

THÈME D6 La responsabilité des prestataires internes et externes du SI**D 6.3 La responsabilité des administrateurs systèmes et réseaux**

Mots clés : Responsabilité légale ; administrateurs système

Fiche synthèse

Idée clé →	La responsabilité des administrateurs systèmes et réseaux est engagée s'ils ne respectent pas le cadre légal de leur activité
Donner du sens →	L'administrateur système et réseau dispose de prérogatives étendues au sein de l'organisation. Il peut mettre en œuvre tous les moyens utiles au soutien du système d'information.

1. Les missions de l'administrateur système et réseau (ASR) au sein de l'organisation

L'ASR est chargé de la mise en place et du suivi du SI au sein des grandes entreprises, des SSII ou des administrations (*la responsabilité des agents publics n'est pas abordée ici*). Il a précisément pour mission de gérer l'utilisation du réseau de l'organisation (performances, optimisation, migration, évolution, sécurité...), les postes de travail (accès à internet, mots de passe, sauvegardes), d'intégrer les nouveaux équipements au réseau. Il est important pour lui d'identifier clairement ses missions et ses responsabilités afin de prendre toutes les mesures utiles pour ne pas encourir de risques.

L'ASR doit :

- ✓ Informer, former, conseiller, alerter les acteurs de l'organisation pour tout ce qui concerne le système informatique et notamment les risques encourus (atteinte aux fichiers, captation de données à caractère personnel ...). Il a en charge les bonnes pratiques informatiques. Une directive européenne de 2002 précise le devoir d'information de l'administrateur système et réseau.
- ✓ Sécuriser le système (article 29 de la LIL 2004). Il doit tout mettre en œuvre pour prévenir :
 - toute intrusion susceptible de détruire les données, de les modifier ou de les révéler à des tiers non habilités (la *Directive 2002/58 du 12/7/2002* précise que l'ASR doit prendre toutes les « mesures appropriées » pour assurer la sécurité,
 - toute introduction de programmes malveillants.
- ✓ Contrôler l'activité sur le réseau afin de prévenir les risques (à son initiative ou à la demande de l'employeur).
- ✓ Pratiquer une veille juridique (loi, directive européenne, jurisprudence, recommandations Cnil) afin d'être toujours en conformité. Il doit également pratiquer une veille technique (évolution des outils et des risques : biométrie, RFID...).

L'ASR bénéficie d'un statut particulier qui peut être attesté par une charte dédiée rédigée par l'employeur. Celle-ci précise les responsabilités de l'ASR et prévoit les moyens spécifiques (on parle même de moyens « privilégiés ») dont il disposera pour accomplir sa mission (accès administrateur, droits étendus en matière de connexion à internet...).

2. Les obligations classiques de l'ASR

L'ASR dispose certes de moyens d'investigation (contrôle du débit, durée des connexions, sites web, accès en sa qualité d'administrateur aux serveurs de fichiers, aux serveurs web et aux serveurs de messagerie) mais il doit néanmoins agir en respectant des principes :

- ✓ de loyauté : sa démarche doit être impartiale, sincère et être uniquement justifiée par un impératif de sécurité. Elle doit être conforme à la finalité pour laquelle le contrôle a été décidé. Dans le cas contraire, il engagerait sa responsabilité pénale et professionnelle.
- ✓ de transparence : les acteurs internes à l'organisation ainsi que les tiers doivent être informés de l'éventualité d'un contrôle. Le règlement intérieur et la charte informatique informent les acteurs de l'entreprise des dispositifs de contrôle mis en œuvre. Les conditions d'intervention, de contrôle et les

moyens utilisés par l'ASR pour investiguer doivent également et spécifiquement être portés à la connaissance des institutions représentatives du personnel (CE, délégués du personnel...).

- ✓ de confidentialité : l'ASR est tenu au secret professionnel : il a l'interdiction de diffuser à quiconque, les informations qu'il aurait eu à connaître dans le cadre de ses fonctions. L'article 432-9 alinéa 2 du code pénal prévoit en effet que, si l'ASR peut accéder aux données à caractère personnel des salariés, il n'est cependant pas autorisé à les divulguer. À défaut, il mettrait en œuvre sa responsabilité pénale en vertu de l'article 226.15 du code pénal. Cette obligation de confidentialité de l'administrateur système et réseau fait également l'objet d'une clause dans son contrat de travail.

Remarque : L'ASR doit à la fois concilier les impératifs de l'organisation (impératifs de sécurité notamment) et les droits des collaborateurs et des tiers (respect de la vie privée, protection des données à caractère personnel.... Son rôle est complexe.

3. Les obligations spécifiques de l'ASR

Des circonstances particulières ou certains événements peuvent contraindre l'ASR à agir :

- ✓ En cas d'atteinte à la sécurité 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 sécurité 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.

Un arrêt de la Cour d'appel d'Aix-en-Provence (17/12/2002) renforce le rôle des administrateurs systèmes quant à la nécessité de surveiller le trafic sur les réseaux de leurs entreprises. La découverte de la consultation par un salarié, de sites pédophiles s'est faite à l'occasion d'une opération ordinaire de maintenance par l'administrateur système. Celui-ci a immédiatement informé son supérieur hiérarchique ce qui a permis de mettre en œuvre une procédure disciplinaire* de licenciement ([Source : www.cadresonline.com](http://www.cadresonline.com)) à l'encontre du salarié fautif lequel encourt également des poursuites pénales.

En résumé :

L'ASR occupe une place déterminante dans l'entreprise dont l'objectif est d'optimiser l'utilisation des ressources informatiques lesquelles sont perçues comme des outils de la compétitivité. Il dispose de pouvoirs très étendus pour sécuriser le système informatique mais doit, dans le cadre de ses contrôles, respecter le secret des correspondances ainsi que la vie privée de ses salariés. Son rôle et ses responsabilités évoluent du fait de l'externalisation des SI.

Un exemple pour illustrer :

Récemment, l'audit du réseau d'une association a révélé la présence sur le poste de l'ASR, de fichiers en provenance d'internet. La taille des fichiers stockés sur le disque dur du salarié était telle qu'elle laissait présager d'un téléchargement 24 h/24 et 7 jours/7... Lors de cet audit, il a été découvert la présence d'un logiciel de partage de données baptisé « GNUTELLA » qui a permis à l'administrateur de télécharger des logiciels et fichiers MP3 en quantité impressionnante. L'audit a également révélé que l'administrateur avait modifié les procédures de sécurité du réseau informatique de l'association afin de mettre en place ce type de programme... (Ces modifications avaient mis en péril la sécurité du SI)... L'association a donc licencié son administrateur réseau pour faute grave. La cour d'appel a confirmé le licenciement au motif que l'administrateur réseau avait *profité de ses fonctions et de l'accès privilégié au système informatique de son employeur pour, à l'insu de celui-ci, utiliser ce système à des fins personnelles étrangères à l'activité de l'association* ». www.alain-bensoussan.com