridiques et managériaux en France et aux États-Unis

Etude par Martine BOURRIÉ-QUENILLET Maître de conférences de droit privé à l'Université Montpellier II, CREGO Béziers (Centre de recherche en gestion des organisations)

par Florence RODHAIN Maître de conférences en sciences de gestion, Centre de recherche en gestion des organisations de l'Université Montpellier II

Accès au sommaire

L'émergence de la messagerie électronique n'est pas sans poser des problèmes, qui peuvent être étudiés conjointement sous les angles juridiques et managériaux. Les principales sources de conflit concernent les violations de différentes natures qu'autorise le support informatique sur lequel repose le courrier électronique. En l'absence de loi spécifique applicable à la messagerie électronique, le juriste s'appuie sur différents textes ayant pour but de protéger la vie privée des salariés et sur la jurisprudence émergente des juges du fond et de la Cour de cassation Note 1. Après avoir présenté le cadre réglementaire et judiciaire de l'utilisation du courrier électronique en France, les auteurs proposent d'examiner l'état de la question aux États-Unis. L'objectif final est de sensibiliser les juristes et les entreprises au problème de l'explicitation et de la diffusion d'une politique claire d'utilisation de la messagerie électronique auprès des salariés.

1.

1. - 1 - Moyen privilégié de communication sans papier, le courrier électronique permet à la fois la transmission de messages avec des ordinateurs extérieurs à l'entreprise mais encore une communication interne dans l'entreprise. Ainsi, il peut remplacer non seulement le traditionnel courrier de l'entreprise mais encore les notes de service, les appels téléphoniques d'ordre privé des salariés et les visites personnelles. Les possibilités de transmettre diverses formes de données électroniques sont multiples. Il peut s'agir de fichiers textes, de feuilles de calcul, de messages vidéo, de photographies... La messagerie électronique, de par sa nature, présente un véritable risque de violation du caractère confidentiel des communications. C'est ainsi que d'aucuns considèrent, à l'instar du commissaire canadien Ronald L. Rivest (1992), que le message électronique se situe "au même niveau de sécurité qu'une carte postale", et non pas au niveau d'une lettre enveloppée. Le courrier électronique est vulnérable aux atteintes à la vie privée. Ce terme de vie privée ne doit pas ici être entendu au sens traditionnel, classique "vie cachée, tranquille, choisie". Il s'agit plutôt de la maîtrise par l'individu de l'information qui circule à son propos, de la maîtrise de son image informationnelle.

2. - Le courrier électronique peut être à l'origine de diverses atteintes. Il permet de créer des pistes électroniques de messages et d'obtenir facilement des renseignements personnels sur les salariés. La surveillance peut se faire jour et nuit à partir d'un lieu éloigné. Elle peut être mise en place pour différentes raisons : simple curiosité,

évaluation du rendement ou des activités du personnel, collecte de renseignements, protection de l'ordre public et des bonnes mœurs, prévention d'infractions éventuelles ... Elle peut également exister sans motif réel, du seul fait d'une technologie productrice de traces Note 1. Des liens avec des fichiers personnels ou banques de données peuvent être établis par des systèmes de communication inter-réseaux. Selon le 20e rapport de la CNIL, ces technologies permettent d'établir le profil professionnel, intellectuel ou psychologique du salarié sans que celui-ci en ait conscience. Le salarié peut donc perdre le contrôle sur les données qui le concernent et sur les utilisations qui peuvent en être faites. Il ne sait généralement pas quelles données sont collectées, par qui, auprès de qui, dans quel but.

3. - Les adresses électroniques peuvent également être détournées et réutilisées par la suite pour l'envoi de messages publicitaires ou autres dans les boîtes aux lettres électroniques. Un message électronique peut être facilement lu et intercepté par des tiers plus ou moins autorisés. Ceux-ci peuvent être des collègues de travail, un supérieur hiérarchique, l'administrateur réseau. Il peut s'agir également de personnes mal intentionnées, un collègue mécontent ou jaloux, des pirates informatiques, etc. Par exemple, on a signalé certains incidents où des correspondants avaient porté atteinte à la réputation, à la vie privée de personnes. On ne peut garantir totalement le caractère confidentiel des communications par courrier électronique. En cas d'erreurs par exemple, l'administrateur réseau a le plus souvent la possibilité de lire les messages. L'émetteur d'un message n'est jamais tout à fait certain de l'identité de la personne à qui il envoie des informations.

4. - Après réception, le message peut être facilement transmis à un certain nombre de personnes sans le consentement ou la connaissance de l'expéditeur. Le destinataire ne sera donc pas le seul à lire le courrier électronique. Le message peut être retransmis, par exemple, au sein d'un débat public (dans des forums ou newsgroup). Certains systèmes sont reliés par réseaux avec d'autres entreprises ou organismes privés ou publics. Des copies des messages peuvent en outre être faites en apportant des modifications au contenu avant de les transmettre à des tiers (cependant, la plupart des systèmes de courrier électronique empêchent le changement du message avant sa retransmission). Par ailleurs, se pose le problème de l'archivage des messages qui ne disparaissent pas forcément après leur transmission. Une impression du message peut être faite sans prendre de précaution sur sa conservation. Ceci peut également se produire lorsque le salarié a accès à sa messagerie électronique depuis son domicile et qu'il l'entrepose dans ses archives personnelles non protégées. En effet, des copies peuvent être créées automatiquement dans des fichiers implicites de sauvegarde de certains systèmes à l'insu de l'utilisateur.

