www.droit-tic.com

MIEUX COMPRENDRE LES IMPLICATIONS JURIDIQUES DU PROGRES TECHNOLOGIQUE

REVUE D'ACTUALITE JURIDIQUE DU DROIT DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

Novembre 2003

SOMMAIRE

Les Etats-Unis se dotent d'une législation fédérale relative aux pourriels et optent…out - Julien Le Clainche *Allocataire de recherche*

Le principe de disponibilité des données publiques : mythe ou réalité ? - M. Sulliman Omarjee *Juriste* .

Application classique des règles de la distribution sélective au commerce électronique – Me. Nicole Bondois *Avocate* et M. Nicolas Samarcq *Juriste BRM AVOCATS*.

Le rôle de l'administrateur réseau dans la cybersurveillance - Me. Murielle-Isabelle Cahen *Avocate*

24/11/2003

Les Etats-Unis se dotent d'une législation fédérale relative aux pourriels et optent…out

Auteur : Julien Le Clainche *Allocataire de recherche* .

Abstract :

Pourriel - Etats-Unis- Législation fédérale - opt-out (oui)

Domaine : Informatique et libertés

Sous thème : Pourriel, spam, courriel, vie privée

Ordre juridique :

Après 6 ans de discussion et de projets avortés [1], la chambre des Représentants et le Sénat du Congrès américain viennent d'adopter largement (HR, 392 voix pour, 5 contre) le premier texte d'application fédérale destiné à clarifier le cadre juridique des courriers électroniques non sollicités.

Après 6 ans de discussion et de projets avortés [1], la chambre des Représentants et le Sénat du Congrès américain viennent d'adopter largement (HR, 392 voix pour, 5 contre) le premier texte d'application fédérale destiné à clarifier le cadre juridique des courriers électroniques non sollicités (***"Controlling the Assault of Non-Solicited Pornography and Marketing Act" ou CAN-SPAM***). Ce texte que le président, G.W Bush, s'est engagé à signer, est assorti de sanctions pouvant aller jusqu'à cinq ans d'emprisonnement et deux cent cinquante mille dollars (250.000$) d'amende. Certains y verront cependant une certaine forme de légalisation des pourriels [2] ne serait-ce que dans l'intitulé abgrégé de la loi nouvelle... CAN-SPAM.

Le texte adopté dans la nuit du 20 au 21 novembre 2003 par le Congrès des Etats-Unis est le résultat non seulement d'une longue gestation législative qui a connu de nombreuses "fausses couches", mais aussi d'un compromis entre les différents acteurs du milieu. En effet, d'un côté les défenseurs des libertés individuelles, dont de nombreux juristes, se référaient à la définition de la **Privacy** traditionnellement reçue dans son acception la plus large comme étant *"The right to be left alone"*[3], littéralement **le droit d'être laissé tranquille**. Cette approche de la protection de la vie privée, qui n'est pas celle traditionnellement acceptée par les ordres juridiques européens, fondait une demande de consécration de l'"**opt-in**". L'individu doit "*être laissé tranquille*" et pouvoir garder la maîtrise de sa messagerie électronique. Les acteurs du commerce électronique invoquaient quant à eux la liberté d'entreprendre pour réaliser des fichiers d'adresses électroniques, destinés à l'expédition de messages commerciaux en l'absence d'opposition expresse de la personne concernée. Parmi eux, tous n'étaient d'ailleurs pas en faveur d'une intervention législative au niveau fédéral.

Le Controlling the Assault of Non-Solicited Pornography and Marketing Act

doit fournir, selon les déclarations du président américain *un ensemble d'outils techniques, administratifs, civils et criminels* permettant aux *consommateurs* de réduire considérablement le nombre de messages non sollicités qu'ils reçoivent. Plus largement, il s'agit de réduire le coût engendré par les pourriels, de préserver les consommateurs des pratiques trompeuses et de certaines collectes déloyales, ainsi que de lutter contre les messages à caractère pornographique.

