RAPPORT

INTELLIGENCE JURIDIQUE ET SYSTÈMES D'INFORMATION

CIGREF

SEPTEMBRE 2004

www.cigref.fr

LE CIGREF

Le Cigref, Club informatique des grandes entreprises françaises, existe depuis 1970. Sa finalité est la promotion de l'usage des systèmes d'information comme facteur de création de valeurs pour l'entreprise. Il constitue un lieu privilégié de rencontre et d'échange d'informations entre les responsables des grandes entreprises françaises ou européennes utilisatrices d'importants systèmes d'information. Ce partage d'expériences vise à faire émerger les meilleures pratiques. Chaque année, le Cigref réalise des études sur des sujets d'intérêt commun.

Publications du Cigref en 2003-2004 :

Accompagnement du changement

Évolutions et pratiques

Accroître l'agilité du système d'information

Urbanisme : des concepts au projet

Challenges pour les DSI (avec HEC et l'École des Mines de Paris)

Éditions Dunod

Charte Cigref-Syntec informatique

Conseil en organisation et systèmes d'information
Infogérance et TMA
Ingénierie et intégration de systèmes
Progiciels

Géopolitique de l'internet

La fonction Achats informatiques et télécoms

Entre optimisation des coûts, performance et création de valeur

Le marché de la mobilité en France et à l'international

Modèles économiques, technologies et standards

Parties prenantes du système d'information

Un nouveau regard sur la maîtrise d'œuvre et la maîtrise d'ouvrage

Usages business des technologies sans fil

Maturité des usages, bilan des projets

Ces publications peuvent être obtenues en se connectant sur le site web du Cigref :
www.cigref.fr

PARTICIPANTS

Ce rapport a été rédigé par Béatrice Theureau, chargée de mission du Cigref, dans le cadre de sa thèse professionnelle pour l'obtention du mastère spécialisé en management des systèmes d'information et des technologies de HEC – École des Mines de Paris, avec des apports complémentaires de Stéphane Rouhier, chargé de mission du Cigref.

Ce document est le résultat de travaux personnels ainsi que d'activités menées au Cigref, en particulier des entretiens juridiques.

L'auteur remercie ses directeurs du mastère spécialisé en « management des systèmes d'information et des technologies » de HEC et de l'École des Mines : Alain Berdugo et Robert Mahl.

L'auteur remercie également les directeurs des systèmes d'information qui ont bien voulu lui faire part de leurs expériences en matière de droit des nouvelles technologies.

L'auteur remercie enfin l'IHEDN et Merkatis pour leurs commentaires, participations et contributions à l'élaboration de ce rapport.

Le Cigref tient à remercier tout particulièrement :
- maître Piette-Coudol, pour avoir contribué à l'actualisation des informations figurant dans ce rapport ;
- maître Thibault Du Manoir de Juaye, pour nous avoir fait bénéficier des ses précieux avis qu'il développe dans son ouvrage « Le droit pour dynamiser votre business » (Éditions d'organisation), à paraître en septembre 2004.

SOMMAIRE

TABLE DES ILLUSTRATIONS

1. AVANT PROPOS

En sa qualité d'association de grandes entreprises, le Cigref œuvre depuis sa création en 1970, à la promotion de « l'usage des système d'information comme facteur de création de valeur pour l'entreprise ».

Le projet stratégique « Cigref 2005 » a ancré cette mission dans une compréhension plus globale des enjeux de la société de l'information. Il s'agit entre autre des interactions entre l'économie et le droit dans le cadre d'une mondialisation des échanges qui exige une gouvernance globale de l'information.

Comme le montrent les récents travaux du Cigref sur l'intelligence économique et stratégique[1], les directeurs des systèmes d'information (DSI) savent mieux que d'autres combien, dans la compétition internationale actuelle, le seul véritable avantage concurrentiel, défendable et durable, réside pour l'entreprise, dans sa capacité à maîtriser l'information, en temps réel, à tous moments et en tous lieux.

Dès lors, au Cigref, nous considérons que l'intelligence juridique est « au service de l'entreprise » et « s'inscrit de ce fait dans la famille des disciplines de l'intelligence stratégique ».

C'est donc tout naturellement que la publication de ce rapport s'inscrit dans la suite logique des travaux déjà menés au Cigref sur ce thème[2]. Il renforce deux de nos convictions :

- l'Intelligence juridique est d'abord une affaire de culture managériale, c'est-à-dire une volonté singulière de penser, de décider et de coopérer afin de mieux agir collectivement. Elle est de ce fait, une affaire de comportement entrepreneurial qui concerne aujourd'hui toutes les parties prenantes de l'entreprise ;
- l'intelligence juridique n'est pas une fin en soi mais un moyen pour atteindre les objectifs vitaux que sont: la compétitivité et l'innovation permanentes. Ces objectifs vitaux sont de la responsabilité première des dirigeants.

[1] Intelligence économique et stratégique. Le système d'information au cœur de la démarche, Cigref, mars 2003.

[2] Entretiens juridiques du Cigref ; Géopolitique de l'internet, septembre 2003 ; et Charte Cigref – Syntec informatique.

Dès lors, au Cigref, nous considérerons que l'intelligence juridique est un « mode de gouvernance dont l'objet est la maîtrise de l'information 'juristratégique' utile aux métiers de la DSI et qui a pour finalité la compétitivité et la sécurité de l'entreprise toute entière ».

Jean-François Pépin
Délégué général du Cigref

N.B. : Pour faire connaître les préconisations de son rapport, le Cigref a contribué aux travaux de Merkatis, comme partenaire de l'étude que lui a confiée l'IHEDN (Institut des hautes études de défense nationale), étude publiée chez Economica sous le titre « Intelligence Juridique : un nouvel outil stratégique » en mai 2004.

2. PRÉAMBULE

« Le XXI[e] siècle sera le siècle du droit. » Cette affirmation de Jacques Marseille, professeur d'histoire économique et sociale à l'université Paris I, traduit la place considérable que tend à prendre l'environnement juridique dans l'activité de l'entreprise.

Le droit devient omniprésent. La complexité de cet environnement juridique, liée notamment à l'inflation des règles de droit (il existe actuellement en France 9 000 lois, 90 000 textes réglementaires, 5 millions de jugements), implique la nécessité pour l'entreprise de bâtir une « intelligence des situations juridiques ».

Les dirigeants doivent faire preuve de vigilance vis-à-vis du droit et se donner les moyens d'être en conformité juridique, sous peine de voir leur responsabilité engagée. Mais la règle aujourd'hui ne représente plus seulement une contrainte, elle propose également un modèle susceptible d'apporter un avantage à l'entreprise. Par « intelligence », il faut en effet entendre l'organisation des ressources en vue de prises de décisions stratégiques. Cette approche anglo-saxonne de la connaissance permet de conférer au droit un caractère dynamique, visant à en faire un atout stratégique pour l'entreprise.

Le droit et l'informatique, deux domaines très différents sur le plan historique et culturel, connaissent néanmoins un facteur de rapprochement dans l'entreprise avec la responsabilité spécifique du directeur des systèmes d'information (DSI).

L'« intelligence », c'est avant tout une question d'organisation, basée sur un système automatisé de collecte et de diffusion de l'information. De ce point de vue, le DSI garantit la transversalité de l'information juridique au profit des différentes directions de l'entreprise. Mais le DSI est également acteur de l'intelligence juridique par le biais du droit des nouvelles technologies. Dans ce domaine, le DSI joue un rôle majeur dans la mise en conformité juridique du système d'information, sa responsabilité pouvant être engagée en cas de manquement à ses obligations légales. Car le droit s'applique naturellement aux NTIC[3]. Le web notamment, même numérique, n'en est pas moins un support pouvant faire l'objet de protections légales, pour l'entreprise dans le cadre de la propriété intellectuelle, pour le particulier dans le cadre de la loi relative à l'informatique, aux fichiers et aux libertés. L'internet[4] n'est pas un vide juridique.

[3] Nouvelles technologies de l'information et de la communication.

[4] Internet, l'Internet ou l'internet ? Ce sera « l'internet » pour les raisons exprimées par le professeur Le Tourneau lors du 16[e] forum de l'APP (19-20 novembre 1998 à Toulouse) : « *Faut-il*

Afin d'élargir le champs de ses connaissances au profit des DSI de ses entreprises membres, le Cigref, dans le cadre de sa stratégie « Cigref 2005 », a lancé un cycle juridique : participation à des études et colloques, organisation d'entretiens juridiques animés par des professionnels du droit des nouvelles technologies, colloque annuel sur le nommage internet, travaux sur les contrats informatiques. L'objectif de cette thèse professionnelle est de présenter la démarche et les conclusions de ce cycle juridique.

Pourquoi le DSI est-il concerné par le droit ? Telle est la question sous-tendant la première partie de ce rapport. Compte tenu de la responsabilité spécifique du DSI, la manière dont il peut prévenir les risques informatiques sera abordée dans une deuxième partie.

rappeler, avant de commencer, que le mot « internet » n'est pas une marque, mais un nom générique qui, comme tel, doit recevoir un article et point de majuscule, exactement comme le téléphone, le minitel, la radio, le télex ou la télévision » (extrait de la revue Expertises, janvier 1999). Précisons néanmoins – et cela ne change rien à l'argumentaire qui précède – que « Minitel » est un nom déposé.

3. POURQUOI LE DSI EST-IL CONCERNÉ PAR LE DROIT ?

3.1 La responsabilité spécifique du DSI

Dans une concurrence économique vive et de plus en plus internationale, le droit devient une arme stratégique pour les entreprises et un moyen d'information et d'influence pour les praticiens de l'intelligence économique. Mais étendre l'intelligence économique au domaine juridique conduit nécessairement à repenser les méthodes de gestion de l'information juridique, qui n'est plus systématiquement l'apanage de la direction juridique de l'entreprise.

Dans ce contexte, le DSI est responsable de l'architecture technique du système d'information de l'entreprise, il participe à l'organisation de l'information juridique dans l'entreprise, en permettant la recherche et la diffusion à des fins stratégiques.

Son domaine de compétence le place également dans une sphère à laquelle le droit n'est pas étranger. Sa responsabilité peut en effet être engagée pour manquement à la sécurité du système d'information, lequel se situe tant sur un plan physique que juridique.

3.2 La recherche et la diffusion de l'information juridique

Afin d'établir un état des ressources juridiques et de leur utilisation dans les administrations et les entreprises, l'IHEDN[5] a entrepris en 2001 de faire réaliser par Merkatis, cabinet de conseil spécialisé dans les NTIC une étude sur le thème de l'intelligence juridique. Une série d'enquêtes a été menée dans ce cadre auprès d'organisations professionnelles représentatives des administrations et du monde des entreprises.

Le Cigref a accepté d'être partenaire de l'IHEDN afin d'apporter des éléments de réponse sur ce qui se fait dans les grandes entreprises françaises en termes d'outils et de méthodes dédiés à l'intelligence juridique. Cela s'est traduit par une série de réunions avec des organisations telles la Conférence des bâtonniers, le Conseil supérieur du notariat, la Compagnie nationale des commissaires aux comptes, l'Association française des juristes d'entreprise.

