

# Législation et droit d'un administrateur réseaux

***Réalisé par :***

GUENGOU Mourad  
OULD MED LEMINE Ahmedou

# Plan de présentation

- I. Introduction générale
- II. L'Administrateur Réseaux
  - 1) Mission de l'administrateur réseaux
  - 2) statut de l'administrateur réseaux
  - 3) L'obligation de confidentialité
  - 4) Le contrôle doit être loyal, transparent et proportionné
    - Un contrôle loyal
    - Un contrôle transparent
    - Un contrôle proportionné
  - La mise en place d'une charte
  - Conclusion
    - Droits d'administrateur réseaux
    - Devoir d'administrateur réseaux
- III. La solution sonde réseaux

# I. L'archivage

- 1) Introduction
  - 2) Les objectifs de l'archivage
  - 3) Le cadre légal
  - 4) L'archivage électronique
    - La réforme du 13 mars 2000 sur la preuve électronique
    - Difficultés liées à l'archivage des documents électroniques
- Définition des besoins
  - Conclusion

# II. Conclusion générale

# I. Introduction générale

- Pour des nécessités de maintenance et de gestion technique
  - ❖ l'utilisation des ressources matérielles ou logicielles
  - ❖ les échanges via le réseau,

peuvent être analysés et contrôlés par les administrateurs dans le respect de la législation applicable.

# Introduction générale(suite)

- 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,
  - ❖ prévenant l'apparition de virus
  - ❖ empêchant la circulation de contenus illicites sur le réseau,

# Introduction générale(suite)

A l'inverse:

les salariés revendiquent le droit à une vie privée sur leur lieu de travail (connexion à Internet à des fins personnelles).

# I. L'Administrateur Réseaux

L'administrateur réseau est à ce jour l'homme de toutes les situations.

Il lui appartient de:

➤ assurer la sécurité du réseau,

Tout en respectant les données personnelles des salariés couvertes par le secret des correspondances et par le droit à la vie privée.

# L'Administrateur Réseaux(suite)

- Afin d'encadrer et de limiter un usage excessif de l'Internet sur le lieu de travail:
- Il dispose au titre de son pouvoir de direction d'un droit de contrôle et de surveillance sur ses salariés.
- Mais ce pouvoir ne doit pas méconnaître les principes du droit à la vie privée.



# L'Administrateur Réseaux(suite)

- Pourquoi le droit à une vie privée au travail ?  
La (CNIL) l'a reconnu au salarié.
- ❖ L'administrateur réseau est au carrefour de ses deux logiques, il est en charge d'assurer à la fois:
  - la sécurité du réseau, à la demande de son hiérarchie.
  - ❖ la sécurité des données professionnelles et personnelles des salariés.

# L'Administrateur Réseaux(suite)

- C'est pourquoi la jurisprudence lui a conféré un statut particulier.

Il doit toutefois agir dans :

- la transparence,
- la loyauté,

et avec cohérence, et confidentialité même vis à vis de sa hiérarchie sur les données auxquelles il pourrait avoir accès dans le cadre de sa mission.

# 1) Mission de l'administrateur réseaux

- Dans l'article 29 de la « Loi Informatique et Liberté », Il s'engage à prendre toutes les précautions utiles afin de préserver la sécurité des informations.

d'empêcher qu'elles ne soient :

- ❖ déformées,
- ❖ endommagées
- ❖ ou communiquées à des tiers non autorisés

# Mission de l'administrateur réseaux (suite)

La loi prévoit une obligation de moyen et:

- ❖ la directive 95/46 dans son article 17 énonce une obligation de mettre en œuvre les mesures techniques, pour protéger les données à caractère personnel, par l'administrateur.

# Mission de l'administrateur réseaux (suite)

- ❖ la directive 2002-58 du 12/7/2002 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. statut de l'administrateur réseaux

- La Cour d'appel dans un arrêt du 17/12/2001 a annoncé:

que la mission des administrateurs réseaux, implique qu'ils aient accès aux informations user:

- ❖ leurs messageries
- ❖ leurs fichiers logs ou de journalisations,
- ❖ leurs connexions à Internet.

# statut de l'administrateur réseaux (suite)

Les 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

# statut de l'administrateur réseaux (suite)

- ❖ Il peut contrôler les extensions des pièces jointes d'un fichier, leurs volumes.