La consécration de l'opt-out
Jusqu'à présent, le droit américain, comme le droit français, n'exige pas l'accord de la personne avant de réaliser un traitement portant sur son adresse électronique. La différence de protection entre la France et les Etats-Unis (EU) se fait surtout dans la précision de l'information devant être donnée à la personne dont l'adresse électronique est collectée. Les différences sont également notables dans le domaine des droits d'accès, de rectification et d'opposition. Ainsi, la France comme les Etats-Unis ont néanmoins une tradition d'opt-out. Pourtant, le développement impressionnant des pourriels a amené de nombreux ordres juridiques à consacrer le principe de l'opt-in. Ainsi, **la directive européenne 2002/58 CE [5] et la nouvelle loi californienne [6] exigent le consentement de la personne avant tout traitement de son adresse électronique en l'absence de relations antérieures**.
Les principaux acteurs du marché, en particulier la puissante Digital Marketing Association (DMA) et Microsoft, préféraient cependant que la personne puisse s'opposer à être contactée à nouveau, mais n'ait pas à consentir préalablement au premier envoi. C'est finalement dans leur sens que le consensus fédéral a évolué puisque **le Controlling the Assault of Non-Solicited Pornography and Marketing Act n'exige pas le recueil préalable du consentement de la personne avant de lui adresser un courriel non sollicité**.

Le texte, décidément timide, n'impose pas à certaines autorités, notamment la Federal Trade Comission (FTC), de tenir des **listes d'opposition**. Les professionnels du marketing doivent pourtant être en mesure de connaître le souhait de certaines personnes de ne pas être démarchées. Heureusement, le texte ouvre cependant expressément la faculté de créer et de gérer de telles listes, notamment à la FTC. Cette consécration fédérale fait écho à la récente condamnation de la FTC. En effet, la DMA avait attaqué l'application que faisait la FTC de la loi fédérale sur le télémarketing en invoquant le défaut de compétence de la commission pour gérer le fichier de données personnelles constitué par la liste d'opposition (do not call list) [7]. Depuis, les lois étatiques ayant constitué des listes d'opposition étaient donc elles aussi menacées d'inconstitutionnalité. Le nouveau texte est désormais en mesure de les valider en partie.

Un problème aigü va pourtant se poser aux Etats, comme la Californie, qui ont souhaité garantir une protection forte des individus contre les pourriels et ont notamment consacré le principe l'opt-in. En effet, **le texte fédéral prime sur la législation étatique, même plus protectrice**. Nous assistons à une sorte de nivellement par le bas qui n'est guère souhaitable. Le texte aurait du ménager la possibilité pour les Etats de conserver des législations plus protectrices.

La nouvelle loi fédérale n'est donc pas destinée à éradiquer les pourriels, mais plus à établir un cadre juridique énumérant clairement les conditions de licéité d'un message non sollicité. Il s'agit donc de préserver les internautes des formes les plus agressives de pourriels notamment, les messages

trompeurs, déloyaux ou à caractère pornographique. **Il ne s'agit donc pas de protection de la vie privée ou du droit d'être laissé tranquille, mais plus, de réguler les pratiques commerciales et de garantir le respect des bonnes mœurs**.

La lutte contre les pratiques trompeuses et déloyales
Si les courriels non sollicités sont d'une certaine manière légalisés, les pratiques les plus agressives sont cependant lourdement sanctionnées. En effet, la modification des entêtes du message dans le but de **tromper la personne** quant à l'identité de l'expéditeur est désormais punie non seulement par une amende, mais encore par une peine d'emprisonnement pouvant aller jusqu'à trois ans. Ces sanctions sont alourdies en cas de récidive. Si les entêtes du message ne doivent pas induire le destinataire en erreur, il en va de même du sujet du message. Le texte nouveau n'évoque pas le contenu même du message qui relève du droit de la consommation (consumer law).

Le texte se propose également de **réglementer la collecte des adresses électroniques** en prohibant les aspirateurs et leurs dérivés ainsi que les générateurs aléatoires d'adresses électroniques. De même l'enregistrement de plusieurs noms de domaine ou la création de plus de cinq comptes de messagerie électronique sous une fausse identité dans le but d'envoyer des courriels à caractère commerciaux sera passible d'une peine d'amende et d'emprisonnement pouvant aller jusqu'à trois ans.