Les développements qui suivent présentent quelques éléments de réflexion ayant été dégagés au cours de ces réunions, les résultats de l'étude faisant l'objet d'un rapport remis à l'IHEDN en septembre 2002.

[5] Institut des hautes études de la défense nationale.

3.2.1 Le droit : outil stratégique de l'entreprise

Bien souvent, il faut que les entreprises se trouvent confrontées à la survenue de risques pour qu'elles prennent conscience de la dimension juridique de leurs activités. Or le droit dans l'entreprise a aujourd'hui une dimension transversale, qui ne relève plus exclusivement de la direction juridique, mais qui se déploie sur l'ensemble du spectre des activités, donc dans l'ensemble des directions opérationnelles et fonctionnelles.

Cette évolution de l'utilisation du droit coïncide en fait avec l'évolution de l'entreprise elle-même, où la pluridisciplinarité est devenue omniprésente.

3.2.1.1 L'utilisation du droit

Le droit dans l'entreprise

Les entreprises publiques et privées évoluent dans un environnement juridique qui, s'il est appréhendé en amont des prises de décision, peut fournir des outils stratégiques. Ainsi, le droit ne représente plus seulement un cadre contraignant, il est au cœur de toute prise de décision.

Jusqu'à il y a une vingtaine d'années, la dimension principale du juridique se réduisait au contentieux.

Il s'est développé depuis une prise de conscience du juridique, notamment dans le domaine contractuel : le droit est progressivement apparu comme un élément stratégique dans le cadre des relations avec les tiers, et ceci est particulièrement vrai avec les contrats informatiques.

De la même façon, la propriété intellectuelle est devenue rapidement un domaine stratégique pour la direction des grandes entreprises avec une augmentation des ressources de propriété intellectuelle (notamment les logiciels et les bases de données).

Chercher à optimiser le paramètre juridique, en faire un outil de « proactivité » et de management, est aujourd'hui encore une idée nouvelle mais qui fait son chemin. Suivre la règle de droit ou user de tel « outil » juridique plutôt que tel autre peut en effet présenter de sérieux avantages : pouvoir s'adresser aux tribunaux, disposer vis-à-vis des partenaires de moyens légaux de pression fortement dissuasifs. Pratiquement, toute décision prise dans une entreprise comporte une dimension juridique, déplaçant par là même le terrain de la concurrence (un exemple dans les NTIC, avec l'affaire Napster).

De façon pratique, l'accompagnement juridique des activités quotidiennes des services de l'entreprise passe essentiellement par trois tâches :

- assurer le contrôle juridique du contenu des contrats ;
- assurer l'examen systématique des possibilités de couvrir juridiquement les risques ;
- garantir la mise à disposition rapide de l'information juridique à chacun des services.

Mais l'intégration du droit dans la culture de l'entreprise présente des difficultés, liées à des problèmes comme l'information juridique des non-juristes ou la persuasion des individus et services concernés sur l'utilité de l'effort qui est imposé pour « être en règle ». Les règles ne font rien d'elles-mêmes. Pour qu'elles puissent faire l'objet d'une exploitation stratégique, il faut qu'elles soient mobilisées, insérées au sein d'un système, exploitées, et ce à partir d'une volonté managériale clairement affirmée.

Les enjeux pour l'entreprise d'une utilisation stratégique des ressources juridiques

Relevant de l'intelligence économique et stratégique, le vocable de « veille juridique » semblait jusqu'à présent plus approprié que celui d'« intelligence juridique ». Cette veille spécialisée consistait à étudier les systèmes juridiques nationaux et étrangers (réglementations existantes et émergentes, jurisprudence) et à en apprécier les conséquences pour l'entreprise, ainsi qu'à surveiller les contrefaçons (surveillance des dépôts de brevets et des enregistrements de marques).

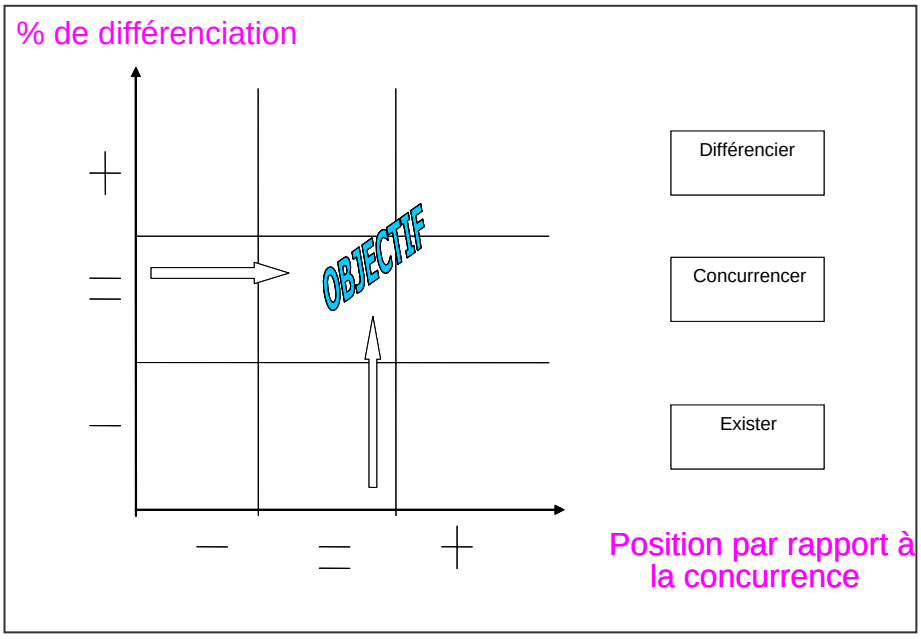
Néanmoins, la prise de conscience par l'entreprise de la nécessité de gérer le risque juridique et de rationaliser les prestations juridiques, ainsi que de la possibilité d'utiliser le droit pour gagner des parts de marché, conduit de nombreux professionnels à observer qu'un « management juridique » est en train de s'imposer, et que le concept d'« intelligence juridique » répond mieux à la corrélation entre droit et stratégie au sein de l'entreprise.

Cette intelligence juridique est essentielle pour l'entreprise, qui évolue dans un cadre juridique de plus en plus précis et mouvant. Elle doit se renseigner en permanence sur cet environnement juridique pour être en mesure d'agir sur celui-ci : éviter les déconvenues (versement de dommages et intérêts, amendes, voire peines de prison) et saisir les opportunités avant les autres (notamment en matière de propriété intellectuelle).

« L'intelligence juridique » peut ainsi se définir comme un système de surveillance de l'environnement juridique de

l'entreprise afin d'en détecter les menaces et opportunités. Elle se fonde sur la recherche et la collecte systématique, continue et rigoureuse d'informations juridiques provenant de sources diverses et ensuite sur le tri, l'analyse, la diffusion et enfin l'exploitation de ces informations (« veille juridique »). Ces informations doivent aider l'entreprise à prendre des décisions stratégiques et à renforcer sa position concurrentielle.

Mais l'environnement concurrentiel détermine le degré d'investissement que doit réaliser l'entreprise en matière d'intelligence juridique. Dans le contexte actuel, la pression concurrentielle vient essentiellement des pays anglo-saxons. La matrice de N. Venkatraman permet de visualiser le positionnement de l'entreprise française, pour laquelle le concept d'intelligence juridique est encore nouveau.



Source : N. Venkatraman

Figure 1 : Matrice de N. Venkatraman.

3.2.1.2 La perception du droit

Le langage juridique

Le système juridique a indéniablement complexifié son langage et ses techniques. Le DSI le ressent très fortement par exemple lors de la négociation et du suivi des contrats informatiques.

Culturellement par ailleurs, le fait de ne pouvoir recenser depuis 1995 qu'une centaine de décisions judiciaires dans le domaine de l'internet, dont un tiers relatif aux noms de domaine et un tiers relatif aux droits d'auteur, montre que le corps social n'associe pas spontanément le droit et la technique.

De son côté, épris de l'écrit, le juriste a parfois quelques difficultés à entrer dans le monde des NTIC, dont les enjeux (exemple : vulnérabilité ou performance technique d'un réseau) ne sont pas toujours connus. En ce domaine volontiers « jargonnant », le raisonnement d'un ingénieur ou d'un expert en informatique peut lui paraître infaillible. Combien de directeurs juridiques en savent par exemple autant que ceux des systèmes d'information en matière de contrôle des connexions des salariés ?

Maître Alain Bensoussan[6] constate un décalage entre l'abondance de la littérature sur le thème des risques informatiques et la faiblesse des poursuites devant les tribunaux.

En ce domaine en effet, la connaissance et la compréhension mutuelle des termes utilisés tant par les juristes que par les informaticiens est essentielle. Lorsqu'il s'agit de qualifier des atteintes à la sécurité du système d'information, les juristes ont besoin de comprendre le langage technique utilisé par les informaticiens pour comprendre la finalité des attaques et monter un bon dossier pour agir en justice.

Les rapports direction juridique - direction des systèmes d'information

Les fonctions du DSI

- Le DSI assume des fonctions de direction des systèmes d'information et la gestion de la coordination des informations traitées automatiquement dans les différents services de l'entreprise.
- Il assure la gestion technique et administrative de toutes les opérations effectuées dans l'entreprise grâce à l'informatique.

[6] Cabinet d'avocats Alain Bensoussan, cabinet spécialisé en droit des nouvelles technologies.

Ses missions sont, en conséquence, très variées puisqu'il prend en charge :

- la négociation et le suivi des contrats d'acquisition des matériels, logiciels et prestations de services informatiques ou télécoms ;
- la gestion informatisée de la paie du personnel et de son avancement ;
- la prévention quant à la fraude informatique ;
- l'accomplissement des formalités relatives à la loi Informatique et libertés.

Ses fonctions placent ainsi le DSI au cœur d'un système qui allie technique et droit, domaines qui jusqu'à présent étaient étrangers l'un à l'autre.

La formalisation des rapports avec la direction juridique

Dans le lien que doit assurer le DSI entre les données recueillies et la prise de décision stratégique, il peut se poser un problème de circulation de l'information, d'ailleurs pas forcément lié aux insuffisances de la technologie.

De ce point de vue, le droit ne peut représenter un outil stratégique et offensif que si les outils technologiques prennent en compte la culture de l'entreprise et pas seulement les aspects purement juridiques ou informatiques. La collaboration entre les deux directions fonctionnelles, juridique et systèmes d'information, contribue à véhiculer l'information juridique utile à la prise de décision stratégique, c'est-à-dire celle que les décideurs peuvent s'approprier compte tenu de la culture de l'entreprise.

Au cours de l'étude menée au Cigref sur le thème de l'intelligence juridique, on constate que les relations entre la direction juridique et la direction des systèmes d'information existent mais ne sont pas, dans la majorité des entreprises, formalisées. Les DSI recourent ponctuellement dans le cadre de leurs activités aux juristes de la direction juridique, essentiellement pour la négociation des contrats informatiques. Le point essentiel est d'identifier qui est le « *stakeholder* » et le chef de file sur les dossiers portant sur le droit des TIC (noms de domaine, contrats, contentieux, lobbying, veille…) et de se mettre d'accord sur la répartition des rôles et des responsabilités.

