La responsabilité de l’administrateur systèmes et réseaux

Veille juridique



Sommaire

I. Fonctions de l’administrateur Systèmes Réseaux 3

II. Obligation 3

1. Obligations générales d’un salarié 3

2. Obligations spécifiques de l’ASR 4

II. Responsabilités 4

1. La responsabilité civile 5

2. La responsabilité pénale 5

3. Responsabilités spécifiques de l’ASR 5

III. Sanctions 6

IV. Jurisprudence 7

V. Sources 9

## Fonctions de l’administrateur Systèmes Réseaux

Tout d’abord l’administrateur systèmes réseaux exerce son activité au sein d’une DSI ou SSII, sont travail va être définie en fonction de la taille de l’entreprise, l’effectif de la DSI et le recours ou non à l’externalisation (l’entreprise fait appel à une société externe, spécialisée en informatique, pour prendre en charge la gestion de l’informatique).

Un administrateur systèmes réseaux est très polyvalent, il peut être amené à effectuer des taches de développement, bases de données, stockage et sauvegarde, télécoms, cependant le cœur de son travail se repose sur les missions suivantes :

* Installation et paramétrage des équipement et logiciel réseaux et télécoms
* Conduite et participation à des projets relevant de son périmètre
* Mettre en place et contrôler les procédures de sécurité (droits d’accès, mots de passe)
* Apporter son aide aux utilisateurs sur un problème lié au réseau
* Prévenir les anomalies et les pannes de fonctionnement du réseau
* Faire de la veille technologique

## Obligation

### Obligations générales d’un salarié

L’exécution consciencieuse du travail fourni par l’employeur est la principale obligation découlant du contrat de travail. Elle n’est en fait que la contrepartie du salaire versé par l’employeur au salarié. Cette exécution consciencieuse suppose que le salarié adopte un comportement de nature à éviter les erreurs ou négligences répétés.

Le salarié se doit de respecter la discipline, les directives, les clauses du règlement intérieur.

S’il est contraint à un nombre d’heures et à des horaires de travail précis, le salarié doit justifier de ses retards comme de ses absences.

Le salarié est, par ailleurs, redevable d’un devoir de loyauté. Il ne doit pas porter atteinte aux intérêts de l’entreprise en commettant des actes de concurrence déloyale. Toutefois, le contrat de travail peut comporter des clauses qui renforcent cette obligation.

Le salarié est tenu à une obligation de discrétion qui lui interdit de divulguer un certain nombre d’informations auxquelles ses fonctions lui donnent accès. Il s’agit des secrets de fabrication (C. trav., art. L. 1227-1), des renseignements sur la situation financière de l’entreprise, etc.

### Obligations spécifiques de l’ASR

**Responsabilité Loyauté́**

La démarche doit être impartiale, sincère et être uniquement justifiée par un impératif de sécurité́. Elle doit être conforme à la finalité́ pour laquelle le contrôle a été́ décidé́.

**Responsabilité de transparence**

Les acteurs internes à l’organisation ainsi que les tiers doivent être informés de l’éventualité́ d’un contrôle, comme l’administrateur collecte ces données c’est de son devoir de répondre à cette responsabilité

**Obligations de confidentialité**

L’ASR à l’accès à des données personnelles il est soumis au secret professionnel qui l’empêche de divulguer ces données.

**Respect des droits des tiers**

Les acteurs internes à l’organisation ainsi que les tiers doivent être informés de l’éventualité́ d’un contrôle. Le règlement intérieur et la charte informatique informent les acteurs de l’entreprise des dispositifs de contrôle mis en œuvre, afin de respecter la vie privée des tiers ainsi que leur propriétés.

En cas d’atteinte à la sécurité́ du réseau et aux intérêts de l’organisation : l’ASR a l’obligation d’avertir le salarié à l’origine de l’atteinte afin de lui proposer des solutions. Il a également le droit de supprimer des fichiers, mêmes personnels, illicites. Dans un second temps, l’employeur sera informé et pourra prendre des sanctions à l’encontre du salarié négligent.

En cas de contenus illicites (atteinte à l’ordre public, à la sécurité́ intérieure du pays, menace d’actes terroristes, contenus à caractère pédophile, incitation à la haine raciale...), l’ASR a une obligation de dénonciation :

* auprès de son employeur,
* auprès des autorités : services de police, de justice, CNIL.

