Contexte juridique du métier d'ASR : où en est-on ?

Ce document est un recueil de notes et une synthèse des formations sur le thème sus-cité par Me Eric Barbry, Avocat au cabinet Bensoussan
Formations réalisées à :

- *Marseille à la DR12 CNRS les 9 et 10 janvier 2008 (35 participants)*
- *Rouen à la Maison de l'Université les 4 et 5 mars 2008 (24 participants)*
- *Caen à la DR19 CNRS les 10 et 11 avril 2008 (28 participants)*
- *Strasbourg les 24 et 25 avril 2008 (61 participants en poste université et CNRS)*

Rédaction : Laurette Chardon (DR19 CNRS) & Maurice Libes (DR12 CNRS) avec les corrections de Frédérique Ostré (Université Strasbourg) sur les 3 premiers chapitres.
v 3.0
Juillet 2008

Table des matières

- Préambule

Le Droit en matière de SSI (Sécurité des Systèmes d'Information) est apparu assez récemment. De 1998 à 2004, à part 2 ou 3 articles dans le Code Pénal et quelques cas de Jurisprudence, il n'y a pas eu d'événements majeurs.

De 2002 à 2007 on assiste a une explosion du Droit en matière de SSI. De nombreuses entreprises dont le CNRS, sont amenées à créer leur propre PSSI (Politique de Sécurité des Système d'Information). Le Ministère de l'Education Nationale est également un gros demandeur en la matière et a formé plusieurs centaines de ses cadres.

Depuis 2004 : une nouvelle « ère juridique » : on assiste à un renforcement des condamnations

Le maître mot et l'objectif premier de cette formation était de connaitre : Quelles sont nos responsabilités juridiques ? ». Mais le problème ne se pose pas exactement en ces termes ! Mais plutôt il se pose plutôt en termes d'être sensibilisé à la Responsabilité et de savoir où se situe et que signifie la Responsabilité en terme de Droit?

- Compléments au support papier de la formation :

1- Panorama de la responsabilité

On se trouve en présence de différents « environnements juridiques ». Il faut parler des responsabilités eu égard à la Sécurité du Système d'Information... Dans ce cadre seules les responsabilité civiles et pénales sont couramment invoquées.

- Responsabilité civile
  - avec contrat : Loi des différentes « parties » : diffamation, contrefaçon etc...
  - hors contrat
- Responsabilité Pénale
- Responsabilité Administrative : Elle est surtout utilisée pour les sanctions disciplinaires . Elle est peu impliquée dans le cadre de la SSI... on ne trouve aucune jurisprudence actuellement en responsabilité administrative dans les SSI.

Un exemple de juridiction civile : en 1996, un site web personnel a été créé par quelqu'un qui affichait des œuvres de Brel et Sardou ==> contrefaçon ==> Juridiction « Civile »... idem pour le cas de contrefaçon concernant le recueil de poèmes de Raymond Queneau « 1000 milliards de poèmes », les éléments fautifs sont des éléments du « civil » (contrefaçon)

Une faute pénale est civile. Une faute civile n'est pas forcément pénale. L'attaquant choisi : soit il attaque en civil (il , recherche de réparation d'un préjudice subit) ou en pénal (il recherche la punition). Dans ce dernier cas, il peut ensuite attaquer en civil.

Au niveau pénal, toute personne a l'obligation de dénoncer un crime (et d'intervenir). En tant que fonctionnaire on doit dénoncer tout délit pénal auprès des autorités compétentes .

En Responsabilité Civile, en cas de faute de service, l'Etat peut se substituer à son personnel et prendre en charge les frais financiers... sauf si il y a faute personnelle de l'agent (Voir le chapitre sur « les règles du jeu de la SSI »). C'est une règle de substitution.

Responsabilité Civile non contractuelle (hors contrat avec employeur)

La responsabilité (hors du cadre de tout contrat) est définie par les articles 1382, 1383 et 1384 du Code civil: la faute directe, la négligence fautive et la faute du fait des autres.

- http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070721&idArticle=LEGIARTI000006438819&dateTexte=20080523
- http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070721&idArticle=LEGIARTI000006438829&dateTexte=20080523
- http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070721&idArticle=LEGIARTI000006438839&dateTexte=20080523

Art. 1382 : Tout fait quelconque de l'homme, qui cause un dommage à autrui, oblige celui par la faute duquel il est arrivé, à le réparer.
En cas de faute, il faut réparer le dommage (exemple : téléchargement 7j/7, lecture d'un mail privé)
Art. 1383: Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence. Cela concerne les fautes par négligence fautive ou l'imprudence de son propre fait

- Exemple de négligence fautive (= « laisser faire ») sur un SI : si un hébergeur a connaissance d'un contenu illicite et qu'il ne fait rien pour l'enlever
  La loi a changé pour les hébergeurs de site Web (loi de 2004).
  L'hébergeur n'a pas d'obligation générale de surveillance, mais il a une obligation spéciale de surveillance (point de la négligence fautive).
  L'hébergeur est responsable lors de la notification d'un contenu. Si un problème de contenu est signalé, alors l'hébergeur doit dans un délai bref (la loi dit : immédiatement) supprimer ce contenu. On va chercher à combattre la négligence par un triptyque : information, contrôle, action.

Art. 1384 : 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.
Un employeur est responsable des agissements de ses employés. Les enseignants, artisans sont responsables des fautes des élèves, apprentis sous leur garde. La responsabilité de l'employeur est engagée (article 1384) lors d'un fait d'un salarié, lors d'un dommage ou d'un fait « commis dans le cadre de ses fonctions ». Mais la fiche poste ne suffit pas pour définir ce cadre.

Pour qu'il y ait responsabilité, il faut :

- une faute,
- un dommage, et
- un lien de causalité entre faute et dommage

Exemple :

- 1 faute (un pot de fleur qui tombe d'un balcon)
- 1 dommage (il touche quelqu'un, il pourrait tomber à coté)
- 1 lien de causalité (le pot de fleur a blessé quelqu'un, la blessure de la personne aurait pu être provoquée par quelque chose d'autre que le pot de fleur)

Au niveau du lien de causalité, il existe des causes d'exonération : la force majeure, la faute du tiers ou la faute de la victime. Un exemple de cause d'exonération : pour la formation juridique à Marseille, les supports sont arrivés en retard . Si la délégation du CNRS de Marseille « attaque » Comundi, celle-ci devra prouver une cause exonératoire : crash (forte majeure) , retard de livraison (faute du tiers) ou lieu de livraison incorrecte (faute de la victime).

La durée maximale pour engager la responsabilité de base en civil en général est de 30 ans sauf prescription spéciale (10 ans pour les contrats électroniques, 1 an pour les facture Télécom...).

Pour être sûr d'avoir des preuves valables, il vaut mieux travailler dans un contexte juridique

(demander à un juge, à un huissier), même lorsqu'il existe des preuves en local.

Qu'est-ce qu'une preuve fiable ?

. est-ce que vous dites la vérité ?
(seul l'huissier a l'obligation de dire la vérité)
. éléments conservés dans des conditions fiables
(l'huissier garde sous scellés la preuve).

Responsabilité Civile contractuelle

Un contrat peut être unilatéral (engagement de confidentialité) ou signé par deux ou plusieurs parties.

Si la charte informatique est annexée au règlement intérieur du laboratoire elle n'a pas à être signée par les agents CNRS. Une charte ne peut concerner que les personnels de l'établissement. Les personnes détachées sont soumises à la charte si la convention entre les deux établissements indique que le personnel doit suivre le règlement intérieur de l'endroit où il est détaché.

En ce qui concerne les étudiants majeurs, il n'y a pas de loi dans leur cas sur l'utilisation résiduelle car du point de vue juridique il n'y a pas de cadre professionnel (ils ne font pas partie du personnel de l'établissement).

Respect du Contrat : entre employeur et employé, règlement intérieur du Labo, la responsabilité est engagée en cas de :

- Inexécution d'une obligation
- retard dans l'exécution
- Mauvaise exécution

Pour expliquer une mauvaise exécution, il faut avoir un référentiel de base. Souvent nous avons un cahier des charges. Mais comme nous travaillons sur de gros projets, nous avons des évolutions sur le projet. Donc le référentiel de base n'existe plus.

