

MÉMOIRE SUR
LES RISQUES JURIDIQUES DES DSI
dans un environnement mouvant, mondial et externalisé.

Nicolas Pujol
Université Paris X - Nanterre
Septembre 2008

*Master 2 Droit des nouvelles technologies
et de la société de l'information.*



Glossaire

APE : Activité Principale Exercée

ARCEP : Autorité de Régulation des Communications Électroniques et des Postes

CIGREF : Club Informatique des Grandes Entreprises Françaises

CIO : Chief Information Officer (en) ou Directeur des Systèmes d'Informations (fr)

CJCE : Cour de Justice des Communautés Européennes

CLUSIF : CLU**de** la Sécurité Informatique Français

CNIL : Commission Nationale de l'Informatique et des Libertés

COB : Commission des opérations en bourse

CPCE : Code des Postes et Communications Électroniques

DHS : Department of Homeland Security (en) ou Ministère de la sécurité intérieure (fr)

DSI : Directeur des Systèmes d'Informations ou Direction des Systèmes d'Informations

EEE : Espace Economique Européen

ERP : Enterprise Resources Planning (en) ou Progiciels de Gestion Intégrée (fr)

FAI : Fournisseur d'Accès à l'Internet

FSA : Financial Services Authority (en) ou Autorité des services financiers (fr)

IT : Information Technologies (en) ou Technologies de l'Information (fr)

KM : Knowledge Management (en) ou Gestion des connaissances (fr)

LCEN : Loi pour la confiance dans l'économie numérique

MSSP : Managed Security Services Provider (en) ou Fournisseur de services de sécurité administrée (fr)

NTIC : Nouvelles Technologies de l'information et de la communication

OCDE : L'Organisation de Coopération et de Développement Economiques

PGI : Progiciels de Gestion Intégrée

PGRJ : Politiques de Gestion des Risques Juridique

PNR : Passenger Name Records (en) ou Données des dossiers passager (fr)

RM : Risk Manager (en) ou Gestionnaire du risque (fr)

RSSI : Responsable de la Sécurité des Systèmes d'Informations

TIC : Technologies de l'Information et de la communication

TGI : Tribunal de Grande Instance

Sommaire

<i>I. Le directeur des systèmes d'informations et le droit</i>	5
A) Du directeur informatique au directeur du système d'information	5
1) La fonction du directeur des systèmes d'informations	5
2) Les responsabilités juridiques des directeurs des systèmes d'informations	10
B) Les risques liés aux systèmes d'informations	16
1) La perturbation et l'entrave à la sécurité	16
2) L'atteinte à la protection des données personnelles et à la liberté de créer	22
<i>II. Les outils de prévention à la portée du directeur des systèmes d'informations : une solution pragmatique quant aux risques juridiques liés aux systèmes d'informations</i>	32
A) La mise en place de moyens de prévention adaptées	32
1) La nécessaire intervention d'un professionnel	32
2) La rédaction de chartes et la sensibilisation des salariés de l'entreprise	39
B) L'ouverture de la direction des systèmes d'informations au droit des nouvelles technologies	47
1) La pratique de la veille juridique et jurisprudentielle	47
2) Anticiper la transposition des directives européennes	53
<i>III. Annexes</i>	59
Annexes 1 et 2 : les principaux risques liés aux systèmes d'informations	59
Annexe 3 : sanctions pénales applicables au non-respect de la loi Informatique et Libertés	61

Introduction

Si le succès économique d'une entreprise reposait, par le passé, principalement sur la transformation qu'elle faisait des matières premières et de son capital matériel, les clés de sa réussite ont nettement changé.

L'entreprise évolue de nos jours dans un monde où l'immatériel occupe une place de plus en plus importante et de nombreux salons et conférences sont là pour en témoigner. Le succès d'une entreprise est étroitement lié à sa capacité de créer, d'innover et d'évoluer. Ces facteurs sont étroitement rattachés aux technologies de l'information et de la communication, aussi bien pour les nouvelles techniques mises en œuvre, que par les nouveaux usages qu'ils permettent.

La direction des systèmes d'informations est la clé de voûte qui permet d'assurer la cohérence de l'ensemble et est de ce fait en relation étroite avec les métiers de l'entreprise. C'est cette direction qui permet à l'entreprise de relever les défis qui s'imposent et de repenser son système d'information et même de fonctionnement tout entier.

Ainsi, les technologies de l'information et de la communication font partie des éléments clés de la stratégie des entreprises, tout comme la communication, la recherche, l'innovation et la protection de sa propriété intellectuelle. Elles constituent un actif essentiel dans le capital des entreprises, au même titre que les marques, les brevets, la connaissance et le savoir-faire.

L'internet et ses services populaires ont apporté un véritable bouleversement. La puissance et la facilité de mise en œuvre de ces outils, combinées à la vitesse de diffusion de l'information et du nombre d'accès élevé en tout point du globe, ont fait de ce média un extraordinaire outil de coopération et de développement. Après avoir submergé le grand public, l'internet a provoqué l'ouverture des systèmes d'informations des entreprises et leur interdépendance, les forçant même à adopter progressivement de nouvelles organisations internes et de façons de travailler.

Toutefois, si ces outils se révèlent être un atout majeur en termes d'efficacité et de coûts, le succès de ce progrès est à pondérer avec l'ampleur des risques qui planent aujourd'hui sur les entreprises, par ce biais.

Le patrimoine informationnel de l'entreprise, et principalement son système d'informations, est devenu la cible privilégiée de nouvelles menaces qui ne cessent de se multiplier et de se diversifier. De plus, la compétition sans merci que se livrent les acteurs

économiques dans un environnement mouvant, mondial et externalisé, constitue un facteur aggravant des menaces qui pèsent sur les entreprises et leurs représentants.

L'entreprise doit non seulement faire face à des menaces externes, mais aussi des menaces internes qui proviennent directement des agissements d'un petit nombre de collaborateurs indéclicats. Elle ne peut plus être considérée comme un bastion qu'il faut fortifier pour empêcher l'ennemi d'entrer, mais comme un lieu qu'il faut sécuriser en permanence, de tous côtés.

Les Directions des Systèmes d'Informations sont au cœur de la sécurité du système d'information de l'entreprise et donc au centre de ces problématiques. Ce mémoire s'adresse avant tout à leurs dirigeants et a pour objectif de les éclairer sur le sujet, d'un point de vue juridique. Le DSI (Directeur des Systèmes d'Informations) doit avoir une base de connaissances dans le domaine puisque la sécurité technique participe à la sécurité juridique de l'entreprise et de sa personne, et qu'elles peuvent être étroitement liées.

Nous définirons dans une première partie qui sont les directeurs des systèmes d'informations et quels sont les principaux risques pour lesquels ils peuvent voir leur responsabilité engagée (I), avant d'aborder en deuxième partie les mesures à adopter pour les limiter au maximum (II).

I. Le directeur des systèmes d'informations et le droit

A) Du directeur informatique au directeur des systèmes d'informations

1) La fonction du Directeur des systèmes d'informations

a. Définition du DSI

Le Directeur des Systèmes d'Informations (DSI) ou Chief Information Officer (CIO) en anglais, est le responsable du traitement de l'information dans une organisation.

Les fonctions d'un DSI sont primordiales pour l'entreprise et couvrent principalement l'architecture des systèmes, le développement d'applications, la gestion de bases de données, tout comme la sécurité des réseaux et du système d'information.

Ainsi, le DSI consacre une part importante de son activité à convaincre la direction de l'entreprise qu'il faut débloquer, ou du moins maintenir, les budgets qui lui sont alloués. Ils sont nécessaires pour fournir un service de qualité et s'assurer que le fonctionnement de l'entreprise reste optimal ; ce qui est préférable étant donné l'importance des systèmes d'informations pour les entreprises.

Le DSI est également force de propositions pour faire évoluer les systèmes mis en place et offrir de nouveaux services aux collaborateurs. C'est également lui, en relation avec les directions métiers, qui peut-être l'élément déclencheur dans le développement de nouvelles opportunités ou de nouvelles façons de travailler, puisqu'il a pour objectif de promouvoir de nouveaux usages et de développer le business de l'entreprise.

b. Le système informatique et le système d'information.

Il est important de distinguer deux notions fondamentales : le système informatique et le système d'information, qui sont trop souvent confondus, aussi bien dans de nombreux ouvrages que dans le langage courant. La compréhension de ces deux termes permettra de mieux appréhender leurs fonctions respectives.

LE SYSTÈME INFORMATIQUE

Le système informatique est défini par le Larousse comme « *l'ensemble des moyens de saisie, de traitement et de transmission de l'information mis en œuvre pour une application donnée* ». Il s'agit plus explicitement de l'ensemble des matériels et des logiciels, ainsi que tous les moyens de télécommunications qui permettent d'automatiser les fonctions et les informations.

LE SYSTÈME D'INFORMATION

Le système d'information est défini par le Larousse comme « *l'ensemble des moyens et des ressources informatiques dont dispose une entreprise pour recueillir, traiter, stocker et diffuser les données nécessaire à son activité* ». Il s'agit donc de l'ensemble des moyens non seulement informatiques (qui en sont partie intégrante), mais aussi humains, matériels et immatériels.

Le système d'information gère tous les processus au sein de l'entreprise et doit traiter des informations, qu'elles soient automatisées ou non.

La confusion qui est faite entre les systèmes informatiques et les systèmes d'informations persiste depuis le début des années 1980, lorsque les directeurs informatiques sont devenus des DSI.

En effet, lorsque l'informatique est entrée dans l'entreprise dans les années 1950, l'environnement dans lequel évoluait l'entreprise était stable et prévisible. Le Directeur informatique était nommé à cette époque pour répondre à des besoins de traitements de données à caractère répétitif et les applications informatiques s'articulaient autour d'eux.

Les domaines concernés étaient ceux du back-office, tel que la paie, la facturation ou le calcul de stock, et visaient à obtenir des gains de productivité. Les tâches auxquelles se consacrait le personnel dans ces domaines avaient une faible valeur ajoutée pour l'entreprise et pouvaient être traitées par des systèmes informatiques cloisonnés, peu communicants et bâtis sans une vision d'ensemble, conformément au modèle très hiérarchique des entreprises dans les années 1970.

Au cours des années 1980, l'onde de choc provoquée par les deux crises pétrolières, l'inflation, la disparition des marchés traditionnels, l'intensification de la concurrence, etc. a bousculé, de façon radicale, le paysage dans lequel évoluaient les entreprises. La complexité croissante de l'environnement externe de l'entreprise nécessitait une nouvelle forme d'organisation et de management, ainsi qu'une refonte du service informatique pour qu'il puisse procurer à l'entreprise un avantage concurrentiel décisif sur le marché.

C'est à ce moment que le concept d'informatique stratégique apparut. Désormais, les applications informatiques allaient être étroitement liées à la stratégie de l'entreprise. L'objectif principal était de se différencier des concurrents et d'apporter des services innovants: catalogues accessibles par minitel, banque à domicile, etc. Ces applications stratégiques nécessitaient une réelle collaboration avec les partenaires externes tels que les clients et les fournisseurs, mais aussi une prise en compte des modifications engendrées en interne.

C'est dans ce contexte que le concept de Système d'Information apparaît au milieu des années 1980 et "cannibalise" le système informatique. Cependant, les années 1980 étaient une période de transition et les directeurs informatiques, devenus presque tous des DSI, n'avaient pas les mêmes périmètres de compétences et de responsabilités que leurs homologues d'aujourd'hui.

Les DSI de l'époque avaient une vision encore trop technique alors que la problématique devait être stratégique. Aussi, les tâches d'un DSI dans les années 1980 se limitaient principalement à :

- assurer la cohérence de toutes les structures informatiques ;
- veiller à l'intégration des technologies dans l'existant ;
- anticiper les nouveaux besoins informatiques de l'entreprise.

c. Les missions du DSI

Dès le début des années 1990, l'entreprise est entrée dans une nouvelle ère, celle de l'internet et du commerce électronique.

L'internet et ses services populaires ont été un véritable bouleversement pour la société et ce média, qui est un extraordinaire outil de coopération et de développement, a facilité à l'extrême la diffusion et la recherche d'informations. Ces qualités ont provoqué l'ouverture et l'interconnexion des systèmes d'informations des entreprises et leur interdépendance, les forçant même à adopter progressivement de nouvelles organisations internes et de façons de travailler.

À l'intérieur de l'entreprise, le développement de l'intranet et de l'extranet avec des applications de travail collaboratif et de gestion de savoirs (Knowledge Management) encourage le travail en équipe et impose de nouvelles formes de structures organisationnelles, plus ouvertes et soucieuses de leur environnement. Elles doivent être capables de faciliter la communication, la coordination et la coopération entre tous les acteurs et d'améliorer la qualité des processus de travail de l'entreprise.

Ainsi, les impacts stratégiques des Nouvelles Technologies de l'Information et de la Communication (NTIC) sont devenus une évidence pour les entreprises. Les NTIC font aujourd'hui partie des éléments clés de la stratégie des entreprises, tout comme la communication, la recherche, l'innovation et la protection de sa propriété intellectuelle. Elles constituent un actif essentiel dans le capital des entreprises, au même titre que les marques, les brevets, la connaissance et le savoir-faire.

En outre, depuis le milieu des années 1990, le développement des Progiciels de Gestion Intégrée (PGI ou ERP en anglais pour Enterprise Resources Planning), dont la supervision nécessite une bonne connaissance des processus métiers de l'entreprise, donne

une autre dimension au rôle du DSI que celui qu'il occupait jusqu'alors.

En effet, l'entreprise évolue et tout comme elle impose de nouveaux styles de management, elle impose de nouvelles missions aux DSI qui voient leurs fonctions se complexifier.

Le profil d'un DSI est désormais davantage axé sur le système d'information dans sa globalité, intégrant toutes les fonctions (ressources humaines, marketing, commerciales, production, etc.), plutôt que sur l'aspect purement technique.

Le rôle du DSI est donc devenu un enjeu stratégique pour l'entreprise et EuroCIO définissait déjà au début des années 2000 son nouveau rôle, à savoir : *«Le DSI ne gère surtout pas la technologie, mais il a la responsabilité de l'efficacité du système d'information, il aide à la définition de la stratégie du système d'information et à l'expertise financière. Il est garant de la sécurité du système et doté d'une grande capacité d'adaptation».*

Comme nous l'avons vu, les missions du DSI sont donc actuellement très vastes et couvrent de nombreux domaines. Néanmoins, il est possible de lister les objectifs clés de sa fonction qui sont : la conception du schéma directeur du SI, les relations MOE-MOA, l'alignement stratégique du SI, le benchmarking, l'organisation par les processus, l'urbanisation du SI, la gouvernance du SI, la capitalisation des connaissances, le Knowledge Management, ainsi que la conduite du changement, l'infogérance, les relations avec les prestataires et les contrats.

Malgré l'importance de ces domaines, le rôle du DSI n'est pas encore figé, il est même en pleine mutation. En effet, les Directeurs des Systèmes d'Information souhaitent s'engager davantage dans le business de leur entreprise et positionner l'information au cœur de la stratégie, ainsi que de bénéficier d'une réelle reconnaissance de la part des dirigeants, qui n'est actuellement pas à la hauteur de leur fonction.

Certains DSI peinent même à faire reconnaître l'importance de leur poste par les comités de direction et d'exécution alors qu'ils ont une véritable responsabilité de dirigeant comme nous allons le voir dans la seconde sous partie. Est-ce que leur reconnaissance dans l'entreprise ne proviendra-t-elle justement pas des responsabilités grandissantes auxquelles ils sont soumis en matière pénale?

2) *Les responsabilités juridiques des DSI*

a. *La responsabilité pénale et civile du DSI en tant que personne physique*

En droit français, l'on distingue deux types de responsabilités juridiques :

- La **responsabilité pénale** qui sanctionne une atteinte à l'ordre public, ou à une réglementation impérative. « *L'infraction, en tant que violation de la loi pénale, fait naître l'action publique, exercée au nom de la société et tendant en principe au prononcé d'une peine ou d'une mesure pénale (répression)* ». Les Tribunaux prononcent dans ce cas des peines privatives de libertés (peines de prison, interdiction d'exercer les droits civiques) ou des peines pécuniaires (amendes) versées à l'État.
- La **responsabilité civile**, qui elle, est consécutive à un fait qui cause dommage à autrui.
 1. 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, lorsqu'elle est engagée, peut donner lieu à réparation sous forme de dommages-intérêts (et non sous la forme d'une exécution forcée du contrat).
 2. 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.

Toutefois, il ne faut pas oublier qu'une atteinte à l'ordre public (responsabilité pénale) peut aussi engendrer la responsabilité civile si une victime se déclare et demande réparation.

Par exemple, si Monsieur X s'introduit frauduleusement dans le système d'information de Monsieur Y et lui supprime des données, il s'agit d'un délit sanctionné par l'article 323-3 du Code pénal. Monsieur X encourt alors 5 ans de prison et 75 000 euros d'amendes

pour avoir violé la loi. De plus, Monsieur Y peut se déclarer comme victime et obtenir des dommages de la part de Monsieur X qui viendront réparer le préjudice qu'il a subi.

