



CEDHYS
CENTRE D'ETUDES DANS LES
DOMAINES DE L'HYGIENE ET DE LA SANTE

Association des Directeurs des Systèmes
d'Information de l'Industrie Pharmaceutique

B M H AVOCATS 29, rue du Faubourg St Honoré

75008 Paris

www.bmhavocats.com

Le DSI et les risques juridiques

B M H AVOCATS

André MEILLASSOUX, Avocat associé

Julie FABRE, Avocat



CEDHYS

www.cedhys.com

Tous droits de reproduction et d'utilisation réservés

Le DSI et les risques juridiques
BMH Avocats

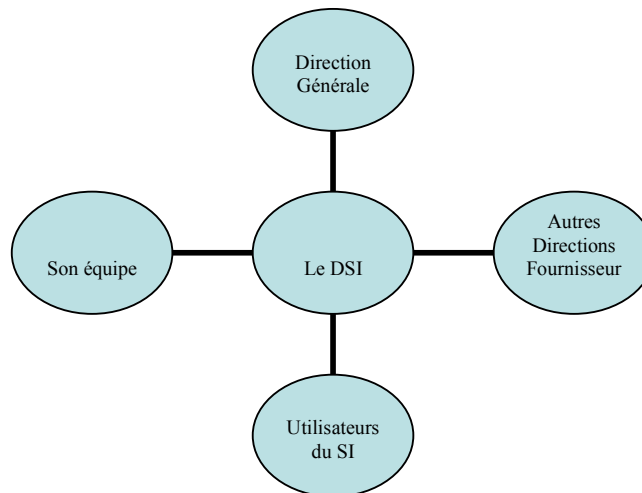
Préambule	6
Première partie Les principales sources de risques pour le DSI	9
1 Gestion et Sécurité des Données Personnelles	9
1.1 Loi du 6 janvier 1978.....	9
1.2 Gestion et sécurité des données personnelles	10
2 L'Utilisation Abusive des Outils du Système d'Information.....	13
2.1 Les infractions aux règles régissant la propriété intellectuelle	13
2.2 Les autres infractions.....	17
3 Sécurité du système d'information.....	19
4 Les relations avec les prestataires	20
5 Règlementations particulières	21
Deuxième partie Les moyens de prévenir la réalisation des risques.....	23
1 Approche générale.....	23
2 Les actions concrètes par niveau de responsabilité	23

Le DSI et les risques juridiques
BMH Avocats

Préambule

1. Le DSI dans son environnement

La notion de système d'information est bien plus vaste que celle de système informatique : elle recouvre la grande majorité des activités de l'entreprise. A la différence de la fonction informatique, qui se limite à l'ensemble des professionnels de l'informatique, le **système d'information intègre les utilisateurs.**



2. Contexte : Un accroissement des obligations et des risques pesant sur le DSI

- Constat d'une multiplication des risques pour les chefs d'entreprise et leurs organisations du fait de :
 - L'intrusion des technologies de l'information dans toutes les couches de l'entreprise
 - Prise de conscience des risques induits par les techniques
 - Souci sociétal d'accroître les responsabilités, en touchant les personnes physiques
 - Prolifération des initiatives législatives aggravant la responsabilité des chefs d'entreprises
- Constat d'une législation dispersée induisant des risques mal identifiés à différents niveaux
- Nécessité d'un transfert de responsabilité du chef d'entreprise sur les directions fonctionnelles : les DSI sont concernés
- Accroissement des responsabilités propres des DSI du fait de l'extension de leur champ de compétences

Le DSI doit doter son entreprise ou son organisation d'un **réseau d'échanges opérationnel et sécurisé.**

La mission du DSI, sur le plan juridique, se décompose aujourd'hui en trois volets :

- 1) il doit détecter la législation applicable aux systèmes d'information : il s'agit tant de la réglementation générale, applicable à tous les SI, que les réglementations métier, applicables au secteur particulier dans lequel le DSI exerce ;
- 2) il doit veiller à appliquer ces réglementations par la mise en œuvre des dispositifs adéquats ;

Le DSI et les risques juridiques

BMH Avocats

- 3) il doit sensibiliser son entourage aux obligations découlant des dispositions légales et réglementaires définies: cette sensibilisation doit viser non seulement son propre service, mais aussi l'ensemble du personnel de l'entreprise, en amont comme en aval, ainsi que les prestataires extérieurs.

Ainsi, il appartient au DSI, le cas échéant, d'expliquer en amont, aux directions générales, les changements organisationnels et techniques induits par un nouveau dispositif informatique.

3. Les types de responsabilités encourues

Le DSI peut voir sa responsabilité civile ou pénale engagée, voire les deux cumulativement. Il peut également engager sa responsabilité professionnelle, en interne, au regard des dispositions du Code du Travail.

a) Responsabilité civile :

La responsabilité civile peut revêtir deux formes : responsabilité civile contractuelle, en présence d'un contrat entre les parties, ou délictuelle, en l'absence d'un tel contrat.

- La responsabilité civile contractuelle, régie par les articles 1147 et suivants du Code civil, est susceptible d'être engagée en cas d'inexécution ou de mauvaise exécution, par l'une des parties, de l'une des obligations prévues au contrat. Cette responsabilité, lorsque elle est engagée, peut donner lieu à réparation sous forme de dommages-intérêts (et non sous la forme d'une exécution forcée du contrat).
- La responsabilité délictuelle trouve son fondement dans l'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* ». La responsabilité délictuelle est donc susceptible d'être engagée toutes les fois où, **en l'absence d'un contrat**, un dommage a été causé à quelqu'un.
- La responsabilité délictuelle d'une personne peut être engagée non seulement pour un dommage qu'elle a causé par son propre fait, mais également pour celui causé par le fait de son préposé (article 1384 du Code civil). La responsabilité délictuelle donne, elle aussi, lieu à réparation sous forme de dommages-intérêts.

b) Responsabilité pénale

La responsabilité pénale est encourue en cas d'infraction aux dispositions du Code pénal. Celui-ci définit trois catégories d'infractions : les contraventions, les délits et les crimes.

Les peines encourues sont des peines d'amende ou/et d'emprisonnement (ou de réclusion criminelle), ainsi que des peines accessoires ou complémentaires, qui peuvent par exemple prendre la forme d'interdictions (interdiction d'exercer une activité, d'exercer certains droits, etc.).

En cas de responsabilité civile cumulative, il peut y avoir lieu, en sus de la (ou des) peine(s) prononcée(s), d'indemniser la victime par l'octroi de dommages-intérêts.

