

# Le rôle de l'administrateur réseau dans la cybersurveillance

Par

Me Martine Ricouart-Maillet  
Avocat, cabinet Bondois Ricouart Maillet  
<http://www.brmavocats.com/>

Caroline Requillart  
Juriste, DESS Cyberspace

email : [contact@brmavocats.com](mailto:contact@brmavocats.com)

## Introduction

Un arrêt de la Cour d'appel de Paris en date du 17 décembre 2001<sup>1</sup> apporte un éclairage nouveau sur l'utilisation de la messagerie électronique après l'arrêt *Nikon*<sup>2</sup> de la Chambre sociale de la Cour de cassation rendu le 2 octobre 2001, considéré par la doctrine comme un arrêt de principe en matière de surveillance des courriers électroniques.

Plusieurs incidents intervenus au sein du laboratoire de l'Ecole supérieure de physique et de chimie de Paris ont éveillé les soupçons sur un étudiant. Trois cadres de l'école ont alors exercé une surveillance de la messagerie électronique de l'étudiant indélicat.

La Cour d'appel a considéré qu'il y avait là divulgation de correspondances émises, transmises ou reçues par la voie des télécommunications, le courrier électronique devant être considéré comme une correspondance privée bénéficiant à ce titre de la protection de la loi du 10 juillet 1991 sur les télécommunications.

Sur ce point, l'arrêt s'inscrit dans la continuité de l'arrêt *Nikon*. Il s'en distingue néanmoins par son contexte : il n'y a en effet aucun lien de subordination entre l'utilisateur de la messagerie et la structure qui l'abrite. Nous sommes ici en matière délictuelle et non plus en matière sociale.

En première instance, le Tribunal de grande instance de Paris, par jugement du 2 novembre 2000<sup>3</sup>, avait condamné le directeur du laboratoire de l'école et deux administrateurs réseau chacun à une amende allant de 5 000 à 10 000 francs pour avoir ordonné et réalisé « *l'interception des messages électroniques de l'étudiant* » sur le fondement de l'article 432-9 du Code pénal qui réprime les atteintes au secret des correspondances par une personne dépositaire de l'autorité publique ou chargée d'une mission de service public.

La Cour d'appel vient confirmer le jugement dans ses dispositions pénales, tout en les assortissant du sursis au motif notamment que les prévenus étaient « *confrontés à une situation inédite qui perturbait gravement le fonctionnement d'un laboratoire scientifique de haut niveau* » et qu'ils ont agi « *dans l'ignorance probable [...] de leur véritable marge de manœuvre* ».

On peut en premier lieu, à la lumière de cette observation, s'interroger sur l'existence de l'élément intentionnel qui doit être constaté et caractériser toute infraction pénale. Peut-il y avoir infraction sans conscience de la commettre ?

D'ailleurs la « probabilité » de l'ignorance ne plaiderait-elle pas en faveur d'une relaxe au bénéfice du doute ? Il nous faut attendre la censure éventuelle de la Cour de cassation sur ces points précis puisque l'étudiant a formé un pourvoi.

---

<sup>1</sup> L'arrêt de la Cour d'appel de Paris du 17 décembre 2001 est disponible sur [foruminternet.org](http://www.foruminternet.org) : [http://www.foruminternet.org/documents/jurisprudence/dossier.phtml?id\\_dossier=15](http://www.foruminternet.org/documents/jurisprudence/dossier.phtml?id_dossier=15).

<sup>2</sup> L'arrêt de la Cour de cassation du 2 octobre 2001 est disponible sur [foruminternet.org](http://www.foruminternet.org) : <http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=171> ; Expertises novembre 2001, p.369 ; Semaine sociale Lamy, n° 1045 et n° 1046, 8 octobre 2001 et 15 octobre 2001.

<sup>3</sup> La décision du Tribunal de grande instance de Paris du 2 novembre 2000 est disponible sur [Juriscom.net](http://www.juriscom.net) : <http://www.juriscom.net/txt/jurisfr/prv/tcorrparis20001102.htm>.