La protection des bonnes moeurs
Le Congrès a finalement consacré l'opt-in pour les messages commerciaux à caractère pornographique, (*« sexually oriented material »*), à moins que le courriel comporte un élément, à établir par la FTC, mettant en évidence sa nature « explicite ». Les personnes qui contreviendraient à cette disposition encourent des sanctions pouvant aller jusqu'à **deux cent cinquante mille dollars (250.000$) d'amende [9] et une peine d'emprisonnement de cinq ans**. Si les sanctions sont fortes, il est cependant toujours opportun de s'interroger sur le sort du message à caractère pornographique mais non commercial qui ne rentre par conséquent pas dans le champ d'application du texte. S'il est adressé à un enfant, il sera prohibé par le *Children's On-line Privacy Protection Act de 1998* (COPPA) [8]. En revanche, le courriel non sollicité à caractère pornographique mais non-commercial adressé à un adulte ne pourra être sanctionné que si le destinataire arrive à établir l'un des griefs suivants : Invasion of privacy, Trepass to property, Trepass to chattels, Unjust enrichment, Misrepresentation, Negligence, torts...
Le Controlling the Assault of Non-Solicited Pornography est une réaction symptomatique des préoccupations américaines. Il faut rappeler que les Etats-Unis ne sont pas dotés d'un texte général garantissant la protection de la vie privée comme peuvent le faire l'article 9 du code civil français et la loi 78/17 du 5 janvier 1978, dite « informatique et Libertés ». Le nouveau texte américain n'a donc pas à s'intégrer dans une architecture juridique préexistante et a été d'autan plus influencé par le douloureux conflit entre les acteurs du marché et les défenseurs des libertés individuelles. Un texte fédéral a finalement été adopté sous la menace de voir les messageries électroniques reléguées au rang d'outils inutilisables. Il s'agit donc d'une protection minimum, mais qui a néanmoins le mérite de lever la menace d'inconstitutionnalité qui planait sur plusieurs législations étatiques. Naturellement à l'heure ou non seulement l'Europe, mais aussi certains Etats de la fédération et non des moindres puisqu'il s'agit de la Californie consacrent, l'opt-in nous ne pouvons que constater l'absence de

rapprochement des positions européennes et américaines dans le domaine de la protection de la vie privée sur les réseaux informatiques. Cette initiative législative fédérale a été approuvée par la chambre des Représentants avec une écrasante majorité de 392 votes pour et seulement 5 contre ce qui traduit une volonté quasi universelle d'endiguer le phénomène des pourriels. Il n'en reste pas moins qu'il semble difficile d'organiser une lutte efficace sans un consensus international. Cette volonté américaine de légiférer au niveau fédéral, sans être dupe des motivations de la DMA notamment, est néanmoins un signe fort apportant de l'eau au moulin des partisans d'un cadre juridique global de la privacy de plus en plus discuté au niveau fédéral.

14/11/2003

Le principe de disponibilité des données publiques : mythe ou réalité ?

Auteur : M. Sulliman Omarjee *Juriste* .

Domaine : Informatique et libertés

Sous thème : Administration_electronique

Ordre juridique :

Abstract :

données publiques, diponibilité des données publiques, information, information publique, bases de données, droit d'auteur de l'etat, concurrence

Ce principe en vertu duquel les données produites par l'administration dans le cadre de leur activité de service publique devraient être mises à la disposition du public souffre en effet d'une absence de consécration législative.

Le principe de disponibilité des données publiques : mythe ou réalité ? (1) L'enjeu est pourtant de taille lorsque l'on sait que le marché des données publiques représente 10 milliards d'Euros en France et 68 milliards d'Euros en Europe (source : Pyra International)

Certes, il existe bien quelque textes qui prônent la reconnaissance de son existence : la Commission Européenne dans son soucis de construire un marché européen de l'information, a émis une « proposition de directive concernant la réutilisation et l'exploitation commerciale des informations du secteur public » qui se prononce en ce sens, mais demeure toujours en cours de discussion. De même, la récente recommandation du Forum des Droits sur l'Internet intitulée « Quelle politique de diffusion pour les données publiques » invite à sa consécration. Enfin, au niveau national, le défunt projet de loi sur la société de l'information du précédent gouvernement Jospin comportait une disposition affirmant le principe dans son volet consacré aux données publiques. L'actuel gouvernement a cependant préféré ne pas reprendre cette question dans son projet de loi CEN, laissant la construction du cadre juridique de la disponibilité des données publiques toujours en chantier.

Faut il pour autant en conclure qu'en l'absence de consécration législative, ce principe ne serait qu'un mythe ?