5. - Nouveau mode de communication, la messagerie électronique ne connaît pas de législation spécifique, que ce soit aux États-Unis, en France ou dans la plupart des autres pays. Cependant, il existe en France une protection juridique de la vie privée et une législation sur le secret des correspondances qui peuvent s'adapter à la messagerie électronique. Cet article se propose de faire le point sur les textes juridiques pouvant être utilisés dans ce cadre et sur la pratique judiciaire émergente. Après avoir étudié la situation en France, nous examinerons la situation aux États-Unis où est largement répandue la pratique du *monitoring* (pistage électronique des salariés) par l'employeur. Cette pratique a suscité dans ce pays un large débat, à la fois managérial et juridique quant à sa légalité ou son illégalité. L'exploration de ces problèmes nous amènera à conclure qu'au réseau "espace de liberté", les organisations doivent répondre par le réseau "espace de responsabilité". Cette responsabilité passe par une prise de conscience, une information et une formation des utilisateurs aux questions de sécurité du courrier électronique.

2. 1 - La situation en France

6. -

7. - 2 - Il n'existe pas de législation spécifique régissant l'utilisation de la messagerie électronique. Cependant, de nombreux textes du dispositif législatif français permettent de sanctionner sur notre territoire les atteintes à la vie privée et garantissent la protection des données à caractère personnel ; quelques décisions de justice récentes illustrent l'application de ces textes au courrier électronique.

A. - A - Le cadre réglementaire

8. -

9. - 3 - En ce qui concerne la correspondance, le droit distingue la communication audiovisuelle et la correspondance privée. Cette segmentation juridique est difficilement transposable à Internet car la plupart des services sont hybrides. On passe en effet indifféremment d'une communication audiovisuelle à une communication privée sur le net. Selon les circonstances, le courrier envoyé peut être public ou privé. Le législateur ne définit pas la correspondance privée mais la circulaire du 17 février 1988 relative aux services télématiques précise "*qu'il y a correspondance privée lorsque le message est exclusivement destiné à une (ou plusieurs) personne physique ou morale, déterminée ou individualisée*". S'agissant de correspondances privées, le respect de leur secret est garanti par la loi de 1991 sur le secret des correspondances émises par voie de télécommunications et par des dispositions pénales.

1° 1° La protection de la vie privée et des données personnelles

10. -

11. - 4 - La combinaison des articles 9, 1382 et 1383 du Code civil permet au juge de prononcer toutes mesures propres à faire cesser l'atteinte à l'intimité de la vie privée (*art. 9, al. 2*) et de décider, le cas échéant, d'une réparation du préjudice occasionné par l'auteur de l'atteinte (*art. 1382 et 1383*). L'article 8 de la Convention EDH prévoit également que "*toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance*". Par ailleurs, l'enregistrement ou même la simple écoute des propos d'une personne, sans son consentement, constituent une atteinte à l'intimité de la vie privée sanctionnée par l'article 226-1 du Code pénal.Les informations à caractère personnel ne sont librement disponibles ni dans leur accès ni dans leur traitement ; elles ne peuvent être librement publiées ou stockées dans une base de données ou un autre *corpus* qu'après

autorisation et selon certaines modalités. En vertu de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, les fichiers comportant des mentions nominatives doivent faire l'objet soit d'une autorisation, soit d'une déclaration préalable auprès de la Commission Nationale de l'Informatique et des Libertés. Ainsi, les entreprises ayant installé des autocommutateurs téléphoniques permettant d'enregistrer des données nominatives doivent consulter le comité d'entreprise Note 2, informer les salariés, prévoir une conservation limitée des données et ne pas procéder à des traitements à d'autres fins. À l'instar des autocommutateurs, le respect de la loi informatique et libertés devrait s'imposer aux acteurs de l'Internet et assurer une garantie aux utilisateurs des courriers électroniques notamment contre le détournement des adresses électroniques et les fichiers implicites de type *cookies*. La CNIL préconise quant à elle un équilibre entre les prérogatives de l'employeur et les droits du salarié. Elle prône la transparence et la proportionnalité dans l'usage du courrier électronique. Elle rappelle dans ses recommandations la nécessité d'une information préalable des salariés et une tolérance de l'usage à des fins privées de la messagerie électronique par les salariés, ceux-ci devant en avoir un usage raisonnable Note 3.Enfin, la directive européenne du 24 octobre 1995 protége les libertés et droits fondamentaux des individus, notamment leur vie privée, par le biais de la protection des données à caractère personnel, afin d'assurer en contrepartie la liberté des flux d'information sur tout le territoire communautaire. Ce régime de protection repose sur deux principes, le principe de la transparence (chaque individu doit savoir qui sait quoi sur lui et pour en faire quoi), et le principe de la finalité (tout traitement doit avoir une finalité précise et légitime).