L'arrêt de la Cour d'appel contribue à définir le rôle de l'administrateur réseau de toute entreprise. Ce dernier dispose d'un pouvoir de contrôle des messages électroniques, pouvoir limité par l'interdiction qui lui est faite de divulguer le contenu des messages à ses supérieurs hiérarchiques.

## **I. Le pouvoir de contrôle de l'administrateur réseau**

Le pouvoir de contrôle de l'administrateur réseau sur les e-mails du personnel est justifié, d'une part, par le fait qu'il ne commet pas de véritable interception des messages (A) et, d'autre part, par l'essence même de ses fonctions qui est d'assurer la sécurité du réseau (B).

### **A. l'absence d'interception du courrier électronique**

Le Tribunal de grande instance de Paris avait condamné l'administrateur pour avoir réalisé « *l'interception des messages électroniques de l'étudiant* » sur le fondement de l'alinéa 2 de l'article 432-9 du Code pénal. Le tribunal s'est référé à une définition de l'interception qui consiste dans une « *prise de connaissance par surprise* ». La Cour d'appel a infirmé la décision du tribunal sur ce point.

L'apport intéressant de l'arrêt réside dans la définition que donne la Cour d'appel de la notion d'interception. Ce terme avait déjà fait l'objet d'une interprétation à propos d'appareils « *Tatoo* » et « *Tam-Tam* » et à l'occasion de l'écoute d'une conversation téléphonique.

La Cour a appliqué ces solutions aux e-mails. Selon elle, il n'y a interception que lorsque la lecture et la retranscription de messages nécessitent une « *dérivation* » ou un « *branchement* » et est effectuée avec quelque « *artifice* » ou « *stratagème* ».

En l'espèce, la Cour a jugé que les actes incriminés ne répondaient pas à la qualification d'interception de courrier électronique puisque l'administrateur réseau prend connaissance des messages dans l'exercice de ses fonctions. Ainsi la Cour a-t-elle adopté une conception restrictive de la notion d'interception puisqu'elle subordonne sa qualification au recours à des manœuvres.

Il n'en demeure pas moins que dans les relations salarié-employeur, ce dernier est tenu d'informer le salarié, à travers le règlement intérieur de l'entreprise ou encore une charte, de la mise en place d'une surveillance quelle qu'elle soit. A défaut, le procédé est illicite.

Il se déduit également des fonctions de l'administrateur réseau que son objectif essentiel est d'assurer la sécurité du réseau.

### **B. L'objectif de sécurité 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.* »

L'administrateur réseau peut donc filtrer, contrôler le bon usage de la messagerie par le personnel, légitimé par la nécessité d'assurer le bon fonctionnement et la sécurité du réseau.

Sa fonction en l'occurrence était précisée dans la charte RENATER. En effet, l'établissement est connecté à Internet par l'intermédiaire du réseau RENATER, spécialisé dans le domaine de la recherche. Cette charte prescrit certaines contraintes d'utilisation : usage conforme aux finalités scientifiques, usage légal pour éviter de perturber le réseau, usage licite interdisant de commettre des infractions.

De plus, l'adhérent à RENATER prend l'engagement de respecter et de faire respecter ces prescriptions par tous les utilisateurs.

Il relève donc bien de la fonction de l'administrateur réseau d'en contrôler l'usage selon la charte RENATER, ce qui implique nécessairement l'accès aux messageries et à leur contenu, mais dans quelles limites ?

La Cour est venue apporter un début de réponse. Si « *la préoccupation de la sécurité du réseau justifiait que les administrateurs de réseaux fassent usage de leurs positions et des possibilités techniques à leur disposition pour mener des investigations et prendre des mesures que la sécurité imposait* », de la même façon que la Poste doit réagir à un colis ou à une lettre suspecte, en revanche « *la divulgation du contenu de ces messages [...] ne relevait pas de ces objectifs.* »

## II. L'interdiction de divulgation

L'administrateur réseau ne peut pas divulguer les données auxquelles il a accès, il est tenu au secret professionnel (A). L'interdiction de communication de ces données aux supérieurs hiérarchiques n'exclut pas pour autant les actions de vérification et de contrôle. L'employeur dispose-t-il en effet d'autres solutions (B) ?