Le Code pénal pose un principe de responsabilité personnelle : « *Nul n'est responsable que de son propre fait* » (article 121-1 C. pén.). Néanmoins, les personnes morales sont responsables pénalement des infractions commises **pour leur compte, par leurs organes ou représentants** (article 121-2 C. pén.).

La responsabilité pénale de la personne morale n'exclut toutefois pas celle des personnes physiques auteurs ou complices des mêmes faits : il peut y avoir cumul des responsabilités.

Les peines applicables aux personnes morales sont prévues par les articles 131-37 et suivants du Code pénal. Le principe est que le montant maximal de l'amende encourue par la personne morale est égal au **quintuple du montant prévu pour une personne physique** par la loi qui réprime l'infraction. (art. 131-38 C. pén.).

Le DSI et les risques juridiques **BMH Avocats**

Les peines encourues sont de surcroît aggravées au cas de récidive.

Enfin, il est à noter que la tentative et la complicité d'infraction sont punies au même titre que la commission de l'infraction.

c) Responsabilité professionnelle

La responsabilité du DSI peut enfin être engagée « en interne » : il s'agit de sa responsabilité professionnelle, liée à l'inexécution de son contrat de travail (et, le cas échéant, du règlement intérieur de l'entreprise). Cette responsabilité peut donner lieu à des sanctions disciplinaires allant jusqu'au licenciement. Elle n'est pas exclusive de l'engagement de ses responsabilités civile et pénale vues ci-dessus.

4. Les types d'agissements susceptibles d'engager sa responsabilité

Le DSI peut voir sa responsabilité engagée :

- par un acte positif qu'il a commis (ex : utilisation d'un logiciel sans licence d'utilisation)
- par une simple omission, négligence ou imprudence de sa part (article 1383 du Code civil) : ex. : l'entreprise – ou le DSI – qui n'aura pas pris des mesures de sécurité raisonnables pour protéger son système informatique pourra voir sa responsabilité engagée au titre de sa négligence.
- par le fait d'un salarié de l'entreprise, que celui-ci se trouve, ou non, sous sa direction (ex : responsabilité pour fourniture des moyens ayant permis la réalisation de l'infraction par le salarié).

5. Les personnes susceptibles de voir leur responsabilité engagée

Le DSI n'est toutefois pas le seul maillon de l'entreprise exposé au risque de voir sa responsabilité engagée. Peuvent également être concernés :

- Les Directions générales : les premières visées par les textes de loi (d'où l'obligation jurisprudentielle de pratiquer des délégations de pouvoirs) ;
- les informaticiens sous la direction du DSI, et notamment les administrateurs, susceptibles de se voir confier certaines responsabilités ;
- Les salariés, utilisateurs bien ou mal intentionnés des matériels informatiques mis à leur disposition ;
- Les prestataires extérieurs.

6. Sujets non traités

Ce document s'attachant à traiter les responsabilités du DSI (dans son métier), les réglementations « métiers » ne sont pas traitées ni les responsabilités attachées à sa qualité standard de manager.

Ainsi, ne sont pas abordées dans le détail les réglementations:

- Financières : Sarbanes-Oxley
- Pharmaceutiques : bonnes pratiques et FDA notamment
- HSE, social, ...

Première partie

Les principales sources de risques pour le DSI

Les risques que rencontre le DSI dans l'exercice de sa profession et susceptibles d'engager sa responsabilité peuvent être regroupés selon quatre domaines :

- La gestion et l'utilisation des données personnelles
- La gestion et l'utilisation des moyens
- La sécurité du système d'information
- Les relations avec les prestataires

Pour les besoins de la présente étude, une cinquième catégorie sera ajoutée afin d'attirer l'attention du lecteur sur les obligations pesant sur le DSI en application des réglementations particulières – notamment financières – éloignées de son champ de compétence initial.

1 Gestion et Sécurité des Données Personnelles

Face à l'essor d'une véritable industrie des données à caractère personnel dont l'exploitation s'est révélée sensible, voire dangereuse, la Loi n°78-17 du 6 janvier 1978 (dite « *Loi Informatique et Libertés* »), modifiée par La loi n°2004-801 du 6 août 2004, est venue encadrer les traitements automatisés de données à caractère personnel.

Nous rappellerons quelques grands principes dégagés par cette Loi dans sa version en vigueur, avant d'insister sur les principaux risques et sanctions encourus en matière de gestion et de sécurité des données personnelles.

1.1 Loi du 6 janvier 1978

Principes dégagés par la Loi du 6 janvier 1978, modifiée par la Loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel)

Aux termes de la Loi :

- Est une **donnée à caractère personnel** :
« toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification, ou à un ou plusieurs éléments qui lui sont propres » (article 2).
Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification à disposition du responsable du traitement ou de toute autre personne.
- Est un **traitement de données à caractère personnel** :
« toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ».
- Le **responsable d'un traitement de données à caractère personnel** est, « sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, le personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens ».

Le DSI et les risques juridiques

BMH Avocats

- Les conditions de licéité des traitements sont fixées par l'article 6 de la Loi (finalité du traitement, conditions de réutilisation, principe de proportionnalité des données dans la collecte, exactitude et mise à jour des données, durée de conservation...)
- Sauf exceptions, il est interdit de « collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci » (article 8).
- Des exceptions à cette interdiction de principe existent notamment lorsque le traitement est nécessaire à la recherche dans le domaine de la santé (voir Chapitre IX de la Loi).
- La CNIL dispose désormais de **pouvoirs d'investigation** (dans les locaux notamment) **et de sanction renforcés** (sanctions administratives telles que l'avertissement, sanctions pécuniaires jusqu'à 150.000 euros, doublées en cas de récidive, ou encore injonction de cesser un traitement non conforme à la Loi).

1.2 Gestion et sécurité des données personnelles

Les infractions ayant pour effet de porter atteinte aux droits de la personne et résultant des fichiers ou traitements informatiques sont réprimées par les dispositions des articles 226-16 à 226-24 du Code pénal.

Les infractions à la Loi *Informatique et Libertés*, qu'elles soient ou non réprimées par des dispositions du Code pénal, sont susceptibles de donner lieu à sanctions par la CNIL (article 45) : avertissement et, éventuellement, sanctions pécuniaires.

Les principaux risques encourus sont les suivants :

1. La création d'un traitement automatisé de données sans déclaration auprès de la CNIL :

« Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300.000 € d'amende » (article 226-16 du Code pénal).