Nous, ASR avons un engagement contractuel : respecter le circuit fonctionnel en cas d'incident de sécurité.

Obligation de résultat *vs* obligation de Moyens : faux débat et faux amis... dans les 2 cas on a un objectif et donc un résultat à atteindre

Si le contrat comporte une obligation de moyens pour le client.C'est au client d'apporter la preuve que la prestation n'est pas correcte. c'est au créancier/client de prouver que le débiteur n'a pas mis les moyens en oeuvre pour atteindre les résultats.

Si le contrat comporte une obligation de résultats : c'est celui qui doit la prestation qui doit apporter la preuve que si elle n'a pas été faite c'est un cas de force majeure ou de la faute de l'autre.

Dans le contrat de travail, il n'y a pas d'obligation de moyens, ni de résultat.
==> on ne peut pas être responsable si les moyens ne se sont pas donnés.
Pour les ASR, si nous avons formulé une demande et que l'on ne nous donne pas les moyens, nous ne sommes pas tenus à une obligation impossible.

Un Labo CNRS est un environnement complexe et dangereux en matière de SI

- beaucoup de données sensibles
- les utilisateurs sont mal identifiables et peu sensibilisés
- le droit est -d'application stricte

Responsabilité Pénale

Il y a peu de recul jurisprudentiel en Droit Pénal en matière de SSI car les lois nouvelles datent de 2001, et un jugement complet dure environ 6 ans (affaire : 2ans, appel : 2 ans, cassation : 2 ans), et donc peu de recul jurisprudentiel sur les nouvelles lois.

Schématiquement, on peut distinguer :

Contravention	pas de prison
Délit	moins de 10 ans de prison
Crime	plus de 10 ans de prison

On a obligation de dénoncer les délits et les crimes

Concernant la responsabilité pénale, les auteurs et les complices sont punis de la même peine.

Pour être poursuivi il faut :
- 1 élément légal : un texte du Code pénal
- 1 élément matériel : 1 faute
- 1 élément psychologique : avoir eu conscience de commettre une faute

Dépend du Pénal, notamment:
- Contrefaçon
- diffamation
- Injures
- Racisme
- Révisionnisme
- Incitation
- ouverture correspondance privées
- intrusion SI
- Altération SI
- Modification Suppression de données preuves
- Mise à disposition
- Enregistrement audio/vidéo sans autorisation
- Diffusion et stockage d'image à caractère « pédo »...
- non déclaration à la CNIL
- pas de notices Légale sur site Web
- (...)

Attention : en matière de SI : Les rôles sont renversés
- si infraction pénale *traditionnelle* : par exemple un intrus dans une maison... ça n'est pas à quelqu'un de dire qu'il y a un intrus chez moi... quelqu'un qui entre sans autorisation dans une maison n'est pas chez lui et est considéré comme un intrus:
- Dans le cadre d'un SI ; l'ASR ***doit apporter la preuve qu'il y a un intrus*** et ***qu'il a mis les moyens en oeuvre pour spécifier que c'est un intrus***!

Un élément légal : s'il n'y a pas de texte, il n'y a pas d'infraction.

Vol de login/mot_de_passe : c'est de la captation d'identité numérique. Il faut attendre que le voleur utilise ces "login/mot_de_passe" pour qu'il puisse être accusé d'usurpation d'identité.

- Responsabilité personnelle

La responsabilité personnelle est engagée dans quelques cas comme refus illégitime d'accomplir un acte, ou manquement à une obligation.
Par exemple si on télécharge massivement des données à titre personnel, notre responsabilité

personnelle est engagée.

- Responsabilité partagée

On peut déléguer une responsabilité pénale à quelqu'un. Par exemple un chef d'Entreprise délègue sa responsabilité à un chef de chantier

Il n'y a pas de délégation Pénale en Administratif ==> Le Directeur d'unité ne peut pas déléguer sa Responsabilité sur le plan Pénal

Pour qu'il y ait délégation de responsabilité pénale : il faut un document signé par la personne qui accepte la délégation. La personne doit avoir l'autorité et les moyens.
L'acte de Délégation DOIT définir ce sur quoi on fait porter la Délégation !

Si on n'a pas les moyens d'appliquer correctement une politique de sécurité, il faut l'indiquer PAR ECRIT! « Pour agir efficacement il me faut .... »

Il n'existe pas de délégation dans les organismes publics. L'ASR n'a pas de délégation pénale : il n'a pas la responsabilité de l'employeur au niveau pénal.

- La plupart des infractions liées à notre métier : ouvrir la boite mail des utilisateurs, intrusion, altération des données...(voir le chapitre sur la « Lutte contre la cybercriminalité » pour le reste des infractions relevant du pénal) relèvent du pénal. Mais dans la jurisprudence actuellement, la plupart des affaires sont jugées en civil.

- - Rappel : N'oubliez pas que « nul n'est censé ignorer la loi », pas plus les ASR que les autres

- En fait, on considère les 3 catégories suivantes: le FAI (fournisseur d'accès Internet), l'hébergeur et l'éditeur dans la loi. Mais cette loi a commencé en 1996. Donc le web2 (blog, forums, chat, enchères électroniques,etc..) n'est pas traité. La responsabilité de l'éditeur est beaucoup plus importante que celle de l'hébergeur ou du FAI.

- De nombreux contrats comportent des clauses abusives (ex: Apple, les fournisseurs de téléphone...), qui permettent de les faire déclarer nuls devant une juridiction. Il est même parfois intéressant de signer un tel contrat, quitte à l'attaquer en justice si besoin.

- Cas pratique : Affaire CYBERLEX.

- Cyberlex est une association loi 1901 créée en 1996 : cyberlex.org. Le directeur de la publication, également président est un avocat. Le contenu est libre et gratuit. Cette association comprend 80 membres qui se réunissent une fois par mois sur un thème : échanger les meilleures techniques dans les TICE.
  Le webmaster écrit un article sur « comment (ne pas) payer sur l'internet » et cite des logiciels qui génèrent des numéros de cartes bleues bidon. Il dit que ce n'est pas bien mais donne sur son site 2 liens sur 2 logiciels. Dans le magazine « Que Choisir » : l'article apparaît et l'auteur est cité comme un voyou ... Cyberlex demande au magasine "Que Choisir?" de retirer l'article ou d'avoir un droit de réponse.. qui est refusé.
  Le président de Cyberlex intente une action en justice pour diffamation contre « Que choisir? », et le webmestre une action pour contrefaçon.
  Conclusion : L'association a finalement été considérée comme « coupable » de négligence fautive n'ayant pas spécifié de règles de vérification des articles à mettre en ligne. Le jugement donne raison à « Que Choisir ? » : on est dans un cas d'imprudence et de négligence fautive de la part de Cyberlex qui a laissé des liens vers des sites de pirates, qui malgré l'objectif pédagogique, ont été jugés comme une «incitation au

délit»

Il aurait pu être accusé de complicité (faute pénale).
Le jugement a eu lieu en référé donc la contrefaçon n'a pas été traitée.

2- Responsabilité et SSI

On a renversé la donne en matière de politique de sécurité des Systèmes d'Information.

Ex : un intrus est un intrus que s'il a conscience d'être un intrus.

- Lois de sécurité intérieure (LSI) et quotidienne (LSQ), loi pour la confiance dans l'économie numérique (LCEN), loi de sécurité financière (LSF), accords de Bâle II, loi Sarbanes-Oxley (Sox), Convention de Budapest, Règles européennes, constituent maintenant un véritable droit autonome sur la SSI.

  Le droit à la sécurité devient un droit fondamental et l'une des conditions de l'exercice des libertés individuelles et collectives.