### A. Soumission de l'administrateur réseau au secret professionnel

L'arrêt de la Cour d'appel confirme la condamnation de l'administrateur réseau pour avoir divulgué à ses supérieurs le contenu des messages dont il avait pris connaissance, alors que le Tribunal était entré en voie de condamnation sur le fondement de l'interception de correspondances.

La Cour dit clairement et de façon didactique en analysant la notion d'interception au regard de la définition du dictionnaire et de son interprétation à la lumière de décisions récentes, que l'administrateur réseau ne se rend pas coupable d'une « *interception* » car il n'utilise aucun artifice, aucun stratagème. Il est dans ses attributions « *d'avoir accès aux messageries et à leur contenu ne serait ce que pour les débloquer ou éviter des démarches hostiles* ».

Cet arrêt semble donc donner un statut particulier à l'administrateur réseau qui serait « *habilité* » à lire les contenus des messages, mais à la condition de ne pas les divulguer.

Au cas d'espèce, l'administrateur réseau avait mis en place une véritable surveillance de la messagerie de l'étudiant afin de connaître le contenu des correspondances émises ou reçues, à la demande du Directeur du Laboratoire.

L'arrêt de la Cour d'appel contribue à clarifier le rôle et la responsabilité des administrateurs réseau. Cependant, il les place dans une situation délicate dès lors que, dans le cadre des contrôles auxquels ils procèdent, ils sont confrontés à des abus et à des indélicatesses dont la seule révélation est susceptible d'engager leur responsabilité pénale.

Dès lors, quelle devra être leur attitude face à la constatation de faits graves préjudiciables à l'entreprise (fuite d'informations stratégiques par exemple) ? L'arrêt ne répond bien évidemment pas à cette question cruciale qui nécessairement va se poser en pratique, se limitant à permettre à l'administrateur réseau de prendre des mesures « *que la sécurité impose* ».

Quelles sont ces mesures ? La cour ne le dit pas. Comment l'administrateur peut-il mettre un terme à un comportement frauduleux sans en informer la personne qui détient le pouvoir de décision ?

Ce qui revient à s'interroger sur la signification à donner au terme de « *divulgation* » que la Cour n'explique pas véritablement. Le texte pénal est quant à lui plus précis puisqu'il incrimine la simple « *révélation du contenu* ».

Le sujet est sensible et la CNIL (*Commission Nationale Informatique et Libertés*) a récemment pris en compte les inquiétudes des administrateurs réseau en demande de règles du jeu plus claires. Ainsi, dans un second rapport sur la cybersurveillance au travail en date du 11 février 2002, la CNIL a-t-elle tenté de préciser le rôle de ces derniers. Selon ce rapport, les administrateurs de réseaux 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. Le rapport de la CNIL est donc dans le droit fil de l'arrêt commenté.

Néanmoins, le rapport précise que les administrateurs sont libérés du 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.

Cependant, ces exceptions ne répondent pas de façon précise aux questions ci-dessus quant à la marge de manœuvre des administrateurs réseau et de l'employeur.

L'employeur dispose-t-il de solutions alternatives qui lui permettent de contrôler les e-mails de ses salariés ?

## **B. Les alternatives à l'interdiction de divulgation**

Une première solution préventive consiste à respecter les conditions du droit social d'exercice du pouvoir de contrôle de l'employeur.

En effet, l'employeur a le droit de contrôler l'activité professionnelle de ses salariés s'il respecte un certain nombre de conditions :