Il en va donc ainsi du traitement mis en place sans déclaration auprès de la CNIL lorsqu'une telle déclaration est requise : la CNIL définit en effet les traitements susceptibles de faire l'objet d'une déclaration simplifiée, voir d'une dispense de déclaration, et ce compte tenu de leur **finalité, destination, des données à caractère personnel traitées, de la durée de conservation de celles-ci et des catégories de personnes concernées** (article 24 de la Loi).

Pour plus de détails sur les traitements faisant l'objet de dispenses ou de déclarations simplifiées, se référer aux délibérations de la CNIL.

Il est à noter que la nomination d'un « correspondant à la protection des données à caractère personnel » par le chef d'entreprise, portée à la connaissance des IRP et de la CNIL, permet un allègement des obligations déclaratives.

La CNIL soumet enfin certains traitements à une autorisation préalable (article 25) : il s'agit principalement des traitements relatifs à la **santé publique**, aux **données génétiques**, biométriques (notamment dans le cadre du contrôle de l'identité des personnes intéressées), aux opinions politiques, religieuses ou syndicales, aux mœurs, aux origines raciales et ethniques.

Un traitement est donc soumis à une « déclaration normale » dès lors qu'il ne fait l'objet ni d'une dispense, ni d'une déclaration simplifiée, ni d'une autorisation préalable.

2. La collecte illicite de données :

Le fait de collecter des données à caractère personnel par un **moyen frauduleux, déloyal ou illicite** est puni de cinq ans d'emprisonnement et de 300.000 euros d'amende (article 226-18 C. pén.).

Exemple : est considéré comme déloyal le fait de recueillir, à leur insu, des adresses électroniques personnelles de personnes physiques sur l'espace public d'Internet (par exemple, en vue de la diffusion de messages publicitaires aux titulaires de ces adresses), ce procédé faisant obstacle à leur droit d'opposition (Cass. Crim., 14 mars 2006).

Les personnes concernées par la collecte de données devront donc impérativement se voir informées de ce qu'elles font l'objet d'un traitement informatisé et de leur droit d'accès et de rectification des données collectées.

3. Infraction aux droits de la personne faisant l'objet du traitement :

Les personnes faisant l'objet d'un traitement jouissent en effet de droits, définis aux articles 32 ainsi que 38 et suivants de la Loi :

a) Droit à l'information (articles 32 et 39)

Ce droit à l'information revêt deux aspects :

- L'article 32 de la Loi impose au responsable du traitement d'indiquer à la personne faisant l'objet du traitement l'identité du responsable du traitement, la finalité poursuivie par le traitement, le caractère obligatoire ou facultatif des réponses, les conséquences éventuelles d'un défaut de réponse, l'existence d'un droit d'accès et d'opposition, et le cas échéant, les transferts de données envisagés à destination d'un Etat non membre de l'Union européenne.
- D'autre part, en vertu de l'article 39 de la Loi, toute personne physique justifiant de son identité pourra obtenir des précisions sur les finalités du traitement, les données traitées ainsi que l'origine de celles-ci.

b) Le droit d'opposition (article 38)

Sauf dans les cas où le traitement répond à une obligation légale ou lorsque l'application de ces dispositions a été écartée par une disposition expresse de l'acte autorisant le traitement, toute personne peut s'opposer, **pour des motifs légitimes**, au traitement de ses données à caractère personnel.

c) Le droit d'accès (articles 39 et 41)

La personne faisant l'objet du traitement dispose d'un droit d'accès aux données collectées la concernant. Le responsable du traitement peut s'y opposer en cas de demande manifestement abusive (par exemple en raison de son caractère répétitif).

d) Droit de rectification (article 40)

Toute personne peut demander que soient rectifiées, effacées, complétées, mises à jour ou effacées les données la concernant si elles sont inexacts, incomplètes, équivoques, périmées ou si leur collecte, utilisation, communication ou conservation est interdite. Les données pourront également être verrouillées à sa demande.

L'infraction consistant pour le responsable du traitement à refuser à la personne faisant l'objet du traitement d'exercer l'un des droits précités n'est pas prévue en tant que telle par le Code pénal.

Néanmoins, un tel refus pourrait donner lieu à la prononciation de sanctions par la CNIL (article 45 de la Loi) : avertissement, suivi le cas échéant d'une mise en demeure de faire cesser le manquement constaté et, à défaut de mise en conformité, sanctions pécuniaires (article 47 de la Loi).

Le DSI et les risques juridiques **BMH Avocats**

4. Le délit de détournement de finalité :

Les données collectées ne peuvent être détournées de leur finalité initiale : l'art. 226-21 C. pén. punit l'inobservation de cette règle de cinq ans d'emprisonnement et de 300.000 euros d'amende.

5. Manquement à l'obligation de préserver la sécurité des informations faisant l'objet d'un traitement automatisé :

L'article 34 de la Loi impose au responsable du traitement de « *prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès* ».

L'article 226-17 C. pén. punit l'absence de mise en œuvre des mesures prescrites à l'article 34 de la loi de cinq ans d'emprisonnement et de 300.000 euros d'amende.

De surcroît, le fait, pour une société, de ne pas respecter cette obligation de sécurité prive celle-ci de tout recours contre le pirate qui a détourné son fichier client (CA Paris, 30 octobre 2002, « Tati »).

Le DSI peut ainsi engager sa responsabilité s'il ne prend pas les mesures suffisantes pour assurer l'absence de faille de sécurité du système, qui permettrait à un pirate de détourner des données nominatives.

Au niveau professionnel, la gravité des conséquences d'un tel manquement pourra, le cas échéant, caractériser une faute grave justifiant un licenciement immédiat du DSI sans préavis ni indemnité. Le manquement sera toutefois apprécié au regard non seulement du degré de difficulté de la tâche du DSI et des moyens mis à sa disposition pour l'accomplir, mais aussi de l'expérience et de l'ancienneté du DSI au sein de l'entreprise, un parcours jusque là « sans faute » atténuant la gravité d'une erreur ou d'une négligence unique.

Ces dispositions s'appliquent même en cas de sous-traitance : l'article 35 de la Loi prévoit que toute personne qui traite des données pour le compte du responsable du traitement est considérée comme un sous-traitant. Elle doit présenter des garanties suffisantes en matière de sécurité et de confidentialité. Néanmoins, **le respect des obligations de sécurité et de confidentialité continue à peser sur le responsable.**

Il appartient donc au responsable du traitement de veiller à faire figurer dans le contrat écrit le liant au sous-traitant l'indication des obligations incombant au sous-traitant en matière de protection de la sécurité et de la confidentialité des données. Le contrat doit en outre indiquer que le sous-traitant ne peut agir que sur instruction du responsable du traitement.