- L'acronyme STAD signifie « Système de Transmission Automatisé de Données »
- La notion de traçabilité apparaît dans la LSQ (Loi Sécurité Quotidienne) vers 2001.
- LSI : Loi sur la Sécurité Intérieure
  On donne autorité au juge de pouvoir décrypter
- LSQ : loi de sécurité quotidienne
  loi qui permet la fouille des sacs à main à l'entrée des magasins
  C'est là aussi qu'il y a une première opération qui demande aux hébergeurs de conserver les traces de connexion (mais pas le contenu) pendant 1 an.
- LSF : Loi sur la Sécurité Financière
  Cette loi introduit deux obligations pour les banques : audit interne, mettre en place des plans de continuité d'activité (PCA).
- LCEN : Loi pour la Confiance en l'Economie Numérique (nous donne tout le cadre juridique de l'utilisation d'Internet) :
- Le terme de cybercriminalité apparaît pour la première fois dans la LCEN. La LCEN comporte plusieurs décrets. Tous ne sont pas parus. La cybercriminalité permet lutte contre les atteintes au système d'informations.

- Dans la Convention de Budapest, il s'agit d'harmoniser les condamnations dans quasiment tous les pays industriels. Elle autorise la perquisition sur des serveurs à l'étranger... Un service disponible 7j/7j et 24h/24h est mis en place en cas de crise.
  Cette convention veille à ce que tous les pays signataires ait les mêmes infractions informatiques, les mêmes peines, et qu'il y ait une collaboration entre les différents services de chacun de ces pays.

- Norme ISO 27001 : 1ere norme de certification sur la sécurité des SI
- Terrorisme : cette loi renforce l'obligation de tracabilité à tous ceux qui offrent un accès Internet. Elle donne une OBLIGATION de traçabilité de tous les moyens donnant accès aux SI (cyber café, chambres universitaires, bornes wifi y compris celles personnelles, etc...

- La loi n^{o} 78-17 du 6 janvier 1978 Informatique et Libertés a été modifiée en Juillet 2004. La CNIL voit ses pouvoirs de contrôle et de sanction renforcés. Le code pénal prévoit 5 ans d'emprisonnement et 300 000€ d'amende pour un traitement de données à caractère personnel sans mise en oeuvre des mesures prévues par la loi. Pour rappel, est considérée « donnée personnelle », toute information qui permet d'identifier une personne physique. La simple consultation des données est considérée comme un traitement de données.

Des « correspondants Informatique et Liberté" doivent être nommés au sein des entreprises. CIL sont les garants du respect de la loi.

- Exportation de données hors de l'Union Européenne: il est interdit d'exporter des données hors de l'U.E., sauf avec les pays avec lesquels il existe un accord explicite: Suisse, Australie, Canada, Argentine, Iles anglo-normandes. Dans les autres cas il faut s'assurer que le sous-traitant applique le même niveau de sécurité dans les traitements que le nôtre et établir une convention de flux transfrontière. Ces règles concernent par exemple les laboratoires CNRS implantés à l'étranger.
  (Actualité: 10/04/08 - Les moteurs de recherche sommés de respecter la protection des données personnelles selon l'UE : http://www.legalis.net/article.php3?id_article=2269)

- L'union européenne commence tout juste à s'intéresser à la sécurité informatique.

-

- . Par exemple, s'il entre dans un intranet, il faut que les pages soient marquées comme « appartenant à l'intranet » ou confidentielles. **Un espace privé (un site intranet, un document interne) doit être non seulement protégé contre les accès non autorisés mais faire connaître à tout visiteur (autorisé ou non) qu'il se trouve sur un espace privé. Pour les documents internes l'usage de modèles, comportant les mentions de confidentialité, est une bonne méthodologie.**

-

Exemples de Jurisprudences pour illustrer l'obligation d'informer et de Sécuriser

- Jurisprudence CNRS (1996) :

- Le jugement est sur le lien http://www.legalis.net/breves-article.php3?id_article=107
- Il n'y a pas de résumé (c'est la raison pour laquelle il n'est pas repris dans ce document) et le jugement rendu est exceptionnel

Ce qui est à retenir plus globalement, c'est qu'on ne peut pas traduire, modifier, adapter, transformer, arranger, reproduire, représenter, et diffuser une oeuvre sans le consentement de son auteur. A la seule exception :

1. d'une utilisation à des fins privées comme la représentation dans le cercle de famille
2. d'une revue de Presse
3. d'une courte citation

- Jurisprudence TATI (2001)

Résumé du jugement (http://www.legalis.net/breves-article.php3?id_article=936) :
Fraude informatique : l'animateur de kitetoa.com relaxé 04/11/2002

L'animateur du site kitetoa.com, condamné en première instance pour accès frauduleux dans un traitement automatisé de données, vient d'être relaxé par la cour d'appel de Paris, le 30 octobre 2002. Le juges ont ainsi suivi les réquisitions du parquet général de la cour de Paris qui avait demandé l'infirmation du jugement TGI de Paris du 13 février 2002. Pour le procureur général, le caractère frauduleux de la manipulation n'a pas été établi par la procédure. Le webmaster de kitetoa.com avait pris connaissance d'un répertoire-clients sur le site tati.fr, en utilisant les fonctionnalités du navigateur Netscape. Or, remarque le procureur général, il n'a utilisé aucune méthode de piratage mais une manipulation "accessible à tout internaute averti, non ingénieur, non technicien, non spécialisé, mais qui sait lire un mode d'emploi". Le procureur général a, par ailleurs, estimé que l'élément intentionnel de l'acte n'a pas davantage été établi, d'autant moins que l'animateur de kitetoa.com avait averti les administrateurs de Tati de cette faille de sécurité. "Lorsqu'une base de données est, par la faute de celui qui l'exploite, en accès libre par le biais de l'utilisation d'un logiciel de navigation grand public (...),

le seul fait d'en prendre connaissance (...), d'en réaliser une copie (par simple copie d'écran, ce qui a été le cas) sans intention malveillante, sans révélations permettant d'éventuelles identifications (de codes, de chiffres comptables, de clients d'une société par exemple, ...) ne saurait constituer une infraction". Le parquet général avait fait appel afin de permettre à la cour de se prononcer sur la définition et la portée du délit d'accès et de maintien frauduleux dans un système d'information. Il faudra attendre le texte de la décision de la cour, pas encore disponible à ce jour, pour savoir si elle a suivi les arguments du parquet général.

- Le détail du jugement : http://www.legalis.net/jurisprudence-decision.php3?id_article=136

- Jurisprudence Lucent :

- Le résumé (http://www.legalis.net/breves-article.php3?id_article=359):
- Un employeur jugé responsable d'un site litigieux réalisé par son salarié 08/08/2003

Par un jugement du 11 juin 2003, le tribunal de grande instance de Marseille a condamné sur le fondement de l'article 1384 alinéa 5 du code civil, l'employeur du créateur d'un site internet litigieux pour avoir mis à disposition de son salarié les moyens techniques nécessaires à la mise en ligne dudit site.

Nicolas B. employé par la société Lucent Technologie avait créé à son domicile un site internet satirique dénommé « escroca.com » pour dénoncer les abus dont faisait preuve selon lui la société Escota, concessionnaire de la construction et de l'exploitation d'autoroutes du sud-est de la France, à l'encontre de ses usagers. Il avait par la suite procédé à la mise en ligne de son site personnel depuis son poste de travail. Bien que Nicolas B. ait qualifié sa démarche d'humoristique et de parodique, le tribunal a considéré, pour rejeter le bénéfice de l'exception de parodie de marque, que « l'imitation de la marque n'était pas guidée par l'intention d'amuser sans nuire mais motivée par des sentiments haineux et dont l'objet est de dénigrer la société et d'atteindre son image de marque » (Cf. a contrario, les deux précédents : « Jeboycottedanone.com » et « Greenpeace » dans lesquels les juges avaient estimé que le droit constitutionnel à la liberté d'expression primait sur le droit des marques).

Le créateur des pages personnelles a donc été condamné à payer à la société Escota 1€ de dommages-intérêts et à supporter les frais de publication de cette condamnation Ã hauteur de 8 000 € maximum. Il devra en outre relever et garantir son ancien employeur des condamnations prononcées à son encontre, le tribunal ayant également retenu la responsabilité de la société Lucent Technologie du fait des fautes commises par son employé. Le tribunal a considéré que la faute de Nicolas B. a été commise dans le cadre des ses fonctions, puisque « le site litigieux a été réalisé sur le lieu de travail grâce aux moyens fournis par l'entreprise ». Dès lors, il importe peu que le salarié ait agi en dehors de ses attributions professionnelles et sans autorisation de son employeur.