Il possède un mot de passe administrateur qui lui permet d'accéder aux:

- ❖ serveurs de fichier,
- ❖ serveurs web,
- ❖ serveurs de messagerie, et par conséquent avoir accès à l'ensemble des informations émises, reçues, créées par un salarié.



# 1) L'obligation de confidentialité

- Qui dit confidentialité, dit données confidentielles c'est à dire vie privée.
- L'administrateur est soumis au secret professionnel et ne peut divulguer les données personnelles auxquelles il a accès.
- 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
- 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.

# 1) Le contrôle

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

# Le contrôle (suite)

- *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.

# Le contrôle (suite)

- l'administrateur doit 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 ?

# Le contrôle (suite)

La Cour de cassation a reconnu deux types de répertoires:

- ❖ Répertoire personnel: présumé contenir des données personnelles.
- ❖ Répertoire professionnel.

La CNIL considère qu'un message est présumé professionnel sauf s'il est indiqué qu'il s'agit d'un message personnel.

# Le contrôle (suite)

- *Un contrôle transparent:*
  - La démarche doit se faire dans une logique de transparence vis à vis des salariés,
  - qui doivent être informés par l'employeur de la mise en place d'un dispositif de contrôle.
  - Si le dispositif constitue un traitement automatisé de données personnelles alors il doit être déclaré à la CNIL avant sa mise en œuvre

# Le contrôle (suite)

- *Un contrôle proportionné:*

Le contrôle effectué par l'administrateur réseau dans le cadre de sa fonction doit être proportionnel au but recherché.

Il doit remplir sa mission sans aller au-delà

# 1) La mise en place d'une charte

- La mise en place d'une charte est 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.
- Toutefois, il est important de souligner que seule une charte établie selon les modalités du règlement intérieur peut donner lieu à des sanctions disciplinaires.



# I. Les solutions sonde réseaux & Filtrage de paquets

Rôle:

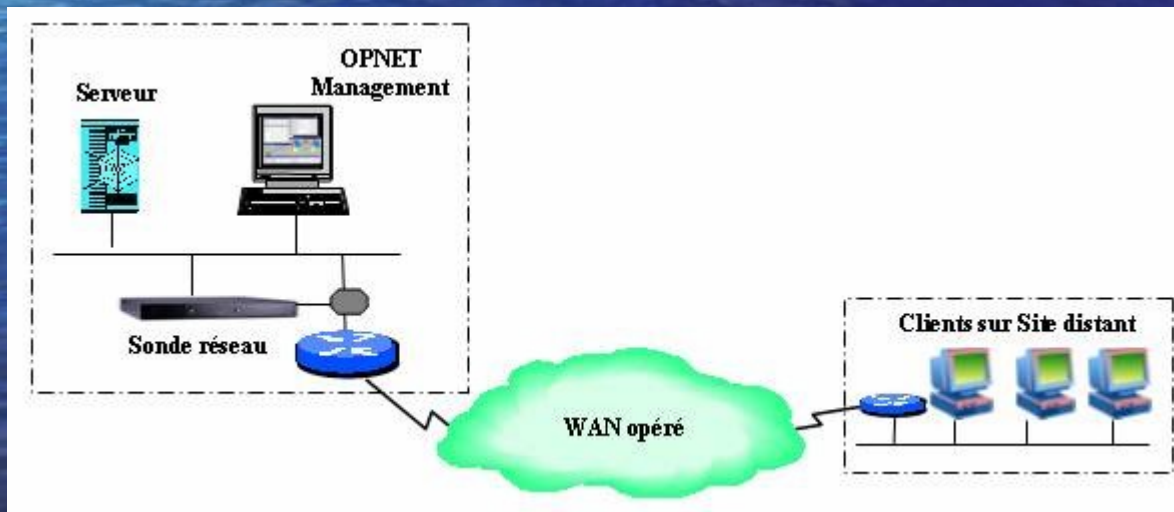
- ❖ Permettent de garantir la sécurité d'un réseau informatique par l'analyse des flux de données transitant.

# Sonde Réseaux

Sondes réseaux est un système distribué pour la surveillance des réseaux. C'est une solution puissante qui permet de surveiller les flux sur tous types de réseaux : WAN, LAN ou ATM, adaptée aux grands et petits réseaux, et cela de la couche 1 à la couche 7 du modèle OSI.

