Ce chapitre rédigé par le groupe de travail GBP a été réalisé à partir de diverses formations et conférences juridiques données par Maître BARBRY [22].

Schéma du droit de la Sécurité des Systèmes d'Information

La présente note vise à actualiser le schéma de synthèse des ***textes applicables au droit des systèmes d'information*** élaboré en juin 2015 à la lumière des évolutions législatives et réglementaires françaises et européennes intervenue en 2016 et 2017

- SchemaDroitSSI2015NotesActualisation

Le schéma ci dessous donne une vision synoptique des textes impactant le travail des ASR. Il fait suite à un travail de mise a jour régulier que nous avons entrepris avec Me E. Barbry (cabinet Racine, spécialiste du droit en SSI) car le droit en SSI a connu de fortes évolutions ces dernières années

L'idée de ce schéma est de donner un panorama du droit de la SSI et de l'état des textes réglementaires qui affectent les interventions informatiques des ASR dans nos unités CNRS

Schéma juridique du droit en SSI (mise à jour 2018)

Dans cette vidéo Me Barbry explique les principales évolutions de la SSI en 2018 : GBP-schema-SSI-Barbry

http://gbp.resinfo.org/wp-content/uploads/2018/08/GBP-schema-SSI-Barbry.mp4

Référentiel légal du métier d'ASR

Il n'existe pas de référentiel légal concernant le métier d'ASR. Autrement dit, le terme d'« Administrateur Systèmes et Réseaux » n'apparaît dans aucune loi, décret ou texte réglementaire, contrairement au Correspondant Informatique et Liberté (CIL), dont la fonction et les responsabilités sont bien définies dans un cadre légal.

Deux points sont tout de même à noter. Tout d'abord, l'arrêté du 18 juillet 2010 relatif au secret défense [23] parle de l'administrateur dans sa fonction « sécurité » : on commence donc à lui attribuer un statut juridique dans un cadre particulier. Ensuite, le second point concerne deux guides pratiques de la CNIL [24a] et [24b]. Ce ne sont pas des textes réglementaires mais ils sont une conséquence de la loi « Informatique et Libertés » du 6 janvier 1978. Le premier guide à destination des employeurs et des salariés définit dans sa fiche pratique n°7 la mission de l'administrateur réseau. Le second guide relatif à la sécurité des données personnelles parle, entre autres, de la sécurité des postes de travail et de celle des serveurs et des applications (fiches n°4 et n°11).

La jurisprudence nous apporte également quelques précisions sur le régime juridique des ASR. L'une précise [25] que la fonction des ASR nécessite de pouvoir faire des investigations, certes, mais indique que les résultats de celles-ci n'ont pas à être divulgués. Un devoir déontologique de réserve s'impose.

La seconde [26] confirme le licenciement de l'ASR d'une association qui a téléchargé 24h/24 et 7j/7 environ 6 Go d'images, de sons et de vidéos considérant qu'il avait abusé de ses droits privilégiés au système informatique.

L'ASR, de par sa fonction, a des accès privilégiés aux ressources et systèmes de son unité. Il doit donc être particulièrement vigilant dans la mise en œuvre des moyens qu'il utilise. L'environnement juridique actuel nous permet de retenir quelques bonnes pratiques énoncées ci-après.

[forum : annoter le chapitre]

Ne pas ignorer le droit.

Avec ses accès privilégiés sur les réseaux et systèmes, l'ASR peut accéder plus facilement à des données relevant de la vie privée résiduelle des utilisateurs, à leurs données personnelles, à des données relevant de la propriété intellectuelle, etc. Toutes ces notions sont encadrées d'un point de vue juridique. L'ASR n'est certes pas juriste, ni avocat mais il ne peut ignorer sa responsabilité dans ce cadre.

Cette première bonne pratique peut se résumer ainsi : « En savoir assez pour ne pas en faire trop ».

[forum : annoter le chapitre]

Faire de la veille juridique

L'environnement dans lequel évolue l'ASR évolue de façon permanente à trois niveaux :

- technique : les mises à jour et les nouveaux logiciels ;
- des usages : les utilisateurs sont à la fois demandeurs et utilisateurs des nouvelles techniques et des fonctionnalités apportées au travers de celles-ci ;
- du droit : qui apporte plus ou moins rapidement des réponses d'ordre juridique.

L'ASR est la personne à laquelle les utilisateurs adressent des demandes informatiques. Ces demandes sont souvent relatives à l'accès aux données professionnelles comme personnelles, et aux besoins de confidentialité et de disponibilité. Il est donc amené à y répondre avec le plus de justesse et de précision possible dans le cadre technique et légal. Et, pour ce faire, une bonne pratique est de se tenir au courant régulièrement et au besoin de se faire assister d'un professionnel du droit [27].