Retrouvez l'ensemble de l'étude de M.Omarjee au format pdf (11 pages, 116Ko) en vous rendant dans la rubrique *"Informatique et Libertés"* ou en cliquant directement sur ce lien : *Le principe de disponibilité des données publiques : mythe ou réalité ?*

09/11/2003

Application classique des règles de la distribution sélective au commerce électronique

Auteur : Me. Nicole Bondois *Avocate* et M. Nicolas Samarcq *Juriste BRM AVOCATS*.

Abstract :

Domaine : Commerce électronique

Sous thème : Droit de la concurrence

Ordre juridique :

Le 30 janvier dernier, le Tribunal de commerce de Bobigny a ordonné à la société « Rue Du Commerce » de retirer de l'ensemble de ses sites internet les matériels hifi des marques « Onkyo » et « Jamo » que la société Jamo France réserve à son réseau de distribution sélective.

Le cybermarchand a interjeté appel de cette ordonnance, estimant notamment que le juge de l'urgence était incompétent en l'absence de trouble manifestement illicite ou de dommage imminent (conditions qui subordonnent sa compétence [1]).

A ce stade de la procédure, il est utile de rappeler qu'un réseau de distribution sélective est « *un système de distribution dans lequel le fournisseur s'engage à vendre les biens ou les services contractuels, directement ou indirectement, uniquement à des distributeurs sélectionnés sur la base de critères définis, et dans lequel ces distributeurs s'engagent à ne pas vendre ces biens ou ces services à des distributeurs non agréés[2]*.».

Ce mode de commercialisation déroge au principe de liberté du commerce et de l'industrie, de sorte qu'il n'est admissible que s'il a un effet positif sur la concurrence sous peine d'être lui-même illicite.

Au niveau communautaire, le règlement d'exemption du 22 décembre 1999[3] a consacré expressément la licéité des réseaux de distribution, dont la validité n'avait jusqu'à alors été reconnue que par la jurisprudence[4].

Pour mémoire, un réseau de distribution sélective sera licite dès lors qu'il contribue « *à améliorer la production ou la distribution des produits ou à promouvoir le progrès technique ou économique, tout en réservant aux utilisateurs une partie équitable du profit qui en résulte[5]* ».

Et s'il est démontré :

- qu'un tel système est nécessaire de par la nature des produits distribués afin d'en préserver la qualité et d'en assurer le bon usage,

- que le choix des revendeurs est opéré sur la base de critères objectifs (de caractère qualitatif), fixés de manière uniforme et appliqués de façon non discriminatoire,

- et qu'enfin les critères ainsi définis ne vont pas au-delà de ce qui est strictement nécessaire pour assurer une commercialisation dans des conditions optimales des produits.

Ces conditions ont été jugées indispensables pour qu'un réseau de distribution sélective ne puisse restreindre ou fausser le jeu de la concurrence à l'intérieur du marché commun et tomber sous le couperet de l'article 81 §1 du Traité CE.

Au regard de la réglementation européenne et française ci-dessus rappelée, la Cour d'appel[6] a considéré que le réseau de distribution sélective mise en place par Jamo France n'était pas contestable puisqu'il s'applique à des produits présentant « *une haute technicité dans le domaine de la haute fidélité, qui justifie des conditions de commercialisation particulières afin d'en préserver la qualité et le bon usage, ainsi que le renom* ».

Ainsi, la société « Rue Du Commerce » en commercialisant certains produits du réseau de distribution, sans en être membre, a-t-elle porté « *atteinte à l'unité et l'intégrité de celui-ci, tout en pratiquant des prix nettement plus bas* » ce qui constitue, de surcroît, des actes de concurrence déloyale.

Cet arrêt rappelle utilement que les règles de la distribution sélective sont également applicables au e-commerce.

04/11/2003

Le rôle de l'administrateur réseau dans la cybersurveillance

Auteur : Me. Murielle-Isabelle Cahen *Avocate* .

Abstract :

Domaine : Informatique et libertés

Sous thème : droit social, droit du travail

Ordre juridique :

La cybersurveillance peut être définie comme tout moyen de contrôle technique, sur une personne ou un processus, lié aux nouvelles technologies et plus particulièrement aux réseaux numériques de communication. Plus précisément, la cybersurveillance regroupe les voies et moyens aboutissant à l'accès des données ou signaux transmis par voie électronique ainsi que le contrôle des moyens techniques permettant ces transmissions.