2° 2° La garantie du secret des correspondances

12. -

13. - 5 - L'article 226-15 du Code pénal réprime d'une peine délictuelle d'un an d'emprisonnement et de 300 000 F d'amende "*le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance*". Devrait être réprimé de la même peine le fait d'intercepter ou encore de détourner, d'utiliser, ou de divulguer des correspondances transmises par la voie des télécommunications.La loi du 10 juillet 1991 a pour but de protéger les libertés individuelles par la garantie du secret des correspondances transmises par la voie des télécommunications et d'éviter que l'autorité publique porte atteinte à ce secret en dehors des seuls cas de nécessité prévus par la loi. Au-delà des correspondances téléphoniques, la loi vise tous les réseaux et télécommunications, c'est-à-dire au sens de l'article L. 32 du Code des Postes et télécommunications "*toute transmission, émission ou réception de signaux, d'écrits, d'images, de sons ou de renseignements de toute nature par fil optique, radioélectricité ou autres systèmes électromagnétiques*". Cette loi couvre de fait par extension le domaine de l'internet compte tenu d'une part de l'assimilation des correspondances électroniques en tant que correspondance à part entière au sens de la loi, et l'utilisation de réseaux de télécommunication pour leur acheminement d'autre part. La loi du 10 juillet 1991 est conforme à l'article 8 de la Convention EDH qui garantit également le droit au respect de la correspondance.Toutefois, la protection n'est pas absolue. L'ingérence d'une autorité publique est admise lorsqu'elle constitue une mesure nécessaire à la protection des droits et libertés d'autrui. Ainsi sont autorisées les interceptions du juge d'instruction dans le cadre de procédures pénales et de certains services de l'État en cas de risques pour la sécurité nationale, le potentiel scientifique et économique, la prévention du terrorisme, de la criminalité ... Par ailleurs, selon la CNIL Note 4, les messageries électroniques échangées par les salariés ne sont pas protégées de manière absolue par le secret des correspondances "*d'une part, parce que la loi de 1991 ne prive pas un employeur de la possibilité de placer les salariés sous écoute téléphonique, dès lors qu'il atteste de sa bonne foi, d'autre part, parce qu'il est trop tôt pour considérer comme*

incontestablement établi, compte tenu des termes divergents de la jurisprudence à cet égard, que la lecture d'un mail stocké sur un serveur de messagerie ou sur le disque dur d'un micro-ordinateur serait constitutif d'une interception de communication au sens de l'article 226-15 du Code pénal".

3° 3° La loi du 5 janvier 1988 et la réglementation de la cryptologie comme éléments de sécurisation de la messagerie électronique

14. -

15. - 6 - La loi du 5 janvier 1988 dite *loi Godfrain* protège les systèmes informatiques du piratage ou de la fraude. Elle concerne toutes les atteintes que pourraient subir les systèmes informatiques des utilisateurs. Elle permet de sanctionner pénalement (C. *pén., art. 323-1 et s.*) le fait d'accéder ou de se maintenir frauduleusement dans tout ou partie d'un système de traitement automatisé de données (1 an d'emprisonnement, 100 000 F d'amende), d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données (3 ans d'emprisonnement, 300 000 F d'amende) et d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient (3 ans d'emprisonnement, 300 000 F d'amende).Pour assurer la confidentialité des messages, il faudrait pouvoir les coder de la même manière qu'une enveloppe soustrait le contenu d'une lettre à la vue des tiers. Il existe une réglementation spécifique concernant le chiffrement des données Note 5. L'assouplissement des règles de cryptologie permet de résoudre partiellement les problèmes par l'utilisation de la certification et de l'authentification. Le régime en vigueur autorise la cryptographie pour s'assurer de l'authenticité, de l'intégrité et de la non-répudiation d'un message mais interdit le chiffrage s'il est destiné à rendre le message confidentiel. L'autorisation octroyée par la loi de chiffrer les données grâce "*à des conventions secrètes gérées selon les procédures et par un organisme agréé dans les conditions définies à l'article 28 de la loi du 29 décembre 1990*" ne garantit pas la confidentialité absolue du message. L'efficacité de la loi en terme de lutte contre les actes de captations illicites d'informations informatisées est de ce fait incertaine et relative.

B. - B - La pratique judiciaire émergente

16. -

17. - 7 - Quelques décisions de justice ont été rendues ces deux dernières années à propos de conflits suscités par l'utilisation de la messagerie électronique. Après quelques hésitations des juges du fond, on constate l'émergence d'une jurisprudence favorable aux salariés. L'arrêt de la Cour de cassation du 2 octobre 2001 témoigne de la volonté d'appliquer strictement les textes sur le respect de la vie privée et le secret des correspondances.