- Détail du jugement : http://legalis.net/analyse_statistique.php3?id_article=1611

- Jurisprudence ESPCI (1998)

Le résumé (http://legalis.net/breves-article.php3?id_article=1007):
Pas de cybersurveillance à l'insu des personnes 25/12/2001

La décision de la cour d'appel de Paris du 17 décembre 2001, sur une affaire relative au secret dû au courrier électronique, dans le cadre d'une mission d'enseignement, fait l'objet d'un pourvoi en cassation. L'étudiant avait porté plainte contre les dirigeants de l'Ecole supérieure de chimie qui étaient intervenus sur sa boîte aux lettres pour conforter un certain nombre de soupçons qu'ils développaient à son encontre. Le TGI de Paris les avaient condamnés, le 2 novembre 2000, pour violation du secret des correspondances effectuée par voie de télécommunications, par personne chargée d'un service public, à des demandes respectives de 10 000 F et 5 000 F, ainsi qu'à une

somme globale de 10 000 F à titre de dommages-intérêts. La cour d'appel a confirmé le statut de correspondance privée du mail. Mais la complexité de l'affaire et les circonstances troublées du délit ont été prises en compte pour conduire à une réformation des peines, assorties de sursis. L'étudiant a été invité à faire valoir son préjudice auprès d'une juridiction administrative. Cette décision va dans le même sens que bien d'autres sur ce sujet : des mesures de surveillance prises à l'insu de la personne sont illicites, et seul le juge a autorité pour faire ouvrir un courrier personnel. Les circonstances de sécurité informatique ne sauraient constituer, à elles seules, des éléments justifiant des empiètements sur la vie privée de l'individu.

Détail du jugement : http://www.legalis.net/jurisprudence-decision.php3?id_article=1182

- Jurisprudence administrateur :

- Un ASR a été licencié pour avoir téléchargé illégalement et en grande quantité des logiciels,... ce qui relève de l'art. 1382.

3- Les règles du jeu de la SSI

- Information-Contrôle-Action

- La solution pour se prémunir est de **Informer, Contrôler et d'Agir**

- Le RSSI se doit d'avertir, de renseigner, d'informer, de mettre en garde, aussi bien le responsable légal, les autorités compétentes, et surtout les utilisateurs, des risques dont il a connaissance de préférence par écrit (mails ou notes papier)

- **Informer et former:** faire des rapports réguliers (annuel) et sur situation particulière. Il faut informer les responsables légaux, les autorités compétentes, informer et former les utilisateurs.

- Alerte et conseil: En tant qu'experts sur un domaine technique classé dangereux (depuis la jurisprudence IBM-Flammarion) au même titre que le nucléaire et le risque chimique (SEVESO), les administrateurs sont tenus à une obligation de conseil renforcé. Il peuvent émettre des **alertes** (sur des risques connus) ou des **mises en garde** (sur des risques possibles)... La mise en garde permet de signaler qu'il est possible qu'un problème intervienne. L'alerte permet d'informer d'un problème bien défini et connu (et non hypothétique). La ***présence de ces mot-clés*** dans un rapport peut avoir un poids utile en cas de contentieux ultérieur

- Droit d'agir: diagnostic, analyse, contrôle, maintenance préventive, identification des comportements illicites. Le plan de sauvegarde concourt non seulement à garantir la continuité de l'activité mais aussi à maintenir la disponibilité des preuves.

- Droit de réagir: pour assurer la continuité du service, en cas de crise ou d'urgence, et droit de refuser des demandes qui mettraient le SI en danger.

- Notion de crise : c'est une situation qui paralyse le laboratoire ou l'établissement entier ou 1 personne à un moment critique (rendre un rapport de contrat).

- **Confidentialité:** les administrateurs sont tenus au secret professionnel, mais ont l'obligation de dénoncer des actes délictueux: contenus illicites, notamment la pédo-pornographie ou la diffamation.

- A propos des logiciels "libres" : le libre "de droits" n'existe pas (libre de royalties tout au plus) du fait que le libre est associé à une sorte de contrat d'utilisation qui définit des

règles donc des droits d'utilisation. Le bon terme juridique à utiliser est la licence libre (= contrat).

- **Respect du droit des tiers:** la vie privée résiduelle est constituée des activités et documents qu'un employé possède ou réalise sur son lieu de travail: rendez-vous, urgences familiales...Cet espace doit être repéré par des conventions de nommage: dossier « Privé », entêtes de message [Prive], de façon à garantir leur caractère. L' utilisation des logiciels selon les licences, respect des droits d'auteur, dispositifs contre les téléchargements pirates.

- **Responsabilité professionnelle:** La clarté des missions, la mise en place de référentiels (Schéma directeur, charte, recueil des procédures, guide utilisateur,..) et le respect de normes et des règles de l'art participent à la qualité professionnelle.

- La responsabilité personnelle est engagée dans quelques cas comme refus illégitime d'accomplir un acte, ou manquement à une obligation. Par exemple si on télécharge massivement des données à titre personnel, notre responsabilité personnelle est engagée

- On peut déléguer une responsabilité pénale à quelqu'un. Par exemple un chef d'Entreprise délègue sa responsabilité à un chef de chantier

- Il n'y a pas de délégation Pénale en Droit Administratif ==> Le Directeur d'Unité ne peut pas déléguer sa responsabilité sur le plan Pénal

- L'acte de Délégation DOIT définir ce sur quoi on fait porter la Délégation ! Si on n'a pas les moyens d'appliquer correctement une politique de sécurité, il faut l'indiquer PAR ECRIT! « Pour agir efficacement il me faut .... »

- On peut définir une charte basée sur le principe de l'éthique, « règle de bonne conduite » ou celui de la « régulation » qui suppose une procédure de mise en place précise. On obtient, au niveau du droit, respectivement un « code » ou un « encadrement » (dans ce cas, la charte est annexée au règlement intérieur). Dans le cas d'une charte/code, si les règles ne sont pas suivies, elles ne peuvent pas être sanctionnées. Dans le cas d'une charte/encadrement, elles peuvent l'être.

- Une charte acceptée (qu'elle soit signée indépendamment ou annexée au règlement intérieur) est un élément de droit. Elle est assimilée à un contrat, et doit donc être **comprise pour être valide**. Elle complète un dispositif qui peut être constitué de normes, plan de continuité d'activité, audit, actions de sensibilisation.
- **A noter:** pour les visiteurs il peut être avantageux et rapide de créer un **contrat « Clic ».** C'est un contrat souscrit par acceptation sur un formulaire électronique et qui ouvre un accès temporaire aux moyens informatiques.

- La charte – Le livret des procédures

- Dans la charte : on parle des droits, des obligations et des sanctions. Elle doit couvrir tout un champ technique. Le problème est que les technologies évoluent très vite et le risque, si on se limite à ce champ technique uniquement, est de ne pas pouvoir les traiter dans la charte (web2, blogs, podcast ...). La solution est d'avoir une charte qui aborde également un ***champ fonctionnel***, c'est-à-dire une régulation par le comportement. Ce champ couvre les usages au niveau de la correspondance, du surf, des discussions et de l'édition.

- Le champ fonctionnel définie les usages au niveau de la correspondance, du surf, de la discussion et de l'édition. La notion de correspondance est assez large pour englober, à

la fois ce qu'on connaît actuellement comme la lettre normale, le mail, la messagerie instantanée mais également d'autres technologies avenirs liées à la notion de correspondance. La discussion concerne les blogs, le chat, les espaces collaboratifs. L'édition inclut le journal d'entreprise, les tracs, les blogs, le web.

- Ce n'est pas possible d'interdire l'internet à usage personnel et la correspondance privée au sein de l'entreprise dans la charte car il y a la ***notion de vie privée résiduelle :*** c'est un «espace» de vie privée au travail. C'est la possibilité d'avoir du courrier et un dossier personnels.