LES CONDITIONS DE LA RESPONSABILITÉ PÉNALE

La responsabilité pénale n'est engagée que si trois conditions sont réunies :

- Il faut dans un premier temps qu'il y ait **un élément légal**. La loi doit prévoir et punir explicitement l'acte qui a été commis, comme le vol, l'escroquerie, l'accès frauduleux à un système d'information, etc. Aucune interprétation de la loi n'est possible, ce qui implique qu'en dehors des cas prévus l'on ne peut pas prononcer de peines. De plus, les sanctions devront être elles aussi prévues par la loi et non un règlement par exemple.
- La seconde condition requise est **un élément matériel**. Une preuve rapportant l'existence de l'infraction doit être apportée.
- Enfin, la dernière condition est **l'élément intentionnel**. L'intention de commettre l'infraction doit exister et en principe il n'est pas possible d'être condamné pour quelque chose que l'on n'a pas voulu. L'article 121-3 du Code pénal énonce en effet qu'« *il n'y a point de crime ou de délit sans intention de le commettre* » à l'exception de la mise en danger délibérée d'autrui et de l'infraction d'imprudence qui constituent des délits.

Il convient donc de souligner que si la responsabilité pénale peut ne pas être engagée en présence d'un élément intentionnel, l'inverse est aussi possible.

En effet, l'article L. 121-3 du Code pénal dispose qu'« *il y a également délit, lorsque la loi le prévoit, en cas de faute d'imprudence, de négligence ou de manquement à une obligation de prudence ou de sécurité prévue par la loi ou le règlement, s'il est établi que l'auteur des faits n'a pas accompli les diligences normales compte tenu, le cas échéant, de la nature de ses missions ou de ses fonctions, de ses compétences ainsi que du pouvoir et des moyens dont il disposait* », ce qui permet d'engager la responsabilité pénale d'une personne de bonne foi n'ayant pas agi avec l'intention de commettre un délit, comme nous le verrons un peu plus tard.

En matière de responsabilité pénale, signalons également que la Loi Perben II du 10 mars 2004¹ a généralisé la possibilité d'engager celle des personnes morales², auparavant réservée à quelques délits.

S'il ne peut bien évidemment être question de mettre en prison une société en tant

¹ Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité, JORF du 10 mars 2004, page 4567.

² Les personnes morales dont la responsabilité peut être engagée sont les personnes morales de droit privé et les personnes morales de droit public, à l'exception de l'État.

que telle, celle-ci peut néanmoins être condamnée à des peines d'amende, mais aussi à une suspension de son activité, voire dans l'hypothèse la plus grave, sa dissolution.

En outre, l'engagement de la responsabilité de la société n'exclut pas celle de son chef, pour cette fois-ci, des peines privatives de libertés en plus d'éventuelles amendes. La loi prévoit en effet que la responsabilité pénale d'un chef d'entreprise ne peut être engagée que s'il a agi intentionnellement pour commettre le délit ; mais comme nous l'avons vu, sa responsabilité peut-être engagée en cas de faute d'imprudence, de négligence ou de manquement à une obligation de prudence ou de sécurité prévue par la loi ou le règlement, compte tenu du pouvoir et des moyens dont il dispose.

LES CONDITIONS DE LA RESPONSABILITÉ CIVILE

Par responsabilité civile, il faut comprendre qu'une faute a été commise et qu'elle a causé un préjudice à une victime qu'il faut dédommager.

Comme pour la responsabilité pénale, trois conditions sont à réunir pour qu'il soit question de dommages et intérêts. Il s'agit de l'**existence d'une faute** et d'un **préjudice**, avec un **lien de causalité entre les deux**.

Toutefois, dans le monde de l'entreprise, la responsabilité civile est quelque peu aménagée. En ce sens, l'article 1384 alinéa 5 du Code civil dispose que « *les maîtres et les commettants [sont responsables] du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés* ».

De façon plus explicite :

- Si le salarié a commis une faute dans l'exercice de ses fonctions, l'entreprise devra s'acquitter des dommages et intérêts ;
- Si la faute est commise en dehors de l'exercice de ses fonctions, la responsabilité civile du salarié pourra être engagée.

b. La responsabilité de l'entreprise en tant que personne morale

Le manquement à la sécurité du système d'information peut être sanctionné pénalement et civilement, parfois lourdement comme nous l'avons vu. Dans ce domaine, l'entreprise, en tant que personne morale, peut voir sa responsabilité engagée ; mais elle peut également se retourner à l'encontre de ses salariés, par le jeu des délégations.

Seule une personne physique peut, en principe, répondre d'une faute par une sanction pénale. Cette situation a changé depuis l'entrée en vigueur, le 1^{er} mars 1994, de l'article 121-2 du Code pénal³, qui pose le principe de la responsabilité pénale des personnes morales.

Les motifs du projet de loi étaient, d'une part, «*vaincre l'immunité des personnes morales qui, par les moyens de grande ampleur dont elles disposent sont à l'origine d'atteintes graves à la santé publique, à l'environnement, à l'ordre économique ou à la législation sociale...*», d'autre part, de cantonner dans de plus justes limites la responsabilité personnelle des dirigeants sociaux afin de mieux assurer le respect du principe «*nul ne répond que de son propre fait*».

Ainsi, l'article 121-2 du Code pénal dispose que :

- «*Les personnes morales, à l'exclusion de l'État, sont responsables pénalement...*
- *des infractions commises, pour leur compte, par leurs organes ou représentants*»

QUELLES SONT LES PERSONNES MORALES VISÉES ?

Sont concernées par ces dispositions :

- les personnes morales de droit privé dotées de la personnalité morale,
- les personnes de droit public (à l'exclusion de l'État), avec la limitation que les collectivités territoriales et leurs groupements ne sont responsables que pour les infractions commises dans l'exercice d'activités susceptibles de faire l'objet de conventions de délégation de service public,
- les personnes morales de droit étranger ayant commis une infraction sur le territoire français.

QUELLES SONT LES INFRACTIONS CONCERNÉES ?

Jusqu'au 31 décembre 2005, la personne morale ne pouvait être poursuivie que sur le fondement de textes répressifs prévoyant expressément sa responsabilité pénale. À compter du 1^{er} janvier 2006, cette disposition n'est plus nécessaire et la personne morale peut être poursuivie pour tous types d'infractions.

³ Loi n° 92-1336 du 16 décembre 1992 relative à l'entrée en vigueur du nouveau Code pénal et à la modification de certaines dispositions de droit pénal et de procédure pénale rendue nécessaire par cette entrée en vigueur, JORF du 23 décembre 1992, page 17568.

QUELS SONT LES AUTEURS SUSCEPTIBLES D'ENGAGER LA RESPONSABILITÉ DE LA PERSONNE MORALE ?

L'article 121-2 du Code pénal dispose que la responsabilité pénale de la personne morale est engagée pour les infractions commises « *pour son compte* » par ses « *organes ou représentants* ». Cela signifie que l'organe ou le représentant qui a agi pour son compte personnel n'engage pas la responsabilité de la personne morale, de même si celui-ci a outrepassé son pouvoir.

SANCTIONS PÉNALES APPLICABLES À LA MISE EN CAUSE DE LA RESPONSABILITÉ DE LA PERSONNE MORALE

Qu'elle soit civile ou pénale, la mise en cause de la responsabilité de la personne morale constitue l'un des soucis majeurs des dirigeants d'aujourd'hui. Dans un communiqué du 21 février 2000, la Commission des opérations en bourse (COB) a par exemple mis en garde les banques contre certains salariés « *se livrant à des faits répréhensibles (proposition de produits financiers à des tiers sans y être habilités) en raison de l'insuffisance manifeste de leurs entreprises dans les procédures de contrôle relatives à l'accès au réseau depuis les locaux professionnels* ».

En effet, les sanctions pénales sont lourdes : l'article 323-6 du Code pénal prévoit en ce sens que les amendes encourues par les personnes morales sont égales au quintuple de celles prévues par les personnes physiques.

c. Les délégations de pouvoir

Les structures des entreprises sont de plus en plus complexes. Elles évoluent dans un environnement mouvant, mondial et externalisé qu'il est impossible de maîtriser entièrement. L'employeur a donc la possibilité d'opter pour des délégations de pouvoir et confier, par ce biais, certaines missions qui relèvent en temps normal de sa responsabilité à ses salariés. Une telle pratique apporte également un avantage à l'employeur qui peut dégager ainsi sa responsabilité pénale.

LES MODALITÉS DE LA DÉLÉGATION DE POUVOIR

Depuis 1993, la Cour de cassation a unifié sa position sur le principe de délégation considérant dans cinq arrêts de principe que *«sauf si la loi en dispose autrement, le chef d'entreprise, qui n'a pas personnellement pris part à la réalisation de l'infraction, peut s'exonérer de sa responsabilité pénale s'il apporte la preuve qu'il a délégué ses pouvoirs à une personne pourvue de la compétence, de l'autorité et des moyens nécessaires»*⁴.

Cependant, si les tribunaux ont admis ce principe, cela se fait dans un cadre étroitement vérifié tant sur la forme que sur le fond, ce qui laisse une possibilité aux DSI et RSSI (Responsable de la Sécurité des Systèmes d'Informations) d'être exonérés.

Ainsi, un DSI ou un RSSI ne pourra être valablement investi d'une délégation de pouvoir que si :

- il a les compétences nécessaires : techniques certes, mais aussi des connaissances juridiques,
- il a l'autorité nécessaire,
- il dispose des moyens nécessaires pour accomplir sa mission.

Mais d'autres conditions sont également requises :

- La délégation doit être précise (par exemple : mesures de sécurité liées au système d'information).
- La délégation doit revêtir un caractère de permanence (pas de délégation à une personne occupant un poste temporaire).
- La jurisprudence exige par ailleurs que le salarié soit informé des conséquences de la délégation de pouvoir, à savoir un transfert de responsabilité pénale.

Un arrêt de la Cour de cassation du 8 février 1983⁵ admet la subdélégation, à condition que le subdélégué soit investi des mêmes pouvoirs que ceux énoncés précédemment. Cette disposition est difficile à concevoir entre un DSI et un RSSI par exemple, sauf dans le cas d'un très grand groupe. En effet, dans ce cas, le DSI pourrait très bien déléguer ses pouvoirs à des responsables informatiques chargés de filiales ou de départements. Par contre, il faudra faire attention au principe de non-cumul des délégations de pouvoir.

⁴ Cour de cassation, chambre criminelle, Bulletin criminel n° 112 du 11 mars 1993, page 270.

⁵ Cour de cassation, chambre criminelle, 8 février 1983, Jean-Pierre B. c/ Mathy A., pourvoi n° 82-92364.

Enfin, la délégation verbale est admise, mais une délégation de responsabilité pénale effectuée sous la forme d'un écrit aura plus de poids auprès d'une juridiction éventuellement saisie pour établir l'existence réelle de la délégation. L'acceptation expresse de la délégation présume en effet que le salarié l'a acceptée en pleine connaissance des conséquences (attention donc aux "notes de missions" dont disposent certains RSSI) et le refus expressément exprimé par un salarié rend invalide la délégation de pouvoir.

Comme nous venons de le voir, les directeurs des systèmes d'informations sont bel et bien concernés par le droit, et à plus d'un titre. Comment cette influence se manifeste-t-elle au quotidien dans l'exercice de leurs fonctions ? Pour illustrer nos propos nous allons maintenant prendre pour exemple les quatre principaux risques auxquels ils sont confrontés et pour lesquels leur responsabilité peut être engagée.

B) Les risques liés aux systèmes d'informations

1) La perturbation et l'entrave à la sécurité

Le DSI, qui est au cœur de la sécurité du système d'information de l'entreprise doit avoir un minimum de connaissances juridiques dans le domaine puisque la sécurité technique participe à la sécurité juridique de l'entreprise et de sa personne, et qu'elles peuvent être étroitement liées.

Les risques s'appliquant aux systèmes d'informations sont très vastes puisqu'ils sont une infrastructure vitale pour l'entreprise et qu'ils font appel à un grand nombre d'usages, de technologies et de personnes différentes. Par ailleurs, ils sont de plus en plus complexes aussi bien vis-à-vis des traitements qui sont effectués, que des technologies utilisées ou encore par la variété et le nombre d'intervenants s'impliquant dans les systèmes d'informations. Ces évolutions sont nécessaires pour répondre aux besoins qui sont énoncés dans un environnement mouvant, mondial et externalisé, mais cela ne doit pas se faire sans en maîtriser les risques.

Parmi les principaux risques liés aux systèmes d'informations que j'ai énoncés dans les deux cartes heuristiques en annexe 1 et 2, seuls quelques-uns ont une implication dans le domaine juridique. La carte ne couvre bien évidemment pas tous les risques et ce n'est pas son objectif ; elle vise seulement à mettre en valeur les risques auxquels il faut impéra-

tivement prêter attention et ils concernent aussi bien les risques d'entraver la sécurité des systèmes d'informations (1) comme l'utilisation des outils informatiques pour commettre un délit (a) et le manquement à la sécurité du système d'information (b) ainsi que les risques attentatoires à la protection des données personnelles et à la liberté de créer (2) que nous aborderons avec le traitement des données à caractère personnel (a) et l'atteinte au droit d'auteur (b).

a. Les outils informatiques de l'entreprise utilisés par un salarié dans la commission de l'infraction.

La totalité, ou presque, des entreprises⁶ ont un accès internet. Par ce biais, les salariés peuvent exercer leur activité professionnelle et des activités annexes plus personnelles, par des moyens fournis par l'employeur. Dans ce cas, que se passe-t-il lorsqu'un salarié est responsable d'un délit commis par les outils informatiques mis à sa disposition pour l'exercice de ses fonctions?

Nous prendrons pour exemple un jugement du TGI de Marseille⁷, qui a condamné un employeur pour avoir mis à disposition d'un salarié les moyens techniques nécessaires à la réalisation de son délit et qui a été confirmé par un arrêt de la cour d'appel d'Aix-en-Provence⁸.

COMMENT LA RESPONSABILITÉ D'UN CHEF D'ENTREPRISE PEUT-ÊTRE MISE EN JEU DU FAIT DES AGISSEMENTS DE L'UN DE SES SALARIÉS ?

À priori, le chef d'entreprise n'a pas agi avec l'intention de mettre à la disposition de son salarié les moyens lui permettant de commettre son délit. L'hypothèse la plus courante à laquelle une entreprise doit faire face est celle d'un salarié ayant agi à son insu.

Néanmoins, toutes les fois où il sera possible de démontrer qu'un employeur savait ou aurait dû savoir que de telles pratiques s'étaient développées au sein de son entreprise,

⁶ 97 % des entreprises de plus de 10 salariés ont un accès à l'internet selon l'INSEE (Insee Première n°1184 - avril 2008).

⁷ Tribunal de grande instance de Marseille, 1^{re} chambre civile, 11 juin 2003, SA Escota c/ Société Lucent Technologies.

⁸ Cour d'appel d'Aix-en-Provence, 2^e chambre, 13 mars 2006, SA Escota c/ Société Lucent Technologies.

ce dernier pourra se voir reprocher des actes de complicité par la fourniture de moyens.

La jurisprudence précise toutefois que sa responsabilité personnelle ne peut être engagée que si les 3 conditions suivantes sont réunies :

- Le salarié doit toujours être sous la subordination de son employeur ;
- Il doit avoir causé le dommage à l'occasion de son travail ;
- Avec les outils de l'entreprise, utilisés conformément à leur destination.

La jurisprudence française⁹ tend à considérer que l'employé a agi dans ses fonctions dès le moment où le délit a eu lieu durant son temps de présence en entreprise et avec les moyens mis à sa disposition par l'employeur. Ainsi, l'employeur « *ne s'exonère de sa responsabilité que si son préposé a agi hors des fonctions auxquelles il était employé, sans autorisation et à des fins étrangères à ses attributions* ».

AFFAIRE SA ESCOTA C/ SOCIÉTÉ LUCENT TECHNOLOGIES, 11 JUIN 2003

Dans l'affaire opposant les sociétés Escota et Lucent Technologies¹⁰, le tribunal a condamné un employeur pour un usage illicite de l'internet effectué par un des ses employés (ce dernier ayant créé un site dénigrant hébergé sur le serveur de l'entreprise), sur le fondement de l'article 1384 du Code civil pour avoir mis à disposition de son salarié les moyens techniques nécessaires à la mise en ligne du site dénigrant l'autre société.

En effet, en l'espèce le tribunal a estimé que :

- le salarié avait agi dans le cadre de ses fonctions en tant que « *technicien dont l'activité est la construction d'équipements et de systèmes de télécommunication [...], et dans laquelle l'usage d'un ordinateur et d'internet doit être quotidienne* » ;
- ses actes avaient été réalisés avec l'autorisation de son employeur puisque le directeur des ressources humaines autorisait, dans une note de service, les salariés à utiliser les équipements informatiques mis à leur disposition pour consulter des sites autres que ceux présentant un intérêt en relation directe avec leurs activités au sein de la société ; même si cela était à la condition que « *ces utilisations demeurent raisonnables [...] et respectent les dispositions légales régissant ce type de communication et les règles internes de la société, les accès aux sites à caractère explicitement sexuel et contrevenant aux valeurs de la société Lucent Technologies étant prohibés* » ;

⁹ Ass. plén., 19 mai 1988, Bull. civ. n° 5.

¹⁰ Affaire SA Escota c/ Société Lucent Technologies, TGI de Marseille, 11 juin 2003

- il n'avait pas agi à des fins étrangères à ses attributions puisque, selon la même note, les salariés étaient également autorisés à disposer d'un accès internet en dehors de leurs heures de travail.

b. Le délit de manquement à la sécurité du SI

L'interconnexion croissante des réseaux et des systèmes d'informations, ajoutée à la complexité des applications et des technologies est un facteur à l'origine de l'accroissement des vulnérabilités des systèmes d'informations.