6. Les transferts de données personnelles hors UE

La loi du 6 août 2004 n'autorise les transferts hors UE que si le pays destinataire assure un « *niveau de protection suffisant de la vie privée et des libertés et droits fondamentaux des personnes à l'égard du traitement* » dont ces données font ou peuvent faire l'objet (article 68).

Exceptions (article 69 alinéa 1^{er}):

- consentement exprès de la personne concernée par le transfert ;
- le transfert est nécessaire au respect de certaines obligations ou à la sauvegarde de certains intérêts (article 69, 1° à 6°).

Il en va de même en cas d'informations « locales » recueillies ou stockées sur des installations situées à l'étranger : la CNIL se réserve le droit de vérifier le niveau de protection accordé à ces données.

Là encore, l'article 226-22-1 du Code pénal punit l'inobservation de ces règles de cinq ans d'emprisonnement et de 300.000 euros d'amende.

7. La collecte de données « à caractère discriminatoire »

Sauf exceptions, il est interdit de « collecter ou de traiter des données à caractère personnel qui font apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes, ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci » (article 8 de la Loi).

L'article 226-19 du Code pénal punit l'inobservation de ces règles de cinq ans d'emprisonnement et de 300.000 euros d'amende.

8. L'accès frauduleux à un système de traitement automatisé de données

L'accès ou le maintien frauduleux dans un système de traitement automatisé de données, le fait d'en entraver le fonctionnement, d'y introduire frauduleusement des données, etc. est réprimé par les articles 323-1 et suivants du Code pénal. Les peines encourues vont de deux à cinq ans d'emprisonnement et de 30.000 à 75.000 € d'amende, éventuellement assortis de peines complémentaires.

9. L'archivage et la sauvegarde des fichiers

Un DSI peut être conduit à subir une sanction disciplinaire pouvant aller jusqu'au licenciement pour faute grave en cas de manquement à son obligation de mise en place de mesures (techniques, outils, organisation) nécessaires à l'archivage et à la sauvegarde des données.

2 L'Utilisation Abusive des Outils du Système d'Information

Le Directeur des Systèmes d'Information d'une organisation (entreprise, association) y est responsable de l'ensemble des composants matériels (postes de travail, serveurs, équipements de réseau, systèmes de stockage, de sauvegarde et d'impression, etc.) et logiciels du système d'information, ainsi le plus souvent, que du choix et de l'exploitation des services de télécommunications mis en œuvre¹.

Les outils mis à la disposition des utilisateurs du système d'information et susceptibles d'engendrer des risques, sont nombreux. L'on peut notamment citer : les logiciels, la mise à disposition d'Internet (notamment via les infractions de presse, le secret des correspondances, les noms de domaine, les liens hypertexte), les moteurs de recherche, les bases de données, ainsi que les graveurs et les périphériques de stockage.

2.1 Les infractions aux règles régissant la propriété intellectuelle

Remarque préliminaire : On a assisté à un durcissement de la réglementation pénale applicable à la contrefaçon :

La loi du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité (dite *Loi Perben II*) a augmenté le plafond des amendes et des peines d'emprisonnement encourues. Les sanctions pénales de la contrefaçon de droit d'auteur, de droit des marques et des brevets d'invention sont dorénavant plus sévères.

Ainsi, pour le droit d'auteur, le droit des producteurs de vidéogrammes et phonogrammes, le droit des dessins et modèles et les brevets d'invention, les amendes encourues sont désormais de 300.000 euros (contre 150000 euros auparavant) et les peines de prison peuvent aller jusqu'à trois ans au lieu de deux ².

¹ Wikipédia, *l'Encyclopédie libre*, 19 août 2006.

² C.Caron, *Revue Communication.Commerce Electronique*, mai 2004.

Le DSI et les risques juridiques **BMH Avocats**

1) Les logiciels :

Les logiciels sont considérés comme des œuvres de l'esprit et bénéficient, à ce titre, de la protection par le droit d'auteur : article L112-2, 13° du Code de la Propriété Intellectuelle (ci-après, CPI).

Le droit moral de l'auteur du logiciel est toutefois restreint : il ne jouit que du **droit au nom** (article L.121-1 CPI), valable même quand les droits patrimoniaux ont été cédés, et **du droit de divulgation** (possibilité pour l'auteur de diffuser ou non son logiciel, article L.121-2 CPI), à l'exclusion des droits de retrait et de repentir (article L. 121-7 2° CPI).

Quant au **droit au respect de l'intégrité de son œuvre**, en application de l'article L. 121-7 1° du CPI, si l'auteur d'un logiciel passe un contrat avec un éditeur, ce dernier peut, « sauf stipulation contraire plus favorable à l'auteur », modifier le logiciel sans que l'auteur s'y oppose, sauf atteinte à l'honneur et à la réputation de celui-ci.

L'exception de copie privée ne trouve pas à s'appliquer en matière de logiciels : si la copie de sauvegarde est autorisée (copie unique et de substitution conservée pour constituer une sécurité en cas de dégradation du logiciel d'origine), il est en revanche interdit à l'utilisateur d'effectuer une copie strictement privée de son logiciel (articles L.122-5 2° et L.122-6-1 II du CPI).

L'articulation entre les droits de l'auteur du logiciel et son utilisateur est régie par les articles L122-6 et suivants du Code de la Propriété intellectuelle.

Le logiciel bénéficie également d'une protection au titre du droit des brevets (Livre VI du CPI). Celle-ci remplit un rôle différent de la protection par le droit d'auteur : alors que le droit d'auteur protège l'œuvre contre une reproduction à l'identique par un contrefacteur, le droit des brevets protège l'inventeur contre toute réutilisation de la technique dans un autre produit.

La contrefaçon de logiciel:

Aux termes de l'article L.335-3 du Code de la Propriété intellectuelle, est un délit de contrefaçon la violation d'un des droits dont dispose l'auteur du logiciel sur son œuvre et définis à l'article L.122-6 CPI.

Il en est par exemple ainsi de l'utilisation du logiciel sans licence : le DSI doit veiller à disposer de licences en nombre suffisant pour l'ensemble des postes sur lesquels est utilisé le logiciel. En effet, en cas de licence « monoposte », la mise sur réseau informatique en vue d'une possible utilisation du logiciel par plus d'une personne simultanément constitue une contrefaçon.

De même, le DSI doit veiller au respect par ses équipes de l'interdiction d'effectuer une copie du logiciel : la duplication de logiciel sans autorisation de l'auteur ou de l'éditeur constitue, le plus souvent, une contrefaçon susceptible de poursuites.