Plus précisément, la cybersurveillance regroupe les voies et moyens aboutissant à l'accès des données ou signaux transmis par voie électronique ainsi que le contrôle des moyens techniques permettant ces transmissions. La cybersurveillance se fait techniquement, au moyen de logiciels de surveillance permettant d'enregistrer tous les évènements ou messages survenus pendant un temps donné et à un endroit déterminé. Les écoutes téléphoniques font partie intégrante de la cybersurveillance, tout comme le traçage d'internautes sur le web ou encore sur un réseau Intranet. La surveillance et l'interception de courriers électroniques sont considérés comme de la cybersurveillance.

La cybersurveillance peut être utile, tant pour des raisons de sécurité et de bonne gestion d'un système informatique que pour des raisons de vérification de la bonne transmission de correspondances. Elle est le fait de l'administrateur réseau. Celui ci a plusieurs fonctions au sein de l'entreprise :

- Il gère l'utilisation du réseau en s'occupant de toutes les instructions qui réglementent l'accès au système d'information
- Il gère la configuration du réseau, il fait évoluer l'architecture conçue par l'ingénieur en fonction des besoins des usagers
- Il participe à la gestion technique des équipements. Cet à dire qu'il réceptionne les matériels d'informatiques et de télécommunications, il les teste, les adapte, les insère dans le réseau en fonctionnement et effectue le suivi du parc de matériel
- Il a un rôle de conseil, il informe l'utilisateur des performances des matériels et logiciels et lui sert de guide en cas de difficulté

- Il est responsable de l'enregistrement des nouveaux utilisateurs et de la répartition des droits d'accès ainsi que de l'installation du système d'exploitation réseau et de la sécurité des données sur l'ensemble du réseau.

Il peut accéder, une fois qu'il est inscrit comme utilisateur privilégié du réseau, à toutes les fonctionnalités du système (par exemple accès en lecture et en écriture à toutes les données ou bien modification du profil des utilisateurs). L'administrateur réseau peut ainsi, dans le cadre d'une cybersurveillance, accéder à toutes les correspondances privées ou non des utilisateurs du réseau puisque le réseau est une structure permettant à plusieurs entités d'échanger des informations. En matière de correspondances privées et plus précisément de messagerie électronique des utilisateurs du réseau , l'administrateur à donc un large pouvoir de contrôle.

L'on peut donc s'interroger sur la portée et les limites des pouvoirs de l'administrateur réseau dans la cybersurveillance. Comment concilier l'objectif de sécurité du réseau et la non atteinte à la vie privée des utilisateurs ?

Le courrier électronique doit être considéré comme une correspondance privée

L'arrêt *Nikon* de la Cour de Cassation en date du 2 octobre 2001, considéré comme un arrêt de principe par la doctrine, a érigé au rang de correspondance privée le courrier électronique, devant bénéficier à ce titre de la protection de la loi du 10 juillet 1991 sur les télécommunications. La Cour de Cassation a rendu sa décision en se fondant sur l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, l'article 9 du Code civil, l'article 9 du nouveau Code de procédure civile et l'article L. 120-2 du Code du travail.

Dans cette affaire, un employeur avait pris connaissance des messages électroniques personnels de l'un de ses salariés. La Cour de Cassation a considéré 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* " qualifiant ainsi implicitement le courrier électronique de correspondance privée.

Un arrêt en date du 17 décembre 2001 de la Cour d'appel de Paris a apporté un éclairage nouveau sur l'utilisation de la messagerie électronique après l'arrêt *Nikon* et a contribué à définir le rôle de l'administrateur réseau dans toutes entreprises, et non plus seulement dans une relation employeur - employé. Dans cette affaire, plusieurs incidents étaient intervenus au sein du laboratoire de l'Ecole supérieure de physique – chimie de Paris. Des soupçons sur un étudiant ont conduit trois cadres de l'école à exercer une surveillance des courriers électroniques de l'étudiant. Les faits poursuivis se sont passés dans le cadre de l'utilisation d'un réseau de télécommunication Internet et relevaient donc des dispositions de l'article 432-9 du Code pénal disposant que " *Le fait, par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public, agissant dans l'exercice ou à l'occasion de l'exercice de ses fonctions ou de sa mission, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, le détournement, la*