- La charte CNRS est un exemple qui marie bien le champ fonctionnel et le champ technique. (Texte de la charte : http://www.dsi.cnrs.fr/BO/2007/03-07/415-bo0307-dec070007dAj.htm, et la FAQ : http://www.sg.cnrs.fr/fsd/securite-systemes/faq.htm)

- L'idéal serait, concrètement, de mettre en place les documents suivants :
  - Une charte pour les utilisateurs extérieurs,
  - une charte administrateur,
  - une charte personnels, un guide et un livret des procédures. La charte des personnels doit citer un guide dans lequel on trouvera toutes les références aux textes de lois et citer également un livret des procédures. L'avantage est d'avoir ainsi une charte valable assez longtemps sans modification. Le guide et le livret pouvant être révisés régulièrement et la procédure en est simplifiée (pas de re-validation devant un conseil de laboratoire ou d'administration).

Le livret des procédures est une déclinaison technique de la charte :

- Exemple 1 : Charte : « L'utilisateur doit se conformer aux dispositifs mis en place pour lutter contre les virus et les programmes ... ». Livret technique : toute machine connectée au réseau doit comporter un antivirus à jour. Les machines gérées par le service informatique sont automatiquement reliées au serveur antivirus.
- Exemple 2 : Charte « il lui appartient de protéger ses données en utilisant différents moyens de sauvegardes individuels ou mis à sa disposition ». Livret technique : expliquer ce qui est sauvegardé, la fréquence, comment récupérer ce qu'on a détruit par erreur.
- Exemple 3 : Charte « il doit choisir des mots de passe sûr ». Livret technique : citer la note du CERTA sur le choix d'un mot de passe. Préciser qu'un renouvellement automatique annuel est programmé.

- Pour mettre en place les documents cités ci-dessus, des supports et des moyens sont nécessaires comme les IRP (les Instances Représentatives du personnel) , la commission I & L (Informatiques et Liberté), le contrat clic (qui fait référence au bouton « I agree » à la fin d'un texte à lire). Sont nécessaires également l'information, la formation; l'assistance et la médiation.

  Concernant la charte administrateur, il est préférable de parler d'une charte des droits d'administration plutôt que d'une charte des administrateurs . Cela permet d'étendre cette charte aux personnes qui disposent de ces droits sans avoir pour autant une fonction d'administrateur. Un exemple de charte administrateur a été distribué à la session de Caen.

- Il n'existe pas de délégation dans les organismes publics. L'ASR n'a pas de délégation pénale : il n'a pas la responsabilité de l'employeur au niveau pénal.

4- SSI et numérique

- Il existe plusieurs types de preuve civile : celle d'un fait juridique, d'un acte juridique, la preuve contractuelle et la preuve hors contrat. Un acte juridique est un contrat, écrit ou électronique. Un fait est libre, cela peut-être n'importe quel type de preuve.
- La preuve électronique admise : (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 identifié la personne dont il émane et qu'il soit conservé dans des conditions de nature à en garantir l'intégrité »

- Tout ce qui est électronique depuis 2004 est probant (= peut servir de preuve). Avant c'était l'écrit. Elle est admise si on est sûr de l'identité de l'auteur et des conditions d'archivage. Il faut donc privilégier les signatures électroniques par certificat. Par contre, rien ne définit dans le droit ce qui est intègre. La justice se base donc sur la norme AFNOR Z42-013 sur archivage électronique
  - http://www.boutique.afnor.org/NEL5DetailNormeEnLigne.aspx?&nivCtx=NELZNELZ1A10A101A107&ts=1680673&CLE_ART=FA118461
- Le hic : Cette norme AFNOR Z42-013 ne concerne que les supports non réinscriptibles.
- Convention sur la preuve : « *Lorsque la loi n'a pas fixé d'autres principes, et à défaut de convention valable entre les parties, le juge règle les conflits de preuve littérale en déterminant par tous moyens le titre le plus vraisemblable* » : Si la preuve n'est pas conforme aux conditions citées ci-dessus au (1), alors ça se discute : selon le bon sens et l'avis du juge. L'existence d'une convention de preuve est aussi prise en compte (Qu'est-ce qu'une convention de preuve ? :( )

5- Lutte contre la cybercriminalité

I*l existe 4 articles fondamentaux du Code Pénal concernant la fraude Informatique:* ***323-1, 323-2, 323-3*** *concernant les atteintes aux systèmes de traitement automatisé des données :*

- *http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070719&idArticle=LEGIARTI000006418315&dateTexte=20080523*
- *http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=836251FC3C56DB0A0D74C1C931C22FDB.tpdjo17v_3?idArticle=LEGIARTI000006418319&cidTexte=LEGITEXT000006070719&dateTexte=20080523*
- *http://www.legifrance.gouv.fr/affichCodeArticle.do;jsessionid=836251FC3C56DB0A0D74C1C931C22FDB.tpdjo17v_3?idArticle=LEGIARTI000006418322&cidTexte=LEGITEXT000006070719&dateTexte=20080523*

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit 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

- Un rappel sur les articles du code pénal 323-1, 323-2, 323-3, 323-4 :
  - sont réprimés l'accès frauduleux, la tentation elle-même est punissable,
  - le maintien sur un système, l'entrave au fonctionnement ,
  - l'introduction, la suppression, la modification de données,
  - mais également la mise à disposition de tout dispositif permettant de le faire, contrefaçon, diffamation, injures, racisme, révisionnisme, incitation, ouverture de correspondance privées, enregistrement audio/vidéo sans autorisation, diffusion et stockage d'image pédophile, la non déclaration à la CNIL, pas de notice légale sur site Web.

- Un huissier ne peut pas venir de sa propre volonté c'est sur décision de justice.

6- Données personnelles

- Utilisation des moyens numériques à des fins personnelles : Vie privée Résiduelle

Au niveau du Laboratoire , il est nécessaire de définir les règles du Jeu : par exemple : A t-on le droit de brancher un portable personnel dans le réseau de l'entité? Avec contrôle? Sans contrôle?

- Il n'est pas permis d'interdire l'utilisation des outils de communication pour la vie privée résiduelle. On autorise l'utilisation des outils de l'entreprise de manière exceptionnelle (téléphoner 2h à des fins personnelles avec le téléphone de l'entreprise ne fait plus partie de la vie privée résiduelle)

- Cas sur la DR12 (Marseille) ; 1 PC utilisateur échange +100Go de contenu en quelques heures. Le PC est retrouvé, l'utilisateur n'est pas son propriétaire. Quelle est la responsabilité du laboratoire si l'utilisateur télécharge depuis son PC ou depuis un poste en libre accès ? A t-on le droit de faire le contrôle sur ce PC? Il a fallu ouvrir des fichiers pour voir le contenu illicite (film DIVX), en a t-on le droit ? La personne reconnaît verbalement avoir téléchargé.

  Il faut faire un compte rendu du problème et des actions engagées. Il faut apporter des preuves du contrôle et des actions engagées.
  Ne pas sanctionner la personne qui a effectué le téléchargement rendrait le laboratoire complice! Il faut apporter une preuve de sanction pour se couvrir : faire une lettre au contrevenant, effectuer une copie du disque, sanctionner ou donner un blâme
  Il faut donc mettre en place une charte très claire sur les utilisations autorisées à partir de la connexion Internet. Pour ne pas être poursuivies pour négligence, les entreprises doivent également effectuer des contrôles et intervenir si des abus sont constatés.

  Bien répartir les rôles : l'ASR a informé, contrôlé, et agi... les preuves sont récoltées et sauvegardées. Pour porter plainte s'il y a un problème de procédures, ce n'est plus le problème de l'ASR

- Les contrôles doivent répondre à des objectifs légitimes: exigence de sécurité, de prévention, gestion et optimisation des ressources, protection des intérêts de l'institution. Les actions doivent répondre aux obligations légales de sécurité et de traçabilité.

- La nouvelle loi Informatique et Libertés (7 Aout 2004) transpose une directive européenne 95/46/CE, renforce les sanctions (pénales, financières et administratives) et les droits des fichés.