1° 1° Les hésitations des juges du fond

18. -

19. - 8 - Les premières décisions sur la question ont été rendues par les conseils de prud'hommes. Ces derniers ont fait preuve de rigueur vis-à-vis des salariés. En présence d'un règlement intérieur interdisant au personnel de se faire adresser de la correspondance privée à son adresse professionnelle, le Conseil de prud'hommes de Paris Note 6 a donné raison à l'employeur en jugeant que le licenciement d'un salarié avait une cause réelle et sérieuse dès lors que le salarié avait envoyé, par erreur, à l'ensemble des salariés de la société un message initialement destiné à un proche, extérieur à l'entreprise, révélant l'homosexualité de son expéditeur. Les faits reprochés n'étant pas contestés, le conseil a considéré qu'ils constituaient "*une infraction au règlement intérieur et aux règles propres à l'utilisation des micro-ordinateurs*" caractérisant la cause réelle et sérieuse du licenciement (le motif du licenciement était fondé sur la seule violation du règlement intérieur et n'était pas lié aux mœurs du salarié). Dans un autre jugement de conseil de prud'hommes Note 7, il était reproché à une salariée d'avoir utilisé à des fins personnelles et pendant son temps de travail le matériel de l'entreprise en entretenant au moyen de la messagerie électronique une correspondance avec une ex-salariée à laquelle avaient notamment été communiquées des informations sur la réorganisation en cours de l'entreprise. La salariée ne rapportant pas la preuve de l'accès à son courrier par l'employeur dans des conditions frauduleuses, la juridiction prud'homale considère comme régulier le licenciement dès lors qu'une note de la direction avait rappelé que la messagerie électronique était réservée à une utilisation professionnelle et que l'employeur conservait un droit de regard à tout instant.Cependant, les juges mettent de plus en plus l'accent sur un droit de contrôle de l'employeur limité par l'obligation de ne pas porter atteinte à la vie privée. Dans le cadre de la bonne exécution du contrat de travail, l'employeur peut contrôler l'activité et la productivité des salariés mais il ne doit pas porter atteinte à la vie privée de ces derniers (C. *civ., art. 9*). Certes la vie professionnelle relève en principe de la vie publique mais la jurisprudence développée sur le fondement de ces articles devrait permettre d'appréhender les atteintes à la vie privée résultant de l'utilisation d'une messagerie électronique à l'instar des décisions judiciaires relatives à l'enregistrement des conversations téléphoniques Note 8. La surveillance des salariés ne peut avoir lieu que pendant le temps de travail. L'emploi d'un procédé clandestin est illicite Note 9 et l'employeur ne dispose d'un droit de contrôle que pour les messages relevant de l'activité professionnelle. En ce qui concerne les messages personnels, il ne peut pas en prendre délibérément connaissance.Ainsi, trois fonctionnaires chargés d'une mission de service public ont été condamnés pour atteinte au secret des correspondances sur le fondement de l'article 432-9 du Code pénal pour avoir intercepté et consulté un courrier électronique de caractère privé qui ne leur était pas destiné Note 10. En l'espèce, la défense s'était attachée à démontrer les différences entre la correspondance traditionnelle et un e-mail. La victime (étudiant koweïtien à l'école supérieure de physique et de chimie industrielle), qui s'estimait être l'objet d'une discrimination de la part de son ex-école, dont il avait été évincé pour des raisons encore peu claires sur fond de différend sentimental, avait constaté que certains de ses e-mails avaient été ouverts (90 % de sa messagerie était d'ordre privé). Le directeur du laboratoire où travaillait la victime, le responsable du service informatique et son prédécesseur avaient reconnu leur responsabilité mais soutenaient qu'ils avaient agi pour préserver "la sécurité du réseau". Le tribunal a relevé que l'excuse de bonne foi n'était pas prévue en cas de délit commis par une personne en charge d'une mission de service public et a estimé que les mobiles étaient indifférents. Ainsi, il a considéré qu'il y avait lieu "*de leur faire une application bienveillante de la loi pénale, eu égard au fait que les actes délictueux retenus à leur encontre ont été commis dans le contexte particulier d'un laboratoire de recherche scientifique de haut niveau dont la vie a été perturbée par des conflits de personnes, compliquée de certains phénomènes de fraude, auxquels les responsables de cette unité ont tenté maladroitement de trouver une solution*" (peine d'amende de 10 000 F pour le directeur et l'administrateur réseau, peine de 5 000 F pour l'ancien administrateur réseau plus une condamnation solidaire des trois à payer à la victime la somme de 10 000 F à titre de réparation de son préjudice moral). Ce jugement a fait l'objet d'un appel devant la Cour d'appel de Paris.L'obligation d'informer les salariés est impérative. La Cour d'appel de Montpellier Note 11 rappelle que l'usage des écoutes téléphoniques ou

les vérifications de l'acheminement des correspondances par Internet doit, pour être licite, avoir été porté préalablement à la connaissance des salariés. En l'espèce, un salarié avait été licencié pour avoir utilisé de manière frauduleuse son poste de travail informatique à des fins personnelles pendant son temps de travail par l'envoi de nombreux courriers électroniques. La lettre de licenciement reposant sur des constatations effectuées par voie d'huissier, en l'absence du salarié et sans son autorisation, la cour considère qu'il appartenait à l'employeur de démontrer qu'il avait averti le salarié de son intention de contrôler l'usage de son poste téléphonique et informatique, or l'employeur ne produisait qu'un courrier interne adressé au salarié au moment de l'installation du système informatique de l'entreprise et ne mentionnant pas l'éventualité d'un contrôle. Les juges en déduisent que ce courrier ne pouvait constituer un avertissement et que la faute grave du salarié n'étant pas établie, il convient de lui attribuer des dommages-intérêts d'un montant égal à six mois de salaires.

2° 2° L'arrêt de la Cour de cassation du 2 octobre 2001

20. -

21. - 9 - La Chambre sociale de la Cour de cassation Note 12, dans une affaire opposant la société Nikon à un de ses salariés, s'est prononcé dans un sens favorable au salarié, l'employeur ne pouvant pas "*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*". La Cour fonde sa décision sur l'article 8 de la Convention EDH, l'article 9 du Code civil et l'article L. 120-2 du Code du travail. En l'espèce le salarié avait été licencié en 1995 pour faute grave, motif pris d'un usage à des fins personnelles du matériel mis à sa disposition par la société à des fins professionnelles. Pour le salarié, le licenciement est sans cause réelle et sérieuse, l'employeur ayant en son absence ouvert et reproduit sur disquette le contenu d'un fichier intitulé "personnel". En appel, la Cour d'appel de Paris considère cependant que le licenciement est justifié par une faute grave, retenant que *"le salarié avait entretenu pendant ses heures de travail une activité parallèle*". Le salarié se pourvoit alors en cassation, et la Cour de cassation casse et annule l'arrêt rendu le 22 mars 1999 par la Cour d'appel de Paris.L'arrêt de la Cour de cassation limite considérablement le pouvoir de contrôle et de surveillance de l'employeur sur l'activité de ses salariés pendant le temps de travail. L'intimité de la vie privée et le secret des correspondances doivent être respectés, même au temps et au lieu du travail. L'avocat général rappelle dans ses conclusions Note 13 que "la vie professionnelle n'absorbe pas la vie personnelle du salarié qui ne s'interrompt pas totalement une fois franchi le seuil du bureau ou de l'atelier" et que "l'entreprise ne peut être un espace où l'arbitraire et le pouvoir discrétionnaire s'exercent sans frein, un terrain d'espionnage où seraient bafoués les droits fondamentaux. Le tout numérique facilite le contrôle patronal mais une part, résiduelle, certes, mais irréductible de liberté et de vie personnelle doit subsister dans l'entreprise*...".* Cet arrêt devrait obliger les employeurs à revoir leur politique d'utilisation de la messagerie électronique dans l'entreprise. Les chartes informatiques devront en tenir compte en prévoyant non pas une interdiction d'un usage privé du courrier électronique mais plutôt un usage modéré et responsable de la messagerie à des fins personnelles.