Régulièrement, la presse se fait l'écho d'attaques virales susceptibles de nuire à nos ordinateurs et de se propager à travers des applications aussi courantes que la messagerie instantanée et le courrier électronique, voire en étant simplement connecté sur le réseau internet. À ces attaques, il faut ajouter les intrusions, les actes de piratage et de malveillance en tous genres, ainsi que failles affectant régulièrement les logiciels et les systèmes d'exploitation utilisés, pour se rendre compte de l'ampleur de la menace.

La sécurité informatique nécessite donc une véritable prise de conscience et la mise en place de mesures techniques et organisationnelles adéquates.

Ainsi, le 25 juillet 2002, l'OCDE (l'Organisation de Coopération et de Développement Economiques) mettait à jour ses Lignes directrices sur la sécurité des systèmes et réseaux d'information¹¹ et soulignait la nécessité de développer une culture de la sécurité, précisant que chacun, gouvernements, entreprises, organisations, utilisateurs individuels a un rôle à jouer pour assurer la sécurité des systèmes d'informations et des réseaux.

La politique législative fait partie de l'ensemble des mesures destinées, non seulement à sanctionner, mais également à sensibiliser les personnes concernées par la nécessaire adoption et mise en œuvre de procédures améliorant la sécurité informatique.

Définition de l'obligation de sécurité

Le principe de l'obligation de sécurité est posé par l'article 29 de la loi du 6 janvier 1978 dite Informatique et Libertés¹² : « *Toute personne ordonnant ou effectuant un traitement*

¹¹ Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité - Recommandation du Conseil de l'OCDE du 25 juillet 2002.

¹² Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF du 7 janvier 1978, page 227.

d'informations nominatives s'engage de ce fait, vis-à-vis des personnes concernées, à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés».

L'obligation de sécurité

La législation sur les données personnelles soumet le responsable d'un traitement de données à l'obligation d'assurer la confidentialité et la sécurité des traitements de données, sous peine de sanctions pénales. Plus généralement, le dirigeant peut être accusé de délit de manquement à la sécurité du système d'information s'il s'avère qu'il «*n'a pas mis en œuvre les systèmes adéquats pour protéger son système d'information*».

Le non-respect de ces précautions est sanctionné par l'article 226-17 du Code pénal qui dispose : «*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 déformées, endommagées ou communiquées à des tiers non autorisés est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende*».

La directive européenne 95/46/CE du 24 octobre 1995 relative au traitement de données à caractère personnel comporte des dispositions détaillées sur la confidentialité et la sécurité des traitements.

L'article 17.1 «*Sécurité du traitement*» de la directive précise ainsi que «*Le responsable du traitement doit mettre en œuvre les mesures techniques et d'organisation appropriée pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des transmissions de données dans un réseau, ainsi que contre toute autre forme de traitement illicite*».

Par ailleurs, la directive définit de manière précise les obligations incombant aux prestataires traitant des données pour le compte du responsable du traitement. L'article 16 relatif à la confidentialité des traitements prévoit que toute personne agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, ainsi que le sous-traitant lui-même, qui accède à des données à caractère personnel, ne peut les traiter que sur instructions du responsable du traitement, sauf en vertu d'obligations légales. Cette disposition vise les obligations incombant aux prestataires qui traitent des données pour le compte d'un organisme, par exemple un hébergeur.

Enfin, l'article 17.2 relatif à la sécurité des traitements prévoit que le responsable du traitement, lorsque le traitement est effectué pour son compte, doit choisir un sous-trai-

tant qui apporte des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives aux traitements à effectuer. Il doit également veiller au respect de ces principes¹³ et ne pas oublier qu'il demeure responsable de la confidentialité des données traitées pour son compte.

La portée de l'obligation de sécurité

Bien que l'article 226-17 du Code pénal ne précise pas quelles sont les « *précautions utiles pour préserver la sécurité de ces informations* », il s'agit uniquement d'une obligation de moyens; la loi n'exige pas une sécurité absolue. Le besoin de sécurité des informations est notamment apprécié en fonction du triptyque DIC: Disponibilité, Intégrité et Confidentialité.

Aussi, la mise en œuvre d'une politique de sécurité nécessite de mettre en place des mesures variées, d'ordre logique (pare-feu, cryptage, mots de passe, installation d'antivirus, etc.), organisationnel (accès aux données en fonction des habilitations, sauvegardes, maintenance, mise à jour des logiciels pour installer les correctifs, etc.) et physique (contrôle d'accès aux locaux, protection contre les incendies, etc.). Elle suppose également des actions de sensibilisation et de formation du personnel; le tout consigné dans un document de référence et intégré aux procédures de l'organisme. Enfin, les mesures doivent être auditées et réexaminées périodiquement pour conserver leur efficacité.

La mise en place de toutes ces mesures représente évidemment un poste de coût pour les organismes concernés. L'article 17.3 de la directive précise que les mesures de sécurité « *doivent assurer, compte tenu de l'état de l'art et des coûts liés à leur mise en œuvre, un niveau de sécurité approprié au regard des risques présentés par le traitement et de la nature des données à protéger* ». En d'autres termes, les mesures adoptées doivent être adaptées à la nature des données à protéger: un simple fichier client de noms et adresses n'exige pas le même degré de sécurisation que des données médicales ou bancaires, couvertes par le secret professionnel. On raisonnera donc en termes de gestion des risques afin de trouver un compromis entre les besoins de circulation de l'information, de rapidité d'exécution et le niveau de sécurité exigé au regard des données.

Édictée en ces termes, la portée de l'obligation de sécurité, lourdement sanctionnée pénalement, apparaît très contraignante. Elle nécessite la mise en place de véritables poli-

¹³ Notamment les obligations en matière de sécurité qui lui incombent également (article 17-3 de la directive)

tiques de sécurité au sein des organismes et de gérer avec rigueur les relations contractuelles avec les prestataires informatiques extérieurs. Dans la mesure où tout organisme est appelé à gérer des données personnelles, ne serait-ce que les données relatives aux clients ou usagers, et au personnel, le champ d'application de l'obligation de sécurité apparaît relativement large.

Certains auteurs soulignent ainsi que les risques de mise en cause de la responsabilité s'avèrent particulièrement élevés. Néanmoins, les exemples de manquement à l'obligation de sécurité, et spécialement sur l'internet, sont légion. Pourtant, les poursuites pour manquement à l'obligation de sécurité informatique demeurent exceptionnelles en France¹⁴.

En effet, bien que dans les textes les peines encourues soient plus importantes pour le manquement à l'obligation de sécurité, la répression pénale préférera s'intéresser au pirate plutôt qu'à sa "proie". Le fait de ne pas avoir adopté les mesures de sécurité informatique adéquates n'entraînera donc pas un grand risque de poursuites pénales, c'est du moins sous cet angle que le ratio risques-coût d'une politique de sécurité pourrait être envisagé par les dirigeants des organismes concernés.

Il faut tout de même rappeler que les peines encourues sont de cinq ans d'emprisonnement et de 300 000 euros d'amende (1 500 000 euros pour les personnes morales) ce qui est loin d'être négligeable. De plus, nous nous dirigeons vers d'avantages de responsabilisation en matière de sécurité, la situation actuelle peu donc changer très rapidement et il est préférable, en tant que DSI ou Responsable de la sécurité des systèmes d'informations, de s'assurer d'un niveau de protection adéquat dès aujourd'hui.

2) *L'atteinte à la protection des données personnelles et à la liberté de créer*

a. *Le traitement de données à caractère personnel*

Avant d'entrer dans le vif du sujet, deux définitions sont à connaître : celle de la notion de donnée personnelle et d'un traitement de données telle que prévue par la Loi Informatique et Libertés du 6 janvier 1978.

¹⁴ On peut par exemple citer un arrêt de la chambre criminelle du 30 octobre 2001 mais les condamnations font plus offices d'exceptions que de règles.

Données personnelles : Les données personnelles sont toutes les informations permettant d'identifier, directement ou indirectement, une personne physique. Cela peut être un nom, un prénom, une adresse de courrier électronique, un numéro de téléphone, un numéro d'abonné, etc.

Traitement de données : Un traitement est défini par la loi comme « *toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données à caractère personnel, telle que 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* ».

Lors de mon stage au CIGREF (Club Informatique des Grandes Entreprises Françaises), j'ai été amené à gérer la problématique des traitements de données à caractère personnel, principalement dans le cadre des associations. C'est sur cet exemple que je me baserai tout au long de mon argumentation. Elle ne couvrira donc pas toutes les problématiques et sera centrée sur les besoins du CIGREF. Cependant, les informations données dans ce contexte permettront d'avoir les clés nécessaires à une bonne compréhension de la problématique et pourront être réexploitées pour être appliquées à d'autres structures, aussi bien des associations que des entreprises.

Comme nous l'avons vu, la notion de donnée personnelle est très large, c'est pourquoi la majorité des traitements effectués dans un système d'information peuvent être considérés comme des traitements de données à caractère personnel. Tous ces traitements ne doivent pas toujours faire l'objet d'une déclaration à la CNIL (Commission Nationale de l'Informatique et des Libertés) avant leur mise en œuvre puisque cet organisme autorise de nombreuses dispenses. La possibilité ou pas d'être dispensé sera fonction de la finalité des traitements et du type de données traitées. De plus, en cas de déclaration obligatoire, la CNIL a émis ces dernières années de nombreuses procédures simplifiées qui peuvent être téléchargées à partir de son site internet dans la rubrique « *Déclarer* ».

Comme nous allons le voir maintenant, les mesures imposées par la loi Informatique et Libertés, ainsi que la CNIL, sont très strictes. Le non-respect de ces obligations et

dispositions peut avoir de très lourdes conséquences, surtout depuis la modification de la loi en 2004 qui donne à la CNIL un fort pouvoir de contrôle et de sanctions¹⁵.

D O N N É E S P O U V A N T Ê T R E T R A I T É E S

La dispense prévoit que seules les données relatives à un nombre limité d'informations peuvent être collectées. Elles doivent avoir pour seuls objectifs d'arriver aux finalités autorisées et de ce fait concernent uniquement l'identité physique et bancaire, ainsi que quelques informations nécessaires à la vie associative ou strictement liées à l'objet statutaire de l'association.

Une exception est également autorisée permettant de traiter certaines données de connexion aux seules fins de statistiques.

Pour connaître les données supplémentaires qui peuvent être traitées dans le cadre de la dispense de déclaration, il est donc nécessaire de consulter les statuts de l'association, et particulièrement ses objets, mais cela n'aurait que peu d'intérêt dans le cas présent. Attardons-nous plutôt sur les autres contraintes.

D O N N É E S N E P O U V A N T P A S Ê T R E T R A I T É E S

Toutes les données qui n'ont pas pour objectif de répondre aux finalités citées ci-dessus ou qui ne sont pas strictement liées à l'objet statutaire de l'association feront perdre le bénéfice de la déclaration simplifiée.

De plus, les traitements faisant appel à des données très particulières parmi lesquelles nous pouvons citer les origines raciales, les opinions politiques, philosophiques ou religieuses, l'état de santé, etc. devront avoir été autorisés par la CNIL.

F I N A L I T É S D U T R A I T E M E N T

Les traitements ne peuvent être effectués que s'ils ont pour objet certaines finalités, délimitées par un cadre plus ou moins strict selon la procédure suivie. Classées par ordre croissant de permissivité, les procédures sont : la dispense de déclaration (très peu de libertés), la déclaration simplifiée, la déclaration et enfin, la demande d'autorisation qui peut être le seul moyen de traiter des données ou ayant des finalités particulières.

¹⁵ Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JORF du 7 août 2004, page 14063.

DESTINATAIRES DES DONNÉES

Les données collectées ne peuvent être accessibles et transmises qu'à un nombre restreint de personnes, dans la limite de leurs attributions respectives.

Néanmoins, sous réserve des conditions à respecter décrites ci-après, les informations relatives aux membres et donateurs d'une association peuvent faire l'objet :

- d'une diffusion au public sous la forme d'un annuaire ;
- d'une cession, location ou d'un échange à des fins de prospection (à l'exclusion d'opérations de prospection politique).

DURÉE DE CONSERVATION

La conservation des données à caractère personnel doit être limitée dans le temps. Par exemple, concernant un membre, ses données ne peuvent pas être conservées après sa démission ou sa radiation, sauf son accord exprès. De même que les informations relatives à son parcours professionnel devront respecter les finalités du traitement et une durée de conservation en adéquation avec ses objectifs. Il ne sera pas considéré comme raisonnable ou utile de conserver toute sa vie professionnelle et une limite dans le temps devra être fixée. Elle peut être égale à une période de 5 ans ou aux 3 derniers postes occupés par exemple.

CONDITIONS À RESPECTER : INFORMATION ET CONSENTEMENT DES PERSONNES CONCERNÉES

Les personnes concernées par des traitements de données personnels doivent être informées, lors de la collecte de ces informations, de l'identité du responsable de traitement, des finalités poursuivies ainsi que d'autres informations dont leur droit d'opposition, d'accès et de rectification avec leurs modalités d'exercice.

Lorsque les données peuvent être diffusées (Exemple : le cas d'un annuaire), les adhérents doivent être préalablement informés et en mesure de s'opposer à ce que tout ou partie des données les concernant soient publiées, et cela, à l'aide d'un moyen simple.

En ce qui concerne la prospection commerciale, l'envoi de messages par voie électronique est subordonné au consentement préalable des personnes concernées, toujours à l'aide d'un moyen simple et dénué d'ambiguïté. Il convient dans ce cas de noter que la notion de prospection commerciale est très large puisqu'elle concerne « *tout message destiné à promouvoir, directement ou indirectement, des biens, des services ou l'image d'une personne vendant.*

des biens ou fournissant des services ». Cette définition englobe par exemple, la promotion d'un événement organisé par une tierce personne, mais dont l'inscription serait payante ou vantant les produits d'une société. De plus, lorsque les données sont utilisées à des fins de prospection, les personnes concernées doivent être informées qu'elles peuvent s'y opposer sans frais et sans justification.

S É C U R I T É

Comme nous l'avons abordé rapidement, le responsable du traitement est tenu de prendre toutes les précautions utiles pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

La loi n'impose encore aucune mesure pour parvenir à cet objectif; le juge aura pour seuls critères les moyens (techniques, humains, financiers...) qui ont été mis en œuvre pour assurer la sécurité du système et il faudra justifier qu'ils étaient appropriés dans l'éventualité d'une plainte faisant suite à l'exploitation d'une faille.

T R A N S M I S S I O N S D E D O N N É E S V E R S D E S P A Y S T I E R S À L ' U N I O N E U R O P É E N N E

La notion de transfert n'est pas définie par la directive 95/46, ni par la loi du 6 janvier 1978, mais doit s'entendre au sens large. Ainsi, constitue un transfert de données vers un pays tiers toute communication, toute copie ou tout déplacement de données par l'intermédiaire d'un réseau, ou de tout autre support, dans la mesure où ces données ont vocation à faire l'objet d'un traitement dans le pays destinataire¹⁶.

De façon générale, il est impossible de transmettre des données à caractère personnel vers des pays tiers à l'Union européenne ou n'offrant pas une protection équivalente, y compris lorsque cette transmission est réalisée à des fins de sous-traitance (cela inclut le cas où le serveur serait localisé à l'étranger, mais propriété de l'entreprise puisque c'est la localisation géographique des données qui s'applique), sans avoir reçu l'autorisation de la CNIL¹⁷.

Un pays peut-être reconnu comme offrant une protection adéquate ou suffisante,

¹⁶ CNIL - Guide transfert d'informations vers les pays n'appartenant pas à l'Union européenne.

¹⁷ Prévu par l'article 25 de la directive 95/46 et l'article 68 de la loi informatique et libertés.

dans les “*décisions d’adéquation*” prises à cet effet. À ce jour, la Norvège, le Liechtenstein et l’Islande, en raison de leur appartenance à l’EEE (Espace Economique Européen) et l’Argentine, le Canada, la Suisse, Guernesey et l’Ile de Man sont les seuls pays à figurer sur cette liste ; avec également les États-Unis pour les entreprises qui ont adopté la sphère de sécurité (Safe Harbor) et les transporteurs aériens qui transfèrent les données des dossiers passagers (PNR) au ministère américain de la sécurité intérieure (DHS).

La CNIL peut néanmoins autoriser un transfert vers un pays tiers ne disposant pas d’un niveau de protection adéquate lorsque «*le traitement garantit un niveau de protection suffisant de la vie privée, ainsi que des libertés et droits fondamentaux des personnes, notamment en raison des clauses contractuelles ou règles internes dont il fait l’objet*»¹⁸. Mais également par quelques exceptions¹⁹ dont la plus importante est si «*la personne à laquelle se rapportent les données a consenti expressément à leur transfert*».

Lorsque les données sont susceptibles d’être transférées, les personnes concernées doivent être informées de l’existence de ce transfert²⁰ par des informations suffisamment détaillées et indiquer notamment la finalité du transfert, le pays destinataire des données et, le cas échéant, de la nature de la protection assurée aux données transférées (contrat, règles internes, Safe Harbor, etc.).

Les transferts de données ne répondant pas aux conditions énoncées ci-dessus seront illégaux et pourront, à ce titre, engager la responsabilité pénale du responsable du traitement.