Ainsi la majorité des directions des systèmes d'information des grandes entreprises assurent-elles une pré-négociation des contrats informatiques, avant même que la direction juridique ne les examine sur le plan du droit. En effet, l'informatique au sens large est une activité à haute technicité. La rédaction d'un contrat suppose une connaissance approfondie des éléments

techniques qui concourent à l'exécution du projet ainsi qu'une parfaite cohérence entre la terminologie employée et les obligations définies.

Par ailleurs, le droit des nouvelles technologies est sujet à des difficultés en matière de délimitation de responsabilité entre la direction juridique et la DSI : « sociétéY.com, c'est forcément pour la DSI ». Cette petite phrase entendue à la DSI d'une société membre du Cigref signifie qu'à partir du moment où il s'agit de l'internet, c'est alors le problème de la DSI. Or, celle-ci n'est pas nécessairement la plus compétente pour traiter seul tous les aspects de la problématique des noms de domaine.

Dans cette relation DSI - direction juridique, plusieurs grands groupes ont pris des initiatives intéressantes en mettant en œuvre l'une des options suivantes :

- Certains juristes appartenant à la direction juridique ont plus particulièrement une « orientation informatique ».
- Une division « droit des nouvelles technologies » a été créée à la direction juridique.
- La direction des systèmes d'information a une compétence « contrats et négociation ».
- Un juriste a été affecté à la direction des systèmes d'informations pour traiter avant tout des contrats informatiques mais également de toutes les questions liées au droit des nouvelles technologies.
- Un responsable de la sécurité informatique est affecté à la direction de la qualité (affaires juridiques), et un juriste est affecté à la division achats de la DSI pour suivre les contrats.

Mais d'une façon générale, on constate que la culture informatique est assez étrangère aux juristes d'entreprise. Deux faits corroborent ce constat :

- Les DSI recourent fréquemment à des avocats pour traiter certains dossiers à caractère juridique, tels les contrats informatiques.
- Les « Entretiens juridiques du Cigref » ont beaucoup attiré les juristes des directions juridiques des entreprises.

Ce constat semble également signifier que dans les grandes entreprises, même si les DSI sont tout à fait conscients de leur responsabilité en matière de droit des nouvelles technologies, la veille juridique est majoritairement le fait du juriste, ce dernier étant ensuite chargé d'apporter la connaissance juridique à l'informaticien.

Il faut aussi souligner que d'autres fonctions de l'entreprise peuvent aussi intégrer des compétences juridiques (les directions des achats par exemple).

3.2.2 Le DSI : garant de la transversalité de l'information

La place et la responsabilité du DSI dans l'entreprise lui permettent de garantir à l'ensemble des flux d'information qui circulent dans l'entreprise un caractère transversal et sécurisé. Il connaît les outils à mettre en place pour permettre à chaque direction de récupérer les informations qui l'intéressent.

Il est donc dans ce contexte au service des métiers : il a un rôle à la fois d'organisateur, de gestionnaire, de coordinateur des besoins informationnels des différents services de l'entreprise.

3.2.2.1 Les outils méthodologiques

Un facteur de succès : la légitimité du DSI

La pression subie par les DSI dans le traitement de dossiers tels que l'an 2000, la mise en place des ERP ou le passage à l'euro montre qu'une organisation tout entière peut s'arrêter de fonctionner en cas de problème. Cela témoigne de la dépendance de nos organisations modernes par rapport aux technologies de l'information et de la communication.

Le titre du responsable de la fonction informatique n'a cessé d'évoluer ces dernières années. Ces changements terminologiques ne sont que le reflet de la prise de conscience des enjeux (cf. le rapport « Intelligence économique et stratégique » du Cigref). On est passé d'un titre centré sur la technologie, le directeur informatique, à un titre orienté gestion de l'information, le directeur des systèmes d'information. Philippe Baumard, chercheur à l'IAE d'Aix en Provence, n'hésite pas à définir le terme de DMSI (directeur du management des systèmes d'information).

Cette progression est cohérente et correspond aux préoccupations fondamentales des entreprises. L'enjeu n'est pas la gestion de la technologie, mais la gestion de l'information, la ressource plutôt que son support. L'informatique n'est qu'une technique permettant de mieux gérer l'information.

Compte tenu des enjeux, la gestion efficace de l'information conditionne inéluctablement la performance des organisations. C'est la véritable mission du DSI, encore doit-il en posséder la légitimité au sein de son entreprise.

Cette légitimité est facilitée par le positionnement du DSI dans l'entreprise, qui a largement évolué ces dernières années. Les DSI rapportent en majorité directement à la direction générale et se placent au même niveau que les directions

opérationnelles. Ce positionnement du DSI lui permet de contribuer aux objectifs stratégiques de l'entreprise.

La gestion de l'information

La direction des systèmes d'information fait le lien entre les données recueillies, par l'intranet de l'entreprise ou l'internet, et la prise de décision stratégique. L'informatique se trouve dans toutes les directions métiers et le DSI est justement responsable de la cohérence et de l'efficacité du système d'information.

Néanmoins, un travail de collaboration de la part de l'ensemble des directions de l'entreprise est nécessaire pour permettre cette utilisation stratégique de l'information. Il s'agit de déterminer les informations dont elles ont besoin pour aider à la prise de décision stratégique. Dans ce travail de réflexion, le DSI est légitimé pour aider le décideur à définir ses besoins informationnels puisqu'il sait comment circule l'information et connaît les ressources informationnelles de l'entreprise.

Il s'agit également de désigner la source et le propriétaire de l'information ; l'information n'a en effet pas la même valeur selon qu'elle est en ligne ou dans une base de données.

La gestion de l'information implique enfin la mise en œuvre de tous les moyens visant à la performance du système informationnel car, si la quantité d'informations est aujourd'hui, compte tenu des possibilités techniques, facile à obtenir, la qualité demande plus d'énergie, de volonté et de temps.

Dans ce défi, le DSI a tous les atouts de son côté, atouts liés avant tout à la technologie de l'information : « Avant, c'était le récepteur de l'information qui avait le pouvoir, aujourd'hui, c'est le transmetteur. »

Le partage de l'information

Des modifications fondamentales du rôle et de la place de « l'information » sont apparues ces trente dernières années. Ces modifications ont bien sûr des répercussions sur l'individu et l'entreprise. Pour cette dernière, une information bien maîtrisée est rapidement apparue comme un « facteur clé de développement ».

Face à ce processus, l'entreprise doit évoluer :

- elle doit savoir maîtriser la chaîne qui part des « données » pour aboutir à une « action concrète » ;
- elle doit savoir produire et générer des informations ;

- pour cela, elle doit mettre en place un système d'information adéquat, et « manager » les savoirs ;
- un système d'intelligence juridique est une des formes possibles de gestion des savoirs et des informations.

Mais un système de gestion des informations ne peut fonctionner sans une réelle volonté de partage des informations. Or cela demande des capacités individuelles indispensables. D'abord dans l'analyse de ses propres besoins en information ; puis dans l'exploitation, la protection et enfin la communication des informations à ses collègues.

Le système d'information n'est alors plus seulement l'outil qui permet la collecte, le traitement et la diffusion de l'information. Il apporte une réelle valeur ajoutée en matière de partage des savoirs entre toutes les parties prenantes (internes et externes) de l'entreprise.

Dans ce contexte, le DSI agit comme un créateur de liens. Il facilite la coopération entre tous les acteurs de l'entreprise en optimisant la circulation des connaissances (ce qui donne du sens à l'information).

Et, même si le partage de l'information est plus difficile dans une entreprise étendue, la place du DSI est centrale quelle qu'en soit la taille, dans la mesure où ses fonctions l'amènent à garantir sur le plan technique et fonctionnel la transversalité de l'information.

L'organisation de la ressource juridique

L'organisation des informations juridiques répond à quatre impératifs :

- contribuer au positionnement juridique de l'entreprise ;
- les rendre adaptables à la prise de décision stratégique ;
- permettre d'établir l'état des ressources disponibles ;
- permettre d'évaluer l'efficacité opérationnelle des ressources utilisées.

Quelle que soit l'organisation de ces ressources juridiques dans l'entreprise, il apparaît que la perception de leur intérêt par les différentes directions de l'entreprise est liée :

- à la taille de l'entreprise ;
- au métier de l'entreprise ;
- à la dimension de la cellule juridique.

Parmi les entreprises membres du Cigref, on peut noter certains exemples intéressants en termes d'organisation de la ressource juridique :

- Cofinoga se distingue par l'existence d'une base documentaire juridique de vulgarisation, alimentée par la direction des affaires juridiques, destinée plus spécialement aux services opérationnels, mais consultable néanmoins par toute l'entreprise.
- Le groupe Accor a opté pour un intranet juridique auquel ont accès tous les juristes ainsi que les hôtels, ces derniers devant souscrire un abonnement spécifique.

L'étude menée pour l'IHEDN conclut que bien souvent, si l'information juridique existe et est transversale, son exploitation n'est pas formalisée. Le recours à l'information juridique est ponctuel, il n'y a pas d'« intelligence juridique », mais des juristes utilisés dans l'entreprise en fonction des besoins. Or l'« intelligence » au sens anglo-saxon du terme, c'est de l'organisation en vue de prises de décisions stratégiques. Et l'organisation nécessite une systématisation des flux d'information.

La finalité de la veille

Pour faire de la veille, il faut avant tout se poser les questions :

- Quels objectifs ?
- Quels enjeux pour l'entreprise ?
- Quelle structure ?

Les professionnels de l'« intelligence » s'accordent à dire que la veille est une compétence clé pour l'entreprise. Les entreprises performantes se distinguent en effet par la combinaison des trois éléments suivants :

- cohérence R&D / politique produits / stratégie ;
- équilibre des pouvoirs (commercial / production / R&D) ;
- système d'information performant :
  - en interne : rapide et précis, permettant l'action et l'anticipation,
  - pour l'environnement : système de veille efficace.

Une enquête réalisée par l'IHEDN en 2000 révèle un large recours à la veille juridique et réglementaire, qui fait partie des veilles les plus utilisées en entreprise :

- veille concurrentielle : 77 % des entreprises la pratiquent ;
- veille marketing et clientèle : 75 % ;

- veille juridique et réglementaire : 62 %.

Ces trois types de veille représentent en effet un fort enjeu stratégique, notamment en termes de gestion des risques. Elles deviennent globales lorsqu'elles dépassent la seule exploitation des informations recueillies, en intégrant une dimension stratégique. Le tableau qui suit détaille les caractéristiques de chaque degré de veille.