3. 2 - La situation aux États-Unis

22. -

23. - 10 - Depuis plusieurs années déjà, des conflits sur l'usage approprié de la messagerie électronique opposent les employés à leurs employeurs aux États-Unis. Le phénomène a conduit nombre d'entreprises et de salariés devant les tribunaux. Nous proposons dans un premier temps de donner des exemples de conflits entre employeurs et employés, ce qui nous amènera à étudier les aspects juridiques liés à l'utilisation de la messagerie électronique aux États-Unis. Nous verrons que le droit semble, contrairement à la France, se trouver plutôt du côté de l'employeur. La pratique du *monitoring* serait donc une pratique licite, ce qui explique que plus d'un tiers des organisations nord-américaines déclarent sans vergogne pratiquer le *monitoring* ! Pourtant, les employés américains ne semblent pas être au courant de cet état de fait. Ils pensent majoritairement que la messagerie électronique est privée. Cette fausse perception (dans le contexte culturel nord-américain) est source potentielle de conflits. Elle débouche sur des problématiques managériales sur lesquelles nous terminerons cette dernière partie de l'article.

A. - A - Les conflits

24. -

25. - 11 - La façon dont les tribunaux nord-américains ont traité les conflits entre employeurs et employés liés au pistage électronique est intéressante à étudier car il n'existe pas de texte autorisant les organisations à mener cette surveillance. De la même façon, aucune loi ne les en empêche. Il existe pourtant bien une loi, au niveau fédéral, datant de 1986, dont le but est de protéger le caractère privé des communications électroniques. Cette loi précise qu'une tierce partie (individu, police, Gouvernement) ne peut intentionnellement prendre connaissance d'un message électronique sans obtenir au préalable une autorisation. Pour obtenir l'autorisation, preuve doit être faite qu'une action d'ordre criminel pourrait être commise à travers l'utilisation de la communication électronique. Cependant, cette loi est peu explicite lorsque le problème se concentre au sein d'une organisation donnée (Bjerklie, 1993). Et les juges retiennent généralement le fait qu'étant la possession de l'employeur, les ordinateurs des salariés peuvent être consultés à leur insu. En conclusion, si aucune loi ne permet de dire que le *monitoring* est illégal, aucune loi ne permet non plus de dire que la pratique est légale. C'est alors devant les tribunaux que la loi, on va le voir à travers les exemples qui suivent, se dessine progressivement et très nettement en faveur de la légalité de la pratique.

1° 1° Le cas Bourke versus Nissan (1993) Note 15

26. -

27. - 12 - Deux employées (Bonita Bourke et Rhonda Hall) de l'entreprise Nissan Motor Corp. sont licenciées pour avoir utilisé la messagerie électronique pour échanger des messages où apparaissaient des propos suggestifs d'ordre sexuel. Ces deux employées portent plainte, arguant du fait que ces messages relevaient de leur vie privée, et que la direction avait envahi leur vie privée en contrôlant le contenu des messages envoyés et reçus à partir de

leurs ordinateurs. Nissan gagne le procès. Les avocats de l'entreprise ont en effet réussi à convaincre les juges qu'à partir du moment où Nissan possède le système informatique utilisé par les employées, l'organisation a un droit légal de lecture de tout ce qui s'y trouve.

2° 2° Le cas Shoars versus Epson (1994) Note 16

28. -

29. - 13 - Shoars occupe le poste d'administrateur du réseau de la messagerie électronique à Epson. En 1989, cette employée découvre que son responsable hiérarchique, dénommé Hillseth, surveille et lit régulièrement le courrier électronique de ses employés. Aucune politique d'utilisation de la messagerie électronique explicite n'est diffusée dans l'organisation. Shoars demande alors à son superviseur de stopper cette pratique, ce qu'il refuse. Elle en réfère au Directeur Général de la société. Apprenant la démarche de son employée, Hillseth décide de licencier Shoars après cet acte qu'il définit comme une "insubordination". Shoars porte plainte pour licenciement abusif et perd son procès.