Le DSI doit enfin veiller au respect des dispositions relatives aux apports de modifications et à la décompilation (articles L122-6 et suivants du Code de la Propriété intellectuelle).

Le délit de contrefaçon de logiciel est puni par les dispositions des articles L.335-2 et suivants du CPI. Les peines encourues sont de 300.000 euros d'amende et 3 ans de prison.

Les personnes susceptibles d'être poursuivies sont non seulement les dirigeants légaux de la société mais également les directeurs, et notamment les **DSI ayant donné des instructions claires en ce sens aux salariés** : ainsi, un directeur informatique a par exemple été condamné, aux côtés du PDG d'une société, sur le fondement de l'article L. 335-3 du CPI (cf. ci-dessus) pour avoir donné des instructions à un technicien de son service afin qu'il reproduise en plusieurs exemplaires des logiciels acquis légalement pour les installer sur l'ensemble des postes d'ordinateurs de l'entreprise.

2. La protection des noms de domaines

Le nom de domaine est un signe distinctif.

L'ICANN (Internet Corporation for Assigned Names and Numbers) gère le dépôt et l'attribution des noms de domaine ainsi que les controverses entre marques et noms de domaine.

Des conflits existent entre noms de domaine et droits de propriété intellectuelle. Ces conflits se situent à la croisée de trois domaines du droit :

- Le droit des marques ;
- Les droits d'auteur ;
- Le droit des dénominations sociales.

Les principaux cas de litiges :

- Nom de domaine postérieur à une marque enregistrée (« cybersquatting ») : supériorité de principe du droit de la marque sur le nom de domaine (TGI Draguignan 21/08/1997 Affaire Saint-Tropez).
- Nom de domaine antérieur à une marque enregistrée : l'usage du nom de domaine permet l'annulation de la marque postérieure (TGI Le Mans 29/06/1999 Affaire Océanet ; SA No Problemo/ Sarl Capitale Studio et Sarl COMFM, Tribunal de grande Instance de Paris, 3e Chbre, 27 juin 2000).
- Nom de domaine face à un conflit de droits antérieurs : confirmation du principe de spécialité (un risque de confusion dans l'esprit du publique doit exister eu égard aux domaines d'activité identiques ou similaires des parties) :
 - Face à une dénomination sociale (CA Paris 4/12/98)
 - Face à une marque antérieure (TGI Paris 23/12/99)

Aujourd'hui, **on assimile le nom de domaine à une enseigne virtuelle**. La contrefaçon va s'apprécier au regard du contenu du site que désigne le nom de domaine : aux termes de la jurisprudence actuelle, un nom de domaine enregistré mais non exploité ne constitue plus une contrefaçon mais peut être sanctionné sur le terrain de la responsabilité civile.

3. La protection des bases de données :

Les éléments constitutifs d'une base de données

- Logiciel d'interrogation
- Contenus de la base
- Structure de la base

Le DSI et les risques juridiques BMH Avocats

- a) **Le logiciel d'interrogation va chercher l'information dans la base de données par le biais d'une requête. Pas de spécificité particulière par rapport aux autres logiciels « classiques ».**
- b) **Le contenu : Éléments d'information stockés dans la base et individuellement accessibles aux utilisateurs de la base (ex. les photos dans une base de photos).**
- c) **La structure : Mode d'organisation intellectuelle et méthodologique des contenus de la base (sorte de plan de classement de la base permettant d'accéder à l'information recherchée). C'est elle qui va donner une valeur particulière à la base.**

L'article 112-3 CPI détermine le statut juridique de la base de données : « *Recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique et individuellement accessibles par des moyens électroniques ou d'une autre manière* ».

1) *La protection du contenu de la base de données :*

Les contenus de la base peuvent être ou non protégés par le droit d'auteur : les éléments protégés par le droit d'auteur sont ceux issus d'un processus créatif ; les éléments non protégés sont ceux résultant d'événements factuels (ex. des horaires de trains). Enfin, le contenu peut être mixte.

Si les contenus sont protégés par le droit d'auteur, leur utilisation sans autorisation sera un acte de contrefaçon et pourra être poursuivi au titre des dispositions régissant le droit d'auteur.

La Cour de Cassation autorise néanmoins la constitution de bases de données à partir d'œuvres d'autrui **sous forme de courtes citations** « *lorsque l'œuvre a été divulguée, l'auteur ne peut interdire, sous réserve que soient indiqués clairement le nom de l'auteur et la source, les courtes citations justifiées par le caractère d'information de l'œuvre à laquelle elles sont incorporées* » (Cass. Ass., 30 oct. 1987).

2) *La protection de la structure de la base*

Aux termes de l'article L. 112-3 CPI, les anthologies & recueils d'œuvres « *tels que les bases de données qui, par le choix ou la disposition des matières, constituent des créations intellectuelles* », sont protégés par le Code de la Propriété intellectuelle, sans préjudice des droits de l'auteur de l'œuvre originale.

Si la structure de la base est originale, la création en sera acquise à son auteur (lequel n'est pas nécessairement le producteur).

Le producteur de la base de données jouit lui aussi de droits sur la base, au titre de son investissement dans la constitution de celle-ci. Il s'agit du droit d'interdire :

- l'extraction et/ou la réutilisation de la totalité ou d'une partie substantielle du contenu de la base.
- l'extraction et/ou la réutilisation répétée ou systématique d'une partie non substantielle du contenu de la base, s'il y a abus de droit manifeste.

Ces dispositions visent à prévenir les agissements parasites. **Des sanctions pénales sont prévues aux articles L.343-1 à L. 343-4 du CPI en cas d'atteintes portées aux droits producteur d'une base de données (3 ans d'emprisonnement et 300.000 euros d'amende).**

Les droits sur la base de données prennent effet à compter de l'achèvement de la base et expirent 15 ans après le 1^{er} janvier de l'année civile suivant cet achèvement. Si une base protégée fait l'objet d'un nouvel investissement substantiel, un nouveau délai de 15 ans commencera à courir.

4. Les liens hypertextes

Définition : Mécanisme de référencement localisé dans un contenu et permettant d'accéder directement à un autre contenu.

Les liens peuvent être internes à un site (ce qui ne pose généralement pas de problèmes) ou externes, c'est-à-dire d'un site à un autre. **Ces derniers peuvent poser problème lorsque le lien est dirigé vers une oeuvre ou un contenu illicite.**

Il existe un principe de liberté de création des liens, fondé sur la réciprocité. Ce principe connaît toutefois des limites : en l'absence de règles spéciales, c'est le droit commun de la responsabilité ainsi que le droit de la propriété intellectuelle qui s'appliquent.