Documentation ↓	- Exploitation de sources formelles et ouvertes d'information uniquement - Parfaite connaissance des sources	Diffusion d'informations brutes
Veille documentaire ↓	- Surveillance de certains secteurs - Spécialisation des documentalistes - Profils de veille	
Veille spécialisée ou **sectorielle** (technologique, brevet, juridique, normative, commerciale, concurrentielle...) ↓	- Exploitation d'informations informelles et fermées - Mobilisation des réseaux	
Veille globale (stratégique ou tactique) ↓	- Approche plus globale : fédère les différentes veilles de l'entreprise et intègre la dimension stratégique - Démarche plus orientée vers l'action	
Intelligence économique	- Intègre les actions d'influence et de lobbying - Suppose une culture collective de l'information - Intègre un large ensemble d'acteurs dans l'entreprise - Se doit d'être érigée en véritable mode de management	

Source : rapport IES du Cigref

Figure 2 : De la veille à l'intelligence.

Un précédent rapport du Cigref, « Internet dans l'entreprise », montre que les éléments de dimensionnement de la veille sont :

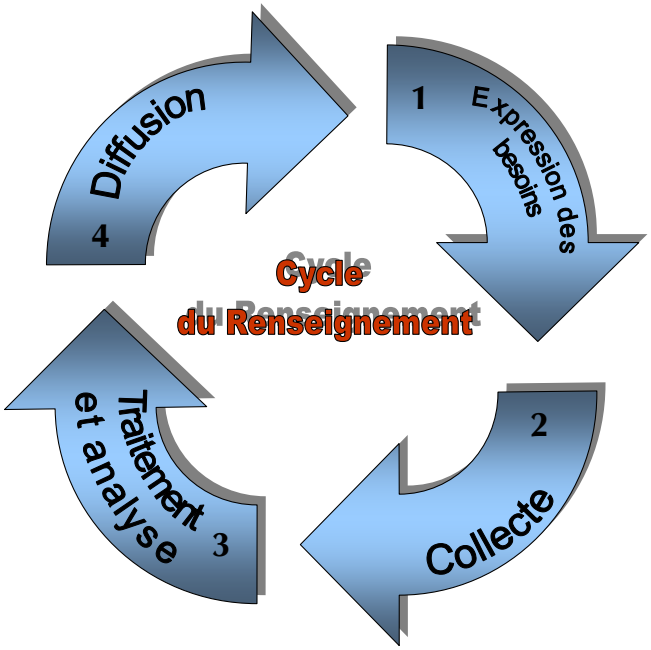
- le coût ;
- le temps ;
- la taille du budget ;
- la taille des équipes ;
- l'exhaustivité des recherches ;
- la volonté de la direction générale.

Par ailleurs, les principales tendances constatées dans les entreprises seraient :

- l'évolution de l'intelligence économique vers la gestion des connaissances ;
- l'évolution de l'intelligence économique vers la notion de portail décisionnel ;
- le développement par des prestataires externes d'offres de solutions de veille sur mesure et à la demande.

Cette gestion des connaissances conduit le veilleur, et donc le décideur, à s'intéresser à d'autres domaines que ceux strictement et traditionnellement opérationnels.

La technique de la veille et le rôle du DSI



Source : Rapport IES du Cigref

Figure 3 : Le cycle de l'information.

La veille juridique induit de la même façon trois actions majeures :

RECHERCHE
COLLECTE
TRAITEMENT
DIFFUSION

DE L'INFORMATION JURIDIQUE

La définition des besoins informationnels

La technique est proche de la technique de travail du DSI : l'encerclement, qui est une technique d'intelligence économique, consiste à aller au contact des autres départements pour voir, avec eux, leurs besoins informationnels et établir des tableaux de bord.

En matière de contrefaçon par exemple, le processus de veille juridique pourrait comprendre :

- l'analyse de la fiabilité de l'information sur l'internet :
  - vérifier systématiquement la source de l'information,
  - croiser plusieurs informations,
  - essayer de dater le document identifié ;
- la définition d'une stratégie de veille juridique :
  - détecter la contrefaçon grâce aux outils de recherche,
  - mettre en place un dispositif de veille grâce aux agents intelligents ;
- la détection de la contrefaçon grâce aux outils de recherche :
  - prendre des mots ou de courts extraits très caractéristiques de l'offre commerciale,
  - lancer des recherches avec les moteurs les plus puissants ;
- la mise en place d'une cellule de veille grâce aux agents intelligents.

Les acteurs

Si c'est le juriste qui assure seul la recherche et la collecte de l'information, il risque de se limiter au droit, en passant à côté de la stratégie et des objectifs à atteindre propres à chaque direction opérationnelle. Il faut au contraire que ces opérations de recherche et de collecte de l'information soient le fait de l'utilisateur, qui en adresse une copie à une « unité de traitement de l'information ».

Le traitement de l'information

D'un point de vue stratégique, le traitement de l'information doit être global et nécessite une synthèse préalable.

Cette synthèse peut être visualisée par la création d'un tableau de bord prenant en compte les spécificités organisationnelles et besoins informationnels de l'entreprise :

	ANALYSE DES FAITS		CONSEQUENCES ?	ACTIONS ?	REMISE EN CAUSE		
		*			ORI	CIB	OBJ
MARCHES							
PRODUITS							
PROCESS							
REGLEMENTATION CONTRATS							
R§D PROPRIETE INDUSTRIELLE							
SOCIAL HUMAIN							
ECONOMIQUE FINANCIER							
STRATEGIE							

* : peut être soit une information recoupée, soit une information à confirmer.

ORI : Origine CIB : Cible OBJ : Objet

Source : Cycle IES 2002 du Cigref

Figure 4 : Le traitement global de l'information.

Le rôle du DSI

Les fonctions du DSI lui permettent d'amorcer et d'entretenir le dispositif d'alerte sur le plan technique. Par sa connaissance des produits technologiques existant sur le marché, il peut aider techniquement à la mise en place d'un dispositif de veille juridique.

Il a par ailleurs la faculté technique de garantir la rapidité de la diffusion de l'information. C'est essentiel dans le domaine de l'« intelligence », où il s'agit avant tout de limiter la perte d'information. Et une information perdue correspond à une information non traitée, non exploitée et non diffusée à temps, c'est-à-dire devenue obsolète.

Enfin, dans la cartographie des enjeux liés au numérique, le DSI a la capacité d'apporter des outils technologiques de détection et de visualisation des risques, par la mise en place de tableaux de bord spécifiquement dédiés à cette veille.

3.2.2.2 Les sources de veille juridique

L'internet

Le système de veille sur l'internet est un élément essentiel du système global de surveillance de l'environnement. Sa mise en place nécessite des compétences spécifiques (connaissance de l'internet, des outils informatiques et du processus de veille) mais reste peu coûteuse et relativement simple par rapport aux gains engendrés.

Une veille juridique quotidienne sur l'internet permet en effet d'avoir gratuitement et en temps réel accès à des informations qui, il y a encore cinq ou six ans, demandaient des semaines d'échanges de courriers.

Mais le ciblage des thèmes et des sources à surveiller sur l'internet doit être bien défini : sites juridiques, sites à accès limité aux abonnés, sites institutionnels, forums de discussion, experts... La quantité d'information exploitable peut s'avérer énorme : il est donc nécessaire de l'organiser si l'on ne veut pas être submergé. Pour cela, il faut pouvoir identifier les points clés de l'environnement stratégique sans pour autant s'y cantonner (parce qu'il évolue sans cesse et qu'il faut capter les signaux faibles souvent hors du ciblage). On peut utiliser des agents dits « intelligents » afin d'être alerté (par courriel par exemple) des évolutions de l'environnement juridique pertinent. Encore faut-il les paramétrer de façon à ce que la surveillance soit à la fois automatisée (selon la quantité souhaitée) et pertinente (selon la qualité souhaitée).

Le ciblage est à l'évidence réalisé par les professionnels qui se servent du droit dans le cadre de leurs fonctions ; ce sont les juristes de l'entreprise bien sûr. Le paramétrage quant à lui ne peut être fait qu'accompagné par la maîtrise d'œuvre ou la maîtrise d'ouvrage.

Le droit des nouvelles technologies

Dans le domaine du droit des NTIC, le DSI a à sa disposition une série d'outils de recherche spécialisée sur l'internet.

- Les moteurs de recherche juridique NTIC
  - Find Law
  - Law Crawler
  - etc.

- La documentation sur le droit des NTIC

Legalis.net	Les aspects juridiques de l'internet et des créations numériques (actualité, jurisprudence, contrats types...).
Jnet	La jurisprudence relative à l'internet.
LEGALnet	Actualité, jurisprudence, contrats types sur les aspects juridiques de l'informatique et de l'internet.
Juriscom.net	Le droit des technologies de l'information.
Les pages personnelles d'informations juridiques de Jérôme Rabenou	Nombreux codes et textes juridiques en ligne, nombreuses ressources internet et diverses.
Celog	Centre d'expertises (liens vers les publications de Celog).
Jurisnet	L'internet pour les juristes (actualités, annuaire, forum...).
Cyberlex Net	Le site juridique des nouvelles technologies (internet et multimédia).
Page personnelle de Michel Toporkoff, président de chambre au tribunal de commerce de Paris	La jurisprudence en matière d'imitation illicite de produits, base de données, comprenant plus de 500 décisions récentes.
Juriline	Site proposé par LAMY (actualité juridique et judiciaire).
Juripôle de Lorraine	Site d'information juridique réalisé par Alexis Baumann.
Lex Electronica	Revue du droit des technologies de l'information par le Centre de recherche en droit public de l'Université de Montréal.
I'M Europe – DG XIII	Law resources for new technology in the EU (site de la Commission européenne relatif aux aspects juridiques de la société de l'information).
Kuester Law	The technology law resource.
Legal Information Institute	Cornell Law School.
Intellectuel Property and Technology Forum	Boston College Law School.
Net Law	New technology law.
Cyberspace law	Base de ressources du droit de l'internet d'Outre-Atlantique.

Source : Cigref

Figure 5 : La documentation en droit des NTIC en ligne.

- La presse juridique et technique

Droit de l'informatique et des télécoms	La revue du droit de l'informatique et des télécoms.
Au fil du net	La Gazette du Palais
Le Journal d'internet	Communication et réseaux
Le Monde informatique / 01 Informatique	Informations générales sur le secteur des nouvelles technologies de l'information et de la communication
Intellectual Property Magazine	revue états-unienne sur le droit des nouvelles technologies

Source : Cigref

Figure 6 : La presse juridique et technique en ligne.

3.3 La sécurité du système d'information

À l'occasion d'une plainte consécutive à une attaque grave contre le système d'information de l'entreprise, le DSI peut se voir inculpé lui-même de délit de manquement à la sécurité, passible de peine de prison.

En édictant des peines visant à sanctionner certaines infractions commises grâce à un usage délictueux de l'informatique ou visant les systèmes informatiques eux-mêmes, il ne fait aucun doute que le droit pénal doit être pris en considération dans le cadre des moyens visant à assurer la sécurité du patrimoine informatique et informationnel de l'entreprise.

Mais en même temps, le recours plus systématique aux actions en justice pour désigner un coupable ainsi que la loi Informatique et libertés rendent le DSI plus vulnérable.