3° 3° Le cas Smyth versus Pillsbury (1996) Note 17

30. -

31. - 14 - Dans la société Pillsbury, une politique d'utilisation de la messagerie électronique a été mise en place. Celle-ci se veut très "ouverte". On peut y lire que le système électronique est mis à la disposition des salariés "afin de promouvoir la communication interne entre employés". La compagnie assure régulièrement ses employés (Smyth y compris) que tout message électronique restera confidentiel. Un jour, Smyth envoie un e-mail à son supérieur hiérarchique dans lequel il tient des propos qui seront considérés par sa hiérarchie comme "inappropriés et non-professionnels" Note 14. Cet e-mail arrive à la connaissance de la direction générale qui licencie immédiatement Smyth pour "commentaires inappropriés et non-professionnels placés sur le système électronique de la société". Smyth poursuit son employeur en justice et perd son procès. La cour déclare : "*nous ne trouvons pas qu'il soit raisonnable d'avoir des attentes en terme de respect du caractère privé des communications électroniques volontairement émises par un employé à son superviseur en utilisant le système électronique de la compagnie... Le plaintif a volontairement communiqué des commentaires non professionnels par le biais du système électronique de la compagnie. Nous ne trouvons aucun aspect privé dans de telles communications... De plus, l'intérêt de la compagnie dans la prévention de tels commentaires non-professionnels ou même dans la prévention d'activités illégales à travers le système électronique pèse bien plus lourd que le souci de respect du caractère privé de ces commentaires que l'employé peut ressentir*". La société Pillsbury assurait pourtant à ses salariés que "les communications électroniques ne peuvent pas être interceptées et utilisées par la compagnie contre ses salariés comme outils de licenciement ou de réprimande". Ce cas crée alors vraisemblablement un précédent dérangeant au regard du respect des politiques d'utilisation du média mis en place par l'organisation.

4° 4° Le cas Tiberino versus Cowles Publishing Company (2000) Note 19

32. -

33. - 15 - Les collègues d'une secrétaire travaillant pour l'État de Washington se plaignent d'avoir à assumer certaines des responsabilités incombant normalement à cette secrétaire car celle-ci consacrerait une part très importante de son temps de travail à l'envoi de messages électroniques privés. Un jour comme un autre, après que la secrétaire ait comme d'habitude quitté son poste de travail, l'administrateur examine sa boîte aux lettres "courriers envoyés" afin de déterminer le pourcentage de courriers personnels *versus* courriers professionnels. L'administrateur fait son rapport au superviseur de la secrétaire : sur les presque 200 messages envoyés, la quasi-totalité serait des messages personnels. En sorte que la secrétaire est immédiatement licenciée puisque son comportement est contraire à la politique d'utilisation de la messagerie électronique. C'est alors que la presse demande à voir l'intégralité des courriers électroniques reçus et envoyés par la secrétaire à travers un ordinateur étant la propriété de l'État. La Cour d'appel de Washington a finalement évité l'humiliation publique de la secrétaire. Elle a certes reconnu l'aspect "public" des messages électroniques de la secrétaire Note 15, cependant, pour les deux raisons suivantes, la cour a trouvé une exception à la règle. Premièrement, la secrétaire avait un droit au respect de sa vie privée sur ces courriers car ils contenaient des détails personnels n'ayant rien à voir avec quelque opération gouvernementale que ce soit. Deuxièmement, il n'y avait pas d'intérêt public sur le contenu des courriers car la secrétaire a été licenciée pour une *utilisation excessive* de la messagerie électronique à des fins personnelles et non à cause du *contenu* de ceux-ci Note 16.Force est de constater que la pratique judiciaire émergente aux États-Unis est en faveur de l'autorisation du pistage électronique des salariés dans les organisations où ils travaillent. Si la pratique de la surveillance électronique aux États-Unis met les employés en danger de perdre leur emploi, il les met également (particulièrement pour les salariés du secteur public), en danger de voir leur vie intime exposée publiquement.Bien que le législateur se place manifestement du côté de l'employeur, les employés nord-américains, quant à eux, continuent massivement à penser que leur e-mail est leur stricte propriété (*Welch, 1991 ; Cappel, 1993 ; Brown, 1994 ; Nelson, 1994 ; Weisband et Reinig, 1995 ; Greengard, 1996 ; Agarwal et Rodhain, 1999*). Cet état de fait nous amène à aborder les problématiques managériales soulevées par ces conflits, un effort de clarification étant peut-être à mener de la part des managers des organisations.

B. - B - Les problématiques managériales

34. -

35. - 16 - Si la recherche a montré que la messagerie électronique facilite la communication non structurée entre salariés, permet une fertilisation d'idées diverses, et accroît l'innovation dans l'organisation (*Sproull et Kiesler, 1986*), elle a également montré que l'utilisation du média peut avoir des effets négatifs du point de vue de l'organisation, et en particulier un temps excessif passé à des activités non productives sur le lieu de travail et pendant le temps de travail (*Machlis et Cole, 1997*). C'est ainsi que certaines organisations nord-américaines considèrent que la messagerie électronique ne peut être utilisée autrement que pour une communication d'ordre strictement professionnel, toute autre attitude étant source d'inefficacité pour l'organisation. Ces organisations