En France, les principes dégagés sont essentiellement jurisprudentiels :

- « N'est pas légal le lien profond qui a pour conséquence de dénaturer, détourner l'image ou le contenu du site cible, de faire apparaître le site comme étant le sien, de ne pas laisser apparaître l'adresse du site cible, et de ne pas en préciser les sources » (Affaire « Keljob », Tribunal de Nanterre, Ordonnance de référé du 26 décembre 2000).
- Le lien n'est en revanche pas illicite « dès lors qu'il fait apparaître l'origine de l'adresse du site ».

Le critère essentiel de licéité du lien hypertexte est donc celui de l'identification du site cible.

Attention aux possibles actes de contrefaçon en cas de lien pointant vers une oeuvre contrefaisante, vers un contenu illicite, ou encore vers un contenu constitutif d'une infraction pénale.

5. La responsabilité du fait du moteur de recherche

- L'exploitant d'un moteur de recherche peut-il voir sa responsabilité engagée du fait d'une référence au contenu d'un site illicite ?
- L'exploitant d'un site peut-il voir sa responsabilité engagée quand un contenu illicite est supprimé mais encore accessible sur le réseau du fait de la mémoire du moteur de recherche ?
- L'activité par référencement publicitaire du moteur de recherche.

Pas de règle particulière en matière de responsabilité du moteur de recherche. Un moteur de recherche est un site constitué de références à d'autres sites dont il n'est pas l'hébergeur. Le régime spécial des hébergeurs ne s'applique donc pas.

Les moteurs de recherche sont aujourd'hui des prestataires au sens de l'article 14 de la Loi sur la Confiance dans l'Economie Numérique : la responsabilité de plein droit prévue par ce texte peut être engagée.

Néanmoins, il ressort de la jurisprudence que pour que l'exploitant d'un moteur de recherche voie sa responsabilité engagée pour avoir référencé ou facilité l'accès à un site dont le contenu est illicite, il est nécessaire de démontrer qu'il a commis une faute, une imprudence ou une négligence en référençant ce site. La preuve d'une telle faute est, en pratique, difficile à rapporter.

2.2 Les autres infractions

1) La cyber-surveillance des salariés :

Elle est réglementée au nom du secret de la correspondance et de la protection de la vie privée.

Le **principe de l'inviolabilité de la correspondance** est posé par :

Le DSI et les risques juridiques

BMH Avocats

- l'article 1^{er} de la Loi du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications : « *Le secret des correspondances est garanti par la loi* » ;
- l'article L 121-8 du Code du Travail : « Aucune information concernant personnellement un salarié ou un candidat à l'emploi ne peut être collectée par un dispositif qui n'a pas été préalablement porté à la connaissance du salarié ou du candidat à un emploi » ;
- l'article L.432-2-1 : « Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés ».
- l'article L. 120-2 du Code du Travail : « Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché ».
- l'article 226-15 du Code pénal: « Le fait, commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance, est puni d'un an d'emprisonnement et de 45.000 € d'amende ».

Le droit du travail protège la liberté individuelle du salarié, y compris pendant le temps de travail et sur le lieu de travail.

Les courriers électroniques étant considérés par les tribunaux comme une forme de correspondance, il résulte des dispositions législatives précitées que la surveillance des courriers électroniques des salariés n'est possible que si elle est annoncée, tend à la préservation des intérêts de l'entreprise, et est proportionnée au but recherché. Un contrôle systématique et général sera bien évidemment exclu.

2. Les infractions de presse via la navigation sur Internet

Attention ! Il est important de noter que le délai de droit commun pour agir en matière d'infractions de presse est très court : « *L'action publique et l'action civile résultant des crimes, délits et contraventions prévus par la présente loi se prescrivent après trois mois révolus, à compter du jour où ils auront été commis ou du jour du dernier acte d'instruction ou de poursuite s'il en a été fait* » (article 65 alinéa 1^{er} de La loi du 29 juillet 1881 sur la Presse).

Ce délai a été porté à un an par la Loi du 9 mars 2004 pour certaines infractions, notamment en matière d'incitation à la haine raciale.

Exemples d'infraction de presse : provocations, outrages, diffamations, injures.

Le délai de trois mois court à compter de la première publication (c'est-à-dire l'acte de mise à disposition du public, que celui-ci consulte ou non le contenu) même si la publication se prolonge dans le temps.

En matière d'Internet, il s'agit donc de la 1^{ère} mise en ligne, et non de la date du retrait, comme cela avait parfois été retenu.

Le DSI peut voir sa responsabilité engagée pour fourniture des moyens ayant permis la réalisation de l'infraction.

3. L'intrusion non autorisée d'un salarié de l'entreprise dans un autre système d'information à partir des moyens fournis par son employeur

(Voir Supra, « *L'accès frauduleux à un système de traitement automatisé de données* », réprimé par les articles 323-1 et suivants du Code pénal).

Là encore, le DSI peut voir sa responsabilité engagée pour fourniture des moyens ayant permis la réalisation de l'infraction.

3 Sécurité du système d'information

Le DSI se livre à une analyse méthodique des vulnérabilités du système d'information.

L'engagement de la responsabilité du DSI en cas d'une analyse insatisfaisante des vulnérabilités du système, s'apprécie en fonction de son expérience et de son ancienneté au sein de l'entreprise, des moyens dont il disposait et, enfin, du degré de difficulté de sa tâche. Ainsi, un parcours professionnel exemplaire atténuera la gravité d'une faute ou d'une négligence unique.

En outre, le DSI peut se voir sanctionné disciplinairement en cas de dysfonctionnement prolongé du système d'information dont il est responsable.

Jurisprudence « Tati c/ Kitetoo » (CA Paris, 30 octobre 2002) : une société qui ne respecterait pas l'obligation de sécurité se verrait privée de tout recours contre la personne entrée illégalement dans le système automatisé des données de l'entreprise. Le DSI peut alors être sanctionné pour faute grave.

La Cour d'Appel de Paris a considéré que la possibilité d'accéder à des données stockées par Kitetoo sur un site Tati avec un simple navigateur, en présence de nombreuses failles de sécurité, n'est pas répréhensible. Le responsable technique de Tati aurait dû mieux protéger ses données et faire une déclaration CNIL du traitement informatique. Selon le Procureur, ces 2 infractions étaient plus graves que celles reprochées par Tati à Kitetoo, à savoir la divulgation d'une faille de sécurité sur le site Tati.fr. et l'intrusion dans le système peu protégé.

