L'administrateur réseau : un voltigeur sans filet

Laurence Freyt-Caffin
GIP Renater
Responsable des affaires juridiques
151 Boulevard de l'Hôpital
75013 Paris
laurence.freyt@renater.fr

14.10.2003

Résumé

L'administrateur réseau : un voltigeur sans filet

L'administrateur réseau est à ce jour l'homme de toutes les situations. Il lui appartient d'assurer la sécurité du réseau au risque de voir sa responsabilité engagée. Il doit en outre opérer ce contrôle tout en veillant au respect des données personnelles des salariés couvertes par le secret des correspondances et par le droit à la vie privée.
C'est pourquoi la jurisprudence lui a conféré un statut particulier. Il doit toutefois agir dans la transparence, la loyauté et avec cohérence et reste soumis à une obligation stricte de confidentialité même vis à vis de sa hiérarchie sur les données auxquelles il pourrait avoir accès dans le cadre de sa mission. La mise en place d'une charte interne, si elle ne permet pas de solutionner la lourde mission qui incombe à l'administrateur, permet tout de même de rappeler le cadre juridique existant et les usages pratiqués dans l'entreprise.

Mots clefs :
Administrateur réseau, droit, statut, données personnelles, CNIL, divulgation, secret professionnel, cybersurveillance, vie privée, divulgation, responsabilité, sécurité, loyauté, transparence, contrôle, secret, correspondances, fichiers.

Introduction

Des intérêts antinomiques mais légitimes sont à gérer dans une entreprise.

L'employeur souhaite protéger les intérêts de son entreprise en protégeant la fuite des informations stratégiques, en prévenant l'apparition de virus ou encore en empêchant la circulation de contenus illicites notamment racistes ou pornographiques sur le réseau. Cela passe par la sécurisation de son réseau.
A l'inverse nombre de salariés revendiquent le droit à une vie privée sur leur lieu de travail qui se matérialise par une connexion à Internet à des fins personnelles. Cette opportunité est pour eux la contre-partie de la porosité entre la sphère professionnelle et la sphère privée intensifiée par l'utilisation des nouvelles technologies.

Afin d'encadrer et de limiter un usage excessif de l'Internet sur le lieu de travail, l'employeur dispose au titre de son pouvoir de direction d'un droit de contrôle et de surveillance sur ses salariés[1]. Mais ce pouvoir reconnu à l'employeur ne doit pas méconnaître les principes du droit à la vie privée et du secret des correspondances.
En effet, la Commission Nationale de l'Informatique et des Libertés (CNIL) a reconnu au salarié le droit à une vie privée au travail en soulignant qu'il était à la fois irréaliste et disproportionné d'interdire strictement une utilisation d'Internet à des fins personnelles.

L'administrateur réseau est au carrefour de ses deux logiques. En effet, il est la personne en charge d'assurer à la fois la sécurité du réseau, à la demande de son autorité hiérarchique qui voit en lui un moyen de faire face aux situations périlleuses, et la sécurité des données professionnelles et personnelles des salariés.

[1] Cass. Soc 14 mars 2000 Dujardin c/ Sté Instinet

1.Rôle de l'administrateur réseau

1.1 Missions de l'administrateur réseau

L'administrateur réseau est chargé de la mise en place du système d'information, de son suivi. Il prévient l'intrusion de virus, veille à l'utilisation optimale du réseau et assure la sécurité des données de l'entreprise.

Les directives communautaires[2] comme la « Loi Informatique et Liberté »[3] lui confèrent l'obligation d'assurer la sécurité des traitements informatiques. Au regard de l'article 29 de la loi précitée, il s'engage, vis-à-vis des personnes concernées, *à prendre toutes les précautions utiles* afin de préserver la sécurité des informations et notamment d`empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non-autorisés[4].
La loi prévoit donc une obligation de moyen alors que la directive 95/46 dans son article 17 semble énoncer une obligation de moyen renforcée dans la mesure où le responsable sécurité « *doit mettre en œuvre* les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite ».
La question de la nature de l'obligation n'est pas solutionnée dans la directive 2002-58 du 12 juillet 2002 qui l'invite d'une part à « prendre les mesures appropriées pour assurer la sécurité de leurs services » et d'autre part à « un devoir d'information des risques encourus par les utilisateurs ».