## Responsabilités

Il faut tout d’abord définir la responsabilité, celle-ci est l'obligation de répondre de certains de ses actes, d'être garant de quelque chose, d'assumer ses promesses. Elle a pour conséquence le devoir de réparer un préjudice causé à quelqu'un de par son fait ou par le fait de ceux dont on a en charge la surveillance, voire de supporter une sanction.

En droit, une personne a l’obligation de répondre d’un dommage :

-          soit envers une victime 🡪 responsabilité civile ;

-          soit envers la société 🡪 responsabilité pénale.

### La responsabilité civile

L’objectif principal de la responsabilité civile est de réparer un dommage causé à autrui.

En pratique, on distingue 2 types de responsabilité civile :

-          contractuelle, dans ce cas il y a réparation d’un dommage lorsqu’un contrat a été mal ou non exécuté.

-     délictuelle ou quasi-délictuelle, s’applique en l’absence de contrat entre l’auteur du dommage et la victime, mais à la suite d’un fait volontaire ou non.

L’auteur d’un dommage a une responsabilité délictuelle s’il a volontairement provoqué le dommage (délit), si le dommage résulte de sa négligence ou de son imprudence sa responsabilité sera alors quasi délictuelle.

### La responsabilité pénale

L’objectif principal de la responsabilité pénale est de punir.

En effet, elle vise d’abord à appliquer à un individu ayant un comportement nuisible à la société une sanction prévue par un texte de loi. Elle ne vise pas la réparation du dommage causé à la victime.

Ainsi, à chaque infraction est attribuée une sanction, crimes délits et contraventions.

### Responsabilités spécifiques de l’ASR

L’administrateur doit respecter un certain nombre de lois, au risque de voir porter sa responsabilité pénale devant les tribunaux.

A partir du moment où l'administrateur récolte d'une façon ou d'une autre des données à caractères personnels, il doit le faire dans le respect des 3 règles du code du travail.

* **Principe de proportionnalité**: Les données à caractère personnel ne peuvent être recueillies et traitées que pour un usage légitime et déterminé
* **Principe de transparence**: Aucune information concernant personnellement un salarié (…) ne peut être collectée par un dispositif qui n’a pas été porté préalablement à la connaissance du salarié
* **Principe de discussion collective**: Tout traitement informatique doit faire l’objet d’une information et consultation auprès du responsable du personnel et du comité d’entreprise.

**L'administrateur doit également respecter la loi informatique et liberté**: Cette loi prévoit que le traitement des données à caractères personnels doit être "non discriminatoire", "confidentiel" et sous la responsabilité du responsable du traitement qui doit déclarer tous types de données qu'il traite.

Au niveau de la **responsabilité civile délictuelle** celle-ci nécessite une faute, un dommage et un lien entre les deux. Par exemple dans le cas d’une intrusion dans un système informatique à l'insu de son utilisateur, le dommage consiste en la perte et /ou la communication de données personnelles et le lien de causalité doit être clairement établi entre cette faute et le dommage subi.

Quand à **la responsabilité pénale** l’administrateur réseaux et systèmes doit avertir l’utilisateur s’il veut collecter des informations personnelles.

Généralement dans les entreprises l’administrateur réseaux et systèmes doit **respecter une charte,** cette chartre contient fréquemment des obligations sur l’archivage, journalisation de données, veille scientifique technologique, attitude à l’égard des violations de la lois et des règles de son entreprise qui l’emploi, c’est à dire que lorsque l’administrateur constate des violations de la loi dans son périmètre d’activité, il en fait rapport au comité de coordination SSI et à ses responsables hiérarchiques, qui prendront les mesures adéquates afin de coordonner leurs actions avec les autorités judiciaires. Il est de la responsabilité de l’ASR de **veiller à la protection des systèmes** informatiques dont il a la charge.

## Sanctions

Une sanction est la conséquence juridique du non-respect d'une règle de droit.

Nous avons vu que l’ASR à des droits sur la manipulation de données personnelles d’autrui, le non respect des obligations qui lui sont conférés peuvent êtres accompagnés de sanctions.