SANCTIONS PÉNALES APPLICABLES AU NON-RESPECT DE LA LOI INFORMATIQUE ET LIBERTÉS

De nombreuses dispositions du Code pénal sont susceptibles de sanctionner les manquements aux règles qui régissent le traitement de données à caractère personnel. Toutes ces dispositions prévoient une peine maximale de 300 000 euros d’amende (1 500 000 euros lorsque le contrevenant est une personne morale) et 5 ans d’emprisonnement, comme détaillé en annexe 3.

La CNIL dispose elle-même de prérogatives fortes en la matière qui lui permettent

¹⁸ Article 69, alinéa 8 de la loi du 6 janvier 1978.

¹⁹ Article 69, alinéas 1 à 7 de la loi du 6 janvier 1978.

²⁰ Article 32 I 7° de la loi du 6 janvier 1978 sauf exceptions prévues à l’article 32-III de la même loi.

de prononcer des amendes d'un montant de 150 000 euros (300 000 euros en cas de réitération) dans la limite de 5 % du chiffre d'affaires²¹.

Ces deux sanctions peuvent bien évidemment être cumulées, ce qui augmente d'autant l'importance que l'on doit accorder au respect des obligations encadrant le traitement de données personnelles.

b. L'atteinte au droit d'auteur

DÉFINITION DU DROIT D'AUTEUR

Les œuvres de l'esprit sont protégées par le droit d'auteur, régi par les lois du 11 mars 1957²² et du 3 juillet 1985²³, codifiées dans le Code de la propriété intellectuelle.

Le droit d'auteur est le droit reconnu par la loi et accordé à un auteur, un compositeur, un éditeur ou un distributeur pour l'exclusivité de la publication, de la production, de la vente ou de la distribution d'une oeuvre littéraire, musicale ou artistique.

Il convient de rappeler que le titulaire des droits possède un monopole sur son œuvre (pour une durée de 70 ans après la mort de l'auteur) assorti de certaines exceptions.

COMMENT OBTENIR CETTE PROTECTION ?

Pour bénéficier de la protection accordée par le droit d'auteur, l'œuvre doit refléter l'expression originale d'une pensée, d'une idée ou d'un sentiment, c'est-à-dire qu'elle doit être marquée par l'empreinte de la personnalité de l'auteur.

Le titulaire des droits pourra alors faire interdire tout acte de présentation, de reproduction, de traduction, de modification, etc²⁴. Les prérogatives relevant du droit moral n'appartiennent qu'à l'auteur et ne sont pas cessibles à des tiers même si le contrat le prévoit (paternité, respect, divulgation, retrait et repentir).

²¹ La CNIL a par exemple condamné le Crédit lyonnais à payer 45 000 euros d'amende le 28 juin 2006, pour enregistrement abusif de plusieurs de ses clients dans le fichier des incidents de paiement de la Banque de France (CNIL, délibération n° 2006-174 du 28 juin 2006).

²² Loi n°57-298 du 11 mars 1957 sur la propriété littéraire et artistique, JORF du 14 mars 1957, page 2723.

²³ Loi n°85-704 du 12 juillet 1985 relative à la maîtrise d'ouvrage publique et à ses rapports avec la maîtrise d'œuvre privée, JORF du 13 juillet 1985, page 7914.

²⁴ Le droit d'auteur sur un logiciel est détaillé à l'article L. 122-6 du Code de la propriété intellectuelle.

Dans le domaine particulier des logiciels, en France comme en Europe et dans tous les États signataires de la Convention de Munich (applicable dans 38 États au 8 juin 2008) sur le brevet européen, le logiciel est protégé par le seul droit d'auteur et non par le droit des brevets ²⁵.

Bien que l'exclusion des programmes d'ordinateurs des inventions brevetables fasse l'objet de remises en cause régulières en France et en Europe, le sujet ne déchaîne pas les passions comme c'est le cas aux États-Unis où la brevabilité des logiciels est très décriée. En effet, l'office des brevets états-uniens (US Patent and Trademark Office) est confronté à une hostilité croissante sur la brevabilité des logiciels et d'autres concepts qui n'ont pas besoin d'une application concrète pour être protégés²⁶.

En France, la loi du 3 juillet 1985²⁷ a levé toute ambiguïté sur le sujet puisqu'elle ajouté le logiciel aux œuvres de l'esprit susceptibles d'être protégées par le droit d'auteur. Le logiciel doit pour cela remplir la condition d'originalité que nous avons mentionné précédemment.

LES ÉLÉMENTS PROTÉGÉS

La protection du logiciel concerne la série d'instructions rédigées par le programmeur en code source ou en code objet. En revanche, sont exclues de toute protection les fonctionnalités mêmes du logiciel qui sont procurées par ce code, comme l'ont rappelé les jurisprudences en la matière²⁸. Il n'est donc pas possible protéger une idée ou une fonctionnalité de son logiciel, mais seulement le moyen d'y parvenir (le code source)²⁹.

De plus, outre le code source du logiciel, le « *matériel préparatoire* »³⁰ est également

²⁵ Les logiciels sont exclus des inventions brevetables par l'article 52-2 de la Convention sur le Brevet Européen entrée en vigueur le 7 octobre 1977.

²⁶ Patent Office finds voice, calls for software patent sanity.

²⁷ Loi n°85-660 du 3 juillet 1985 relative aux droits d'auteur et aux droits des artistes-interprètes, des producteurs de phonogrammes et de vidéogrammes et des entreprises de communication audiovisuelle, JORF du 4 juillet 1985, page 7495.

²⁸ Cour de cassation, chambre civile 1, 13 décembre 2005, Mme Cuadros et autre c/ Microsoft France et autre.

²⁹ Des « *similitudes conceptuelles* » entre deux logiciels ne suffisent donc pas à caractériser la contrefaçon. Décision du Tribunal de grande instance de Paris, 3^e chambre, le 19 mars 1993.

³⁰ Article L. 112-2, 13° du Code de la propriété intellectuelle.

protégé. Il comprend par exemple le manuel d'utilisation qui peut constituer une œuvre littéraire.

La protection accordée aux logiciels est donc limitée. Cela est d'autant plus vrai qu'une série d'exceptions est également prévue pour les utilisateurs licites du logiciel³¹. Celles-ci concernent le droit d'utilisation, les possibilités d'étudier et de corriger le logiciel, ainsi que d'en faire des copies et de le décompiler.

Ce dernier droit est encadré et n'autorise pas toute utilisation des informations recueillies, en imposant notamment qu'elles ne soient pas, sauf nécessité, communiquées à des tiers et utilisées pour mettre au point un autre logiciel.

Enfin, bien que la protection d'une œuvre originale par le droit d'auteur naisse du seul fait de la création et ne nécessite l'accomplissement d'aucune formalité, il peut être judicieux d'effectuer un dépôt privé de l'œuvre chez un huissier, un notaire ou auprès d'organismes d'auteurs. Le dépôt offre en effet l'avantage d'apporter une date certaine à la création, ce qui permettra de faire échouer facilement une revendication effectuée par un tiers de mauvaise foi.

SANCTIONS PÉNALES APPLICABLES AU NON-RESPECT DU DROIT D'AUTEUR

La contrefaçon est un délit (qui se prescrit après 3 ans), créé pour défendre les droits du titulaire. Seul le titulaire des droits sur le logiciel dispose donc de l'action en contrefaçon pour faire condamner le contrefacteur devant les juridictions civiles et pénales.

L'article L. 335-3 du Code de la Propriété Intellectuelle définit le délit de contrefaçon comme la violation des droits de l'auteur d'un logiciel prévus à l'article L. 122-6 du Code de la Propriété Intellectuelle. Il s'agit de toute fixation, quel que soit le support, et sans que soit requise une imitation servile³² (qui n'est que la forme la plus radicale de la contrefaçon).

Le délit de contrefaçon est également constitué d'après l'article L. 335-3 du Code de la Propriété Intellectuelle, par le fait d'utiliser un logiciel sans en avoir le droit (sans avoir

³¹ Article L. 122-6-1 du Code de la propriété intellectuelle.

³² Œuvre dépourvue d'originalité, c'est à dire une simple copie.

de licence par exemple).

Dans ce cas, l'État n'échappe pas au droit commun. S'il reproduit et utilise sans autorisation des programmes, il peut être condamné pour contrefaçon.³³

Les sanctions pénales de la contrefaçon sont 2 ans d'emprisonnement et 150 000 euros d'amende³⁴. Une peine complémentaire telle que la confiscation des objets contrefaisants peut s'appliquer; de même que le produit de ces confiscations sera remis à la victime ou à ses ayants droit pour réparation³⁵.

Les sanctions civiles consisteront quant à elles en la réparation du préjudice subi par l'auteur du logiciel, avec le versement de dommages et intérêts.

Il ne fait donc maintenant nul doute que les chefs d'entreprises et les directeurs des systèmes d'informations sont soumis à des risques importants liés aux systèmes d'informations; aussi bien pour des actes qu'ils ont commis, que pour une simple omission, négligence ou imprudence de leur part et du fait des agissements des salariés.

Après avoir abordé ces principaux risques, nous allons maintenant consacrer la deuxième partie de notre mémoire sur les moyens dont disposent le DSI et le chef d'entreprise pour les réduire au maximum et éviter que leur responsabilité soit engagée.

³³ Tribunal de grande instance de Paris, 3^e chambre, le 13 juillet 1989.

³⁴ Article 335-2 du Code de la propriété intellectuelle.

³⁵ Article 335-7 du Code de la propriété intellectuelle.

II. Les outils de prévention à la portée du directeur des systèmes d'informations : une solution pragmatique quant aux risques juridiques liés aux systèmes d'informations

A) La mise en place de moyens de prévention adaptés

À l'égard des menaces croissantes liées aux systèmes d'informations, les entreprises doivent s'assurer de la sécurité des systèmes, mais toutes ne disposent pas aujourd'hui des moyens d'y parvenir et de maîtriser l'ensemble des paramètres qui contribuent à leur sécurité. La diversité des équipements, des configurations et l'évolution permanente des technologies complexifient la sécurité des systèmes d'information. De plus, les moyens dédiés à ces tâches sont souvent insuffisants et ne permettent pas toujours de garantir une sécurité maximale et un suivi rigoureux de la politique de sécurité dans l'organisation.

Le directeur des systèmes d'informations peut être aidé dans ces missions par un Responsable de la Sécurité des Systèmes d'Informations (RSSI) qui "incarne" la sécurité de l'information au sein de l'entreprise et ses composantes.

Malheureusement, toutes les entreprises n'ont pas en interne la spécialisation nécessaire à une gestion appropriée des risques ; dès lors, l'entreprise s'expose au fait de ne plus disposer de moyens d'anticiper, de détecter, ou de réagir à l'encontre d'un risque. Le rôle du MSSP (Managed Security Services Provider) consiste alors à décharger l'entreprise de cette contrainte en assumant la complexité inhérente à la gestion du risque sécurité du système d'information, tout en apportant des garanties de conformité à la politique de sécurité préalablement définie comme nous allons le voir après avoir abordé le rôle des RSSI plus en détail.

1) La nécessaire intervention d'un professionnel

La sécurité des systèmes d'information s'entend par la sécurité physique des matériels et des systèmes (ordinateurs, réseaux, etc.), mais aussi par une approche proactive et réactive en termes stratégiques et organisationnels, ce qui nécessite l'aide d'un professionnel spécialisé en la matière.

a. Les Responsables de la Sécurité des Systèmes d'Informations

DÉFINITION DU RSSI

Si le poste de Responsable de la Sécurité des Systèmes d'Information (RSSI) était initialement vu comme une fonction technique, la raison en incombait à la nature des risques pesant sur les systèmes d'information.

Tant que l'architecture des SI était basée sur des architectures majoritairement propriétaires et des applications maisons, on attendait du RSSI qu'il connaisse les mécanismes de sécurité à mettre en œuvre, qu'il en vérifie régulièrement la bonne application (par exemple en effectuant des audits MEHARI³⁶ chaque année) et aussi qu'il traite des problématiques de continuité d'activité.

La nature des risques a fondamentalement changé, liée à la complexité accrue des systèmes d'information, à l'ouverture aux réseaux, au nombre de domaines complémentaires qu'on lui demande de traiter (aspects juridiques, communication interne et externe). Le RSSI ne peut plus être un technicien, il lui faut acquérir des compétences organisationnelles et d'architecte de système d'informations, de connaissance des métiers et de conduite du changement. La fonction du RSSI aujourd'hui est d'assurer la protection et la valorisation du patrimoine informationnel de l'entreprise dans son ensemble. Pour y parvenir, plusieurs missions peuvent lui être confiées.

LES MISSIONS DU RSSI

- **Le conseil.**
Le RSSI sera amené à formuler des conseils et des recommandations pour tout ce qui concerne les risques dans le domaine de la sécurité des systèmes d'information à l'intérieur de l'entreprise ou du groupe.
- **La conception de la sécurité des systèmes d'information** est une autre mission primordiale du RSSI.
Le RSSI doit y parvenir en termes organisationnels, procéduraux, stratégiques, technologiques, mais aussi juridiques.
Il lui incombe également d'établir tous les documents qui sont nécessaires pour garantir la sécurité au sein de l'entreprise (politique de sécurité, guides, chartes, etc.). Il doit, de plus, disposer d'une équipe aussi bien dans la société mère que dans les filiales pour gérer la maîtrise d'ouvrage de la sécurité et travailler en collaboration avec les personnes adéquates au sein de la direc-

³⁶ Méthode Harmonisée d'Analyse de Risques : a été mise au point par le CLUSIF - www.clusif.asso.fr/fr/production/mehari/

tion des systèmes d'information et des métiers (« *correspondants* » sécurité logique, plans de secours métiers, continuité et reprise, données à caractère personnel, etc.

- **Le contrôle et la surveillance des systèmes d'information.**

Le RSSI veille à la détection des risques et à l'efficacité des plans d'action pour les réduire et minimiser leurs impacts au maximum.

Il doit aussi mettre en œuvre les modalités d'utilisation des systèmes d'information, les outils de contrôle adaptés et s'assurer de leur efficacité au regard des problématiques de sécurité, mais dans les limites autorisées du contrôle des salariés du point de vue légal et jurisprudentiel.

Le rôle du RSSI s'inscrit par ailleurs dans la prévention des incidents (procédures de détection des risques, alertes pénales, indisponibilité, substitution, mise en route des plans de continuité et de secours des SI, etc.). Il doit le cas échéant, alerter les responsables techniques, superviser la mise en œuvre des procédures et rendre compte de leur efficacité. Une véritable approche de « *risk management* » doit en découler.

- **La conformité (« *compliance* »).**

Les RSSI ont enfin la mission de s'assurer que les axes et procédures en matière de sécurité des systèmes d'information sont en adéquation avec toutes les obligations légales, réglementaires et normatives applicables en la matière, mais que c'est également le cas pour les « bonnes pratiques » et règles déontologiques dans de nombreux domaines.

Le RSSI doit aussi agir dans le respect de la législation applicable directement ou indirectement à la sécurité informatique. L'évolution des règles juridiques relatives aux secteurs d'activité de l'entreprise devra donc être connue et surtout anticipée par le RSSI dans sa mission de veille. Une évolution du cadre juridique peut en effet imposer des modifications organisationnelles, la mise en place de nouvelles procédures ou des changements techniques dont l'anticipation permettra d'éviter toute désorganisation liée à l'urgence et de prendre les bonnes décisions puis de les mettre en œuvre progressivement.

- **La veille stratégique.**

La veille permet aux RSSI d'anticiper les nouveaux risques pour les entreprises, de mieux les prévenir et de les éviter si possible. Elle permet aussi de se mettre à jour sur de nouvelles opportunités économiques, stratégiques et technologiques. La veille doit donc être large et porter sur les projets de textes (directives européennes, lois, décrets, etc.), règles, jurisprudences ou normes ayant une incidence sur le périmètre de la sécurité des systèmes d'information de l'entreprise, pour le protéger à la hauteur de l'enjeu économique majeur³⁷ qu'il constitue.

Dans le cadre de cette veille, la dimension juridique ne doit pas être négligée, bien au contraire et une démarche d'intelligence juridique doit être mise en place, avec les bénéfices que nous verrons plus précisément en deuxième partie. Toutefois, nous pouvons déjà affirmer que l'installation d'un tableau de bord de l'intelligence juridique et stratégique du système d'information permettra un pilotage adapté aux besoins de l'entité et de faire face

³⁷ Rapport d'information sur la stratégie de sécurité économique nationale, N°1664, enregistré le 9 juin 2004 à l'Assemblée nationale et présenté par Monsieur Bernard Carayon, Député.

aux menaces futures, de même que la veille se transformera en outil stratégique majeur pour les entreprises sachant l'exploiter.

GESTIONNAIRE DU RISQUE ET R S S I : UNE COMPLÉMENTARITÉ BÉNÉFIQUE

Le RSSI et le gestionnaire du risque (Risk Manager) n'entretiennent pas suffisamment de contacts alors que les entreprises, soumises à des exigences fortes, doivent disposer d'une cartographie globale des risques.

Le gestionnaire du risque (RM) a habituellement pour tâche de gérer la politique et la police d'assurance de l'entreprise. Ses missions sont notamment de concevoir les méthodes et outils de gestion de risques, ainsi que de conseiller les métiers sur les mesures de prévention, protection, détection, réaction d'un risque. Il doit pour cela être proche à la fois de la direction générale et des directions opérationnelles.