- Quelques incriminations pénales:
  Traitements sans formalités préalables, non respect des normes simplifiées, traitement non autorisé du N° INSEE (idem S.S.), collecte frauduleuse, déloyale ou illicite, non respect des droits d'opposition, enregistrement de données sensible à l'insu des personnes, non respect des durées de conservation, détournement de finalité, divulgation de données à des tiers, transferts de données hors CE sans autorisation...Les sanctions les plus graves sont de 5 ans d'emprisonnement et 300 000€ d'amende.
  La moyenne des sanctions financières se situe à 80 000€.
- L'utilisateur ne peut s'opposer à la publication d'un organigramme de l'entreprise (sur lequel il est présent) sur son web, ouvert à tous (il peut s'opposer à l'ajout de sa photo).

- On n'a pas le droit d'exporter les données en dehors de l'Union Européenne et vers 5 pays de niveau de protection adéquate (dont la Suisse, l'Australie, le Canada, les Iles Anglo-normandes et l'Argentine). En dehors de ces pays (y compris les USA), il faut s'assurer que le prestataire offre un niveau de protection équivalent : il faut un modèle de convention.

- LA CNIL

- La réglementation CNIL qui datait de 1978 a été revue en 2004 :

1) Avant, il y avait deux mondes : le public et le privé . Aujourd'hui le raisonnement porte essentiellement sur la sensibilité de la donnée.
2) ***Les pouvoirs de la CNIL ont considérablement augmentés*** :
    - Le droit d'enquête in situ (comme la police de 6h00 à 22h00)
    - Le droit de juger (sous couvert direct de la cour d'appel)
    - Le droit de prononcer une condamnation pécunière (fait office de huissier de justice)ela a eu pour conséquence une augmentation des procédures et des condamnations.
3) Les sanctions étaient trop dures (elles relevaient du Pénal). On est passé à des sanctions pécunières plus dissuassives (150 k€ la première fois, jusqu'à 300k€ possible).
4) Nomination d'un **CIL**

- Il faut donc respecter les 4 points suivants :

  A – Faire une déclaration (ou "démarche préalable") CNIL. Elle peut prendre 4 formes :
  . régime d'exemption (sites personnels non marchands, annuaires des téléphones portables ..)
  . régime de déclaration simplifiée (des modèles tous faits sont disponibles sur le site de la CNIL comme par exemple la gestion du personnel : il faut néanmoins vérifier que l'on soit conforme aux limites de ces canevas pré-établis)
  . régime de déclaration normale. Ex : pour de la cybersurveillance ou un trombinoscope.
  . régime d'autorisation expresse (à utiliser si on traite des informations sensibles comme le N° de sécu, des données bio-métriques, le casier judiciaire privé, les données génétiques, de santé, de situation financière des personnes ou si on fait une interconnexion de fichiers comme par exemple, dans une mairie l'interconnexion des fichiers « piscine », « accès bibliothèque » pour mettre en place une carte de vie quotidienne.
  . NB : notion de responsable de traitement : dans certains cas, on peut faire des déclarations communes à plusieurs structures si elles sont solidaires dans un traitement de données.

  B – Informer les utilisateurs (en application de l'article 27...? , obligatoire sur tous les formulaires)

  C – Permettre l'accès aux données collectées et leur modification ou rectification par les utilisateurs.

  D - D'assurer le niveau de sécurité soit au niveau du responsable du traitement, soit au niveau du sous traitant éventuel. Il faut prévoir, dans ce dernier cas, cette définition dans le contrat, le sous traitant devant respecter le niveau de sécurité défini par le responsable du traitement.

- Les CIL : Correspondants Informatique et Libertés

Suite à un partenariat entre la CPU (conférence des Présidents d'Université) et la CNIL il y a 1 an environ (http://www.cpu.fr/Partenariat-CPU-CNIL.282.0.html), un CIL doit être nommé dans chaque établissement.

Le CIL :
1 - un homme, une femme, une entité,
2 - il est interne à l'entité ou externe si l'entité est supérieure à 50 personnes).
3 - il doit être compétent. pas forcément informaticien. Ce sont les directeurs RH, directeurs juridiques, ou RSSI.
4 – il est désigné. Ce qui entraine une notification à la CNIL et une information aux institutions représentatives du personnel.

5 – Son objectif est de veiller à la bonne application de la loi Informatique et Libertés.
6 – Le bénéfice d'un CIL : les démarches sont simplifiées : plus besoin de déclaration simplifiée, ni de déclaration normale mais l'autorisation reste à faire. Les relations avec la CNIL sont plus cordiales.
7 – Ce que le CIL doit faire :

- la liste des traitements dans les 3 mois suivant sa nomination,
- permettre l'accès à cette liste à quiconque
- faire un rapport annuel à sa hiérarchie qui le tient à disposition de la CNIL
- être saisi avant tout nouveau traitement

Le CIL doit savoir qu'il n'est pas responsable légalement mais il a un rôle d'alerte et même de dénonciation s'il est en désaccord avec ce que lui impose sa hiérarchie.

7- Propriété intellectuelle

- On parle de propriété intellectuelle sur une oeuvre de l'esprit. La protection vient avec la formalisation/matérialisation de l'idée (cahier des charges et/ou des spécifications techniques).
- L'originalité ou l'inventivité d'une oeuvre de l'esprit n'est pas une condition de protection. La protection s'applique à l'empreinte de la personnalité de l'auteur tout simplement.
- Les différents types d'oeuvres sont :
  - Les oeuvres composites qui sont réalisées avec des oeuvres anciennes (sous réserve des accords adéquates).
  - Les oeuvres collectives. Un exemple est wikipedia.
  - Les oeuvres de collaboration
  - Les créations des salariés qui appartiennent aux salariés. Il est prudent de traiter dans le règlement intérieur les questions d'exploitation interne ou commerciale de l'oeuvre , la rémunération du salarié, les conditions de son départ de l'entreprise.
- On parle de droits d'auteur du vivant de l'auteur et de droits patrimoniaux pour les héritiers dans les 70 ans qui suivent le dépôt de la protection. Après cette période, l'oeuvre passe dans le domaine public : on parle de droit moral.
- Pour les agents publics la dévolution des droits revient automatiquement à l'employeur, au moins tant que la création a eu lieu dans le cadre des fonctions de l'agent. Il y a plusieurs interprétations et controverses sur le sujet.
- Les diverses formes du dépôt du logiciel :

  - Le dépôt sans déplacement et le dépôt chez un tiers : S'envoyer par recommandé son oeuvre constitue une preuve.

  - Le dépôt à l'APP est Agence de protection des Programmes. Elle est identique à la SACEM mais sans gérer de répartition financière. Elle permet le dépôt de programmes.

  - Le dépôt auprès d'organismes spécialisés

- Les droits d'exploitation d'une oeuvre:
  - droit de reproduction (permanente, provisoire, copie privée, copie de sauvegarde) et d'utilisation
  - droit de représentation (communication au public par tout procédé) et droit d'adaptation (livre, film, théâtre...)
  - droit de distribution
  - droit de transmission
  - droit de traduction

- La transmission des droits patrimoniaux est régie par les articles L.131-1 à L.131-8. C'est un acte juridique qui stipule la durée, la localisation géographique, les droits cédés, la modalité d'exploitation et le prix.

- A noter que l'abandon des droits patrimoniaux annoncé dans le logiciel libre est à lire en détail. Un auteur peut reprendre ses droits à tout moment.
- L'utilisation d'un logiciel libre mis en ligne par une personne qui n'en aurait pas les droits peut conduire à être contrefaisant ou complice de contrefaisant. Les sites « creative commons » sont des exemples de ce danger.

- Sites internet

- FDI : forum des droits d'internet : forum internet.org. On y trouve les jurisprudences.

- afcdp.org : Association Française des Correspondants à la protection des Données à caractère Personnel : site sur les CIL

- http://www.legalis.net/ : jurisprudences et actualités du droit du numérique.
- INPI : Institut National de la Propriété Industrielle. http://www.inpi.fr/

- APP : Agence pour la Protection des Programmes. http://app.legalis.net/

- http://www.alain-bensoussan.com/ Droit des technologies avancées

- http://www.ossir.org - Observatoire de la Sécurité des Systèmes d'Information et des Réseaux

- http://www.cnil.fr/ Commission Nationale Informatique et Libertés

- http://www.legifrance.gouv.fr Service public de la diffusion du droit

- A retenir dans le quotidien des ASR:

1- En général :

La Sécurité des Systèmes d'Informations (SSI) et le « nouveau droit » : Le droit numérique n'en est qu'à ses balbutiements.