En résumé : « Un ASR informé en vaut deux ».

[forum : annoter le chapitre]

Disposer d'une boîte à outils juridiques

Cette boîte à outils est constituée de documents que l'ASR doit posséder et dont dépendent les missions qui lui sont confiées :

- la charte informatique (généralement annexée au règlement intérieur de l'établissement) ;
- la charte administrateur qui peut s'appliquer à la fois à l'ASR et à l'utilisateur, le premier ayant des droits privilégiés sur les systèmes de son unité et le second sur son ordinateur de bureau ou portable ;
- le guide des opérations de contrôle sur les postes ;
- une connaissance concrète de sa chaîne fonctionnelle ;
- les mentions légales sur les sites web.

Vous trouverez des informations utiles sur les sites cités en annexe [28].

En résumé : «Un bon ouvrier (ASR) a toujours ses outils ».

[forum : annoter le chapitre]

Ne pas faire ce que tu n'as pas le droit de faire

Cette bonne pratique repose tout simplement sur le bon sens. En effet, au même titre qu'une lettre avec une mention « personnel » ou « confidentiel » doit être donnée à son destinataire sans être ouverte, un courrier électronique ou un répertoire avec ces mêmes mentions n'a pas à être lu par l'ASR sauf dans des cas bien particuliers légitimes. Là aussi, la légitimité d'une demande de ce type faite après de l'ASR passe également par son bon sens.

En résumé, « Ne fais pas à autrui ce que tu ne voudrais pas qu'il te fasse ».

[forum : annoter le chapitre]

Ne pas être négligent fautif : Informer – Contrôler – Agir

Quelque soit son statut, l'ASR doit respecter les règles de responsabilité civile suivantes :

- Article 1382 du Code civil : « Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé, à le réparer » ;
- Article 1384 du Code civil : « *On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde...* » ;
- Et particulièrement, l'Article 1383 du Code civil : « *Chacun est responsable du dommage qu'il a causé, non seulement par son fait, mais encore par sa négligence ou par son imprudence* ».

Cette bonne pratique nous paraît importante à détailler.

Informer

Les administrateurs sont tenus à une obligation de conseil « renforcé » auprès des utilisateurs. En effet, le conseil « renforcé » s'applique à trois domaines : le nucléaire, la chimie risque de type « SEVESO » et l'informatique. Les ASR peuvent émettre des alertes ou des mises en garde. L'alerte permet d'informer d'un problème bien défini, connu et réel. La mise en garde permet de signaler la possibilité d'un problème (hypothétique ou probable). La présence de certains mots-clés comme « alerte », « conseil » ou « mise en garde » dans un rapport, un message électronique et/ou dans une rubrique « informations » ou « sécurité » de l'intranet de l'unité peut avoir un poids utile en cas de contentieux ultérieur.

Il est nécessaire d'informer les utilisateurs de la nature des traces qui sont journalisées et archivées sur nos systèmes, ainsi que de leur durée de rétention par l'affichage sur un site web par exemple. La politique de gestion des traces du CNRS a fait l'objet d'un document officiel disponible dans l'intranet du CNRS [16].

L'information peut porter, par exemple, sur les bulletins du CERT et CERTA [15] (en particulier les alertes), les statistiques de virus, de spams, de débits réseau, les migrations prévues, les interruptions de service pour maintenance, les coupures du réseau avec l'extérieur.

Bien entendu, d'un point de vue légal, il est nécessaire de prouver qu'on a bien dispensé l'information nécessaire et donc, il faut avoir les moyens de donner des preuves de l'information et de la communication que l'on a fournies. Cela peut prendre différentes formes comme par exemple, faire un rapport annuel d'activités, envoyer un message électronique ou tenir la rédaction d'une rubrique « informations » dans l'intranet notamment sur la sécurité.

Contrôler

Depuis la Loi pour la Confiance en l'Economie Numérique (LCEN), il apparaît que le droit des ASR à tracer les activités des services et leur utilisation dans le SI est total et complet : diagnostic, analyse, contrôle, maintenance préventive, identification des comportements illicites.