Si le PDG en tant que mandataire social de l'entreprise est condamné à la place du DSI, le DSI peut ensuite se voir remercié par un licenciement pour insuffisance professionnelle.

L'article 226-17 du code pénal réprime le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations, et notamment, empêcher qu'elles ne soient communiquées à des tiers non autorisés.

Les peines encourues sont de 5 ans d'emprisonnement et 300.000 euros d'amende.

1) Protection des secrets de fabrique :

La protection du secret de fabrique pèse sur le DSI, qui doit faire respecter la confidentialité des données de l'entreprise. L'article L.621-1 du Code de la Propriété intellectuelle, renvoyant à l'article L.152-7 du Code du Travail, prévoit que « *le fait pour tout directeur ou salarié d'une entreprise où il est employé, de révéler ou de tenter de révéler un secret de fabrique est puni de 2 ans d'emprisonnement et de 30.000 € d'amende* ». *Le tribunal peut également prononcer à titre de peine complémentaire, pour une durée de 5 ans au plus, l'interdiction des droits civiques, civils et de famille prévue par l'article 131-26 du code pénal* ».

Aussi le DSI s'expose-t-il au risque d'avoir à justifier, devant le juge pénal, les mesures mises en œuvre pour protéger les données confidentielles de l'entreprise en cas de prise de connaissance de ces données par un tiers non autorisé.

2. Obligation de « mise en clair des données chiffrées nécessaires à la manifestation de la vérité » (pesant sur les fournisseurs de prestation de cryptologie et les éditeurs de logiciels de chiffrement.)

L'article 30 de la LSQ³ a modifié le Code de Procédure pénale en y insérant un chapitre concernant la mise en clair des données chiffrées nécessaires à la manifestation de la vérité. Ainsi, lorsque les données obtenues au cours d'une enquête ou d'une instruction ont été chiffrées, "*le procureur de la République, la juridiction d'instruction ou la juridiction de jugement saisie de l'affaire peut désigner toute personne physique ou morale qualifiée, en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair de ces informations ainsi que, dans le cas où un moyen de cryptologie a été utilisé, la convention secrète de déchiffrement, si cela apparaît nécessaire*".

Un article 11-1 a été inséré dans la loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications, aux termes duquel «*Les personnes physiques ou morales qui fournissent des prestations de cryptologie visant à assurer une fonction de confidentialité sont tenues de remettre aux agents autorisés dans les conditions prévues à l'article 4, sur leur demande, les conventions permettant le déchiffrement des données transformées au moyen des prestations qu'elles ont fournies*».

Le fait de ne pas déférer, dans ces conditions, aux demandes des autorités habilitées est puni de deux ans d'emprisonnement et de 30.000 € d'amende.

En pratique, ces dispositions mettent à la charge des fournisseurs de prestations de cryptologie et des éditeurs de logiciels de chiffrement l'obligation de **prévoir des portes cachées dans leurs produits**, afin de pouvoir procéder au déchiffrement quand cela leur est demandé par les autorités compétentes.

Aux termes de l'article 30 de la LSQ, cette obligation incombe à «*toute personne physique ou morale qualifiée en vue d'effectuer les opérations techniques permettant d'obtenir la version en clair [...]*».

Cette obligation va donc notamment peser, directement ou par le jeu de délégations de pouvoirs, sur le DSI.

4 Les relations avec les prestataires

Principe : interdiction de l'exercice d'une activité de travail temporaire non déclarée et autorisée en tant que telle (article L. 124-1 du Code du Travail).

Deux infractions spécifiques :

1. Le délit de marchandage (article L.125-1 du Code du Travail)

Aux termes de l'article L.125-1, «*toute opération à but lucratif qui a pour effet de causer un préjudice au salarié qu'elle concerne ou d'éluder l'application de dispositions de la loi, de règlement ou de convention ou accord collectif de travail, ou « marchandage », est interdite*».

Le délit de marchandage est donc constitué lorsque :

- les prestations ont un but lucratif de fourniture de main d'œuvre ;
- la fourniture de prestations a pour effet de causer un préjudice aux salariés détachés ou a pour but d'éluder l'application de dispositions impératives régissant leur statut social.

³ La « LSQ » est l'acronyme de la « *Loi sur la Sécurité Quotidienne* » du 15 novembre 2001

2. Le prêt de main d'œuvre illicite (article L.125-3 du Code du Travail)

Mise à disposition de personnel contre rémunération, en principe autorisée dans le seul cadre d'entreprises de travail temporaire. Le prêt de main d'œuvre est illicite s'il est pratiqué dans un but lucratif et s'il consiste exclusivement en un prêt de main d'œuvre.

Pour décider si l'activité est licite ou non, le juge recherchera si certains caractères du contrat d'entreprise sont réunis.

Ainsi, l'activité sera déclarée licite si :

- des prestations techniques précises,
- rémunérées de manière forfaitaire,
- exécutées sous le contrôle et la direction du prestataire (la mission du salarié doit être définie par l'entreprise prestataire),
- incluent un apport de savoir-faire spécifique (que le client n'a pas)
- et sont indissociables du prêt de main d'œuvre.
- dans le seul cas du délit de marchandage, s'ajoute le critère de l'absence de lésion des intérêts des salariés délégués au regard de leur statut social (s'assurer qu'ils ne bénéficieraient pas d'un statut plus protecteur chez le client).

Ces deux infractions sont distinctes mais cumulables. Constatées par l'inspection du travail, elles peuvent donner lieu à saisine du Parquet. Les sanctions maximales encourues, prévues à l'article L. 152-3, sont de 30.000 euros d'amende et/ou deux ans d'emprisonnement pour les dirigeants personnes physiques, outre l'éventuelle condamnation de la société elle-même, personne morale (voir les articles L.121-2 C. Pén. Et L.152-3-1 Code du Travail) et l'interdiction d'exercer l'activité de sous-entrepreneur de main d'œuvre pendant deux à dix ans.

Le prestataire est responsable des infractions commises, mais l'entreprise cliente peut être considérée comme coauteur.

5 Règlements particuliers

- Les textes ou obligations propres au domaine de la pharmacie : v. chapitre IX *Loi Informatique et Libertés*
- Les réglementations financières SOX et Bâle 2 :

De nouvelles obligations pèsent sur les dirigeants d'entreprise et, par là même, sur les DSI qui deviennent responsables de l'exactitude du résultat de l'entreprise.