1.2 Le statut de l'administrateur réseau

Il est incontestable que l'administrateur réseau ne peut garantir la sécurité du réseau ou des outils informatiques s'il ne dispose pas à cet effet des moyens nécessaires à la réalisation de sa mission. Cela implique que celui-ci ait accès à toutes les données contenues dans les messageries ou les fichiers des utilisateurs.

La Cour d'appel dans un arrêt du 17 décembre 2001, « ESPCI » (l'école supérieure de physique et chimie industrielle), a énoncé « qu'il est dans la fonction des administrateurs 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 pour débloquer ou éviter des démarches hostiles ».

Pour garantir la sécurité du réseau ou sa bonne utilisation, l'administrateur peut donc avoir accès aux informations des utilisateurs à savoir leur messagerie, leurs connexions à Internet, les fichiers logs ou de journalisations.
Il dispose de plusieurs moyens de contrôle pour vérifier l'utilisation loyale du réseau ou des outils informatiques. Il peut contrôler les débits, identifier la durée des connexions, répertorier les sites les plus fréquemment visités ou les tentatives de connexion. Il peut également contrôler les extensions des pièces jointes d'un fichier, leurs volumes. Il possède à cet effet un mot de passe administrateur qui lui permet d'accéder aux serveurs de fichier, aux serveurs web, aux serveurs de messagerie. Il peut par conséquent avoir accès à l'ensemble des informations émises, reçues, crées par un salarié.

La CNIL a également souligné que « la possibilité pour les salariés ou agents publics de se connecter à Internet à des fins autres que professionnelles peut s'accompagner de prescriptions légitimes dictées par l'exigence de sécurité de l'entreprise » et « que des exigences de sécurité, de prévention ou de contrôle de l'encombrement du réseau peuvent conduire les entreprises ou les administrations à mettre en place les outils de mesure de la fréquence ou de la taille des fichiers transmis en pièces jointes aux messages électroniques ou encore l'archivage des messages échangés »[5]

---

[2] Directives 95/46/CE relative à la protection des données personnelles et à la libre circulation de ces donnéeS et Directive 2002/58 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive "vie privée et communications électroniques").

[3] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

[4] Article 29 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

[5] Rapport du 5 février 2002 de la CNIL sur la « Cybersurveillance sur les lieux de travail »

La CNIL a également rappelé[6] le statut particulier des administrateurs qui sont conduits par leurs fonctions même à avoir accès à l'ensemble des informations relatives aux utilisateurs… et qu'un tel accès, tout comme l'utilisation de logiciels de télémaintenance, n'est contraire à aucune disposition de la Loi Informatique et Libertés du 6 janvier 1978[7].

Il appartient à l'administrateur réseau d'user des moyens techniques mis à sa disposition pour assurer la sécurité du réseau et il est tout à fait légitime que ce dernier s'en serve afin de déterminer la cause du problème.
Par conséquent la jurisprudence comme la CNIL reconnaissent un statut particulier à l'administrateur réseau en convenant que par la nature même de sa fonction il peut avoir accès aux messageries ou connexions Internet afin de garantir la sécurité du réseau – mission dont il est le garant.

Toutefois ce statut atypique est limité par le secret professionnel et par des modalités de contrôle encadrées.

2. Un contrôle limité et encadré

2.1 L'obligation de confidentialité

Qui dit confidentialité, dit données confidentielles c'est à dire vie privée.
L'arrêt Nikon de la cour de cassation du 2 octobre 2001[8] a reconnu le droit au salarié, « même au temps et 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 ».
La Cour se fonde sur les principes de l'article 8 de la Convention européenne de sauvegarde des Droits de L'Homme et des Libertés fondamentales[9], de l'article 9 du Code civil[10], de l'article 9 du Nouveau code de procédure civile et l'article L120-2 du Code du travail.
La Cour applique aux messages électroniques les dispositions de l'article 226-15 du Code pénal[11].