De son côté, comme nous l'avons vu, le RSSI doit garantir la sécurité logique et physique du système d'information.

Les RSSI et RM ont donc bien tous deux comme préoccupation la gestion des risques liés au système d'information. Ils se rejoignent ainsi sur l'exigence de la disponibilité, l'intégrité des données, leur confidentialité et la traçabilité des opérations. Quatre piliers dont l'altération peut faire courir un risque à l'entreprise, à ses clients et partenaires.

Ainsi, pour surmonter la complexité de la gestion des risques propres aux systèmes d'informations, RM et RSSI doivent contribuer de manière complémentaire à la définition des méthodes d'identification et d'évaluation des risques en élaborant un référentiel commun, ainsi qu'à la mise en œuvre de solutions de maîtrise de risques.

LE RATTACHEMENT DU R S S I

L'efficacité de la sécurité des systèmes d'information est conditionnée par le positionnement interne du RSSI. Son périmètre d'intervention est essentiel et nécessite une position hiérarchique élevée et transversale qui influera directement sur les pouvoirs et responsabilités de celui-ci. Ainsi, l'on constate majoritairement que les RSSI sont soit attachés à la Direction des Systèmes d'Information, soit à la Direction générale.

Mais des rattachements forts différents du RSSI sont également possibles (de la DSI, à la Direction générale, en passant par la Direction financière). Ces différences se comprennent aisément par l'évolution des missions de RSSI qui sont passées « *de l'homme-*

orchestre de la sécurité informatique vers l'homme-orchestre de la sécurité du patrimoine informationnel » et par les préoccupations d'origines des entreprises (par exemple la finance pour les banques) qui ont fait évoluer ce poste vers d'autres domaines.

Le rattachement du RSSI à la Direction générale est aussi éminemment lié à la maturité de l'entreprise face à la sécurité de l'information. Plus l'entreprise aura une maturité élevée dans ce domaine, plus le RSSI sera proche de la Direction générale et non pas de la DSI ou du cœur de métier de l'entreprise.

Cependant, pour simplifier, l'on peut dire qu'en période de démarrage de la sécurité de l'information, il est préférable que le RSSI soit rattaché à la DSI car il doit participer au développement d'une conscience sécurité dans la DSI et elle ne doit pas se faire contre elle ou provoquer des conflits (par exemple si la DSI était impliquée dans le domaine et s'en trouve dépossédée). Ensuite, sa mission devra évoluer vers la gestion du risque (Risk Management), plus liée à l'organisation et à la communication, où un rattachement proche des utilisateurs et des métiers est nécessaire.

b. Les MSSP (Managed Security Services Provider)

Comme nous l'avons écrit précédemment, toutes les entreprises ne disposent pas d'un poste de RSSI, pour des raisons budgétaires évidentes, mais également par difficulté à le positionner entre "*risk manager*" et "*technicien*". Dès lors, les entreprises s'exposent à de graves difficultés et au fait de ne pas disposer de moyens d'anticiper, de détecter, ou de réagir à l'encontre d'un risque. À ce moment-là, il peut être intéressant de faire appel à une société spécialisée pour bénéficier d'un MSSP (Managed Security Services Provider) qui déchargera l'entreprise de cette contrainte en assumant la complexité de la gestion du risque sécurité du système d'information, tout en apportant d'autres garanties.

LE RÔLE DU MSSP

Face aux difficultés, aux coûts de mise en œuvre et de maintien de la sécurité des systèmes d'informations, les entreprises confient depuis plusieurs années tout ou partie de ces tâches à des sociétés spécialisées. Le rôle du MSSP consiste en effet à décharger l'entreprise de la gestion du risque sécurité du système d'information et de s'assurer de

son application auprès de tous. Sur la base des études du cabinet de conseil dans le marketing et les services IDC³⁸, nous reprenons les trois segments de services de sécurité confiés aux MSSP :

1. Les services “ *basiques* ” : gestion de pare-feux, protection contre les intrusions, sécurisation des accès distants et protection contre les virus.
2. Les services “ *avancés* ” : mise à jour des logiciels de sécurité, audit externe de vulnérabilité, mise à jour des systèmes d’exploitation et des applications (hors sécurité) et gestion des identités.
3. Les services “ *sur-mesure* ” : service de veille sécuritaire, contrôle et gestion de la conformité réglementaire et contrôle et gestion de la conformité métier.

Le premier segment est historique et correspond aux services les plus aisés à confier à un tiers. Une part de ces services est souvent couplée à une offre plus large de connexion via un opérateur.

Les services avancés demandent quant à eux une intimité plus forte avec le système d’information de l’organisation. Ils sont en cela plus représentatifs de la capacité du MSSP à endosser une part de la complexité de la gestion d’équipements de sécurité. Si l’audit de vulnérabilité a un sens immédiat à être réalisé à partir de l’extérieur, les opérations de mise à jour de logiciels de sécurité, de systèmes d’exploitation ou d’applications entraînent des contraintes (tests de non-régression, capacités de retour arrière) sur lesquelles le MSSP devra s’engager, permettant ainsi à l’organisation de s’affranchir de tâches complexes, sans valeur ajoutée palpable.

Enfin, les services sur-mesure présentent la réelle nouveauté des MSSP dans la capacité à déléguer des rôles qui relevaient jusqu’à récemment du pré carré de l’organisation. Au-delà de la délégation de tâches de sécurité, nous y trouvons un véritable accompagnement dans la réalisation du métier et un transfert de responsabilités. Le service de veille sécuritaire implique un engagement fort du prestataire dans la compréhension du métier et des enjeux de l’organisation.

L’ÉVOLUTION DE L’OFFRE MSSP

Même si comme nous venons de le voir, le troisième segment des offres MSSP reste émergent, il constitue néanmoins une avancée incontestable dans la capacité des organi-

³⁸ « Le marché français des services d’externalisation de la gestion de la sécurité informatique », Eric Dommage, Karim Bahloul, International Data Conseil, juin 2006.

sations à déléguer tout ou partie de la gestion de leur sécurité, y compris sur des segments critiques de leur métier.

Cette délégation a plusieurs causes. La première, mentionnée en préambule, est la conséquence directe du manque de moyens disponibles. Le coût des spécialistes en sécurité, associé aux difficultés de recrutement de ces profils, conduit à externaliser ces tâches. La deuxième est la rationalisation des investissements de l'organisation, qui se concentre sur métier. C'est probablement cette seconde composante qui conduira à l'évolution de l'offre, en externalisant la sécurité plus largement qu'elle ne l'est aujourd'hui, même au niveau des services «*avancés*».

Au même titre que de nombreuses prestations autour du système d'information, la sécurité peut se mesurer, faire l'objet de contrôles externes et d'engagements de résultats. Elle peut donc être confiée à des tiers qui seront soumis à des contrôles, ce qui explique son taux d'adoption croissant malgré le rôle critique qu'elle revêt.

Ainsi, au-delà de la gestion et de la supervision des équipements de sécurité, il est probable que des services de fourniture de flux “propres” seront à même de séduire les structures n'ayant pas les moyens ou le souhait de procéder à la mise en place et à la gestion des équipements permettant de filtrer les flux de type trafic web, messagerie, transfert de données, etc. De même, des services de gestion d'archivages, garants de l'intégrité et de la traçabilité des documents, permettent d'obtenir un moyen de preuve légal, tout en confiant à un tiers la responsabilité du bon fonctionnement et de l'adéquation des moyens de construction et de restitution de la preuve avec les engagements de l'organisation.

Le champ des possibilités est large pour les services de sécurité à valeur ajoutée pouvant être confiés à des tiers. En permettant à l'organisation de se concentrer sur son métier, les MSSP contribuent à améliorer la gestion du risque. La définition des responsabilités qui leur sont confiées, associée à une délégation qui va au-delà de tâches purement techniques, oblige l'organisation à mieux identifier, mesurer et suivre ses risques, tout en exigeant des résultats sur les moyens mis en œuvre pour leur prévention et leur gestion. En transférant la complexité de la gestion de tâches de sécurité récurrentes, l'organisation peut également se concentrer sur les indicateurs qui lui permettent de gagner en efficacité et en compétitivité avec l'assurance d'une sécurité opérationnelle garantie.

La gestion des risques liés aux systèmes d'informations peut donc être confiée à des professionnels, mais le DSI peut lui aussi prendre part directement à cette activité, surtout dans les structures de taille moyenne; d'une part, en veillant à la sécurité physique et logique du réseau et du système d'information, comme il le fait dans bien des cas, et d'autre part, en limitant l'impact qu'ont les utilisateurs et les usages sur le système d'information. Cette prévention en interne passera par la rédaction de chartes et la sensibilisation des employés.

2) La rédaction de chartes et la sensibilisation des employés et de l'entreprise

Les usages abusifs des ressources informatiques et les comportements malveillants internes doivent amener directions générale et informatique à repenser leur politique d'information et de dissuasion.

L'usage de l'informatique et de l'internet à la maison est maintenant largement banalisé³⁹. Le comportement des utilisateurs en entreprise est donc de plus en plus influencé par la pratique privée, et les frontières entre les deux mondes deviennent plus floues comme le montre⁴⁰ l'enquête du CLUSIF (CLU**U** de la Sécurité Informatique Français) dans son rapport 2008 : un tiers des internautes utilisent l'ordinateur familial aussi à des fins professionnelles, ce qui pose quelques interrogations sur la protection des données de l'entreprise.

La protection seule du système d'information sera toujours insuffisante si les utilisateurs ne sont pas impliqués et sensibilisés à cette pratique. Dans ce cas, l'existence d'une charte informatique et internet, couplée avec des actions de sensibilisation (publication d'articles sur l'intranet et le journal interne, formations périodiques, sensibilisation des nouveaux arrivants, etc.) peut faire face à l'évolution des comportements et responsabiliser les salariés pour des actes qui sont susceptibles de conduire à la mise en cause de la responsabilité civile et pénale de l'entreprise et de son dirigeant.

³⁹ Selon l'ARCEP (Autorité de Régulation des Communications Électroniques et des Postes), la France comptait 16,5 millions d'abonnés à l'internet au 30 septembre 2007 et plus de 31 millions de personnes se connectent au moins une fois par mois d'après Médiamétrie.

⁴⁰ Rapport "Menaces Informatiques et Pratiques de Sécurité en France" présenté le 19 juin 2008.

a. La charte informatique de l'entreprise : quels enjeux juridiques ?

La récente condamnation de Lucent Technologies par la cour d'appel d'Aix en Provence le 13 mars 2006, du fait des agissements de l'un de ses salariés qui avait créé un site internet dénigrant la société Escota, est la parfaite illustration de l'importance des chartes informatiques des entreprises, trop souvent délaissées.

En effet, la responsabilité de Lucent Technologies a été engagée en sa qualité de commettant, à raison de l'autorisation donnée aux salariés d'accéder à l'internet en dehors de leurs heures de travail et d'utiliser les équipements informatiques mis à leur disposition pour consulter d'autres sites que ceux présentant un intérêt en relation directe avec leur activité professionnelle.

CONDITIONS DE VALIDITÉ

La charte informatique a vocation à établir les conditions d'utilisation de l'outil informatique au sein de l'entreprise. Les conditions dans lesquelles elle s'applique ne sont pas spécialement prévues dans le Code du travail mais trois options sont envisageables pour lui donner force obligatoire (et la rendre opposable) auprès des salariés.

1. **Demander l'accord aux employés.**

La charte s'imposera à tous dès lors qu'ils auront signé le document. Ceux qui refuseront de valider le document ne pourront se voir imposer les obligations contenues dans la charte.

2. **Annexer la charte au contrat de travail.**

Cette possibilité d'insertion est envisagée dans le Code du travail mais elle n'est pas spécifique aux règles applicables en matière informatique au sein de l'entreprise.

Elle peut être source de conflit ou tension avec les salariés parce que susceptible d'être imposée de manière quelque peu autoritaire. C'est pourquoi la voie du règlement intérieur est la plus adéquate.

3. **Annexer la charte au règlement intérieur.**

D'après l'article L. 1311-2 du Code du travail (ancien L. 122-33), l'établissement d'un règlement intérieur est obligatoire dans les entreprises où sont employés au moins vingt salariés. Il est tout à fait possible et même recommandé de procéder par ce biais pour rendre la charte informatique opposable à l'ensemble des salariés⁴¹.

En effet, la procédure oblige l'employeur à solliciter l'avis du comité

⁴¹ Cette mesure est également conseillée par le Forum des Droits de l'Internet dans son rapport du 17 septembre 2002 : «*Les définitions des règles d'utilisation d'Internet doivent passer par une annexe au règlement intérieur*».

d'entreprise ou des délégués du personnel. Il en ressort donc une dimension de concertation et de compromis démontrant la bonne foi de l'employeur et la preuve de sa bonne volonté.

Enfin, dans tous les cas, le chef d'entreprise devra assurer la publicité de la charte informatique auprès des salariés. À des fins d'informations mais aussi pour assurer la complète force obligatoire du document, la charte devra être affichée dans les locaux ou communiquée à chacun préalablement à son entrée en vigueur.

En effet, le non-respect des dispositions prévues au sein de la charte informatique ne pourra être sanctionné disciplinairement que dans cette hypothèse. L'adjonction d'une annexe au règlement intérieur nécessite le respect des dispositions qui concernent toute modification du règlement intérieur, et notamment le dépôt au Greffe, la publicité, la concertation avec les institutions représentatives du personnel, etc.

De valeur informative, la charte informatique a également une valeur normative. En conséquence, un syndicat non signataire de la charte en bénéficie également, comme l'a rappelé le TGI (Tribunal de Grande Instance) de Nanterre⁴², et doit la respecter. La même décision reconnaît que la charte peut prohiber certaines pratiques et l'employeur devra apporter une attention toute particulière à son contenu.

LE CONTENU DE LA CHARTE

La charte a pour objectif d'établir un cadre clair et transparent des règles d'utilisation des outils informatique et de l'internet au sein d'une entreprise. Elle applique la présomption selon laquelle les outils mis à disposition par l'employeur sont à vocation professionnelle, comme les connexions à l'internet⁴³, mais rend possible une utilisation personnelle à condition qu'elle soit raisonnable et encadrée.

Ce point crucial est malheureusement trop souvent négligé et ne limite pas suffisamment les pratiques autorisées alors que les juges font de plus en plus une interprétation stricte de la charte : tous les comportements qui ne sont pas interdits sont supposés être autorisés⁴⁴. Il faut donc lister exhaustivement tous les usages et comportements qui

⁴² Tribunal de grande instance de Nanterre, 1^{re} chambre section B, 31 mai 2002, CGT c/ RENAULT.

⁴³ Cour de cassation, chambre sociale, 9 juillet 2008, Franck L. c/ Entreprise Martin.

⁴⁴ Une faute du salarié liée à l'utilisation inadaptée des ressources informatiques ne pourra être retenue que si l'employeur lui avait rappelé les limites d'utilisation de ce matériel (Cour d'appel de Paris, 22^e chambre section C, 16 novembre 2001, M. Laurent B. c/ S.A. Expeditors International France SAS).

doivent être interdits.

Pour ce faire, une clause doit autoriser une utilisation personnelle, ponctuelle et raisonnable des sites internet dont le contenu n'est pas contraire à l'ordre public et aux bonnes mœurs et qui ne met pas en cause l'intérêt ou l'image de l'entreprise. Consulter des sites pornographiques ou pédophiles, échanger de la musique, des films ou tout autre programme contrevenants au droit d'auteur et à la propriété intellectuelle, développer un site internet sans autorisation, dialoguer sur des chats et forums à des fins non professionnelles, porter atteinte à une société ou ses produits, etc. doivent être explicitement listés comme interdits.

La charte prévoira également que le contrôle de l'utilisation personnelle pourra être exercé par l'employeur, en termes notamment de volumes. Ce contrôle, pour être légal, devra être loyal, transparent, proportionné et porté préalablement à la connaissance du salarié⁴⁵.

Le salarié pourra également se voir imposer par la charte plusieurs obligations. Notamment le fait de distinguer ses documents personnels de ses documents professionnels. Cette distinction devra aussi bien se faire sur ses fichiers que sur ses courriers électroniques. Tout document qui ne comporterait pas cette distinction personnelle sera alors considéré comme professionnel et librement accessible par l'employeur⁴⁶.

Les fichiers à caractère personnel sont protégés par le droit au respect de la vie privée du salarié, par conséquent l'employeur ne peut ouvrir les fichiers identifiés comme tels par le salarié qu'en présence de ce dernier ou celui-ci dûment appelé, « *sauf risque ou événement particulier* ». Le salarié doit donc s'engager à ne pas transformer des informations professionnelles en informations personnelles ou en empêcher l'accès à son employeur⁴⁷.

Ainsi, la charte aura parfaitement rempli sa mission quand elle rappellera au salarié la nécessité de respecter l'environnement légal applicable, notamment au regard des droits des tiers et de l'entreprise, telle que la confidentialité.

⁴⁵ Article L. 121-8 du Code du travail.

⁴⁶ Cour de cassation, chambre sociale, 18 octobre 2006, Monsieur J. L. c/ société Techni-Soft.

⁴⁷ Cour de cassation, chambre sociale, 18 octobre 2006, Monsieur J. L. c/ société Techni-Soft.