Dans le cadre des réglementations financières et de la mise en conformité aux textes en vigueur (SOX⁴, LSF⁵, IAS⁶...), le DSI a pour responsabilité d'assurer la prestation de services, l'expertise en système d'information, l'assistance à la maîtrise d'ouvrage et à la maîtrise d'œuvre pour mettre en place les solutions informatiques nécessaires.

En cas de manquement, la sanction est le licenciement. Toutefois, même en l'absence de délégation de pouvoirs, le DSI qui n'avertit pas à temps sa hiérarchie des lacunes du SI en matière de sécurité financière, ou qui ne met pas en place les mesures garantissant la fiabilité du circuit de l'information financière, commet une faute professionnelle, éventuellement condamnable au pénal.

⁴ Loi Sarbanes-Oxley

⁵ Loi de Sécurité financière

⁶ International Accounting Standards

Le DSI et les risques juridiques

BMH Avocats

Il y a malheureusement un vide juridique sur les moyens technologiques devant assurer le contrôle interne du système d'information financier.

- Autres réglementations métier spécifiques : Santé, HSE, ...

Deuxième partie

Les moyens de prévenir la réalisation des risques

1 Approche générale

- Nécessité d'une sensibilisation et d'une responsabilisation des personnes concernées aux risques encourus : mise en place d'une politique et de dispositifs adéquats au sein de la structure.
- Nécessité d'une prise d'initiatives de la part des DSI, sensibilisés aux questions techniques, dans la mise en place des moyens.
- Nécessité d'une gestion concertée des risques et d'échanges entre les directions fonctionnelles concernées (DSI, DG et DRH)

2 Les actions concrètes par niveau de responsabilité

1) Au niveau des Directions Générales :

- Prise en compte des nouveaux risques à l'initiative des DSI
- Décisions de gestion et soutien continu pour la prise en compte des risques par les directions fonctionnelles
- Mise en conformité de l'entreprise aux réglementations en vigueur
- Décisions des directions générales concernant les traitements des données sensibles (Recours au CIL ou non, risque pénal personnel des décideurs...)
- Mise en place de délégations de pouvoirs, écrites et ciblées par domaines, avec les moyens adéquats pour leur validité
- Eventuelle nomination d'un déontologue

2) Au niveau des DSI :

- Identification des risques techniques liés aux outils ;
- Mise en place et diffusion des procédures de sécurité ;
- Le DSI doit mettre en place une procédure d'alerte de sa hiérarchie, de ses subordonnées et collaborateurs sur les problèmes liés à une mauvaise utilisation du système d'information. Exemple : un employé qui communiquerait, par courriel, des propos à caractère injurieux, raciste ou calomnieux, engagerait par ses actes la responsabilité de l'entreprise. Les tribunaux étant sensibles à la prévention, l'apposition par le DSI de messages d'avertissement automatiques en fin de courriels peut s'avérer utile.
- Mise en place de chartes de bonnes pratiques (Protection des outils propriétaires, des bases de données, usage contrôlé des logiciels (libres ou non), etc. par une politique de distribution des mots de passes et d'usage de l'email.
- Ediction d'un Règlement d'utilisation des Ressources Informatiques, mis à jour par un comité de suivi. Sa valeur juridique pourra être celle d'une Note de Service, acte unilatéral opposable aux salariés après consultation des IRP (délégués du personnel, Comité d'entreprise s'il y en a un) ou celle du contrat de travail, si ce règlement est accolé au contrat de travail et signé par le salarié en même temps que ce dernier.

Le DSI et les risques juridiques

BMH Avocats

- Attention toutefois : cette seconde alternative (signature individuelle par chaque salarié) comporte de risque d'être perçue comme une modification du contrat de travail du salarié (si elle intervient en cours d'exécution du contrat), qu'il pourra alors refuser, ce qui rendrait, le cas échéant, son licenciement sans cause réelle et sérieuse, avec les conséquences financières qu'un tel licenciement met à la charge de l'employeur.
- Diffusion de l'information et élaboration de documents de sensibilisation avec les autres directions, notamment juridique, financière et RH.
- Le DSI doit mettre en œuvre les mesures (techniques, outils, organisation) nécessaires à la sauvegarde et à l'archivage des données. Le manquement à cette obligation peut conduire à une sanction disciplinaire pouvant aller jusqu'au licenciement pour faute grave (c'est-à-dire, sans préavis ni indemnités).
- Afin d'alléger ses responsabilités, le DSI a la faculté d'opérer lui-même une délégation de pouvoir au RSSI. La délégation de pouvoirs, accompagnée parfois de délégations de signature, porte sur le fonctionnement opérationnel de l'entreprise, sur la sécurité, le contrôle et à l'usage des moyens techniques. La subdélégation doit être toutefois nécessaire, précise et permanente comme la délégation elle-même, et s'accompagner de pouvoirs réels et de moyens adéquats.
- Désignation d'un CIL : traduit l'engagement du responsable de traitement à respecter les dispositions légales.
- Etre vigilant sur le contenu des délégations de pouvoirs acceptées (v. Annexe).
- Eventuelle pratique de subdélégations de pouvoirs

3) Au niveau des DRH :

- Mise au point d'une politique de sensibilisation des personnels
- Elaboration d'une documentation écrite sur les risques spécifiques liés aux technologies : RI et Charte d'utilisation de l'outil informatique et des moyens de communication encadrant avec précision l'utilisation des moyens informatiques de l'entreprise et adoptée selon des modalités qui permettent de l'opposer à tous les salariés (par exemple, par le biais d'une intégration au moins partielle au règlement intérieur de l'entreprise ou aux contrats de travail des salariés). Cette Charte devra insister sur la nécessité de concilier le besoin de sécurité et l'esprit d'entreprise : elle doit permettre de fixer les bonnes pratiques et les règles à respecter pour le bien-être de chacun. Elle aura pour objectif de rendre l'environnement juridique lié aux usages des outils informatiques plus lisible et compréhensible. Doivent y être définis clairement les droits et obligations de chaque employé vis-à-vis de l'outil informatique. Elle doit enfin prévoir des règles visant à ne pas tomber dans les pièges simples: spécifier quand et comment doivent être changés les mots de passe, quel usage de l'e-mail est autorisé, etc.
- Présentation et négociation avec les IRP (dont le CHSCT pour les aspects d'ergonomie)
- Clauses spécifiques dans les contrats de travail

4) Au niveau des directions juridiques ou d'achat en charge des contrats externes:

- Réviser les clauses des contrats avec les prestataires
- Insérer les obligations spécifiques, les clauses « miroir » (confidentialité, protection des données, obligations de secret ...)