3.3.1 Les risques liés au système d'information

À l'instar des dirigeants d'entreprises, la responsabilité civile et pénale des DSI est de plus en plus souvent invoquée devant les tribunaux, qui peuvent même infliger des peines de prison. Au premier chef, les DSI se trouvent confrontés à de nouvelles problématiques liées à la sécurité du système d'information et à l'utilisation des nouveaux outils de communication, notamment en interne.

3.3.1.1 L'étendue du risque informatique

Le risque est, classiquement, évalué matériellement. C'est le cas du risque informatique puisque au départ, avec les serveurs centraux et autres outils informatiques, la valeur se concentre dans le matériel. Ce n'est qu'à partir des années 80 que le logiciel, bien immatériel, va avoir une valeur propre, indépendamment du matériel duquel il se détache. Cette tendance va s'exacerber dans les années 90 avec la

multiplication des progiciels, les intégrations, les mises en réseau. Il y a alors complexification mais en même temps fragilisation des systèmes informatiques. Il s'agit dès lors de protéger non plus un bien matériel mais un bien immatériel dont les entreprises se sentent fortement dépendantes.

Cet élément immatériel a d'ailleurs une grande valeur industrielle, faisant l'objet d'investissements importants, mais il reste pourtant protégé par le droit d'auteur. Le législateur a toutefois pris en compte la nécessité de protéger cet investissement pour les bases de données alors même que la création n'est pas originale, avec la loi de 1998. En dehors de cette loi, la prise en compte du risque informatique reste encore largement négligée et sa valorisation bien aléatoire.

Lors d'un entretien juridique du Cigref, un avocat spécialisé en droit des nouvelles technologies a mis en exergue le fait que les risques liés à l'informatique sont très largement sous-estimés. D'un point de vue technique, si sur le plan formel certaines mesures sont prises (antivirus, procédures de sauvegarde...), sur un plan pratique le respect de ces procédures n'est pas rigoureux. D'autre part certaines mesures sont souvent négligées (protection électrique et dispositifs incendies, sensibilisation et formation du personnel...). Le risque de sinistre en série du fait de l'interconnexion des réseaux est lui aussi largement négligé.

En outre, d'un point de vue contractuel, la protection est souvent insuffisante. Le simple fait qu'il y ait un contrat ne permet pas de conclure que l'on est protégé. Généralement, ces contrats peuvent être qualifiés de « contrats types » et ne prennent pas en compte les spécificités du client. La gestion du risque informatique reste souvent insatisfaisante puisque les clauses limitatives de responsabilité ne sont pas toujours éliminées.

Quant aux contrats d'assurance, malgré leurs intitulés (« globale informatique »...), leur contenu est rapidement rendu obsolète par l'évolution des techniques et des moyens mis en œuvre, et la difficulté à prendre en compte la dimension immatérielle du système d'information.

L'appréhension des risques informatiques est d'autant plus difficile qu'ils peuvent revêtir une multitude de formes. Ce sont en effet à la fois :

- des risques internes et externes ;
- des risques métier et des risques technologiques ;
- des risques liés aux personnes, aux procédures, aux protocoles, aux matériels ;
- des risques connus et des risques inconnus ;

- des risques supportables ou non ;
- des risques prévisibles ou imprévisibles ;
- des risques maîtrisables ou non.

De l'avis du Gartner, il n'y a pas en France de gestion du risque juridique lié aux nouvelles technologies, contrairement aux pays anglo-saxons, où la gestion de ce risque est appréhendée par des cellules de gestion des risques. Et cette situation devrait perdurer une dizaine d'années encore !

3.3.1.2 Les acteurs de l'appréciation du risque informatique

Entreprendre, produire, diriger, autant de sources de mise en cause de la responsabilité civile et pénale des dirigeants, renforcées par l'émergence de nouveaux risques, notamment informatique. La gestion des risques est devenue partie intégrante de la fonction managériale.

Bien souvent, il existe une relation forte entre les risques industriels liés aux produits (par exemple la chaîne de production) et les risques liés au support informatique (par exemple les bases de données, pour la traçabilité des produits). Cette interdépendance dans l'entreprise des risques industriels et informatiques nécessite que l'outil de gestion des risques intègre une « typologie des risques informatiques ».

Le « *risk management* » peut être le fait d'une direction à part entière. Elle peut également être le fait de la direction des assurances. Dans l'un et l'autre cas, de par sa connaissance de l'entreprise et des possibilités techniques d'attaques de toutes natures, le DSI est en mesure d'avoir une vision globale du patrimoine à protéger et d'établir la cartographie des risques informatiques. Dans les domaines dont le DSI à la charge, il peut utilement définir les risques qu'il lui incombe de prévenir.

Dans le cas particulier des catastrophes, les analystes du Meta Group[7] en appellent à la responsabilité des DSI pour mettre au point les plans de rétablissement après désastre. Objectifs pointés : éviter la destruction des données et la disparition des processus de traitement. Pour ce faire, la direction de l'entreprise devrait notamment s'assurer que ledit plan soit correctement documenté et communiqué.

3.3.2 Le délit de manquement à la sécurité du système d'information

Le délit de manquement à la sécurité du système d'information est mentionné dans l'article 226-17 du nouveau Code pénal.

Le premier niveau repose sur une batterie d'obligations légales incontournables, qu'il faut absolument connaître. Citons, parmi les plus importantes, les déclarations à la Cnil, l'information des

[7] Dans une note de septembre 2001.

salariés et du comité d'entreprise sur les mesures de surveillance et les limites d'utilisation des outils de type internet, messagerie, etc.

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 ».

3.3.2.1 La sécurité physique du système d'information

La nature des atteintes

Sur la base d'une enquête réalisée en 2002 par le Cigref auprès de ses membres, on constate que les principales attaques proviennent de facteurs extérieurs tels que les virus, les attaques par déni de service, etc. On assiste donc à une inversion des tendances puisque, historiquement, les grandes entreprises estimaient que les risques internes étaient plus élevés.

Les motivations des pirates sont nombreuses, qu'il s'agisse du casseur (qui détruit pour le plaisir), du démonstratif (qui cherche avant tout à faire savoir qu'il existe des failles de sécurité), du pirate fraudeur, du pirate voleur... Et pourtant, aux yeux de la loi, chacun appartient à une grande et même famille, celle des auteurs d'infractions à des systèmes de traitements automatisés de données et chacun d'entre eux peut être poursuivi au regard des dispositions du Code pénal en matière de fraude informatique.

Un droit à la sécurité

Au premier rang de ce véritable « droit à la sécurité », on notera les dispositions du Code pénal protectrices des systèmes de traitements automatisés de données, c'est-à-dire « tout ensemble composé d'une ou plusieurs unités de mémoires, de logiciels, d'organes d'entrées-sorties, et de liaisons qui concourent à un résultat déterminé ». Les dispositions du Code pénal permettent ainsi de lutter contre les intrusions frauduleuses (connexion pirate, appel d'un programme ou d'un fichier sans autorisation…), le maintien frauduleux, l'entrave d'un système ou l'altération de son fonctionnement (virus, « *mail bombing* »...), sans oublier l'altération, la suppression ou l'introduction de données pirates.

D'autres réglementations complètent le dispositif, et notamment la loi du 10 juillet 1991 sur le secret des correspondances émises par voie de télécommunications, la loi sur la sécurité quotidienne du 15 novembre 2001 ou encore la loi du 6 janvier 1978, dite Informatique et libertés, qui impose pour sa part la sécurité des traitements de données nominatives.

La politique des entreprises

La problématique pour l'entreprise est la suivante :

- Comment concilier l'ouverture de l'entreprise avec la sécurité du système d'information ?
- Comment trouver un compromis entre le coût d'un système d'information respectant les règles de sécurité et sa performance ?

Si les règles sont bien présentes, encore faut-il que les entreprises adoptent un certain nombre de mesures et précautions pour garantir un « niveau de risque acceptable », prenant en compte l'environnement technique, humain, organisationnel et réglementaire de l'entreprise. Car de l'avis unanime des DSI, il est impossible de garantir un niveau de sécurité à 100 %.

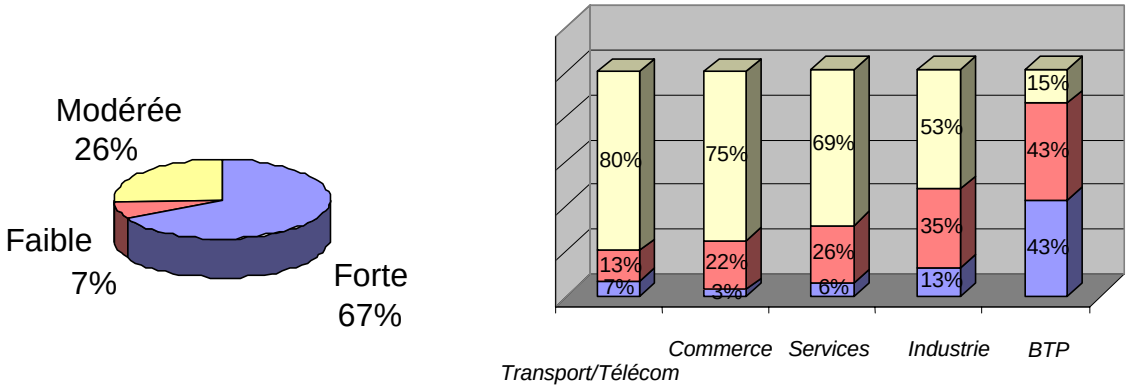
Dans ce domaine, c'est la loi de Pareto qui s'applique : il faut dépenser 20 % d'énergie pour 80 % d'efficacité. Les mesures de sécurité étant souvent coûteuses et contraignantes, leur mise en œuvre doit être adaptée aux réels enjeux. Mais la politique de sécurité souffre encore d'un problème de légitimité dans l'entreprise. Elle est souvent vue uniquement comme un poste de coût par la direction générale, alors que les risques en termes d'image, de dommages financiers et d'immobilisation peuvent être très élevés.

Une enquête réalisée par le Clusif (Club de la sécurité des systèmes d'information français) auprès d'un panel de 450 entreprises en 2001 met en évidence que les sinistres informatiques ont coûté 1,14 milliard d'euros aux entreprises privées françaises. Toutefois, seule une entreprise sur dix évalue systématiquement l'impact financier d'un sinistre.

La dépendance aux systèmes d'information

La pratique révèle une augmentation des risques de survenance de sinistres informatiques liée à la dépendance des entreprises à leur système d'information.

L'enquête du Clusif rapporte que les entreprises s'estiment en majorité très dépendantes de l'informatique, qui a pris une place majeure dans la bonne marche des activités. 67 % d'entre elles estiment avoir une dépendance forte à leur système d'information.



Source : Clusif

Figure 7 : La dépendance au système d'information, par secteur d'activité.

Les priorités des grandes entreprises

La prise de conscience des grandes entreprises des enjeux de la sécurité ne date pas d'hier mais elle a pris une nouvelle envergure. En effet, la dématérialisation des échanges et le passage de l'entreprise étendue à l'entreprise virtuelle a renforcé les besoins des directions des systèmes d'information en matière de sécurité.