# sonde réseaux

- Les sondes sont placées sur les liens principaux et le logiciel poste client est installé sur le micro-ordinateur du responsable de l'exploitation du réseau.



# Filtrage de paquets

(ou pare-feu ou *firewall*) est une machine capable de prendre la décision d'accepter ou non un paquet transitant par une de ses interfaces réseau.

Dans un réseau informatique, le transport des informations étant effectué par TCP/IP, c'est à ce niveau que la majorité des contrôles se fera.

# Filtrage de paquets:

Le filtrage des paquets intervient lors du traitement de paquets transitant par le filtre.

Le filtre de paquets analyse les paramètres de chaque paquet et prend une décision sur le devenir du paquet en fonction de ces paramètres et de la politique de sécurité.

# Filtrage de paquet(suite):

Lorsqu'un paquet est traité, le filtre de paquets applique l'une après l'autre les règles qu'on lui a configurées, jusqu'à ce que l'une corresponde au paquet analysé.

il peut par exemple analyser :

- ❖ le protocole utilisé (TCP, UDP, ICMP, ...) ;
- ❖ l'adresse IP de la machine émettrice ou réceptrice;
- ❖ pour TCP ou UDP, le service du paquet (HTTP, SMTP, SSH, domaine...)
- ❖ pour ICMP, le type ICMP (*destination-unreachable, echo-reply, ...*).

# Filtrage de paquet(suite):

Une fois un paquet analysé, le filtre exécute une action parmi les suivantes :

- continuer à le traiter ;
- le rejeter, ce qui implique d'envoyer un paquet ICMP d'erreur à l'émetteur ;
- l'ignorer, ce qui signifie ne pas le traiter sans même en avertir l'émetteur.

# I. L'archivage

## 1) Introduction

- Archiver, c'est conserver un document dont on a plus l'utilité immédiate, mais qui peut encore servir, soit à titre informatif, soit à titre de preuve dans l'éventualité d'une contestation, d'un litige devant les tribunaux ou lors d'un contrôle de l'administration.



# L'archivage->introduction

- L'archivage correspond à l'idée de pérennité de l'information avec la possibilité de la restituer intacte ultérieurement.
- Dans ses aspects juridiques, l'archivage est lié à la question de la preuve : il est impératif de conserver tous les actes au sens large nécessaires à la justification de droits jusqu'à l'expiration des délais prévus pour effectuer une contestation

# 1) Les objectifs de l'archivage

- L'archivage peut répondre à trois objectifs différents, selon la valeur des documents que l'on archive :

- **juridique** : concerne tous les documents qui portent sur la justification de droits à longue ou courte échéance.

Exemple : conservation de contrats à des fins de preuve en cas de litige avec le client et/ou le fournisseur, conservation des documents comptables en cas de contrôle fiscal.

- **Administrative** : ce sont les documents dont l'organisme a besoin pour sa gestion.
- **Historique** : pour la reconstitution d'événement survenus dans l'organisme.

# 1) Le cadre légal

- La loi de 1979 sur les archives organise la conservation des documents dans l'intérêt public, pour les besoins de la gestion et de la justification des droits des personnes, ainsi que pour la documentation historique de la recherche.
- La loi distingue entre les archives privées et les archives publiques

# Le cadre légal (suite)

- Il n'existe pas de réglementation spécifique en ce qui concerne les modalités de conservation des archives privées. La réglementation fixe uniquement les règles concernant les durées de conservation.
- La durée de conservation n'est pas déterminée en fonction du support du document à archiver (papier ou numérique), mais en fonction de la nature juridique du document à archiver (contrat, facture, bulletin de paie etc..).

# 1) L'archivage électronique

- La réforme du 13 mars 2000 sur la preuve électronique :

La loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information, La loi comporte deux volets novateurs:

- ❖ la redéfinition de la preuve littérale
- ❖ la consécration de la force probante de l'écrit électronique.

Selon le nouvel article 1316 du Code civil : « La preuve littérale, ou preuve par écrit, résulte d'une suite de lettres, de caractères, de chiffres ou de tous autres signes ou symboles dotés d'une signification intelligible, quels que soient leur support et leurs modalités de transmission ».