Il existe trois types principaux de sanction juridiques :

**La sanction pénale** en France est la réponse de l'État contre l'auteur d'un comportement incriminé.

Le délit pénal est sanctionné par une peine infligée au coupable appelée sanction pénale. Exemples : prison, amende, retrait du permis de conduire, etc.

**Une sanction disciplinaire** est une mesure prise par l’employeur à la suite d’agissements du salarié qu’il considère comme fautifs. Avant d’appliquer la sanction, l’employeur est tenu de respecter une procédure destinée à informer le salarié concerné et à lui permettre d’assurer sa défense. Si la sanction envisagée est le licenciement, la procédure de licenciement pour motif personnel doit être respectée.

En cas de litige, le conseil de prud’hommes apprécie la régularité de la procédure suivie et si les faits reprochés au salarié sont de nature à justifier une sanction.

**Sanctions en responsabilité civile professionnelle**

En matière civile, la sanction vise à réparer le dommage causé. Elle peut prendre la forme de :

**🡪 Dommages-intérêts compensatoires** ; ils compensent le préjudice subi par le créancier, en cas d'inexécution ou mauvaise exécution des obligations ;

🡪 **Intérêts moratoires** : il s'agit d'intérêts destinés à sanctionner et à réparer le retard dans l'exécution d'une obligation, notamment le retard dans le paiement d'une somme d'argent. Exemple : retard de livraison, etc.

Une autorité administrative indépendante peut également sanctionner le responsable d’une faute, ainsi la CNIL possède les pouvoir pour effectuer une sanction la CNIL peut prononcer à l’égard du responsable de traitement fautif :

* **Un avertissement**, qui peut être rendu public.

Dans l'hypothèse où le Président de la CNIL a, au préalable, prononcé une mise en demeure, et que le responsable de traitement ne s'y est pas conformé, la formation contentieuse peut prononcer, à l'issue d'une procédure contradictoire

* **Une sanction pécuniaire** (sauf pour les traitements de l’État) d’un montant maximal de 150.000€, et, en cas de récidive, jusqu’à 300.000 €. Cette sanction peut être rendue publique ; la formation contentieuse peut également ordonner l'insertion de sa décision dans la presse, aux frais de l'organisme sanctionné. Le montant des amendes est perçu par le Trésor Public et non par la CNIL.
* Une injonction de cesser le traitement.
* Un retrait de l’autorisation accordée par la CNIL en application de l’article 25 de la loi

**Cas particuliers**

**En cas d'urgence et d'atteinte aux droits et libertés** définies à l'article 1er de la loi, la formation contentieuse peut décider, à l'issue d'une procédure contradictoire : l’interruption de mettre en œuvre le traitement,

L'avertissement, le verrouillage des données pour trois mois. pour certains fichiers sensibles de l'État, l'information du Premier Ministre afin qu'il prenne les mesures nécessaires pour mettre fin aux manquements.

**En cas d’atteinte grave et immédiate aux droits et libertés**, le président de la CNIL peut demander, par référé, à la juridiction compétente, d’ordonner toute mesure de sécurité nécessaire.

La CNIL peut également dénoncer au Procureur de la République les infractions à la loi informatique et libertés, prévues aux articles 226-16 à 226-24 du Code pénal.

**Quelques sanctions**

« Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 € d'amende. »

Article 226-17 du code pénal

La suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende ».

Art. 323-1 Code pénal

## Jurisprudence

**Arrêt Nikon**

Les parties

Demandeur : M. X, ancien employé de la société Nikon, qui demande une indemnité pour licenciement abusif.

Défendeur : La société Nikon.

Les Faits :

La société Nikon à licencié pour faute grave M. X. Motif : usage à des fins personnelles du matériel mis à sa disposition par la société à des fins professionnelles.

La société Nikon s’est fondée pour établir ses accusations sur le contenu de messages émis et reçus par le salarié, que l’employeur avait découverts en consultant l’ordinateur mis à la disposition de M. X par la société et comportant un fichier intitulé “ personnel “.

Procédure : 1er degré : Tribunal des prud’hommes

2ème degré : Cours d’Apelle du 22 mars 1999

Dernier recours : Cour de cassation du 2 octobre 2001.