La charte prévoira enfin que l'accès aux ressources informatiques ne pourra se faire qu'après acceptation des modalités convenues dans la charte, et que le non-respect des dispositions de la charte engagera la responsabilité du salarié.

b. Les chartes informatiques : un frein efficace contre les éventuels abus des salariés ?

Les nouvelles technologies et les nouveaux usages des outils informatiques entraînent de nouveaux abus. Cette problématique est très souvent sous-estimée, voire ignorée et, pourtant, les entreprises subissent les conséquences d'un usage de plus en plus abusif des outils informatiques.

L'exemple de Lucent Technologies qui a été condamné par la cour d'appel d'Aix-en-Provence le 13 mars 2006, du fait des agissements de l'un de ses salariés qui avait créé un site internet sur son lieu de travail dénigrant la société Escota, en est la parfaite illustration : les chartes doivent être mises à jour pour s'adapter à l'environnement mouvant, mondial et externalisé dans lequel les entreprises évoluent !

L'INEFFICACITÉ DES CHARTES EXISTANTES FACE À L'ÉVOLUTION DES COMPORTEMENTS

L'évolution des technologies et des services disponibles sur l'internet donne lieu à une transformation des abus pour lesquels la plupart des chartes existantes se révèlent souvent inadaptées, voire dangereuses comme dans l'affaire "Escota c/ Lucent Technologies".

La mise à jour des chartes existantes doit, en outre, tenir compte du contexte épineux lié à aux dernières décisions jurisprudentielles, des différentes positions de la CNIL et anticiper les nouveaux comportements dans l'entreprise.

Le développement des nouveaux usages et services sur l'internet (blogs, messageries instantanées, communautés Web 2.0) n'est pas étranger à la recrudescence d'affaires ou de dossiers internes qui submergent les directions juridiques, les directions des ressources humaines et les directions informatiques et inquiètent les directions générales, qui n'ont que très récemment pris conscience de cette menace.

Alors que les entreprises craignaient jusqu'ici essentiellement les fraudes et les atta-

ques extérieures, les études les plus récentes⁴⁸ confirment que la principale menace provient de l'intérieur de l'entreprise.

Citons par exemple une étude menée par Olfeo⁴⁹ auprès d'une trentaine d'entreprises françaises. Elle fait apparaître que les Français passent désormais 66 minutes par jour sur le web sur leur lieu de travail dont 75 % est consacré à des tâches purement personnelles, que 25 % des salariés consacrent plus de 1 h 30 par jour à surfer à titre personnel et enfin que 74 % des connexions personnelles se font pendant les heures de travail effectif⁵⁰.

Les entreprises disposent rarement des outils adéquats pour lutter efficacement contre cette menace et s'estiment protégées par la seule mise en œuvre d'une protection technique à la charge de la direction informatique. Or, directions juridiques, directions des ressources humaines et directions informatiques se retrouvent parfois, en dépit des chartes existantes, dans l'impossibilité de sanctionner des comportements abusifs et d'éviter la mise en cause de la responsabilité de l'entreprise et de son dirigeant, comme dans l'affaire Lucent Technologies.

L'inadéquation entre la protection et les risques provient du décalage qu'il y a entre les deux. L'avènement du Web 2.0 et de l'internet participatif a déplacé les risques techniques vers des risques comportementaux. Ce ne sont plus tant les attaques de virus et d'autres logiciels malveillants qui sont redoutées, mais le détournement ou le mésusage des outils légitimes à d'autres fins qu'elles soient intentionnelles ou non.

De plus, les chartes uniformisées des groupes internationaux ont montré de nombreuses limites dans leur application. Elles se sont en effet révélées inadaptées, voire non conformes au droit français. Malheureusement, les prises de conscience interviennent encore trop souvent à l'occasion d'un conflit ou d'un litige qui lui sert de révélateur et l'absence de mesures préventives prive les entreprises d'actions ou de recours efficaces contre ces comportements.

⁴⁸ Par exemple dans le dernier rapport "Menaces Informatiques et Pratiques de Sécurité en France" présenté par le CLUSIF le 19 juin 2008.

⁴⁹ Fournisseur de logiciels et boîtiers de filtrage d'accès à l'internet.

⁵⁰ Le premier alinéa de l'article L. 212-4 introduit la définition «*Est temps de travail effectif le temps pendant lequel le salarié est à la disposition de l'employeur et doit se conformer à ses directives sans pouvoir vaquer librement à des occupations personnelles*».

Le manque de sensibilisation et de formation des salariés avec l'obsolescence des chartes existantes et l'impossibilité d'opposer aux salariés des règles claires et précises sont les points essentiels sur lesquels les entreprises doivent dès à présent travailler. Ces améliorations permettront de garantir leur sécurité, aussi bien technique que juridique.

LA REFONTE LES CHARTES : UNE NÉCESSAIRE ADAPTATION

De plus en plus, les entreprises mettent en place des équipes internes aux compétences plurielles (informatiques et sociales) pour étudier les moyens de lutte efficaces contre les dérives notamment liées à l'usage des sites internet participatifs, des périphériques de stockages amovibles, des accès distants aux systèmes d'information, des téléchargements de fichiers et de logiciels, etc.

Leurs réflexions aboutissent régulièrement à la nécessité de refondre les chartes existantes pour les adapter à l'évolution des comportements tout en intégrant la politique sociale, éthique et la culture de chaque entreprise. Sensibiliser les membres des comités d'entreprise et de la direction sur la nécessité de mieux protéger les intérêts de l'entreprise et des salariés est également primordial. Ceux-ci n'intégreront pleinement leurs responsabilités que s'ils s'identifient à l'entreprise et qu'ils la respectent⁵¹.

Il apparaît clairement que les entreprises doivent dès à présent définir ou redéfinir les règles d'usage des outils informatiques mis à la disposition de leurs salariés pour mettre en œuvre une politique d'information et de dissuasion efficace. Selon une enquête menée par le CLUSIF entre février et mars 2008 auprès de 354 entreprises de plus de 200 salariés, seuls 50 % des entreprises disposent d'une charte sécurité et 35 % d'entre elles ont institué des programmes de sensibilisation à la sécurité de l'information.

Les dimensions informatiques, sociales, de protection des données personnelles et de respect de la vie privée doivent être prises en compte dans les nouvelles chartes, en adéquation avec la réalité des usages dans les entreprises, actuelles et à venir si possible.

La politique de sécurité doit essentiellement s'articuler autour de :

1. la mise en conformité réglementaire et juridique des traitements de données à caractère personnel et de "cybersurveillance" ;

⁵¹ Principes éthiques et pratiques de la responsabilité sociale des entreprises (RSE), Cercle d'Éthique des Affaires, n°28 - Avril 2008.

2. la sécurisation juridique des contrats de travail et plus particulièrement pour les salariés “nomades” ;
3. la mise en place ou la refonte d’une charte d’utilisation des outils informatiques et de l’internet, à intégrer au règlement intérieur ;
4. la sensibilisation des salariés dans le cadre de formations adaptées à des groupes d’interlocuteurs différents et à la culture de l’entreprise.

Pour mettre en œuvre efficacement cette politique de sécurité, il faut réaliser :

1. l’audit des déclarations existantes à la CNIL et leur mise à jour éventuelle ;
2. un consensus entre les instances représentant le personnel et les principales directions concernées (direction des systèmes d’information, direction juridique, direction des ressources humaines) sur les grandes lignes de la future charte ;
3. des arbitrages concernant les conditions et les limites d’utilisation des outils informatiques et internet, avec les sanctions applicables en cas d’infractions ;
4. un choix sur le mode d’opposabilité de la charte aux salariés, en connaissant leurs avantages et inconvénients ;
5. un plan de communication, de sensibilisation et de formation à destination des salariés, des nouveaux arrivants et des personnes extérieures (prestataires, stagiaires, etc.)

Les retours d’expérience de la mise en œuvre de ce type de politique d’information et de dissuasion ont démontré son efficacité et son impact positif sur le comportement des salariés⁵², notamment en termes de responsabilisation, des accès aux informations stratégiques et de leur communication.

Ils confirment également que la plupart des entreprises ne disposaient pas des moyens adéquats pour lutter, prévenir et gérer les risques liés aux usages abusifs et aux comportements malveillants ou irresponsables de leurs salariés.

Les chartes sont un très bon moyen de protection, mais elles ne peuvent pas couvrir tous les risques et un soutien supplémentaire doit lui être apporté. De plus, pour qu’elles soient réellement efficaces, elles doivent être régulièrement actualisées et tenir compte de l’évolution des outils, des usages et du droit.

⁵² Dans le cadre du Cercle de travail Info e-TIC du CIGREF, qui vise à promouvoir un usage éthique et responsable des SI, à faire émerger les bonnes pratiques et à anticiper/influencer les évolutions.

B) *L'ouverture de la direction des systèmes d'informations au droit des nouvelles technologies*

1) *La pratique de la veille juridique et jurisprudentielle*

Les systèmes d'informations, qui occupent une place stratégique dans les entreprises, sont un formidable outil d'échange et sont nécessaires à tous les salariés. Ils sont de ce fait utilisés dans toutes les composantes de la société, pour leurs moindres activités. La variété des données véhiculées par le système d'information et les usages qui en sont faits sont à l'origine du grand nombre de lois qui s'y appliquent, de plus en plus nombreuses et spécialisées.

De plus, le gouvernement tente régulièrement d'encadrer l'utilisation des outils informatiques par l'élaboration ou l'adaptation de lois, tout comme le fait le législateur. Cette situation peut être à l'origine d'insécurité juridiques si l'entreprise n'effectue pas une veille juridique et jurisprudentielle pour vérifier la conformité de son système d'informations aux nouvelles obligations qui peuvent lui être imposées. À ce titre, nous prendrons pour exemple la Loi pour la Confiance dans l'Économie Numérique⁵³ (LCEN) et la jurisprudence de la cour d'appel de Paris du 4 février 2005. Cette loi et cette jurisprudence sont toutes deux importantes puisqu'elles peuvent soumettre n'importe quelle entreprise à de nouvelles obligations sans qu'elles aient changé leurs moindres activités.

a. *Veille juridique*

LA LOI POUR LA CONFIANCE DANS L'ÉCONOMIE NUMÉRIQUE

La loi pour la confiance dans l'économie numérique est la transposition de la directive européenne 2000/31/CE qui visait à promouvoir le commerce électronique au sein de l'Union européenne. Cette loi a été publiée au Journal officiel le 21 juin 2004⁵⁴ et a bouleversé un grand nombre de dispositions.

Parmi ces dispositions, nous n'allons citer que celles relatives à la communication au

⁵³ Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, JORF du 22 juin 2004, page III68.

⁵⁴ JORF n°143 du 22 juin 2004, page III68.

public en ligne, et plus précisément celles relatives aux statuts d'éditeurs et d'hébergeurs qu'elle redéfinit.

Distinction entre le principe du régime d'éditeur et celui de l'hébergeur

Éditeur : Le responsable de la publication du site engage sa responsabilité pleine et entière. Le critère d'engagement de cette responsabilité est la fixation du contenu sur un support préalablement à sa diffusion, ce qui est le cas pour toute diffusion sur l'internet.

Hébergeur : les entreprises ayant le statut d'hébergeur bénéficient d'un régime de responsabilité allégée. Elles ne sont responsables que lorsqu'elles ne retirent pas promptement un contenu après qu'elles aient eu effectivement connaissance de l'activité ou de l'information illicite⁵⁵.

La distinction entre les deux statuts est simple à comprendre. Les éditeurs peuvent, par l'intermédiaire du directeur de la publication, contrôler le contenu qu'ils publient et le supprimer s'il enfreint la loi. Les hébergeurs, eux, ne mettent à disposition qu'une infrastructure technique, ce qui ne leur permet pas d'exercer un contrôle sur le contenu. De plus, si l'hébergeur devait supporter une responsabilité éditoriale, bien peu de contenus seraient en ligne puisqu'ils voudraient tous limiter leur responsabilité au maximum et donc censureraient les contenus au moindre doute. Dans ce cas, la liberté d'expression et la liberté d'entreprendre seraient atteintes.

Il faut également noter que l'hébergeur bénéficie d'un régime dérogatoire qu'il est facile de perdre, comme l'ont prouvé de nombreuses jurisprudences récentes ; l'hébergeur du site devra donc faire attention à la ligne éditoriale qu'il promet. À ce titre, la jurisprudence a reconnu que le fait de choisir les flux d'informations à faire paraître sur son site⁵⁶, mais également de les agréments d'un titre ou de commentaires suffisait à être qualifié d'éditeur ; tout comme le fait de déterminer les sujets sur lesquels les internautes pourront discuter ou d'imposer une mise en forme sur les contenus ou la présentation générale (Dailymotion).

Responsabilités de l'éditeur et de l'hébergeur

Éditeur : La LCEN a remplacé, dans la loi n° 82-652 du 29 juillet 1982⁵⁷, les mots

⁵⁵ Art. 6-I-2 et 6-I-3 de la LCEN.

⁵⁶ TGI de Paris, ordonnance de référé, Monsieur Olivier M. c/ SARL Bloobox Net (Fuzz), 26 mars 2008.

⁵⁷ Loi n°82-652 du 29 juillet 1982 sur la communication audiovisuelle, JORF du 30 juillet 1982, page 2431.

« *communication audiovisuelle* » par les mots « *communication au public par voie électronique* ». En conséquence, la responsabilité en cascade encourue⁵⁸ (article 93-3) par les différentes personnes ayant participé à la diffusion d'un contenu pouvant être réprimée par la loi sur la presse⁵⁹ s'applique désormais aux « *communications au public en ligne* », et donc à l'éditeur du service correspondant, par l'entremise de son directeur de la publication.

Les personnes dont l'activité est d'éditer un service de communication au public en ligne sont également soumises à des obligations supplémentaires par l'article 6-III-1 de la LCEN qui impose de mettre à disposition du public un certain nombre d'informations : les coordonnées, le nom du directeur de la publication⁶⁰ et, le cas échéant celui du responsable de publication et les coordonnées, dont le numéro de téléphone, de l'hébergeur du service. Le non-respect de ces obligations est sanctionné par l'article 6-VI-2 de la LCEN qui prévoit une peine de 75 000 euros d'amende et 1 an d'emprisonnement.

Hébergeur : Même s'il ne peut être tenu responsable, au premier chef, des contenus édités par des tiers, la responsabilité de l'hébergeur peut être engagée si :

1. Il a été prévenu⁶¹ ou avait connaissance effective de l'existence d'un contenu manifestement illicite sur son serveur (contenu pédophile, propos négationnistes, incitation à la discrimination ou à la haine raciale...) et rien n'a été fait pour le supprimer promptement⁶².
2. La personne, dont les contenus sont litigieux, a agi sous l'autorité ou le contrôle de l'hébergeur.
3. Il n'a pas détenu et conservé les données d'identification de la personne ayant contribué à la création du contenu litigieux.

Dans le cas contraire, l'hébergeur ne peut en aucun cas être considéré comme l'auteur principal d'une infraction ni comme coauteur, ou complice.

Cependant, les hébergeurs ont d'autres obligations imposées par les articles 6-I-1 et 6-I-2 de la LCEN et doivent « *détenir et conserver les données de nature à permettre l'identifica-*

⁵⁸ Le directeur de publication sera poursuivi comme auteur principal et l'auteur comme complice. À défaut de fixation préalable, l'auteur et, à défaut d'auteur, le producteur, sera poursuivi comme auteur principal.

⁵⁹ Loi du 29 juillet 1881 sur la liberté de la presse, Bulletin Lois n° 637, page 125.

⁶⁰ L'article 93-3 de la loi du 29 juillet 1982 énonce que tout service de communication au public en ligne est tenu d'avoir un directeur de publication.

⁶¹ Selon la procédure prévue par l'article 6-I-5 de la LCEN.

⁶² D'après le TGI de Paris le 19 octobre 2007, l'action prompte prise par l'hébergeur doit, de surcroît, être durable pour être efficace.

tion de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont ils sont prestataires» en plus de mettre en place «un dispositif facilement accessible et visible permettant à toute personne de porter à la connaissance» de l'hébergeur un contenu illicite et d'«informer promptement les autorités publiques compétentes de toutes activités illicites» comme les crimes contre l'humanité, l'incitation à la haine raciale ou encore la pornographie enfantine qui leur serait signalée.

Pour tout manquement à la conservation des données⁶³ permettant l'identification des auteurs, l'article 6-VI de la LCEN prévoit une sanction d'un an d'emprisonnement et une amende de 75 000 euros. Les personnes morales peuvent de plus être déclarées pénalement responsables de ces infractions dans les conditions prévues à l'article 121-2 du Code pénal. Elles encourent une peine d'amende de 375 000 euros⁶⁴, ainsi que l'interdiction pour une durée de cinq ans au plus, d'exercer directement ou indirectement l'activité, et l'affichage de la décision ou la diffusion de celle-ci soit par la presse écrite, soit par tout moyen de communication au public par voie électronique.

Le fait pour un opérateur ou hébergeur de refuser de répondre aux réquisitions des autorités judiciaires dans le temps de la flagrance ou lors d'une enquête préliminaire⁶⁵ est quant à lui puni d'une amende de 3750 euros.

Les conséquences pénales entre la qualification d'hébergeur ou d'éditeur sont donc très importantes. Les entreprises doivent en prendre conscience pour se soumettre à leurs obligations respectives et limiter au maximum les risques encourus par la fourniture d'un blog, d'un forum de discussion ou d'un espace de travail collaboratif sur l'internet, pour lesquelles elles pourraient être reconnues comme éditrices.