# L'archivage électronique (suite)

Selon le nouvel article 1316-1 : « L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ».

# L'archivage électronique (suite)

- Difficultés liées à l'archivage des documents électroniques:
- La loi du 13 mars 2000 a posé le principe de l'indépendance entre l'écrit et son support.

En pratique, un document numérique est entièrement dépendant de son environnement : matériel informatique, logiciel, système d'exploitation, formats d'encodage et de fichier.

- De nombreuses difficultés d'ordre technique doivent être résolues pour assurer la pérennisation de l'information numérique.

# L'archivage électronique (suite)

- Notamment, les matériels et logiciels évoluent constamment et les systèmes modernes de stockage des données sont fragiles, vieillissent mal.
- L'information enregistrée par un moyen électronique nécessite un équipement spécifique pour la rendre intelligible



# L'archivage électronique (suite)

- Compte tenu de l'évolution rapide des techniques, il est difficile de garantir que l'on disposera au moment voulu des interfaces logicielles et matérielles requises pour accéder à la lecture du document électronique établi des années plus tôt, il faut donc :
  - conserver les matériels et logiciels nécessaires à la restitution des documents (ce qui semble onéreux et irréaliste),
  - procéder à des recopies régulières des données de l'ancien système informatique vers le nouveau système informatique(Migration).

C'est cette deuxième solution qui est actuellement pratiquée par des organismes comme la Direction des Archives de France.

# 1) Définition des besoins

Avant l'établissement du cahier des charges en vue de l'exploitation et/ou du développement du système de gestion de l'archivage électronique de l'entreprise,

il sera nécessaire de déterminer les besoins de l'entreprise, par exemple en effectuant les démarches suivantes :

# Définition des besoins (suite)

- analyse du patrimoine à archiver (identification des documents électroniques à conserver) :
  - Quels documents l'entreprise souhaite/doit conserver sous forme électronique ?
  - Dans quel but (juridique, administratif, historique, comptable, fiscal) ?

# Définition des besoins (suite)

- **analyse des contraintes juridiques :**
  - Quelle est la durée de conservation fixée par les textes pour les documents en cause ?
  - Quelles sont les garanties générales que doit fournir le système d'archivage (intégrité, restitution, fidélité par rapport au contenu initial) ?
  - Existe-t-il des exigences particulières (par exemple exigences de l'administration fiscale, contraintes résultant de la législation sur les données personnelles) ?
  - Quels sont les risques juridiques encourus en cas de non conservation ?

# Définition des besoins (suite)

- **définition des procédures organisationnelles (gestion des droits d'accès au document archivé) :**
    - Qui à accès à quoi ? (services internes, organismes extérieurs)
    - Selon quelle fréquence ?
    - A quelle occasion (nécessité du service, audit, contrôle de l'administration, litige) ?
    - Comment seront indexés les documents (détermination du plan de classement) ?
- Il faudra ensuite déterminer les outils techniques qui permettront d'appliquer ces procédures et de répondre à ces besoins.

# 1) Conclusion

- La réforme de la preuve électronique n'a pas pris en compte la question de la garantie de l'intégrité à long terme de l'acte signé. Or, il s'agit d'une question concrète fondamentale, qui conditionne en outre la validité juridique de l'acte électronique.
- Le passage du monde du papier au monde de l'électronique n'est pas forcément synonyme de simplification.
- Enfin, d'un point de vue pratique, il est essentiel de se préoccuper de la question de l'archivage des documents électroniques dès la phase de conception du système d'échanges électroniques.

# I. Conclusion générale

- 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.

# Conclusion générale (suite)

- 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 tournera vers la voie pénale.

Une plainte au procureur de la République, si elle repose sur des éléments sérieux, entraînera une enquête préliminaire.

Au cours de cette enquête, la police judiciaire a des perquisitions, des interrogatoires, ou à la saisine de pièces.



# Conclusion générale (suite)

- 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.



**Merci  
à  
votre attention**

# Webographie

- <http://www.cnil.fr/index.htm>
- <http://www.droitdunet.fr/>
- <http://www.foruminternet.org>
- <http://www.clic-droit.com>
- <http://www.droit-ntic.com/>
- <http://www.internet-juridique.net>
- <http://www.juriscom.net>