Interrogées en 2002 sur leurs priorités en matière de sécurité, les grandes entreprises membres du Cigref jugent prioritaires la réactualisation des plans de secours, refonte de la politique de sécurité, sensibilisation des utilisateurs.

Pour les années suivantes, ces entreprises entendent axer leurs efforts sur l'élaboration et la mise en place de tableaux de bord, la définition d'architectures de sécurité et la gestion des annuaires.

3.3.2.2 La sécurité juridique du système d'information

Les dirigeants doivent se mettre en conformité avec les lois et réglementations applicables. Cette responsabilité comprend :

- l'identification des exigences auxquelles la structure et son personnel doivent se conformer ;
- la mise en place d'un système élaboré pour arriver à cette conformité du système d'information à la loi.

Les peines encourues sont lourdes. En matière d'atteinte aux droits de la personne résultant des fichiers et traitements automatisés, on peut relever :

- La loi du 16 décembre 1992 :

  Le délit d'entrave à l'action de la Cnil (refus de vérification sur place, dissimulation ou destruction de pièces, informations transformées avant son passage) est puni d'un an de prison et de 15 245 € d'amende.

- Le décret du 23 décembre 1981 :

  Contravention pour avoir « recueilli ou fait recueillir des informations nominatives, oralement ou par voie de questionnaires, sans avoir informé la personne interrogée du caractère facultatif ou obligatoire des réponses, des personnes physiques ou morales destinataires, ainsi que l'existence d'un droit d'accès ou de rectification ».

- Art. 226-16 du NCP[8] :

  Procéder ou faire procéder, y compris par négligence, à des traitements automatisés d'informations nominatives sans les formalités légales préalables [3 ans, 45 735 €].

- Art. 226-17 du NCP :

  Procéder ou faire procéder à un tel traitement sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations, et notamment qu'elles soient déformées, endommagées ou communiquées à des tiers non autorisés [5 ans, 304 898 €].

- Art. 226-19 du NCP :

  Interdiction de faire figurer, sans l'accord exprès de l'intéressé, directement ou indirectement, les origines raciales, ou les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales ou les mœurs des personnes [5 ans, 304 898 €].

- Art. 226-21 du NCP :

  Détourner les informations collectées de leur finalité [5 ans, 304 898 €].

  Ces lois françaises ne s'appliquent qu'aux fichiers implantés sur des matériels en place sur le territoire métropolitain et ne règlent pas la difficulté liée aux fichiers « internationaux ».

[8] Nouveau Code pénal.

La nature de l'obligation du DSI

Un DSI ne peut être inculpé du seul fait qu'une attaque informatique n'a pas pu être repoussée. Les textes sont sur ce point très clairs : c'est une obligation de moyens, et non de résultat. L'essentiel est de prouver qu'on a pris les précautions « *nécessaires et suffisantes* » pour protéger le système d'information et ses données.

Par exemple, l'installation pure et simple d'un pare-feu ne suffit pas. Si ce dernier n'est pas géré, il ne sert à rien. En revanche, les plans informatiques de l'entreprise doivent impérativement inclure un volet relatif à la sécurité, notamment en ce qui concerne la confidentialité des données personnelles.

L'auteur de la plainte

Lorsque des dommages sont causés à des tiers par suite d'un manquement à la sécurité du système d'information, ces derniers peuvent bien évidemment porter plainte et ainsi déclencher une procédure pénale à l'encontre du dirigeant. Mais le ministère public est également habilité à déclencher cette procédure, même en l'absence de plainte.

Les risques en cas de défaut de sécurité

Ce que les directions générales ignorent encore bien souvent, c'est qu'elles risquent de lourdes peines, allant jusqu'à 5 ans d'emprisonnement et 304 898 € d'amende. Sans compter les réparations des dommages subis par l'entreprise ou les tiers. Au cours de l'année 2001, trois dirigeants ont été mis en cause pénalement pour un délit de manquement à la sécurité. L'un d'entre eux a été mis en examen, puis condamné à une sanction pénale.

3.3.3 La recherche de la responsabilité

Le manquement à la sécurité du système d'information est sanctionné. Dans ce domaine, et par exception, l'entreprise en tant que personne morale peut voir sa responsabilité pénale engagée. Mais celle-ci peut légalement se retourner vers ses salariés, par le jeu des délégations consenties.

3.3.3.1 La responsabilité de l'entreprise

En principe, seul l'auteur personne physique répond de ses fautes pénales. Mais dans de nombreux cas désormais (ex. : contrefaçons de logiciels, atteintes aux systèmes informatiques, violations de la loi Informatique et libertés sur la protection des fichiers nominatifs), la personne morale qu'est la société peut voir sa responsabilité pénale engagée.

L'article 121-2 du nouveau Code pénal, entré en vigueur en mars 1994, pose le principe de la responsabilité pénale des personnes morales : la personne morale peut voir sa

responsabilité pénale engagée « si l'infraction a été commise pour son compte par l'un de ses organes ou représentants ».

Les sanctions pénales sont lourdes : l'article 323-6 du nouveau Code pénal prévoit une amende dont le taux est égal au quintuple de celui prévu pour les personnes physiques.

Qu'elle soit civile ou pénale, la mise en cause de la responsabilité de cette 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 ».

Par ailleurs, préposé de l'entreprise, le salarié causant un préjudice à autrui par l'intranet ou l'internet interposé engage la responsabilité civile de son commettant, qui est dans la plupart des cas assuré en ce sens.

Exception : si le salarié a agi « hors de ses fonctions, sans autorisation et à des fins étrangères à ses attributions ». Mais le salarié surfant pendant le temps de travail et à partir du matériel de l'entreprise n'entre pas dans le champ de cette exception, appréciée strictement par la Cour de cassation afin de protéger la victime du dommage (solvabilité + assurance exploitation de l'entreprise). L'entreprise personne morale peut ainsi être civilement sanctionnée en tant que commettant.

3.3.3.2 Le jeu des délégations

Au vu de la structure de plus en plus complexe des entreprises, l'employeur est dans l'incapacité de tout contrôler lui-même et peut opter pour des délégations de pouvoir afin de dégager sa responsabilité pénale.

Mais si les tribunaux ont admis ce principe, cela se fait dans un cadre étroitement vérifié tant sur la forme que sur le fond.

Depuis 1993, la Cour de cassation a unifié sa position, considérant 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 rapporte la preuve qu'il a délégué ses pouvoirs à une personne pourvue de la compétence, de l'autorité et des moyens nécessaires ».

Selon le Lamy social 2000 : « La délégation, lorsqu'elle est établie, exonère l'employeur qui ne peut être pénalement poursuivi sur le fondement des textes sanctionnant les règles de sécurité. »

La compétence recouvre des connaissances techniques et juridiques nécessaires à l'exécution de la fonction. Une circulaire ministérielle du 2 mai 1977 énumère les questions qui doivent se poser pour vérifier la réalité de cette compétence :

- quelle formation ?
- quelle qualification ?
- quelle est sa capacité pour veiller à l'application des textes tant sur le plan technique que sur le plan juridique ?

Les professionnels du droit s'accordent à dire qu'une délégation de responsabilité pénale stipulée de manière conventionnelle, sous la forme d'un écrit, a plus de poids auprès d'une juridiction éventuellement saisie pour connaître de l'existence réelle de la délégation. L'acceptation expresse de la délégation présume en effet que le salarié a accepté en pleine connaissance des conséquences.

3.4 Conclusion

Le droit et l'informatique, deux domaines historiquement et culturellement éloignés, trouvent un terrain de rapprochement dans le monde de l'entreprise, par le biais de :

- l'organisation de la ressource juridique permettant de faire du droit un outil stratégique ;
- la sécurité juridique du système d'information.

La responsabilité du DSI en la matière découle de ses fonctions :

- il garantit la transversalité de l'information juridique par la cohérence et l'efficacité du système d'information ;
- il garantit la sécurité du système d'information par des dispositifs techniques et le respect d'un certain nombre d'obligations légales.

Le DSI est donc, dans le cadre de ses fonctions, concerné par le droit. Comment prévenir les risques juridiques liés au système d'information ? C'est l'objet de la seconde partie de ce rapport.

4. COMMENT LE DSI PEUT-IL PRÉVENIR LES RISQUES INFORMATIQUES ?

Afin d'aider les DSI à mieux cerner les nouveaux contours de leur responsabilité spécifique au plan juridique et à prévenir les risques informatiques, le Cigref a élaboré dans le cadre de son plan d'action un cycle juridique.

On y trouve tout d'abord une série de conférences : « Les Entretiens juridiques du Cigref » réunissant des DSI, des directeurs juridiques et leurs collaborateurs autour d'un intervenant, professionnel du droit des nouvelles technologies, avocat ou expert, sur des thèmes d'actualité tels que la propriété intellectuelle ou le traitement des données personnelles. Une réflexion a par ailleurs été menée en liaison avec l'Isoc[9] , le Medef[10] et la CCIP[11] sur le thème des noms de domaine.

Une façon de prévenir les risques informatiques consiste par ailleurs à négocier avec vigilance avec les fournisseurs de services ou produits informatiques. Les contrats informatiques ont leurs particularités, leurs clauses notamment sont à étudier scrupuleusement.

Enfin, au-delà de l'information et de la négociation des contrats, il convient de mettre en place des moyens de prévention adaptés à l'entreprise et aux risques décelés.

4.1 S'ouvrir au droit des nouvelles technologies

Ses différentes missions situent le DSI au carrefour de tous les aspects du droit, l'obligeant à connaître le droit de la propriété intellectuelle, le droit relatif aux bases de données, le droit spécifique aux logiciels, le droit sur l'informatique et les libertés, le droit du travail.

L'entreprise est riche en effet d'un patrimoine informatique entouré de règles juridiques et d'outils spécifiques que le DSI ne peut négliger sous peine de voir sa responsabilité engagée.

4.1.1 Valeurs informatiques et propriété

Les aspects juridiques prennent une place de plus en plus importante dans l'activité de la DSI. La DSI doit notamment anticiper de nouveaux sujets de préoccupation tels que la propriété intellectuelle. Celle-ci s'attache aux bases de données, aux logiciels et aux noms de domaine.

[9] Internet Society.
[10] Mouvement des entreprises de France.
[11] Chambre de commerce et d'industrie de Paris.

4.1.1.1 Les bases de données

Très souvent, les entreprises ont des bases de données mais elles ne le savent pas ; ou plus exactement, elles le savent mais elles n'ont pas toujours conscience qu'il s'agit là d'un actif issu de l'entreprise, sur lequel sont nés des droits privatifs pouvant être valorisés ou cédés, constituant ainsi un actif de valeur dans le commerce juridique.

La loi n° 98-536 du 1er juillet 1998 définit la base de données comme « un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen. »

Les bases de données sont protégées par deux techniques juridiques distinctes et cumulables :

- le droit d'auteur protège la forme de la base de données en tant qu'œuvre de l'esprit, si celle-ci est originale : « l'originalité résulte du choix et de la disposition des matières » ;
- un droit *sui generis*[12] protège le contenu informationnel de la base indifféremment du critère d'originalité.