suppression ou l'ouverture de correspondances ou la révélation du contenu de ces correspondances, est puni de trois ans d'emprisonnement et de 45000 euros d'amende. Est puni des mêmes peines le fait, par une personne visée à l'alinéa précédent ou un agent d'un exploitant de réseau de télécommunications autorisé en vertu de l'article L. 33-1 du code des postes et télécommunications ou d'un fournisseur de services de télécommunications, agissant dans l'exercice de ses fonctions, d'ordonner, de commettre ou de faciliter, hors les cas prévus par la loi, l'interception ou le détournement des correspondances émises, transmises ou reçues par la voie des télécommunications, l'utilisation ou la divulgation de leur contenu ".

La Cour d'appel a considéré qu'il y avait divulgation de correspondances émises, transmises ou reçues par voie de télécommunication. Elle a confirmé le jugement de première instance du TGI de Paris dans ses dispositions pénales tout en les assortissant du sursis, considérant notamment que les prévenus étaient " *confrontés à une situation inédite qui perturbait gravement le fonctionnement d'un laboratoire scientifique de haut niveau* ".

Il résulte de ces dispositions une nécessaire mais difficile cohabitation entre l'objectif de sécurité du réseau de l'administrateur et la non atteinte à la vie privée par l'interception et la divulgation de correspondances électroniques.

L'objectif de sécurité du réseau face à la vie privée des utilisateurs

L'administrateur réseau, dans le cadre de son travail, peut être amené à prendre connaissance des messages privées des utilisateurs du réseau. La Cour d'appel a rappelé qu' " *il est dans la fonction des administrateurs de réseaux d'assurer le fonctionnement normal de ceux-ci ainsi que leur sécurité ce qui entraîne , entre autre, qu'ils aient accès aux messageries et à leur contenu, ne serait ce que pour les débloquer ou éviter des démarches hostiles* "

De ce fait, " *la préoccupation de la sécurité du réseau justifiait que les administrateurs de systèmes et de réseaux fassent usage de leurs positions et des possibilités techniques dont ils disposaient pour mener les investigations et prendre les mesures que cette sécurité imposait* ", de la même façon que la Poste doit réagir à un colis ou une lettre suspecte. Néanmoins l'accès aux messages et l'interception de ceux ci est différent. Si l'administrateur réseau peut " accéder " aux messages électroniques, il ne peut les intercepter, conformément à l'alinéa 2 de l'article 432-9 du code pénal.

La Cour d'appel, dans l'arrêt précité du 17 décembre 2001, a redéfinit la notion d'interception, infirmant sur ce point la décision du tribunal de première instance qui s'était référé à une définition de l'interception consistant en " *une prise de connaissance par surprise* ". La Cour d'appel, elle, a adopté une conception restrictive de la notion d'interception, subordonnant sa qualification au recours à des manœuvres. Selon elle, il n'y a interception que lorsque la lecture et la retranscription de messages (qui peuvent être des e-mails) nécessitent une " *dérivation* " ou un " *branchement* " et est effectué avec un quelconque " *artifice* " ou " *stratagème* ". En l'espèce, la Cour a jugé que les actes incriminés ne répondaient pas à la qualification d'interception, l'administrateur réseau prenant connaissance des messages dans l'exercice de ses fonctions.

L'administrateur réseau est donc autorisé, dans le cadre de sa fonction et de son objectif de sécurité du réseau, à accéder aux messages des utilisateurs

lorsque cet accès est légitimé par la nécessité d'assurer le bon fonctionnement dudit réseau. Il ne peut cependant en aucun cas intercepter les messages privés, violant ainsi l'article 432-9 du code pénal dans le cas contraire. En outre il convient de relever que le laboratoire s'était donné à lui-même la règle déontologique de ne pas lire le contenu du courrier électronique sauf mise en cause de la sécurité du système, ce qui n'était pas le cas en l'espèce.