De plus, le SSI doit être conscient que le droit n'est pas son métier et qu'il ne peut ni être au courant de tout, ni s'y "réferer" : ce dernier point veut dire qu'il ne doit surtout pas se prononcer au regard d'éléments juridiques (c'est le rôle des avocats) car alors il deviendrait "responsable".

Il doit cependant savoir que ce droit évolue, se comporter en "curieux", surtout en cette période de profonde mutation. On est sur un nouveau droit. On va nous reprocher de ne pas savoir que ce nouveau droit existe.

Les PSSI sont très récentes, et les chartes ne stipulent que les droits et devoirs des utilisateurs au sens large. Il y a une ***absence cruelle de définition de poste d'ASR au CNRS comme à l'EN,*** il y a nécessité :

- de travailler sur des lignes directrices (textes de lois existant et cas de juriprudence...)
- d'améliorer « la visibilité du métier » en:

1. créant un « réseau de compétence », une émulation autour de la sécurité des SSI
2. en réfléchissant à **une charte des ASR** définie ... tout en commencant par un Guide des bonnes pratiques, un document « fourre tout » où on mettrait toutes les spécificités du métier d'ASR. Mais attention, ce document ne doit pas nous être opposable... il ne faut pas qu'on définisse nous même nos responsabilités qui pourraient d'une part ne pas nous couvrir mais en plus nous porter tort en s'appuyant sur des règles qu'on aurait nous mêmes définis

==> Mais un des objectifs final sera d'obtenir une vrai charte métier des ASR avec une FAQ (liste des questions les plus fréquemment posées) et une assistance.

2- Charte, web, logs, messagerie, crypto :

Si la charte informatique est annexée au règlement intérieur et signée par les tutelles du laboratoire (délégué régional Cnrs, Université, Ensicaen ...) alors elle s'applique à tous sans besoin de signature. Sinon elle doit être signée par tous.

La charte est à durée indéterminée. La version qui prédomine est celle qui est en ligne le jour du litige, au moment des faits. Il faut l'afficher dans les lieux du laboratoire.

Nécessité de faire figurer une « notice légale » sur un site web qui indique :

- qui est l'éditeur du site
- qui est l'hébergeur
- qui est le Directeur de la Publication

Le marquage des documents comme étant issus d'un intranet ou étant confidentiels est plus que conseillé. Voir jurisprudence TATI. En exemple : Copyright © année – nom de l'éditeur

La charte n'est pas obligatoire d'un point de vue légal mais en cas de litige, c'est un élément de droit. Mais il faut s'assurer qu'elle est comprise pour être valide.

L'usage de la cryptologie est maintenant légale (vu lors de l'étude de la charte de l'Université de Caen)

- **Les journaux - logs :**

Juridiquement il est nécessaire de logguer (Loi Terrorisme).

La politique de gestion des traces au CNRS a fait l'objet d'un document de 11 pages : il est disponible dans l'intranet du CNRS à partir du lien suivant http://www.sg.cnrs.fr/FSD/gestrace.htm.

Ce document rappelle l'objectif de ces traces (métrologie, détecter des anomalies, fournir des preuves..) et reprend par service par service (ouverture de session sur les serveurs et postes de travail, serveurs de messagerie, serveurs web, services routeurs,pare-feux, bornes d'accès .., les applications spécifiques) les informations à conserver.

Les logs des systèmes de détection d'intrusions (IDS) doivent faire l'objet d'une demande spécifique à la CNIL (ils ne font pas partie de la déclaration sous forme générique du CNRS auprès de la CNIL). La durée maximale est de 1 an.

On n'a pas le droit de supprimer des mails professionnels qui soient virusés ou spammés. Donc si on met en quarantaine la réception de spams ou de messages virusés, il faut prévenir le destinataire dans son laboratoire.

3- Une règlé d'or : le tryptique information - contrôle – action au quotidien :

- **Dans un contexte de faute, un juge jugera si on a informé, controlé et si on a agit**

- Informer :

PAR ECRIT (mail ou papier) et avec les mots clés : CONSEIL, MISE EN GARDE, ALERTE . Il est préférable de garder des preuves électroniques plutôt que écrites (il est plus facile de falsifier un écrit manuel qu'électronique).
Exemples : les bulletins d'alerte du CERT ou CERTA, les migrations prévues sur les services, les interruptions du réseau de l'extérieur, des statistiques de virus/spams, débits réseau, infection PC , un bilan d'activité annuel du service, une rubrique « Sécurité » dans l'intranet de notre site web ...

- Contrôler :

Mettre en place les outils nécessaires pour :
- paramétrer les logs sur la durée maximale légale pour les services demandés,
- pour des statistiques sur le débit, les sites consultés, la consultation du site du labo, la place occupée sur les disques, ...
- avoir des remontées en cas problème.

- Agir :

- L'ASR est tenu d'assurer la Sécurité système du site (passer les correctifs)
- Si un correctif de sécurité n'a pas été passé, et qu'il y a eu un incident grave, comme la sécurité système est le fait des ASR, pour ne pas être responsable, il faudra prouver par exemple qu'il était en vacances, et qu'il n'y avait pas de redondance humaine prévue.
- Pour maintenir la continuité des services communs, pour sécuriser (exécuter les patchs,...), en cas d'urgence ou de crise. C'est assez subjectif et c'est selon les circonstances.

Alors que faire en cas de problème ? : tout d'abord essayer d'en avoir une idée précise et s'il a une incidence grave sur le fonctionnement du service. Prendre conseil auprès du RSSI. En parler a la direction, et agir en conséquence.
Ce qui prime c'est la continuité du service (des jugements ont déjà été rendus). Donc dans le cas d'un utilisateur qui ne veux/n'est plus la , on a le droit d'accéder à son compte.

- La direction peut faire appel à un juge des requêtes : qui ordonne à un huissier une intervention en urgence (48h).

- On peut bloquer le compte ou messagerie de la personne le temps que l'huissier constate.

- C'est préférable de faire les opérations en présence de la personne concernée. En fonction de l'urgence du problème : si la personne dit non, il faut réagir vite pour éventuellement bloquer le compte et faire appel à un huissier. Faire 3 copies : huissier, ASR, l'utilisateur.

- Une copie d'écran ne peut pas servir de preuve. Il faut faire appel à un huissier.

4- Zoom sur la Loi Informatique & Libertés

Préserver la sécurité : empêcher que les données soient déformées endommagées ou que des tiers non autorisés aient accès au SI

Principes actuels :
- il est interdit d'interdire l'usage personnel de la messagerie (notion de vie privée résiduelle)
  - face à une situation de risque on « peut » ouvrir de la correspondance privée pour des raisons de sécurité ou d'urgence
  - on peut alors se poser comme question quelles sont les raisons de sécurité ou d'urgence ?
- tous les éléments qui sont dans un bureau d'un employeur sont réputés professionnels... De ce fait l'employeur peut y avoir accès même en l'absence du collaborateur

- Il faut mettre en place des éléments de distinction entre vie privée personnelle ou professionnelle

- Tous les mails (messagerie électronique) sont réputés à caractère professionnel sauf si il y a écrit [PERSONNEL] dans le sujet du message

La « vie privées résiduelle » ne concerne QUE la correspondance par messagerie électronique!

En cas de téléchargement massif par un utilisateur, l'ASR a le droit de stopper le flux réseau. On peut couper un service sans plus se poser la question du droit de le faire, mais en informant largement ... la Direction, les utilisateurs

Si les fichiers illicites sont déjà dans un répertoire [PRIVE-PERSONNEL] alors il faut faire appel a un huissier de justice

Q: En cas de départ d'un personnel, que faire des données ?
- il est légitime de basculer sa boîte de Mails d'une personne vers une autre.
- Il est nécessaire d'informer et d'écrire dans les procédures d'ouverture de compte que les données seront détruites ou transférées au Responsable au départ de l'utilisateur. De même il est nécessaire d'indiquer ce qui sera fait du répertoire [PRIVE] dans le règlement

Q: Comment traiter une machine personnelle qu'on doit connecter dans le réseau du Laboratoire ?