⁶³ Prévues aux articles L.34-1 du CPCE (Code des Postes et Communications Électroniques) et à l'article 6-II de la LCEN.

⁶⁴ Le quintuple de celle applicable aux personnes physiques selon l'article 131-38 du Code pénal.

⁶⁵ Articles 60-2 et 77-1-2 du Code de procédure pénale.

b. Encadrement jurisprudentiel

LA JURISPRUDENCE DE LA COUR D'APPEL DE PARIS DU 4 FÉVRIER 2005

La cour d'appel de Paris a rendu une décision particulièrement importante pour les entreprises qui fournissent des accès à l'internet à leurs salariés, alors qu'elles n'en fournissent pas à des personnes externes⁶⁶. Cette situation, qui concerne la très grande majorité des entreprises, pourrait être retenue pour les qualifier de fournisseurs d'accès à l'internet (FAI) au sens de l'article 43-7 de la loi du 1^{er} août 2000⁶⁷ et, en vertu de cette qualité, être assujettie aux obligations et responsabilités qui pèsent sur cet intermédiaire technique.

Parmi ces responsabilités, est tout particulièrement concernée l'obligation de conserver les données de connexion pendant une durée d'un an maximum selon les cas. Passé ce délai, les données relatives au trafic doivent être effacées ou anonymisées conformément à l'article L.34-1 du Code des Postes et communications électroniques (C.P.C.E.).

Cette obligation, introduite par la loi sur la sécurité quotidienne (LSQ) du 15 novembre 2001, a été élargie avec l'adoption de la loi du 9 juillet 2004 à tous les « *les opérateurs de communications électroniques, et notamment les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne* » et englobe donc maintenant les entreprises.

Régime juridique de l'entreprise qualifiée de fournisseur d'accès

Dans l'affaire de la cour d'appel de Paris, deux agents commerciaux ont décidé de ne plus travailler avec la société qu'ils représentaient en Autriche et aux États-Unis après la perte de confiance dans cette société. Celle-ci a été provoquée par la réception par chacun d'eux d'un mail anonyme selon lequel la société de presse en ligne (World Press Online) allait fermer.

L'enquête a permis de déterminer que les deux courriers électroniques avaient été envoyés par le salarié d'une banque, sur son lieu de travail. La société demanda donc à la banque de lui communiquer les données d'identification de l'expéditeur de ces messages.

⁶⁶ Cour d'appel de Paris, 14^e chambre section B, 4 février 2005, SA BNP Paribas c/ Société World Press Online.

⁶⁷ Loi n° 2000-719 du 1^{er} août 2000, JORF du 2 août 2000, page 11903, modifiant la loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication, JORF du 1^{er} octobre 1986, page 11755.

Ses demandes restant sans réponse, la société assigna la banque en référé pour obtenir ces informations sur le fondement des articles 43-7 et 43-9 de la loi du 30 septembre 1986 et le 12 octobre 2004 et le Tribunal de commerce de Paris ordonna à la banque de « *communiquer l'identité et plus généralement de toute information de nature à permettre l'identification de l'expéditeur du message* ».

En appel, la juridiction confirme l'ordonnance en ces termes: « *la demande de la société ne se heurte à aucune contestation sérieuse alors qu'en sa qualité, non contestée, de prestataire technique au sens de l'article 43-7 de la loi du 1^{er} août 2000, la banque est tenue, en application de l'article 43-9 de ladite loi, d'une part, de détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elle est prestataire et, d'autre part, à communiquer ces données sur réquisition judiciaire* ». Mais, la Cour tempère l'ordonnance en ce que « *la loi du 1^{er} août 2000 ne lui fait pas (à la banque) obligation de traiter les données qu'elle doit conserver et communiquer ni de procéder elle-même à l'identification de l'auteur du message litigieux, et d'autre part, qu'une telle recherche relève de toute évidence d'une mesure d'instruction que le juge des référés ne peut ordonner que sur un autre fondement que ceux sur lesquels il a été saisi dans le cadre de la présente instance* ».

Ainsi, l'objectif qui consistait à identifier l'auteur des messages pour d'éventuelles suites judiciaires n'a pas été atteint. Pour autant, le risque n'est pas définitivement écarté alors comment se protéger au mieux?

Comment faire face à cette situation?

Les fournisseurs d'accès à l'internet sont à présent définis par l'article 6-I-1° de la LCEN comme étant « *les personnes dont l'activité est d'offrir un accès à des services de communications au public en ligne* ». On peut donc, en première analyse, supposer que le Tribunal adoptera une solution identique pour une autre affaire similaire, étant donné que l'entreprise donne à ses salariés un accès vers l'internet.

Pourtant, le caractère « *non contesté* » de la qualité de FAI par la banque devra être médité par les juristes. Envisagé sous cet angle, on peut penser que la qualification retenue et les conséquences en découlant seront susceptibles d'être entendues différemment par d'autres juridictions dans la mesure où les entreprises en général et les banques en particulier (mais aussi pourquoi pas, les collectivités publiques, telles que les administrations ou les collectivités locales), n'ont en aucune façon pour activité de fournir des accès à l'internet ou d'héberger des contenus autres que ceux liés à son activité économique. L'activité d'une entreprise est indiquée dans l'objet de ses statuts et elle se retrouve dans

son code APE (Activité Principale Exercée).

De plus, si la qualification de prestataire technique devait être retenue pour chaque entreprise proposant en interne d'accéder à l'internet, les obligations juridiques seraient considérables et les dommages pour les entreprises françaises seraient difficilement mesurables. Les entreprises devraient conserver toutes les données de connexion relatives aux échanges et être en mesure de les communiquer à tout moment à l'autorité judiciaire. Une telle analyse extensive de la qualification de fournisseur d'accès ne nous semble pas conforme à la réalité juridique, mais il faut savoir que la situation peut se poser et anticiper le problème pour adopter la meilleure stratégie défensive.

2) Anticiper l'application des directives européennes

Les directives européennes relatives à la société de l'information arrivent dans notre pays à flux continu. Il est donc intéressant pour la direction des services informatiques de mettre en place une veille juridique, ou de la mutualiser avec la direction juridique, orientée vers l'Europe pour être en mesure d'anticiper les nouvelles dispositions à venir.

Les directives engagent les États membres qui doivent les transposer dans leur droit national dans un délai imparti par la directive elle-même (18 mois en moyenne). Lors d'une transposition, l'objectif n'est pas de recopier mot à mot le texte européen en langue française, mais de l'intégrer harmonieusement au droit existant. Un degré d'incertitude règne donc sur l'attitude que va adopter le législateur français lors de la transposition, mais celui-ci est minimaliste et ne fait pas courir de grands risques comme nous allons le voir.

a. Les risques mesurés de l'anticipation.

Dans le monde de l'informatique, et plus particulièrement dans les télécommunications, ne pas transposer rapidement une directive peut occasionner un préjudice réel pour l'entreprise. Elle pourrait surseoir à de nouvelles applications ou de nouveaux services faute de régulation juridique adéquate, tandis que des entreprises situées dans des pays ayant transposé en temps utiles bénéficient d'un avantage concurrentiel indéniable. Ce

principe s'applique bien évidemment aussi aux traités et aux jurisprudences de la Cour européenne qui sont très instructives et qu'il faut suivre de près⁶⁸.

La transposition des directives peut se faire a minima par le législateur, ou avec une certaine valeur ajoutée qui va compléter ou moduler les restrictions et obligations prévues. Aussi, le risque est négligeable d'anticiper sur la partie "dure" de la directive qui sera de toute façon et quel que soit le débat, incorporé dans le droit national. Des directives sont également très minimalistes et leur transposition se fera telle quelle dans le droit, sans interprétation.

Il ne faut également pas oublier que si une entreprise se trouvait en difficulté vis-à-vis d'une personne, d'une autre entreprise ou des pouvoirs publics après avoir anticipé une directive, elle pourrait requérir l'aide du juge. Ainsi, une question préjudicielle pourra être posée en ce qui concerne l'interprétation d'une règle de droit européen. Dans ce cas, le juge pourra saisir la Cour de justice des communautés européennes qui dira de quelle façon il faut interpréter la règle en cause et lui laissera le soin de trancher le litige en fonction⁶⁹.

De plus, si le droit national n'est pas conforme aux prescriptions de la directive invoquée, le juge interne écartera la disposition nationale non conforme et la remplacera directement par la disposition de la directive (invocabilité d'exclusion) ; si au contraire aucune mesure de transposition n'a été prise, le juge interne appliquera directement les dispositions de la directive (invocabilité de substitution) dont les dispositions sont « *inconditionnelles et suffisamment précises* »⁷⁰.

Enfin, si les dispositions d'une directive non transposée ou mal transposée sont dépourvues d'effet direct, le juge interne essaiera d'interpréter le droit national conformément au droit communautaire (principe de l'interprétation conforme).

Les risques liés à l'interprétation d'une directive sont donc très limités et les entreprises ne sont bien évidemment pas obligées de les appliquer si elles ne le souhaitent pas.

⁶⁸ Le monopole des jeux et paris en ligne de la Française des Jeux serait par exemple contraire au droit européen selon l'article 49 du Traité de Rome et l'arrêt Gambelli rendu par la CJCE (Cour de Justice des Communautés Européennes) le 6 novembre 2003 (Cour de Justice des Communautés Européennes, 6 novembre 2003, Procédure pénale contre Piergiorgio Gambelli et autres, affaire C-243/01).

⁶⁹ Cour de cassation, chambre commerciale, 20 mai 2008, Google France c/ Louis Vuitton Malletier.

⁷⁰ Cour d'appel de Toulouse, 2^e chambre section 2, 26 Octobre 2000, époux Barthe c/ Société commerciale andorrane Habitat.

Elles peuvent attendre leur transposition dans le droit national pour en tenir compte, mais elles auront eu au moins l'avantage d'avoir une idée de l'avenir qui les attend et auront pu moduler ou revoir leurs plans futurs en fonction.

b. La directive 2002/58/CE relative à la vie privée et aux communications électroniques

Suite à de nombreux incidents survenus au Royaume-Uni et dans de nombreux pays d'Europe, le débat a été rouvert pour savoir s'il fallait une loi comme aux États-Unis qui obligerait les entreprises à informer aussi bien les particuliers que les autorités de protection de données, lorsqu'elles seraient confrontées à une faille de sécurité ou à une perte de données.

SITUATION ACTUELLE

L'environnement de la protection des données personnelles au Royaume-Uni a fortement changé ces douze derniers mois. L'autorité des services financiers (FSA) a condamné une importante société de services bancaires et hypothécaires à une forte amende (d'environ 1285534 €) à la suite du vol de l'ordinateur portable d'un salarié. Le portable en question contenait des informations personnelles de plus de 11 millions de comptes clients. La FSA a estimé que les systèmes de sécurité de la compagnie et sa réaction au problème n'avaient pas été adaptés.

Le gouvernement révéla lui aussi avoir perdu des informations personnelles, dont une partie concernait son personnel et des informations bancaires de plus de 25 millions de bénéficiaires aux allocations familiales. Marks & Spencer fût également victime d'une perte de données à la même période puisque le portable d'un de ses directement a été volé lors d'un cambriolage. Il contenait les informations personnelles de plus de 26 000 personnes ayant souscrit à un plan épargne. Aucune donnée n'avait été cryptée.

Ces incidents et biens d'autres, ont rouvert la controverse au Royaume-Uni et en Europe pour savoir s'il fallait augmenter les exigences de sécurité, et notamment si les entreprises traitant des données personnelles devaient informer ou pas les personnes victimes de ces failles et les autorités de protection des données.

Alors que la Commission européenne avait proposé à l'origine une obligation pour les opérateurs de télécommunications et pour les fournisseurs d'accès à l'internet d'informer les personnes affectées par ces défaillances, les incidents survenus ont été à l'origine de l'élargissement de cette proposition. En effet, lors des consultations qui ont suivi, il a été proposé d'étendre ce régime à toutes les organisations traitant des données personnelles, c'est-à-dire à toutes les entreprises.

VERS UNE OBLIGATION D'INFORMATION DES FAILLES DE SÉCURITÉ ?

L'obligation d'information en cas de faille de sécurité ou de pertes de données a fait l'objet de plusieurs négociations, principalement dans le cadre de la refonte de la directive européenne sur les télécommunications. À travers des amendements sur la directive 2002/58/CE sur la vie privée et les communications électroniques, la commission européenne a proposé d'introduire une obligation d'information pour tous les « *opérateurs de services de communications électroniques ouverts au public* ».

En réponse à cette proposition, le groupe de travail de l'article 29⁷¹ (ou G29), qui regroupe les autorités de protection des données des États membres de l'Union européenne, a indiqué souhaiter étendre la mesure à toutes les organisations traitant des données personnelles. Peter Hustinx, le Contrôleur européen de la protection des données, a indiqué lui aussi aspirer à une plus large adoption de l'obligation d'information des failles de sécurité et de pertes de données en Europe.

Selon les amendements qui ont été déposés, toutes les organisations devront informer les utilisateurs et les autorités de protection de données, de toutes les failles « *conduisant à la destruction accidentelle ou illicite, la perte, l'altération, la divulgation ou l'accès de données à caractères personnels* ». Il est important de garder à l'esprit que le terme de "données personnelles" en Europe est très large et englobe toute information permettant d'identifier directement ou indirectement une personne physique⁷².

Les organisations devront communiquer « *sans retard excessif* » :

- La nature de la faille de sécurité.

⁷¹ En référence à l'article 29 de la directive européenne du 24 octobre 1995 sur la protection des données qui l'a institué.

⁷² Article 2 de la Directive 1995/46/CE du Parlement européen et du Conseil du 24 octobre 1995.

- Les mesures recommandées permettant d'atténuer si possible les effets négatifs, y compris les pertes économiques et le préjudice social qui pourrait survenir à la suite de la faille.
- Et à l'attention des autorités, les effets possibles et les mesures prises par la société pour remédier à la faille.

Les informations ne seraient donc pas communiquées aux seules victimes potentielles de la faille de sécurité, mais à tous les clients affectés et aux autorités. Le but, selon la Commission, étant que les autorités de protection de données aient la possibilité d'informer le public s'ils considèrent que c'est dans son intérêt.

De plus, afin d'assurer un haut niveau de protection des données personnelles et de la vie privée, les autorités pourraient en outre obtenir des « *données complètes et fiables* » sur l'incident de sécurité survenu. En d'autres termes, cette possibilité permettra aux autorités d'examiner les pratiques de sécurité et de protections des données mises en œuvre et, si elles sont considérées comme insuffisantes, de publier leurs résultats et d'imposer des sanctions.

Les débats sont cependant loin d'être clos avant que cette proposition soit adoptée ou abandonnée et les organisations potentiellement concernées peuvent les ignorer en toute quiétude, pour l'instant. Néanmoins, celles qui anticiperont cette mesure auront deux avantages. Le premier est qu'elles n'auront pas à mettre en œuvre les dispositions qui seront adoptées, si tel est le cas, en urgence avec tous les risques que cela comporte. Et le deuxième avantage sera par rapport à leurs clients qui auront une plus grande confiance dans la société, du fait de sa transparence et de la préoccupation des données et de ses clients dont elle fera preuve.

Le droit est donc omniprésent en informatique et pas seulement à travers les contrats. Le DSI, comme tout directeur ne peut en faire abstraction et compte tenu de la complexité associée du droit et de l'informatique, le directeur juridique et le DSI doivent travailler ensemble sur les sujets qui leur sont communs.

La connaissance et la compréhension mutuelle des termes utilisés tant par les juristes que par les informaticiens sont essentielles : les juristes ont besoin de comprendre le langage technique utilisé par les informaticiens pour réussir à monter un dossier efficace et agir en justice et les informaticiens ont eux besoin de connaître les termes et principes juridiques pour connaître les limites et les risques associés à leurs activités.