partent du principe que le système informatique leur appartenant, elles sont alors propriétaires de tout ce qui peut être conçu à partir de ce système (*Cappel, 1993 ; Brown, 1994*). Ces organisations mettent en avant le coût élevé de maintenance du réseau, le temps et l'énergie requis pour cette tâche, le fait qu'il faille embaucher du personnel qualifié pour administrer le système... C'est ainsi que Michael Simmons, Vice-président de *Bank of Boston*, déclare : "tout ce que l'entreprise achète, maintien, supporte ... peut uniquement être utilisé pour un travail strictement relié aux activités de l'entreprise" (*Sullivan 1993, p. 203*). Ces organisations considèrent également que les messages étant créés durant le temps de travail, ils doivent forcément être d'ordre professionnel (*Brown, 1994*). C'est alors que certaines organisations adhérant à ce point de vue ont commencé des pratiques de surveillance des communications électroniques, pratiques ne posant aucun problème technique. Et les premiers conflits sont apparus. Ces conflits étant dus pour une grande part à un problème de différences de représentations de l'utilisation judicieuse du média entre employeurs et employés. En effet, la pratique, comme bien souvent, a précédé la loi et les politiques d'utilisation mises en place dans les organisations. Lorsque l'outil a émergé, les acteurs ont dû s'approprier ce nouveau média et définir un mode d'utilisation à leur convenance. En l'absence de règles formalisées et diffusées par les organisations, les acteurs se sentent libres d'interpréter à leur manière l'utilisation judicieuse pouvant être faite du média. C'est pourquoi, pour éviter tout conflit, la littérature managériale nord-américaine a commencé à recommander aux organisations d'adopter et de diffuser une politique d'utilisation du média à ses salariés. Il existe deux types de politique : la politique "fermée", dans laquelle les employeurs exigent des salariés qu'ils n'utilisent le média qu'à des fins exclusivement professionnelles. Dans ce cas, l'employeur se réserve le droit de contrôler le contenu des messages. Par exemple, les entreprises suivantes diffusent une politique "fermée" auprès de leurs salariés : Epson, Federal Express, Pacific Bell, Nordstrom, Bank of Boston, Eastman Kodak, Du Pont, Hughes Aircraft, United Parcel Service (*Goode, 1991 ; Cappel, 1993*). C'est ainsi qu'à chaque fois que les employés de la société Epson se connectent sur le réseau de l'entreprise, ils sont informés par un message apparaissant systématiquement sur l'écran que l'entreprise se réserve le droit de lire tout message électronique reçu ou envoyé à partir du système informatique.La politique "ouverte", à l'opposé, consiste à rendre explicite la position selon laquelle les employés sont libres d'utiliser le média comme bon leur semble. Les employés sont alors "propriétaires" de leur courrier électronique, alors qu'ils ne le sont pas dans le cas des politiques "fermées". Les employeurs s'engagent à ne pas contrôler les messages envoyés et reçus par leurs salariés. Exemples d'entreprises adoptant une politique "ouverte" : Mc Donnel Douglas, General Motors, Warner Brothers, Citibank, Hallmark Cards, Media General. Dans la dernière entreprise, Media General, on a même été jusqu'à choisir un système codant automatiquement les messages électroniques reçus et envoyés de telle sorte que même l'administrateur du système ne puisse prendre connaissance du contenu des messages.Quelle que soit la politique adoptée par l'organisation, celle-ci apparaît importante à plusieurs titres :

36. - - tout d'abord pour éviter les poursuites judiciaires (*Goode, 1991 ; Casarez, 1992 ; Cappel, 1993*) qui, non seulement représentent un coût financier important, mais risquent également d'affecter le moral des salariés ;

37. - - ensuite pour ne pas laisser les salariés dans la confusion. En l'absence de politique claire, les salariés interprètent à leur façon ce qui relève d'un comportement acceptable ou non, et tentent d'imaginer ce que leurs employeurs en pensent (*Greengard, 1996*) ;

38. - - enfin pour favoriser un climat de confiance dans l'organisation (*Casarez, 1992*).

39. - La politique doit alors être diffusée de façon à ne pouvoir être inconnue des salariés. Différentes voies de diffusion de la politique sont utilisées, la plus efficace étant sans doute celle consistant à communiquer un message sur l'écran de l'ordinateur à chaque fois que l'utilisateur se connecte sur le réseau. Weisbang et Reinig (1995) suggèrent même aux entreprises de rappeler aux utilisateurs, lorsqu'ils détruisent des messages, que ces derniers ne disparaissent pas à tout jamais dans une poubelle virtuelle, mais restent accessibles.Si la littérature nord-américaine recommande, afin d'éviter les conflits, source évidente d'inefficacité, d'adopter et de diffuser une politique d'utilisation du média, elle ne donne absolument aucun conseil dans le choix de la politique. Quels sont les impacts d'une politique d'utilisation ? Quels sont les effets d'une politique donnée sur la confiance entre les employeurs et les employés dans l'organisation ? Sur le climat ? Sur la performance ? Aucune recherche ne permet de répondre à ces questions. On peut trouver dans la littérature non académique nord-américaine des citoyens s'élevant contre la pratique du *monitoring* de la messagerie électronique, leur argument principal étant qu'une attitude à la *big brother* ne peut qu'être néfaste à la créativité. Cette opinion est partagée par les comités de direction de certaines organisations, comme par exemple celui de General Motors, qui déclare considérer le lieu de travail comme un environnement de confiance mutuelle et de respect, cette philosophie excluant toute politique d'intrusion dans la messagerie électronique des salariés(*Cappel, 1993*). Les recherches menées sur la pratique du *monitoring* en général (non restreint à la messagerie électronique) montrent que les employés peuvent entretenir un sentiment de manque de respect lorsque la surveillance est pratiquée à leur encontre, ce qui par voie de conséquence est susceptible d'affecter négativement la productivité ainsi que l'ambiance dans l'organisation (*V. par ex. Hartman, 1998*). De façon générale, on peut supposer que la pratique du *monitoring* de la messagerie électronique peut provoquer les mêmes aspects négatifs que le *monitoring* pratiqué avec d'autres moyens de communication (V., pour le monitoring en général : *De Tienne, 1994 ; George, 1995*).Du point de vue juridique, la situation est à peu près comparable dans les deux pays, dans le sens où aucune loi spécifique ne régit l'utilisation du média sur le lieu de travail. Cependant, en France, le droit est bien plus présent sur le réseau pour répondre aux problèmes d'atteintes à la vie privée et au secret des correspondances. L'arrêt de la Cour de cassation du 2 octobre 2001 est certainement une étape importante dans l'évolution de la pratique judiciaire française. Toutefois, le droit ne peut avoir réponse à tout. Des questions juridiques et déontologiques complexes peuvent subsister du fait notamment des caractéristiques de la messagerie électronique : trans-nationalité, fugacité et volatilité des contenus, évolution très rapide des techniques et des stratégies. C'est pourquoi une attitude "responsable" doit pouvoir à notre sens être prônée, cette responsabilité passant par l'information des utilisateurs aux questions liées à la sécurité de la messagerie électronique. Code de conduite, charte informatique, règlement intérieur peuvent ainsi constituer des voies contractuelles intéressantes dès lors que leur contenu permet de fixer les objectifs du système, l'accès au courrier électronique par les tiers et les sanctions en cas de non-respect des règles édictées.