- La considérer comme un élément qui fait partie intégrante du SI du Laboratoire, elle suit le même régime
- L'écrire dans le règlement

On voit qu'il manque un corpus de règles d'administration. Objectifs : parvenir à l'établissement d'une charte des Administrateurs Systèmes?

Commencer par un document interne ou les ASR initient le travail de réflexion, et qui vise à délimiter et définir notre travail, et les contours du métier (un guide des bonnes pratiques).. mettre dans ce document ou ce à quoi on pense : règles + techniques + Droit

- Dire comment on gère le nomadisme et les postes privés
- faire un livret de procédures qui définit les techniques pour appliquer la Charte

Quand une charte contient des références au droit ou des références techniques ça pose des problèmes d'actualisation. Il faut faire une charte (fixe les règles du jeu), un livret des procédures (comment respecter les règles du jeu), un guide utilisateur (pourquoi ces règles ont été fixées, pourquoi telle technologie est employée, indiquer les sanctions). On fait valider la charte et on l'annexe au règlement intérieur, le livret des procédures et le guide utilisateur évoluent, pas la charte.

Informer et Former, Alerter et Conseiller

- Nécessité de faire du « reporting » : tracer nos activités dans un rapport d'activités
- Conseiller le Responsable Légale (Directeur d'unité)
- Informer les autorités compétentes
- Informer les utilisateurs

==> L'ASR doit être l'ambassadeur de la culture du SI

Obligation de Confidentialité

Mais on a obligation de dénoncer eu égard au Droit Pénal si on découvre des données illicites concernant la pédopornographie , le révisionnisme etc..

Participer au maintien de la preuve : Collaboration et coopération

On va devoir avoir des collaborations fréquentes avec la Police, la DST, la Justice, la CNIL

- La CNIL devient une autorité de contrôle hyper puissante !
  - La CNIL a désormais le pouvoir de faire une enquête
  - pouvoir d'opérer des vérifications sur place
  - pouvoir d'aller n'importe où dans le SI
  - pouvoir d'instrumentaliser la procédure
  - pouvoir de condamner à une amende

Si on a à faire avec la CNIL.... appeler la DAJ et un avocat ;-)

Il faut pouvoir prouver qu'on a sécurisé! Or dans nos milieux Universitaires et Recherche il y a une faible culture de l'écrit administratif. On ne trace pas beaucoup par écrit les actions qui ont été entreprises.

- ***il faut donc pour nous ASR pour prouver nos actions :***
  - Tracer nos actions
  - Faire un rapport annuel d'activités
  - Montrer qu'on a informé et donc tout écrire :
    - faire des alertes des mises en gardes par des mails ou figurent les mots « Alertes » « Mises en garde »
    - avoir une rubrique sécurité sur notre site Web

- ***Principes à retenir***
  - **tryptique Information/Contrôle/Action**
  - **politique de l'écrit**
  - **traçabilité**

- COMPLEMENTS DE LA FORMATION A MARSEILLE :

La solution pour se prémunir de responsabilités civiles de cet ordre est le tryptique :
Information -> contrôle -> Action

Dans le civil non contractuel, il n'y a pas d'obligation de moyens/résultats car il n'y a pas de contrat.

- Dans un contexte de faute, un juge jugera si on a contrôlé et si on a agit

• Il est donc nécessaire de PROUVER qu'on a mis ou qu'on aura mis en place la chaîne Information/Contrôle/Action ..... et donc le prouver avec des preuves écrites archivées
• Avoir les moyens de donner des preuves : exemple faire une rubrique Sécurité sur le site Web du Labo qui retranscrit les actions d'information et de contrôles engagées • Information : mettre des informations sur l'intranet, dire aux utilisateurs qu'il faut aller les consulter. Contrôle : garder les traces des connexions à l'intranet. Action : procédure automatique qui relance ceux qui ne se sont pas connectés.

Depuis la LCEN le droit à TRACER les utilisateurs dans un SI est total et complet

Exemple : un rapport de stage d'étudiant sur un site Web est jugé désobligeant par une entreprise ou l'étudiant a effectué le stage...
Que faut-il faire? Le RSSI a contrôlé la nature des écrits du rapport, informé le maître de stage, et l'a enlevé du site Web
Qui est fautif? L'étudiant ou le maître de stage.. en tant que Responsable de stage le maître de stage aurait dû contrôler et s'apercevoir des propos douteux du rapport

En civil il peut y avoir plusieurs responsables :

- Le responsable de stage n'a pas respecté la convention de stage en demandant à l'étudiant de mettre en ligne le rapport avant la validation par l'entreprise (faute directe)
- L'étudiant qui a mis en ligne le rapport n'a pas respecté la convention (faute directe)
- L'ASR pourrait être accusé de faute par négligence s'il ne suit pas le triptyque lorsqu'il reçoit la demande de la société. Si l'ASR enlève le rapport car la règle n'a pas été respectée (contrôle de la règle + action) et qu'il informe, pas de problème. Mais s'il n'y a rien dans la convention, L'ASR n'a pas à juger le contenu, s'il n'y a pas de règles il doit informer le responsable de stage du problème.

- Concernant le contrôle de sites Web : L'ASR n'a pas a tout contrôler tout le temps. On est dans un environnement de confiance (LCEN) on n'a pas à contrôler le site en permanence... MAIS on a obligation de participer contre 2 types de fléaux et d'agir le cas échéant contre :
  - la pédo pornographie- le révisionnisme

Pour être le moins négligent possible, il faut :

- informer et garder des preuves qu'on a informé
- effectuer des contrôles a priori : racisme, pédophilie + contrefaçon (contrôles quantitatifs)
- effectuer des contrôles a posteriori
- agir : simple information, suppression, et quand on agit il faut garder une trace des actions faites

L'ASR n'est pas le gardien , le garant de l'application de la Loi, L'ASR est un maillon, un utilisateur comme un autre

L'ASR est tenu d'assurer la Sécurité système du site (passer les correctifs)

Une formule intéressante concernant l'absence de définition de poste d'ASR : *A « mission impossible », responsabilité improbable*

Si un correctif de sécurité n'a pas été passé, et qu'il y a eu un incident grave, comme la sécurité système est le fait des ASR, pour ne pas être responsable, il faudra prouver par exemple qu'il était en vacances, et qu'il n'y avait pas de redondance humaine prévue.

La législation sur les liens Hypertexte se renforce... l'information/Contrôle/action doit etre faite régulièrement pas qu'une seule fois à l'ouverture du site. Il faut vérifier les liens de temps en temps

- COMPLEMENTS DES 2 SESSIONS NORMANDIE

1- Google Apps :

Propos de Cédric Houssier :

L'Université de Rouen réfléchit à l'utilisation de Google Apps Education. Google propose gratuitement l'hébergement de boites mail ainsi que des outils de travail collaboratifs.
(Nota: Les noms de domaine sont conservés, il n'y a pas de publicité et l'authentification reste locale à l'université)

Google insiste sur la réversibilité: On peut revenir en arrière et récupérer nos données quant on veut!
Il faut être très vigilant: il n'est pas forcément facile de reprendre 27000 x 5 Go du jour au lendemain.

Sur la sécurité, ils mettent en avant la méthode de stockage: un message ou un document est "découpé" en morceaux cryptés, chacun est stocké en plusieurs endroits du monde.

=> redondance
=> rapidité d'accès où que l'on se trouve dans le monde
=> cryptage des données
=> le fichier n'est jamais stocké en entier à un seul endroit

Le principe parait réellement très sûr (plus sur que ce que tout ce que nous pouvons offrir à l'heure actuelle).
En revanche, cela ne protège pas d'une consultation "par google". Là dessus, ils opposent leur politique de confidentialité.
(Nota: Le problème serait le même quel que soit le sous-traitant)

Autre problème, ils ne savent pas nous fournir de logs (d'accès, de consultation ou de réception des messages)
(Nota: Des solutions techniques partielles peuvent être mises en place)

Enfin, du point de vue purement juridique, pas de réponse sur notre obligation légale de fixer contractuellement et de contrôler le niveau de protection des données personnelles chez un prestataire extérieur.