Le directeur des services informatiques est donc à la fois "client" et "acteur" de l'in-

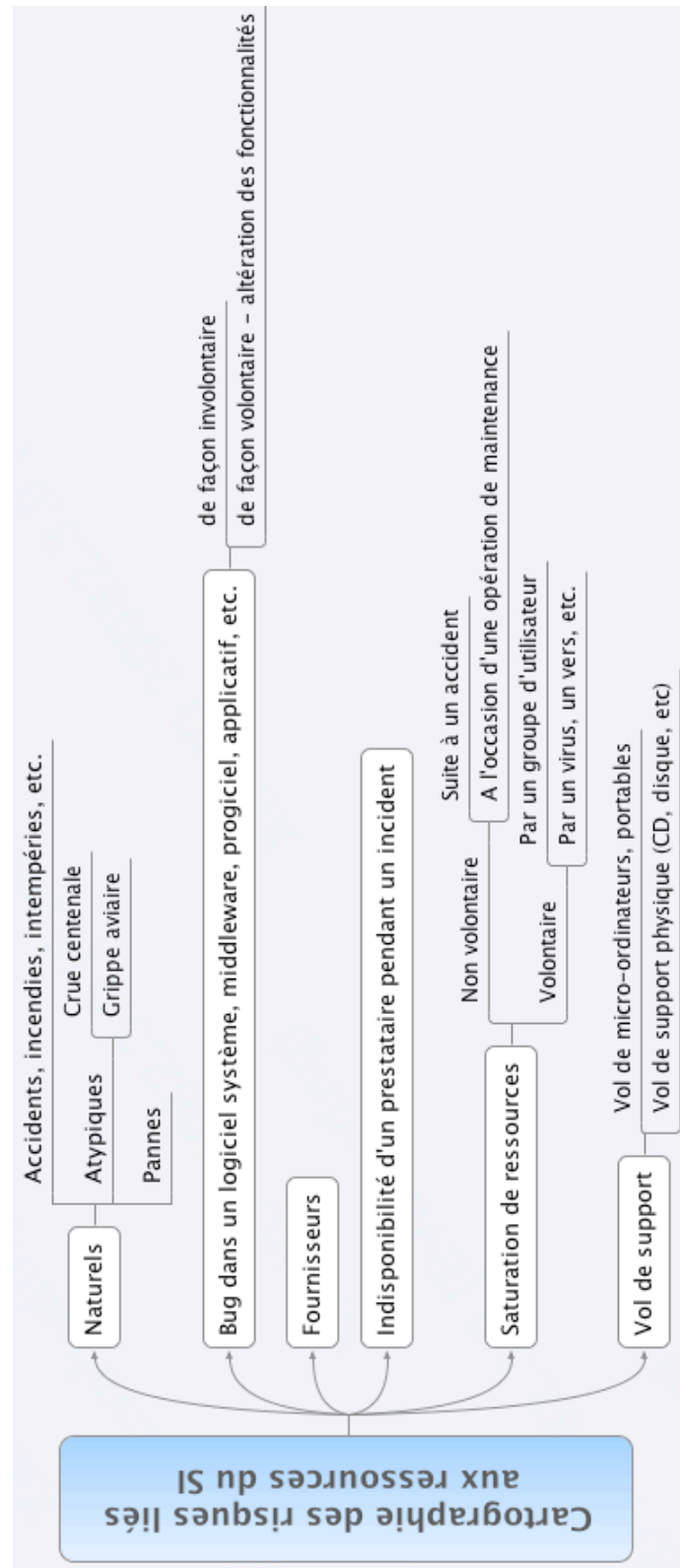
formation juridique. “Client” par le biais des nouvelles technologies qui s’imposent à lui; “Acteur” puisque, garant du processus et de la fiabilité du système d’information, il s’assure sur le plan technique de la circulation de toutes les informations, y compris les informations juridiques et qu’il peut jouer un rôle dans l’aménagement des règles juridiques qu’il côtoie.

Le DSI peut en outre adopter deux attitudes opposées: soit une approche défensive pour se protéger d’éventuelles poursuites, soit une approche offensive et faire du droit des TIC un avantage concurrentiel. Dans les deux cas, son rôle est central et transparait à travers la mise en cause possible de sa responsabilité. Les juristes d’entreprise spécialisés en droit des nouvelles technologies jouent donc un rôle primordial et seront de plus en plus sollicités au fur et à mesure de la maturité grandissante des entreprises sur le sujet et de la prise de conscience de l’importance des politiques de gestion des risques juridiques (PGRJ) au sein de l’entreprise.

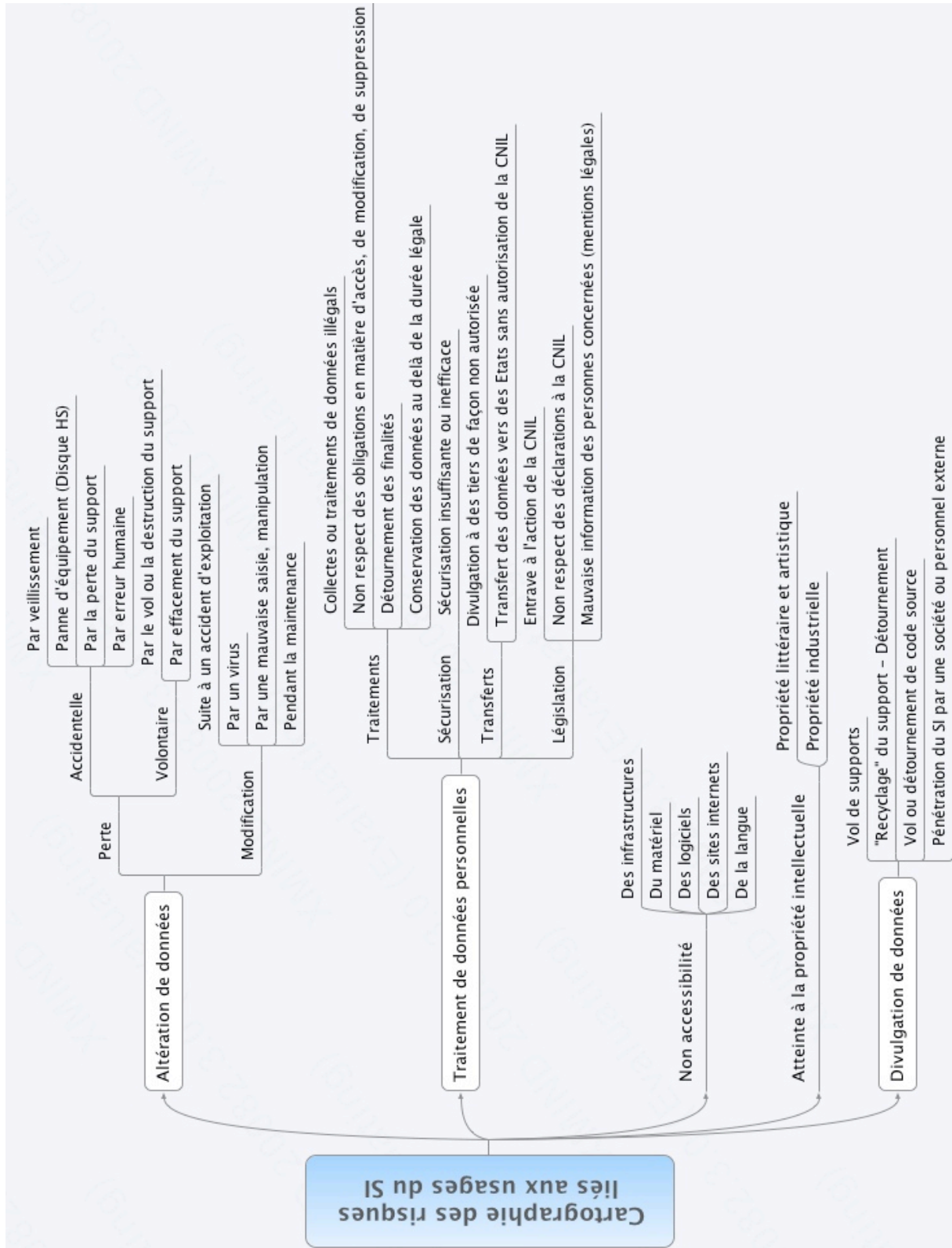
III. Annexes

Annexe 1 et 2 : les principaux risques liés aux systèmes d'informations

Annexe 1. La cartographie des risques liés aux ressources du SI



Annexe 2. La cartographie des risques liés aux usages du SI



Annexe 3. Les sanctions pénales applicables au non-respect de la loi Informatique et Libertés

Infractions	Texte	Peine (maximale)
Ne pas procéder aux opérations tendant à effacer ou à rendre anonymes les données relatives aux communications dans le cas où ces opérations sont prescrites par la loi.	Art. L-39-3 du Code des Postes et des Communications Électroniques (CPCE)	- 75 000 euros d'amende - 1 an d'emprisonnement
Le fait, « y compris par négligence » de procéder ou de faire procéder à des traitements automatisés d'informations nominatives sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi.	Art. 226-15 du Code Pénal	- 300 000 euros d'amende - 5 ans d'emprisonnement
Le fait, « y compris par négligence » de ne pas respecter les normes simplifiées ou d'exonérations établies par la CNIL.	Art. 226-16-1-A du Code Pénal	- 300 000 euros d'amende - 5 ans d'emprisonnement
Le fait de procéder ou de faire procéder à un traitement automatisé de données à caractère personnel sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et qu'elles ne soient pas modifiées ou communiquées à des tiers non autorisés.	Art. 226-17 du Code Pénal	- 300 000 euros d'amende - 5 ans d'emprisonnement
Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite.	Art. 226-18 du Code Pénal	- 300 000 euros d'amende - 5 ans d'emprisonnement
Le fait de procéder à un traitement de données à caractère personnel concernant une personne physique malgré l'opposition de cette personne.	Art. 226-18-1 du Code Pénal	- 300 000 euros d'amende - 5 ans d'emprisonnement
Le fait de mettre ou de conserver dans un système de traitement de données, sans l'accord exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques, religieuses ou les appartenances syndicales des personnes ou qui sont relatives à la santé ou à l'orientation sexuelle. Le fait de mettre ou de conserver dans un système de traitement automatisé, les données concernant des infractions, des condamnations ou des mesures de sûreté.	Art. 226-19 du Code Pénal	- 300 000 euros d'amende - 5 ans d'emprisonnement
Le fait de traiter ou de conserver à des fins autres qu'historiques ou statistiques des données à caractère personnel au-delà de la durée légale.	Art. 226-20 du Code Pénal	- 300 000 euros d'amende - 5 ans d'emprisonnement

Le fait de détourner les finalités d'un traitement.	Art. 226-21 du Code Pénal	- 300 000 euros d'amende - 5 ans d'emprisonnement
Le fait de divulguer des données à caractère personnel à des tiers non autorisés ou sans l'autorisation de l'intéressé ayant pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée (sur plainte).	Art. 226-22 du Code Pénal	- 300 000 euros d'amende - 5 ans d'emprisonnement
Le fait de commettre par négligence ou imprudence les mêmes faits (sur plainte).		- 100 000 euros d'amende - 3 ans d'emprisonnement
Le fait de transférer vers un État n'appartenant pas à l'Union européenne des données à caractère personnel sans autorisation de la CNIL ou en violation des mesures prises par l'Union européenne.	Art. 226-22-1 du Code Pénal	- 300 000 euros d'amende - 5 ans d'emprisonnement
L'entrave à l'action de la CNIL par : <ul style="list-style-type: none"> • L'opposition à l'exercice de sa mission. • Le refus de communication, dissimulation, disparition de documents et renseignements. • La communication d'informations non conformes ou sous une forme non accessible. 	Art. 51 de la loi Informatique et Libertés	- 15 000 euros d'amende - 1 an d'emprisonnement

Table de jurisprudences

Cour de cassation

- Cour de cassation, chambre criminelle, 8 février 1983, Jean-Pierre B. c/ Mathy A., pourvoi n° 82-92364, www.legifrance.fr - page 15.
- Cour de cassation, chambre civile 1, 13 décembre 2005, Mme Cuadros et autre c/ Microsoft France et autre, pourvoi n° 03-21154, www.legifrance.fr - page 29.
- Cour de cassation, chambre sociale, 18 octobre 2006, Monsieur J. L. c/ société Techni-Soft, www.foruminternet.org - page 42.
- Cour de cassation, chambre commerciale, 20 mai 2008, Google France c/ Louis Vuitton Malletier pourvoi n° 06-20230, www.legifrance.fr - page 54.
- Cour de cassation, chambre sociale, 9 juillet 2008, Franck L. c/ Entreprise Martin, www.legalis.net - page 41.

Cour de Justice des Communautés Européennes

- Cour de Justice des Communautés Européennes , 6 novembre 2003, Procédure pénale contre Piergiorgio Gambelli et autres, affaire C-243/01, www.eur-lex.europa.eu/fr/index.htm - page 54.

Cour d'appel d'Aix-en-Provence

- Cour d'appel d'Aix-en-Provence, 2^e chambre, 13 mars 2006, SA Escota c/ Société Lucent Technologies, www.juriscom.net - page 17.

Cour d'appel de Paris

- Cour d'appel de Paris, 22^e chambre section C, 16 novembre 2001, M. Laurent B. c/ S.A. Expeditors International France, www.foruminternet.org - page 41.
- Cour d'appel de Paris, 14^e chambre section B, 4 février 2005, SA BNP Paribas c/ Société World Press Online, www.juriscom.net - page 51.

Cour d'appel de Toulouse

- Cour d'appel de Toulouse, 2^e chambre section 2, 26 Octobre 2000, époux Barthe c/ Société commerciale andorrane Habitat, www.lexisnexis.fr - page 54.

TGI de Marseille

- Tribunal de grande instance de Marseille, 1^{re} chambre civile, 11 juin 2003, SA Escota c/ Société Lucent Technologies, www.juriscom.net - page 17.

TGI de Nanterre

- Tribunal de grande instance de Nanterre, 1^{re} chambre section B, 31 mai 2002, CGT c/ RENAULT, www.legalis.net - page 41.

TGI de Paris

- Tribunal de grande instance de Paris, ordonnance de référé, Monsieur Olivier M. c/ SARL Bloobox Net (Fuzz), 26 mars 2008, www.juriscom.net - page 48.

Bibliographie

Ouvrages

- BERDUGO (Alain) et al. sous la direction de. *Challenges pour les DSI*, Dunod, 2^e édition - 2005
- FÉNOL-TROUSSEAU (Marie-Pierre) et HAAS (Gérard). *La cybersurveillance dans l'entreprise et le droit*, LexisNexis Litec, 1^{re} édition - 2002
- FERAL-SCHUL (Christiane). *Cyberdroit, le droit à l'épreuve d'Internet*, Praxis Dalloz, 4^e édition - 2006
- LARGUIER (Jean). *Procédure Pénale*, Dalloz, 18^e édition - 2001
- LARRIEU (Jacques). *Droit de l'Internet*, Ellipses Marketing, édition 2005
- MALLET-POUJOL (Nathalie). *La création multimédia et le droit*, LexisNexis Litec, 2^e édition - 2003
- MARCELIN (Sabine) et al. *Droit de l'informatique et des réseaux*, Lamy, édition 2005
- RAY (Jean-Emmanuel). *Le droit du travail à l'épreuve des NTIC*, Liaisons, 2^e édition - 2001

Rapports

- *Dynamiques de création de valeur par les Systèmes d'Information*, CIGREF, McKinsey - 2008
- *Intelligence économique et stratégique*, CIGREF - 2003
- « Les mardis de l'ADIJ - Droit du travail et nouvelles technologies : actualité législative et jurisprudentielle », *Lamy Droit de l'Immatériel* n°14 - 2006
- *MEHARI 2007 : Guide de l'analyse des risques*, CLUSIF - 2007
- *Menaces Informatiques et Pratiques de Sécurité en France*, CLUSIF - 2008
- *Panorama de la Cyber-criminalité, Année 2007*, CLUSIF - 2008
- *Sécurité à l'heure d'internet (La)*, CIGREF - 2000
- THEUREAU (Béatrice) et ROUHIER (Stéphane). *Intelligence Juridique et Systèmes d'Informations*, CIGREF - 2004

Principaux sites internet consultés

- *Lamy Droit de l'Informatique et des Réseaux*, édition 2008, www.lamylinereflex.fr
- Diverses publications sur le droit des NTIC, <http://www.lexisnexis.fr>

Table des matières

<i>Glossaire</i>	2
<i>Sommaire</i>	3
<i>Introduction</i>	4
<i>I. Le directeur des systèmes d'informations et le droit</i>	5
A) Du directeur informatique au directeur des systèmes d'informations	5
1) La fonction du Directeur des systèmes d'informations	5
a. Définition du DSI	5
b. Le système informatique et le système d'information	6
c. Les missions du DSI	8
2) Les responsabilités juridiques des DSI	10
a. La responsabilité pénale et civile du DSI en tant que personne physique	10
b. La responsabilité de l'entreprise en tant que personne morale	12
c. Les délégations de pouvoir	14
B) Les risques liés aux systèmes d'informations	16
1) La perturbation et l'entrave à la sécurité	16
a. Les outils informatiques de l'entreprise utilisés par un salarié dans la commission de l'infraction	17
b. Le délit de manquement à la sécurité du SI	19
2) L'atteinte à la protection des données personnelles et à la liberté de créer	22
a. Le traitement de données à caractère personnel	22
b. L'atteinte au droit d'auteur	28

<i>II. Les outils de prévention à la portée du directeur des systèmes d'informations : une solution pragmatique quant aux risques juridiques liés aux systèmes d'informations</i>	<i>32</i>
A) La mise en place de moyens de prévention adaptés	32
1) La nécessaire intervention d'un professionnel	32
a. Les Responsables de la Sécurité des Systèmes d'Informations	33
b. Les MSSP (Managed Security Services Provider)	36
2) La rédaction de chartes et la sensibilisation des employés et de l'entreprise	39
a. La charte informatique de l'entreprise: quels enjeux juridiques?	40
b. Les chartes informatiques: un frein efficace contre les éventuels abus des salariés?	43
B) L'ouverture de la direction des systèmes d'informations au droit des nouvelles technologies	47
1) La pratique de la veille juridique et jurisprudentielle	47
a. Veille juridique	47
b. Encadrement jurisprudentiel	51
2) Anticiper l'application des directives européennes	53
a. Les risques mesurés de l'anticipation	53
b. La directive 2002/58/CE relative à la vie privée et aux communications électroniques	57
 <i>III. Annexes</i>	 <i>59</i>
Annexes 1 et 2 : les principaux risques liés aux systèmes d'informations	59
Annexe 3 : les sanctions pénales applicables au non-respect de la loi Informatique et Libertés	61
 <i>Table de jurisprudences</i>	 <i>63</i>
 <i>Bibliographie</i>	 <i>64</i>
 <i>Table des matières</i>	 <i>65</i>