- la confidentialité des messages « *personnels* » des salariés doit être garantie par l'entreprise et ce même si l'employeur a dans le cadre d'une charte réservé la messagerie à un strict usage professionnel, comme l'a confirmé l'arrêt de la Cour de cassation du 2 octobre 2001 ;
- les salariés doivent être informés sur les dispositifs de surveillance auxquels ils sont soumis (Code du travail, art. L. 121-8). Tout contrôle effectué à l'insu des salariés est illégal ;
- à cette information des salariés s'ajoute celle du comité d'entreprise ou, à défaut, des délégués du personnel. En effet, le comité d'entreprise doit être informé et consulté sur les moyens ou les techniques permettant un contrôle de l'activité des salariés préalablement à leur mise en œuvre (Code du travail, art. L. 432-2-1). L'information doit permettre au comité de donner son avis sur la pertinence et la proportionnalité entre les moyens utilisés et le but recherché ;
- dans le même sens, le recours au contrôle doit être motivé et proportionnel au but poursuivi (Code du travail, art. L. 120-2). Cette condition est remplie en cas de faits jugés graves par l'administrateur réseau ;
- enfin, si le contrôle permet d'établir une liste des connexions informatiques du salarié, il y a alors « *traitement automatisé de données personnelles* » ce qui justifie l'application de la loi « *informatique et libertés* » ; L'entreprise devra alors procéder à une déclaration simplifiée à la CNIL. Le système de contrôle ne pourra entrer en vigueur qu'après délivrance par la CNIL d'un récépissé de déclaration, ce dernier ne pouvant être refusé.

Le respect de ces conditions cumulatives devrait normalement permettre à l'employeur de procéder au contrôle des messages électroniques de ses salariés puisque ce contrôle s'effectue dans la transparence.

Cependant, la jurisprudence antérieure et l'arrêt commenté ne semblent pas aller dans ce sens et sous-entendent au contraire que l'employeur ne pourra agir en toute loyauté qu'après avoir avisé le salarié non pas des possibilités d'un contrôle mais de sa date !

C'est ce qui ressort d'un arrêt de la Cour d'appel de Montpellier, Chambre sociale du 6 juin 2001<sup>4</sup>, qui dans le cadre d'un licenciement a jugé illicite la preuve rapportée par un employeur, la lettre de licenciement reposant sur des constatations effectuées par voie d'huissier, en l'absence du salarié.

---

<sup>4</sup> L'arrêt de la Cour d'appel de Montpellier du 6 juin 2001 est disponible sur [foruminternet.org](http://foruminternet.org) : <http://www.foruminternet.org/documents/jurisprudence/lire.phtml?id=173> ; Communication commerce électronique, nov. 2001, p. 30, observations Agathe Lepage.

Il faut en déduire dans ces conditions que seul le contrôle contradictoire en présence du salarié des messages ne portant pas la mention « personnel » est possible.

Cette seule solution n'est évidemment pas satisfaisante pour l'employeur en cas de constatation ou de suspicion de faits graves nécessitant des mesures non contradictoires.

L'employeur, alerté par l'administrateur réseau grâce à un contrôle statistique ou à un filtrage par mots clés, pourra à l'évidence accumuler les indices lui permettant de solliciter en justice sur requête l'autorisation de faire saisir les traces informatiques des messages du salarié enregistrés sur la mémoire du disque dur.

Le recours à justice de l'employeur se fonde alors sur l'avertissement donné par l'administrateur réseau et la révélation d'indices graves, sans toutefois que ce dernier ne puisse révéler le contenu des messages.

Le juge saisi sur requête appréciera alors les faits incriminés en vertu de son pouvoir d'appréciation souverain. Le juge doit en effet effectuer un contrôle de légalité et de proportionnalité *a priori* de l'action future de l'employeur. Les faits sont-ils suffisamment graves et préjudiciables à l'entreprise pour justifier la surveillance systématique et ciblée de messages électroniques par l'employeur afin qu'il puisse prendre toute disposition de nature à mettre un terme au trouble causé ?

Certains commentateurs de l'arrêt *Nikon*<sup>5</sup> n'ont pas hésité à opposer dans ces hypothèses les notions de légitime défense et de droit à une légitime surveillance de l'employeur.

Les juridictions du fond ont d'ailleurs été sensibles à l'attitude peu scrupuleuse de certains salariés et n'ont pas hésité à la sanctionner. Elles le feront d'autant plus facilement que le contrôle aura été effectué avec la bénédiction du juge.

M. R.-M. & C. R.

---

<sup>5</sup> J. Deveze et M. Vivant : courrier électronique professionnel et secret : où l'oubli du « flexible droit » conduit à un déni de droit , chron. n° 24, communication, commerce électronique, nov.2001.