Cass. soc., 2 oct. 2001, arrêt n° 4164, Sté Nikon c/ O. : JCP G 2001, act. n° 42, p. 1926 ; JCP G 2001, IV, 2838 ; Juris-Data n° 011137 ; www.courdecassation.fr/agenda/arrets/arrets/99-42942arr.htm.

Note 1 "Jadis, nous étions fichés parce que quelqu'un souhaitait nous ficher. Aujourd'hui, nous pouvons aussi être fichés du seul fait de la technologie qui produit des traces sans que nous en ayons toujours pleinement conscience", avant-propos du Président Michel Gentot, 20e rapport d'activité de la CNIL pour 1999.

Note 2 Le Code du travail prévoit une information et consultation du comité d'entreprise préalablement à l'introduction dans l'entreprise de moyens ou techniques permettant un contrôle de l'activité des salariés (C. trav., art. L. 432-2-1).

Note 3 La cybersurveillance des salariés dans l'entreprise, Rapport d'étude et de consultation publique de la CNIL, mars 2001, p. 16-18.

Note 4 La cybersurveillance des salariés dans l'entreprise, Rapport préc. [note 4], p. 35.

Note 5 L. n° 96-659, 26 juill. 1996 : JCP G 1996, III, 68090 ; D. 24 févr. 1998 et DD. n° 99-199 et n° 99-200 17 mars 1999 : JCP G 1999, III, 20059 et 20060.

Note 6 Cons. prud'h. Paris, 1er févr. 2000 : TPS 2001, n° 1, chron. n° 1, p. 4.

Note 7 Cons. prud'h. Montbéliard, 19 sept. 2000 : Gaz. Pal. 14 déc. 2000, p. 39 ; Lamy Prud'hommes act. n° 20, nov. 2000.

Note 8 Exemples de condamnation : employeur qui divulgue devant l'ensemble du personnel l'enregistrement d'une conversation confidentielle entre deux salariés tenue en dehors des heures de service (CA Paris, 22 mars 1989) ou salariés d'une entreprise qui, au moyen d'un magnétophone, enregistrent les communications d'ordre personnel du directeur (Cass. crim., 8 déc. 1983).

Note 9 Cass. soc., 14 mars 2000 : Bull. civ. V, n° 101 ; JCP G 2001, II, 10472, note C. Puigelier et 20 nov. 1991 : D. 1992, jurispr. p. 73.

Note 10 TGI Paris, ch. 17, 2 nov. 2000 : Juris-Data n° 139077 ; Violation du secret des correspondances : Rev. jurispr. soc. 2001, n° 2/01, note p. 116 ; à propos du jugement du Tribunal correctionnel de Paris du 2 novembre 2000, V. X. Linant de Bellefonds, Le petit courriel : Com. comm. électr. 2000, n° 12, Repères p. 3 ; L. Rapp, note : D. 2000, n° 41, cahier rouge, p. 3.

Note 11 CA Montpellier, ch. soc. 6 juin 2001 : Juris-Data n° 149912.

Note 12 Cass. soc., 2 oct. 2001, préc. [note 1].

Note 13 Concl. M. Kœhrig, Avocat général, www.courdecassation.fr/agenda/arrets/arrets/99-42942concl.htm.

Bourke v. Nissan, No. YC-003979 (Cal.Super.Ct.L.A.Cty.) aff'd, No. B-068705 (Cal.Ct.App. 26 July 1993).

Le cas n'a pas été publié, cependant il est possible de trouver une copie de la décision de la Cour sur Internet à l'adresse suivante : www.law.seattleu.edu/fachome/chonm/Cases/shoars.html.

Smyth v. Pillsbury Co., 914 F.Supp.97 (E.D.Penn. 1996).

Note 14 Entre autre discours professionnel, il écrit dans ce mail qu'il menace de tuer les "batards" (traduction non garantie...) que représenteraient à ses yeux certains de ses collègues du service commercial.

On trouvera une copie de la décision de la cour d'appel à l'adresse internet suivante : www.securitymanagement.com/library/Tiberino-Spokane.html.

Note 15 La plupart des États d'Amérique possèdent une loi qui considère les informations manipulées par les employés de l'État comme étant publiques. Par exemple, selon la loi intitulée "The Sunshine law" en Floride, tout contribuable pourrait avoir accès à des informations manipulées par les employés du secteur public. Ce sont en général les journalistes qui connaissent le mieux et savent au mieux utiliser ce droit.

Note 16 Notons cependant que dans un cas quelque peu similaire dans l'Indiana, la cour a décidé qu'un journal local avait le droit d'accès à tous les fichiers personnels d'un directeur d'école ayant démissionné pour avoir été pris en délit de consultation de site web à caractère pornographique.