L'administrateur est soumis au secret professionnel et ne peut divulguer les données personnelles auxquelles il a accès. Cette obligation de confidentialité qui pèse sur lui concerne aussi bien le contenu d'un message personnel dont les dispositions sont couvertes par le secret des correspondances qu'un fichier personnel dont les dispositions relèvent de la vie privée des utilisateurs.

Si la jurisprudence reconnaît la possibilité à l'administrateur de lire les contenus des messages, il n'est pas en revanche autorisé à les divulguer même à ses supérieurs hiérarchiques[12].
La question que tout administrateur est alors légitimement en droit de se poser est « comment réagir face à une situation grave et préjudiciable pour l'entreprise ? ». L'arrêt ne formule pas de réponse précise en autorisant celui-ci à prendre les dispositions « que la sécurité impose ».
Ainsi la délicate mission de l'administrateur sera de mettre fin au comportement frauduleux ou préjudiciable sans en informer son supérieur hiérarchique qui dispose pourtant de l'autorité et du pouvoir de décision.

---

[6] Rapport du 5 février 2002 de la CNIL concernant la « Cybersurveillance sur les lieux de travail »
[7] Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
[8] Cass. Soc. 2 octobre 2001 Nikon France SA c/ M. O
[9] « Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance »
[10] (Loi nº 94-653 du 29 juillet 1994 art. 1 I Journal Officiel du 30 juillet 1994)
Chacun a droit au respect de sa vie privée.
Les juges peuvent, sans préjudice de la réparation du dommage subi, prescrire toutes mesures, telles que séquestre, saisie et autres, propres à empêcher ou faire cesser une atteinte à l'intimité de la vie privée : ces mesures peuvent, s'il y a urgence, être ordonnées en référé.
[11] (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)
« 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, est puni d'un an 'emprisonnement et de 45000 euros d'amende. Est puni des mêmes faits, le fait commis de mauvaise foi, d'intercepter, de détourner, d'utiliser ou de divulguer des correspondances émises, transmises et reçues par la voie des télécommunications ou de procéder à l'installation d'appareils conçus pour réaliser de telles interceptions. ».
[12] CA Paris, 17 décembre 2001, ESPCI

La Cour d'Appel a sanctionné un administrateur pour avoir informé ses supérieurs sur le contenu des messages auxquels il a eu accès. L'arrêt précise que la divulgation du contenu des messages ne se rattache pas aux objectifs de sécurité des réseaux et doit être sanctionnée sur le fondement de l'article 432-9[13] du Code pénal. La Cour d'appel n'a pas sanctionné en tant que tel l'interception du message mais la divulgation de la correspondance privée bénéficiant à ce titre de la protection de la loi du 10 juillet 1991 sur les télécommunications.
En cas de divulgation des informations, l'administrateur réseau risque d'engager sa responsabilité pénale au titre de l'article 216-15 du code pénal qui condamne le fait d'ouvrir ou de prendre connaissance de mauvaise foi des correspondances destinées à autrui.

2.2 Le contrôle doit être loyal, transparent et proportionné.

Pour remplir son obligation de sécurisation sans entraver les droits des salariés, l'administrateur doit veiller à opérer un contrôle loyal, transparent et proportionné.

Un contrôle loyal

La démarche de l'administrateur doit être impartiale et sincère. Il doit agir dans le cadre de ses fonctions et son action ne doit pas découler d'une initiative personnelle ou d'un ordre hiérarchique mais d'une nécessité justifiée par des impératifs de sécurité. Il appartient à l'administrateur d'agir dans le respect de la vie privée des salariés. Mais où commence la vie professionnelle et où s'arrête la vie privée ? Comment distinguer le mail personnel du mail professionnel ?
La Cour de cassation a reconnu qu'un répertoire de messagerie intitulé personnel est présumé contenir des données personnelles et bénéficie à ce titre de la protection de la vie privée. Il ne saurait être contrôlé par l'employeur.
Dans l'affaire Nikon, la société a licencié un employé en produisant comme élément de preuve un fichier intitulé « personnel » récupéré dans sa messagerie. La Cour de Cassation a sanctionné la société. La CNIL considère qu'un message est présumé professionnel sauf s'il est manifestement indiqué dans son intitulé qu'il s'agit d'un message personnel ou s'il a été archivé dans un répertoire identifié comme tel.