Arguments :

Demandeur : l’employeur avait découverts ces fichier en consultant l’ordinateur mis à la disposition de M.X et dans un dossier intitulé “ personnel “.

Défense : « Le salarié avait entretenu pendant ses heures de travail une activité parallèle »

Problème juridique : Le licenciement de M. X est-il justifier ?

Solution :

Le salarié a droit, même au temps et au lieu du travail, au respect de l’intimité de sa vie privée ; celle-ci implique en particulier le secret des correspondances. L’employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance du contenu des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail

PAR CES MOTIFS :

La cour CASSE ET ANNULE, dans toutes ses dispositions, l'arrêt rendu le 22 mars 1999

**Cour de Cassation du 19 mai 2004**

Les parties

Demandeur : La société Nortel, qui demande des dommages-intérêts à M. X

Défendeur : M. Jean-François X, ancien employé de la société Nortel

Les Faits :

Jean-François X a admis que depuis son arrivée au sein de la société Nortel Europe qu’il avait utilisé son outil de travail pour des connexions sans rapport avec son activité salariée ou celles de l’entreprise, que visitant des sites à caractère érotique.

Il a stocké sur son disque dur de très nombreuses photos et messages de même nature en utilisant la messagerie ouverte à son nom au sein de la société Nortel Europe.

Procédure : 1er degré :

2ème degré : cour d’appel de PARIS, du 25 avril 2003(condamnation à payer 20 000€ de dommage-intérêts pour abus de confiance)

Dernier recours : Cour de Cassation du 19 mai 2004

Arguments :

Demandeur : « le prévenu a commis une appropriation frauduleuse constitutive d’un abus de confiance »

La consultation et l’animation de sites pornographiques au moyen de l’ordinateur mis à disposition par l’employeur ne rentre pas dans le cadre de l’intimité de la vie privée au respect de laquelle tout salarié a droit, même pendant le temps et sur le lieu de travail ;

Défense : Il n’avait pas été expressément convenu entre les parties qu’il ne pouvait y avoir la moindre utilisation non professionnelle de l’outil informatique

Problème juridique : Y a-t-il eu abus de confiance et le salarié avait-il le droit d’utiliser le matériel informatique à titre non professionnel.

Solution : La cours rejette le pourvoi et condamne Jean-François X à payer à la société Nortel Networks la somme de 2 000 €

**Cour de Cassation du 29 octobre 2014**

Les parties

Demandeur : M. X, ancien employé de la société Elb Multimédia, qui demande des dommages-intérêts pour licenciement vexatoire

Défendeur : Société Elb Multimédia.

Les Faits : M. X engagé le 12 novembre 2009 par la société Elb Multimédia, a été licencié pour faute grave le 31 mai 2010 en raison de téléchargements illégaux et répétitifs au sein de l’entreprise.

Procédure : 1er degré : tribunal des prud’hommes

2ème degré : la cour d’appel

Dernier recours : Cour de Cassation du

Arguments :

Demandeur : Le motif est que la lettre de licenciement énonce a pour seul motif «téléchargements illégaux et répétitifs au sein de l’entreprise »

Défense : La société Elb Multimédia prétend que M. X a effectué des téléchargements illégaux et répétitifs au sein de l’entreprise.

Problème juridique : Le licenciement de M. X est-il justifié ?

Solution :

Le fait M. X manifeste une connexion à un site permettant des téléchargements, ne caractérise pas l’action même de téléchargement, les données y figurant ne faisant état que de la consultation d’images ou pages cinéma ; que la preuve de téléchargements illicites et réitérés n’est pas faite ; que dès lors le licenciement est sans cause réelle et sérieuse

Par conséquent la cours rejette le pourvoi et condamne la société à payer à M. X la somme de 3 000 euros

## Sources

<http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=4341>

<http://fr.jurispedia.org/index.php/Jurisprudence_de_la_Cour_de_cassation_sur_utilisation_du_courrier_%C3%A9lectronique_par_un_salari%C3%A9_%28fr%29#Cour_de_Cassation_du_2_juin_2004>

<http://www.legifrance.gouv.fr>

<http://www.pearltrees.com/coyla/sio-veille-juridique/id13541972>