Le droit d'auteur

Avec le droit d'auteur, c'est le contenant qui est protégé. Ce contenant est en pratique difficile à distinguer du logiciel qui anime la base. C'est pourquoi bien souvent la protection du logiciel, assurée elle aussi par le droit d'auteur, couvrira indifféremment le logiciel lui-même et la base prise en tant que contenant.

Le producteur de la base de données est-il investi des droits d'auteur ? La question se pose car on sait que les personnes morales ne peuvent bénéficier des droits d'auteur, sauf « œuvre collective et œuvre logicielle créée par des salariés ».

Il est donc important de savoir s'il est possible de qualifier la base en œuvre collective. L'article L.113-2 du CPI[13] précise qu'« une œuvre est collective quand elle est créée sur l'initiative d'une personne physique ou morale qui l'édite, la publie et la divulgue sous sa direction et son nom et dans laquelle la contribution personnelle des divers auteurs participant à son élaboration se fond dans l'ensemble en vue duquel elle est conçue, sans qu'il soit possible d'attribuer à chacun d'eux un droit distinct sur l'ensemble réalisé ».

[12] Droit particulier ou unique en son genre.
[13] Code de la propriété intellectuelle.

Or une base de donnée est le plus souvent réalisée par le travail de plusieurs personnes sans qu'il soit possible d'identifier la participation de chacun, sous la direction de la personne morale qui la diffusera. Cette définition est complétée par l'article L.113-5 du CPI aux termes duquel « *l'œuvre collective est, sauf preuve contraire, la propriété de la personne physique ou morale sous le nom de laquelle elle est divulguée* ». Cette personne est investie des droits de l'auteur. Il est toutefois vivement conseillé de prévoir contractuellement la dévolution des droits avant d'envisager la licence de mise à disposition de la base de données.

Le droit sui generis

Le droit *sui generis* propre aux bases de données peut être présenté comme le droit d'interdire l'extraction ou la réutilisation du contenu de la base.

L'article L.341-1 du CPI prévoit pour les contrevenants une sanction pénale de 152 450 millions d'euros et de 2 ans d'emprisonnement. C'est donc une action au pénal que le producteur de la base doit intenter, en tant que « propriétaire ».

Ce droit de propriété particulier est reconnu au fabricant de la base, c'est-à-dire à celui qui a pris « l'initiative et le risque des investissements correspondant à sa création ».

Le titulaire du droit peut donc être différent de celui qui détient les droits d'auteur sur une même base de données. Par exemple, si l'entreprise n'a pas pris quelques précautions, un salarié pourrait très bien être investi des droits d'auteur sur la base de données alors que ce sera l'employeur qui sera titulaire du droit *sui generis*. Une situation complexe qui peut amener des conflits.

Par ailleurs, le producteur a le droit d'interdire la réutilisation et l'extraction « qualitativement ou quantitativement substantielle » (article L.342-1 du CPI) du contenu de la base de données. L'article L.342-2 du CPI précise que « le producteur peut interdire l'extraction ou la réutilisation répétée et systématique de parties qualitativement ou quantitativement non substantielles du contenu de la base lorsque ces opérations excèdent manifestement les conditions d'utilisation normale de la base de données. »

Il est donc possible pour les utilisateurs de la base d'en extraire des parties non substantielles, qualitativement ou quantitativement du contenu de la base. Reste à définir ce qui est ou non une extraction ou une réutilisation « substantielle ». La jurisprudence considère que ce critère doit s'apprécier en fonction de l'utilisation faite des données extraites, ce qui se justifie par le but de cette loi qui, rappelons-le, participe d'une

logique visant à limiter les actes de concurrence déloyale et de parasitisme.

4.1.1.2 Les logiciels

Les logiciels sont des objets de propriété intellectuelle. En connaître les contours juridiques est essentiel pour négocier efficacement les contrats informatiques y afférant.

Le statut juridique des logiciels

Ils sont considérés comme « œuvres de l'esprit » (art. L112-2 CPI) et, à ce titre, protégés par le droit d'auteur.

LOGICIEL	NON LOGICIEL
Travaux préparatoires	Cahier des charges
Codes sources	Algorithmes et fonctionnalités
Documentation technique	Documentation utilisateur
Documentation en ligne	

Source : Cigref

Figure 8 : Le logiciel.

Le droit d'auteur ne protège que la forme, pas les idées.

Dès lors, pour que le cahier des charges ne soit pas récupéré par les concurrents, il devra être protégé indépendamment du logiciel auquel il se rapporte. Il pourra donc faire l'objet d'une protection par le droit d'auteur s'il répond à la condition d'originalité, ou par le contrat grâce à une clause de confidentialité se rapportant à ce document.

Par ailleurs, le droit d'auteur ne protège pas l'intégralité du logiciel ; il exclut notamment les idées, fonctionnalités et algorithmes puisque le droit d'auteur ne protège que la forme et non le contenu. En tant qu'idées, les algorithmes et fonctionnalités ne peuvent pas être protégés, les idées étant de libre parcours. Pour faire valoir un droit sur un algorithme ou une fonctionnalité, il n'y a donc que la voie de la concurrence parasitaire ou déloyale, si la reprise est massive et servile.

L'originalité est la condition nécessaire et suffisante de la protection des logiciels par le droit d'auteur.

L'originalité s'apprécie dans la forme :

- spécifications internes (conception, suite d'instructions, architecture) ;
- spécifications externes (ergonomie).

ORIGINAL	PAS ORIGINAL
Effort personnalisé	Contrainte logique
Liberté de choix	Contrainte métier
Original	Antériorité

Source : Cigref

Figure 9 : Les caractéristiques du logiciel.

L'effort personnalisé est ainsi caractérisé quand l'écriture ne répond pas à une contrainte logique.

La recherche de ce caractère original du logiciel est surtout importante dans les cas de contentieux pour contrefaçon.

Les prérogatives de l'auteur

L'auteur a sur son logiciel :

- un droit moral, essentiellement constitué du nom ;
- un droit d'exploitation, c'est-à-dire le droit d'effectuer ou d'autoriser :
  - la reproduction ;
  - l'adaptation ;
  - la mise sur le marché à titre onéreux ou gratuit.

Les sanctions de la violation du droit d'auteur se traduisent par des actions en contrefaçon ou en concurrence déloyale.

Les droits du DSI sur les logiciels n'appartenant pas à l'entreprise

Celui qui acquiert un bien intellectuel n'acquiert pas pour autant les droits de propriété intellectuelle sur celui-ci. Tel est le cas du logiciel, dont la licence ne confère en aucun cas le droit moral de l'auteur, qui est incessible, ni même les droits d'exploitation qui eux sont cessibles par contrat, mais que l'on oublie bien souvent de céder.

Cette situation est souvent ignorée en pratique par les non juristes. Il est pourtant nécessaire, lors de la négociation d'un contrat portant sur un bien immatériel, et en particulier un logiciel, de savoir quels sont les droits à prendre en compte, faute de quoi tout son investissement peut se trouver anéanti. De plus, en méconnaissant ces droits (par exemple en effectuant une reproduction ou une adaptation du logiciel sans autorisation), on devient contrefacteur et passible de sanctions pénales.

L'utilisateur a sur le logiciel :

- un droit d'adaptation et de correction ;
- un droit à une copie de sauvegarde ;
- un droit de décompilation.

La reproduction et l'adaptation ne sont pas soumises à autorisation de l'auteur :

- lorsqu'elles sont nécessaires à l'utilisation du logiciel conformément à sa destination ;
- y compris pour corriger les erreurs.

Mais l'auteur peut par contrat :

- se réserver le droit de correction d'erreurs ;
- encadrer le droit d'utilisation.

Contrairement par exemple au MP3, il est interdit de copier un logiciel pour un usage privé. Le législateur a cependant autorisé la copie de sauvegarde, très utile en cas de défaillance, « pour préserver l'utilisation du logiciel ».

Le droit de décompilation consiste en la reproduction du code, indispensable pour obtenir les informations nécessaires à l'interopérabilité du logiciel avec d'autres logiciels. Mais il est interdit de créer un logiciel d'expression substantiellement similaire. En pratique, il n'est pas toujours facile d'intervenir sur les logiciels, car aucune obligation n'est faite à l'auteur de communiquer les codes sources.

La cession des droits d'auteur

L'acquisition des logiciels réalisés hors de l'entreprise est très réglementée.

Règles de forme

L'écrit n'est pas exigé comme condition de validité mais de preuve.

Les droits cédés doivent être énumérés. La lecture du contrat se fait toujours à l'avantage de l'auteur. Un droit qui n'est pas cédé expressément ne pourra pas être revendiqué. Inversement, une clause trop générale ne peut pas répondre aux exigences strictes de l'article L. 131-3 du CPI. Il est donc important de prévoir ce qui fait l'objet de la cession : droits d'adaptation (modifications, intégrations dans d'autres logiciels...), de reproduction (un ou plusieurs exemplaires...), de distribution...

Quant au mode d'exploitation envisagé, il faut ici prévoir le droit de représentation, de distribution (par exemple sur CD-Rom, en ligne...), la destination (commerciale ou non), le lieu, la durée.

Règles de fond

Il est interdit de céder des œuvres futures. Mais on peut toujours céder ce qui n'existe pas encore, à la condition de le préciser dans le contrat.

Si le contrat a pour objet la réalisation d'un logiciel précis, il n'y a donc pas de problème.

Si plusieurs logiciels ou développements sont réalisés dans le cadre de relations régulières, il est judicieux de raisonner de la même façon que dans un contrat cadre. Un contrat général va poser le principe de la cession, alors même que l'on ne sait pas encore ce qui va être fait. Puis, lors de la commande d'œuvres, il suffira de rappeler la clause dans le bon de commande et de l'adapter aux besoins du contrat spécifique.

De même, il semble qu'une entreprise puisse valablement prévoir un contrat de cession global avec son salarié, limité à la durée du contrat et aux œuvres commandées par l'employeur. Mais il est déconseillé de prévoir de faire signer un contrat pour chaque œuvre avec le risque de l'oublier. Cette clause de cession avec les salariés ne présente pas grand intérêt avec les informaticiens, mais elle est utile avec les salariés auteurs de créations autres que les logiciels *stricto sensu* (par exemple les infographistes).

La question suivante a été posée au cours des Entretiens juridiques : « Que négocier lorsque l'on commande des développements spécifiques qui doivent s'ajouter à un progiciel ? Bien souvent, le nombre d'heures passées est très important, le coût s'en ressent, mais on ne souhaite pas en faire bénéficier la concurrence. Le prestataire considère de son côté que ces développements sont mêlés à des parties de logiciels standard et ne peuvent donc pas être cédés. »

Il a été répondu qu'en pratique, le client ne souhaite pas nécessairement exploiter commercialement les travaux réalisés. Il peut donc accepter que ce droit revienne à la société de service en contrepartie de redevances ou encore de la gratuité de la maintenance pour une durée déterminée.