L'arrêt de la Cour d'appel est donc venu " clarifier " le rôle de l'administrateur réseau dans le cadre d'une cybersurveillance. Il relève donc bien de la fonction d'administrateur réseau d'en contrôler l'usage (en l'espèce conformément à la charte RENATER), ce qui implique nécessairement l'accès aux messageries et à leur contenu, mais dans une certaine limite. En revanche, " *la divulgation du contenu des ces messages […]* " ne relevait pas des objectifs de sécurité du réseau. C'est sur ce fondement que la Cour d'appel a condamné l'administrateur réseau, alors que le tribunal était entré en voie de condamnation sur le fondement de l'interception de correspondances

Non divulgation des messages et secret professionnel

C'est donc sur le fondement de la divulgation d'une correspondance privée que les administrateurs réseau ont été condamné. Ceux ci ne peuvent pas divulguer les données auxquelles ils ont accès. Ils sont tenus au secret professionnel. Cependant, comme nous l'avons vu précédemment, les administrateurs réseau semblent avoir un droit de " regard " sur les contenus des messages, dans le soucis d'une bonne gestion du réseau et de sa sécurité, à la condition de ne pas les divulguer.

L'arrêt de la Cour d'appel contribue ainsi à " clarifier " le rôle et la responsabilité de l'administrateur réseau mais le place dans une situation délicate dès qu'il est porté à sa connaissance, dans le cadre de ses fonctions, des faits ou abus dont la seule révélation est susceptible d'engager sa responsabilité pénale.

La jurisprudence se limite à permettre à l'administrateur réseau de prendre des mesures " *que la sécurité impose* ". Or, la divulgation d'informations et de contenus de messages à ses supérieurs hiérarchiques n'est elle pas une mesure que " la sécurité impose " en cas d'atteinte grave, par exemple, à la stratégie de l'entreprise par un salarié ? L'arrêt de la Cour d'appel ne précise pas quelles doivent être ces mesures. Quel sens doit on donner au terme " divulgation " ?

Dans un second rapport sur la cybersurveillance au travail du 11 février 2002, la CNIL a tenté de préciser le rôle des administrateurs réseau. D'après le rapport, ces derniers n'ont pas à exploiter, volontairement ou sur ordre de leur hiérarchie, le contenu de la messagerie des salariés qui reste soumis au secret des correspondances. Cependant, toujours selon le rapport, les administrateurs réseau ne sont pas tenus au secret professionnel dans deux cas :

- Mise en cause du bon fonctionnement des systèmes et de l'intérêt de l'entreprise
- " Dispositions législatives particulières " pouvant contraindre les administrateurs réseau à dévoiler des informations

Malheureusement, ces exceptions restent très vastes et ne déterminent pas de façon précise la marge de manœuvre des administrateurs réseau et des employeurs.

S'agissant plus particulièrement du droit du travail, il est à noté que l'employeur a le droit de contrôler l'activité professionnelle de ses salariés dans certaines conditions :

- La confidentialité des messages personnels du salarié doit être garantie
- L'employeur doit informer le salarié des dispositifs de surveillance mis en place
- L'employeur doit informer le comité d'entreprise ou les délégués du personnel
- Le recours au contrôle doit être motivé et proportionnel au but poursuivi (article L 121-8 du code du travail)
- Une déclaration à la CNIL doit être effectuée en cas d'établissement d'une liste des connexions informatisées du salarié

L'employeur doit ainsi assurer une certaine transparence lors du contrôle et de la surveillance d'un salarié.

En outre, Un administrateur réseau doit-il répondre à la demande qui lui est faite de surveiller les courriers électroniques ou les fichiers des salariés ? Comme nous l'avons vu précédemment, bien qu'ayant accès à l'ensemble des données de l'entreprise dans l'exercice de ses fonctions, l' administrateur réseau n'est pas libre de leur usage. Ainsi, il ne peut divulguer le contenu d'un courrier personnel d'un salarié, y compris à la demande de l'employeur, au risque d'engager sa responsabilité pénale sur le fondement de l'article 226-15 du code pénal ; cet article condamnant le fait d'ouvrir ou de prendre connaissance de mauvaise foi des correspondances destinées à autrui.

Il ressort de toutes ces dispositions que, même si le rôle de l'administrateur réseau dans la cybersurveillance a été éclairé par la jurisprudence de décembre 2001, certaines incertitudes subsistent. En effet, quelle devra être l'attitude d'un administrateur réseau face à un mail personnel d'un employé indélicat ? Ne devrait il pas lui même alerter l'employeur d'agissements déloyaux d'un salarié, conformément à son devoir de bonne administration du réseau, et donc de l'entreprise ?