Un contrôle transparent

La démarche de l'administrateur doit se faire dans une logique de transparence vis à vis des salariés. Ces derniers doivent être informés par l'employeur de la mise en place d'un dispositif de contrôle soit en le spécifiant dans le contrat de travail soit au moyen d'une charte informatique[14].
Le comité d'entreprise, ou à défaut les délégués du personnel, devra avoir été informé et consulté préalablement à la mise en place d'un tel dispositif de contrôle[15].
Si le dispositif de contrôle constitue un traitement automatisé de données personnelles alors il doit faire l'objet d'une déclaration simplifiée auprès de la CNIL préalablement à sa mise en œuvre. A ce sujet, la CNIL recommande un contrôle statistique des sites Internet les plus visités par service sans qu'il soit nécessaire de faire un contrôle nominatif individualisé des sites.

A défaut d'information préalable, la preuve rapportée ne sera pas licite et le mode ne preuve constatant l'abus du salarié ne pourra justifier les sanctions prises par l'employeur.

---

[13] (Ordonnance nº 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)
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.

[14] Article L.121-8-1 du Code du Travail : »aucune information concernant personnellement un salarié ou un candidat ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance ».

[15] Article L 432-2-1 du Code du Travail
Article L 432-2 du Code du travail : « le comité d'entreprise est informé et consulté préalablement à tout projet important d'instruction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur les conditions de travail du personnel »
Article 432-2-1 du Code du travail :« le comité d'entreprise doit être informé et consulté préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou techniques permettant un contrôle de l'activité des salariés ».

Un contrôle proportionné

Le contrôle qu'il soit effectué par le supérieur hiérarchique en vertu de son pouvoir hiérarchique ou par l'administrateur réseau dans le cadre de sa fonction doit être proportionnel au but recherché[16]. Il appartient à l'administrateur d'utiliser les moyens permettant de remplir sa mission sans aller au-delà. Il n'y a pas lieu pour l'administrateur réseau de contrôler le contenu même des messages émis ou reçus si le seul contrôle du volume des pièces jointes ou des extensions des fichiers joints lui permet de vérifier l'utilisation optimale du réseau. Son action doit s'inscrire dans une logique cohérente.
A titre d'exemple, l'inscription à des forums de discussion ou le téléchargement des fichiers non autorisés ne requièrent pas l'ouverture des mails pour prouver le manquement du salarié.

Ainsi afin d'opérer un contrôle efficace, l'administrateur doit suivre les principes énumérés ci-dessous.

3. La mise en place d'une charte ?

La mise en place d'une charte, si elle ne permet pas dans l'absolu de clarifier le statut même de l'administrateur réseau, a toutefois pour objet d'informer les salariées sur le dispositif légal et sur l'usage toléré dans l'entreprise ou l'organisme. Cette charte permet de formuler des recommandations.
Le contenu des chartes est très variable d'une entreprise à l'autre selon l'objectif recherché. Certaines constituent un rappel des textes légaux alors que d'autres vont plus loin et dictent une ligne de conduite.
Elles sont alternativement annexées au règlement intérieur, portées à la connaissance des salariés. Selon les cas de figures, l'entreprise demande l'acceptation par le salarié des stipulations intégrées dans la charte ou elle se contente de mettre à leur portée l'information.