Les bonnes pratiques consistent donc, par exemple, à détecter les fonctionnements anormaux du SI par la mise en place d'outils pour :

- centraliser et paramétrer la conservation des journaux systèmes sur la durée maximale légale pour les services demandés ;
- obtenir des statistiques sur l'utilisation des services, le débit, les sites consultés, la consultation du site du laboratoire, la place occupée sur les disques…
- avoir des remontées d'information en cas de problème avec, par exemple, des sondes d'un système de monitoring (*cf. annexe 2*) ;
- contrôler le contenu du site web. Dans la majorité des cas, les laboratoires éditent et hébergent eux-mêmes leur site web. L'hébergeur n'a pas d'obligation générale de surveillance, mais il a une obligation spéciale de surveillance (point de la négligence fautive). Les ASR sont en effet tenus au secret professionnel, mais ont l'obligation de dénoncer des actes délictueux, comme les contenus illicites et notamment la pédopornographie ou la diffamation. En tant que directeur de la publication, le directeur du laboratoire a une plus grande responsabilité puisqu'il en approuve le contenu.

Une attention particulière sera à observer pour tout ce qui touche les informations personnelles (contexte privé résiduel), tant en terme de diffusion du contenu que de diffusion d'information concernant un contenu suspect ! En effet, les informations personnelles ne peuvent être remises qu'à un officier de police judiciaire dûment habilité. En cas de doute, ne pas hésiter à contacter le Haut Fonctionnaire Défense (HFD)

directement ou via la chaîne fonctionnelle.

Agir

En cas de crise ou d'urgence, l'ASR a donc le droit et le devoir d'agir et de réagir rapidement pour assurer la continuité du service, de même que le droit de refuser des demandes qui mettraient le SI en danger.

En contrepartie, il est tenu d'assurer la sécurité système du site (passer les correctifs de sécurité logiciels). Si un correctif de sécurité n'a pas été passé, et qu'il y a eu un incident grave, pour ne pas être responsable, il faudra qu'il prouve par exemple qu'il était en vacances, et qu'il n'y avait pas de redondance humaine prévue.

En conclusion, l'ASR est amené à faire preuve de vigilance, de perspicacité et de discernement. Il a un devoir de surveillance des systèmes et réseaux, et d'anticipation des problématiques à venir les concernant.

Pour cela, le triptyque d'ordre juridique à retenir est :

- INFORMER les membres de l'unité des risques liés à l'utilisation des systèmes et réseaux mis à leur disposition ;
- CONTROLER l'utilisation des ressources informatiques faites par ces membres ;
- AGIR en rappelant à l'ordre ceux qui s'éloignent des bonnes pratiques et proposer des mesures disciplinaires pour sanctionner les comportements abusifs.

En résumé : « Ne jamais oublier le triptyque : informer, contrôler, agir ».

[forum : annoter le chapitre]

Prouver que l'on fait bien son travail

Il ne s'agit pas vraiment de prouver que l'on est un « bon professionnel » mais plutôt de démontrer que l'on n'est pas dans le cadre de la négligence fautive, autrement dit, de pouvoir prouver que l'on applique bien la bonne pratique n°6 précédemment citée.

Pour cela, il est primordial de garder des traces des actions entreprises dans ce sens comme :

- l'historique de ses échanges par messagerie, en particulier les messages d'alerte, de conseil et de mise en garde ;
- la mise en place d'un système (*wiki* ou autres) où sont enregistrées les interventions réalisées ;

- la réalisation de rapports réguliers d'activités, à insérer si possible dans le rapport quadriennal du laboratoire et dans ses rapports d'activité en tant qu'agent.

En résumé : « ASR, pour vivre heureux, vivons non cachés ».

[forum : annoter le chapitre]

Connaître et utiliser la bonne chaîne d'alerte

Il est important pour l'ASR de connaître cette chaîne d'alerte car en cas de dysfonctionnement, voire de perturbation totale, il est un maillon essentiel auprès de sa direction et des tutelles pour remonter l'information.

Cette chaîne est très souvent propre à chaque établissement et, pour les unités mixtes de recherche dépendant de plusieurs établissements, une telle procédure est logiquement mise en place au niveau des directions pour définir la chaîne retenue dans le cadre des PSSI [6].

En résumé : « L'ASR est un maillon certes mais un maillon essentiel ».

[forum : annoter le chapitre]

Savoir coopérer avec les autorités compétentes

L'ASR peut être amené à répondre à des autorités extérieures telles la police, la gendarmerie, la CNIL et également à des autorités administratives qui ont la possibilité d'exercer leur droit de communication comme l'administration fiscale, l'administration des finances, les douanes, la DGCCRF (Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes), l'AMF (Autorité des Marchés Financiers), le procureur de la République, le juge d'instruction ou le tribunal correctionnel, voire la DCRI (Direction Centrale du Renseignement Intérieur).

L'ASR avec l'appui de sa chaîne fonctionnelle, qu'il doit connaître et informer [29], devra s'assurer des modalités prévues légalement et apporter les réponses demandées ni plus ni moins.

En résumé : « Informer ou cautionner… il faut choisir ».