Toutefois, il est important de souligner que seule une charte établie selon les modalités du règlement intérieur peut donner lieu à des sanctions disciplinaires. Les prescriptions impératives d'une charte doivent être adoptées selon les mêmes formalités que le règlement intérieur dans la mesure où elle en constitue un additif [17]. Par conséquent la charte doit être soumise au comité d'entreprise pour avis ou à défaut à l'avis des délégués du personnel voire au comité d'hygiène et de sécurité. Elle doit également faire l'objet de publicité et être transmise à l'inspecteur du travail[18]. Toute modification à la présente charte doit s'effectuer selon le même processus.

Conclusion

En cas de constat de pratique illicite ou non conforme du réseau ou de doutes sérieux, l'administrateur réseau devra constituer un dossier suffisamment complet pour attester de cette illégalité ou pour justifier la présomption d'utilisation illicite du réseau. Il avertira ensuite son employeur sans toutefois lui révéler le contenu des messages ou fichiers qui demandera par requête au tribunal compétent l'autorisation de faire procéder à la lecture et /ou à la saisine des fichiers visés.
En pratique, comment pourra-t-il susciter l'intérêt de sa hiérarchie en lui présentant seulement des bribes d'informations ? Telle est la délicate mission de l'administrateur car s'il dévoile le contenu d'un fichier personnel, il verra sa responsabilité pénale engagée.
Si l'employeur pense que l'infraction commise par un de ses salariés au moyen de l'outil mis à disposition par l'entreprise est d'ordre pénale, il se tourner avers la voie pénale. Une plainte au procureur de la République, si elle repose sur des éléments sérieux, entraînera une enquête préliminaire[19]. Au cours de cette enquête, la police judiciaire à des perquisitions, des interrogatoires, ou à la saisine de pièces.

Le forum des droits dans son rapport du 17 septembre 2002 sur la cybersurveillance, recommande que la loi reconnaisse à l'administrateur réseau un véritable secret professionnel. Ce « secret » ne devrait pas couvrir le secret des correspondances mais l'ensemble des contenus personnels du salarié comme ses fichiers. L'objectif étant de définir un réel statut de la fonction même d'administrateur en clarifiant de façon expresse ses droits et obligations à la fois vis à vis des salariés et de son supérieur hiérarchique.

---

[16] Art L 120-2 du Code du Travail : « nul ne peut apporter au droit des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas proportionnées au but recherché »
[17] Article L.122-36 du Code du travail.
[18] Article L. 122-36 du Code du travail
[19] Article 75 et s. du Code de procédure pénale

La CNIL recommande la désignation d'un délégué à la protection des données en concertation avec les représentants du personnel . Ce délégué serait en charge des questions relatives aux mesures de sécurité, au droit d'accès et à la protection des données personnelles. Il pourrait travailler conjointement avec l'administrateur réseau.

La CNIL recommande aux salariés de distinguer leurs fichiers personnels de leurs fichiers professionnels car en dépit de toute mention expresse du caractère personnel d'un message (ou fichier), celui-ci est présumé professionnel et pourra alors être contrôlé par l'employeur. De plus, une telle démarche facilite la tâche de l'administrateur qui, s'il peut contrôler lesdits fichiers, procèdera de façon à vérifier en dernier lieu le contenu des données personnelles.

Références

Textes de lois et règlements français: http://www.Legifrance.fr

Les journaux officiels : http://www.journal-officiel.gouv.fr/

http://www.cnil.fr/index.htm

http://www.droitdunet.fr/

http://www.foruminternet.org

http://www.clic-droit.com

http://www.droit-ntic.com/

Rapport du 5 février 2002 de la CNIL concernant la « Cybersurveillance sur les lieux de travail »
La lettre des Juristes d'Affaires, n°5094-5097, pp970-971
Semaine sociale Lamy, 15 octobre 2001-n°1046, pp 462-465 « Entretien avec Ariane Mole »

Jurisprudence :

CA Paris, 11ème chambre, A, 17 décembre 2001, n°00/07565, Françoise V., Marc F. et Hans H. / ministère public, Tareg Al B.
Cass. soc., 2 octobre 2001, pourvoi N°99-42.942 Nikon France SA c/ M. O