Par ailleurs, lorsque l'on acquiert des droits de propriété intellectuelle sur un logiciel, il est nécessaire de savoir à quel moment on devient titulaire de ces droits. En effet, le contrat rédigé par le prestataire prévoit souvent que le transfert de propriété n'a lieu qu'après complet paiement du prix. Pour l'utilisateur, ce moment peut ne pas lui être favorable, puisqu'en cas de problème lors de la réalisation du logiciel, ce dernier souhaitera certainement que la prestation soit finie par un autre.

Pour éviter cet écueil, il faut d'abord prévoir une cession au fur et à mesure des réalisations et prévoir ensuite qu'en cas de rupture fondée sur la faute du fournisseur, le contrat pourra être

achevé par un tiers. Le logiciel, même non achevé, est en effet protégeable par le droit d'auteur ; donc pour qu'il puisse être modifié, il faut que le contrat le prévoit.

La preuve de la titularité des droits

Le titulaire des droits doit être en mesure de prouver ses droits. Pour cela, si on est auteur ou titulaire de droits de propriété intellectuelle sur un logiciel, il est très fortement conseillé d'en déposer les codes sources auprès d'un organisme compétent (ex. l'APP[14]). Ce dépôt permet de bénéficier d'une date certaine, utile en cas de contestation du logiciel sur le fondement de la contrefaçon.

Ce titulaire pourra aussi faire valoir le copyright ©, notion issue du droit américain et qui permet de présumer la titularité. Il est donc recommandé de prévoir ce sigle sur les œuvres susceptibles de bénéficier de sa protection. Pour cela, il n'y a pas de conditions de forme particulières ; il est toutefois recommandé de préciser au minimum le titulaire des droits, la date de création (d'où l'importance du dépôt pour avoir une date certaine) et le symbole ©.

Quant à l'utilisateur, il peut se prévaloir de certains droits qui lui sont légalement reconnus. Ainsi, quatre droits sont prévus à l'article L. 122-6-1 du CPI (adaptation, analyse, copie de sauvegarde, décompilation). Ces droits ont cependant une portée relative puisqu'ils sont susceptibles d'aménagements conventionnels, aménagements qui, en pratique, réduisent systématiquement les droits de l'utilisateur.

Par exemple, le droit d'adaptation peut être expressément réservé à l'auteur. Même quand ce n'est pas le cas, le droit d'adaptation est de portée limitée puisqu'il n'y a aucun droit de l'utilisateur d'accéder aux codes sources. La jurisprudence est sévère, même s'il s'agit de logiciels spécifiques (une exception toutefois pour le cas d'un logiciel spécifique développé par une SSII mise en liquidation).

De même, le droit ne prévoit qu'une copie de sauvegarde ; si l'utilisateur souhaite en faire plus, il est préférable de le prévoir par contrat.

Quant à l'utilisation de ces copies, la loi est silencieuse, et le contrat peut donc utilement prévoir leur destination, par exemple la possibilité de les implanter sur des configurations de test ou d'archivage.

Il n'y a donc que le droit de décompilation qui soit d'ordre public. Mais les conditions de la mise en jeu de ce droit sont strictement encadrées et une utilisation en dehors du périmètre

[14] Agence pour la protection des programmes.

de l'article L. 122-6-1.IV du CPI peut être constitutive d'une contrefaçon.

L'accès aux codes sources

L'approche par progiciels de gestion intégrés constituant aujourd'hui une part importante des projets informatiques, la garantie de pérennité est devenue une clause déterminante : il n'est pas possible de s'engager sur un progiciel pour seulement une année d'utilisation garantie. Dans ce cadre, l'accès aux sources est davantage un moyen d'assurer une transition qu'une vraie possibilité de maintenir la pérennité de l'utilisation. Il est certain que les contrats de licence portent, en général, sur la durée de protection du droit d'auteur. Mais dans ce cas, le contrat de maintenance, qui prend effet aux termes de la garantie, n'est en général que d'un an.

La situation est parfois encore plus préoccupante pour les progiciels commercialisés avec l'option « *année par année* », et dans lesquels la redevance inclut le droit d'utilisation et les mises à jour. Dans les projets d'une certaine envergure, il est en effet important de disposer d'une garantie de pérennité, qui est en général de 3 ans. Cette garantie comprend une double obligation, imposant à l'éditeur le maintien de la commercialisation du produit pendant 3 ans à compter de la signature du contrat d'une part, et l'obligation de fournir une maintenance associée d'autre part. En cas d'annonce de l'arrêt de la distribution, le fournisseur doit cependant s'engager à poursuivre le contrat de maintenance au minimum 2 ans. Une telle organisation contractuelle permet aux sociétés de disposer d'une période de 5 années.

L'accès aux sources, qui est en général extrêmement difficile à mettre en œuvre, a pour objet de pallier un éventuel arrêt de la maintenance s'agissant de bogues extrêmement bloquants. Une telle clause doit être accompagnée de la mise à disposition de spécialistes ou, pour le moins, d'un processus de transfert de savoir-faire. En tout état de cause, il faut pouvoir y accéder, même si l'éditeur défaillant cède ses droits sur le progiciel, de telle manière à pouvoir disposer d'une alternative entre l'accès aux sources et l'acceptation éventuelle d'un repreneur.

En conclusion, le DSI doit toujours vérifier que la garantie de pérennité est assurée par une clause spécifique d'accès aux codes sources.

La brevetabilité des logiciels

L'origine du débat

Le débat, qui existe depuis des années, a pris une ampleur particulière depuis que la Commission européenne a présenté, le 20 février 2002, une proposition de directive concernant la brevetabilité des « inventions mises en œuvre par ordinateur ».

La brevetabilité des logiciels est actuellement déterminée par l'article 52 de la CBE[15] : les programmes d'ordinateur « en tant que tels » ne peuvent pas être brevetés.

En effet, procédé intellectuel, le logiciel ne constitue pas une invention car l'algorithme en tant que méthode mathématique n'a pas d'« effet technique » ; or cet effet est une condition *sine qua non* de l'invention.

Droit d'auteur	Brevet
Tous les logiciels	Effet technique
Forme	Fond
Originalité	Nouveauté
Automatique	Dépôt
Publication	Non divulgation
70 ans	20 ans

Source : Cigref

Figure 10 : Les différences entre droit d'auteur et brevet.

Toutefois, depuis 1978, plus de 30 000 brevets ont été accordés par l'OEB[16] sur des logiciels. La majorité de ces « brevets logiciels » concerne actuellement le traitement de données numériques, la reconnaissance de données, la représentation et le traitement de l'information.

Sans réelle surprise, la Commission a décidé de confirmer dans les grandes lignes la jurisprudence de l'OEB. Ainsi, les programmes informatiques « en tant que tels » demeurent non brevetables. Pour être brevetable, une invention mise en œuvre par l'exécution d'un logiciel sur un ordinateur doit présenter l'un des critères suivants :

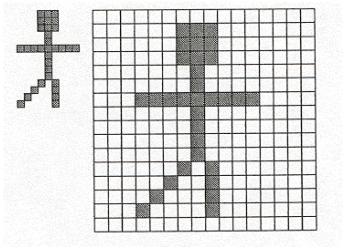
- *effet technique* ;
- *résolution d'un problème technique* ;
- *présence de considérations techniques* ;
- *contribution à l'état de la technique*.

La différence de protection

Prenons un exemple : la compression d'image. Objectif : compression de lignes de bits dont le principe est le suivant : une suite de 0 sera remplacée par un seul 0 suivi du nombre de répétitions de ce pixel. Question : quel type de protection peut-on adopter ?

[15] Convention sur la délivrance des brevets européens.
[16] Office européen des brevets.

Le tableau ci-dessous fait une comparaison entre les deux formes de protection. L'une et l'autre ne protégent en fait pas les mêmes choses.



Le brevet	Le droit d'auteur
Revendication 1 : Procédé de compression d'image en noir et blanc, chaque ligne de ladite image étant constituée de pixels à 0 (noir) ou à 1 (blanc) caractérisé en ce qu'une suite de 0 (resp de 1) sera remplacée par un seul 0 (resp 1) suivi du nombre de répétitions de ce pixel. Revendication 2 : Ordinateur programmé comportant des moyens pour la mise en œuvre d'un procédé de compression d'image en noir et blanc, chaque ligne de ladite image étant constituée de pixels à 0 (noir) ou à 1 (blanc) caractérisé en ce qu'une suite de 0 (resp de 1) sera remplacée par un seul 0 (resp 1) suivi du nombre de répétitions de ce pixel.	Expression de l'algorithme de cette même compression d'image : Pixel, PixelCourant, Nombre = Entiers Début PixelCourant -> LireEntier() Nombre -> 1 Tant qu'il y a des pixels Pixel -> LireEntier() Si Pixel <> PixelCourant Alors AfficherEntier(Pixel) AfficherEntier(Nombre) PixelCourant -> Pixel Nombre -> 1 Sinon Nombre -> Nombre + 1 AfficherEntier(Pixel) AfficherEntier(Nombre) Fin
Méthode mathématique + effet technique (compression d'image, gain de place mémoire...) => protection par brevet possible.	Forme de l'expression du programme => protection par droit d'auteur.
Portée des droits beaucoup plus grande car il permet de poursuivre la contrefaçon "intelligente". Publication, mais pas du code source.	Le logiciel est protégé contre la copie. Comparaison ligne à ligne. Un programme écrit différemment ne sera pas nécessairement la contrefaçon d'un autre programme même s'ils réalisent les mêmes fonctions.

Source : La gazette de la société et des techniques - nov. 2001

Figure 11 : Les différences entre droit d'auteur et brevet : un exemple.

Enjeux pour l'entreprise utilisatrice

Breveter ses innovations n'est pas une obligation et à défaut de brevet, le logiciel sera protégé par le droit d'auteur s'il répond à la condition d'originalité.

Pour les grandes entreprises, le brevet de logiciel est une réalité qu'il est dangereux de négliger. Elles doivent nécessairement s'intéresser à la liberté d'exploitation avant de se lancer dans un projet et effectuer des recherches d'antériorité.

Le débat se développe sur trois terrains.

Le débat juridique Nécessité de clarifier les textes

POUR	CONTRE
L'expression « en tant que tel » doit être comprise comme opposée à « appliqué à ... » (le logiciel comme algorithme n'est pas brevetable, mais il l'est comme solution technique à un problème technique).	Les articles 52 de la CBE et L.611-10 du code établissent clairement l'exclusion.
Le droit d'auteur est destiné à protéger l'expression de l'œuvre et non les concepts qui sous-tendent sa conception ; il y a complémentarité.	Le droit d'auteur comme autre instrument de protection corrobore l'idée d'interdiction des programmes du champ de la brevetabilité.
L'article 27.1 de l'accord ADPIC[17] ne permet pas d'exclure un domaine technologique.	L'accord ADPIC ne précise pas ce qu'est une invention et laisse aux signataires le soin de préciser cette notion.

Le débat moral Des positions irréconciliables

POUR	CONTRE
La propriété industrielle est une forme de la propriété qui constitue une valeur fondatrice de notre société.	On risque la brevetabilité de toutes les activités sociales.
Les logiciels sont de véritables objets ou procédés techniques au même titre que les médicaments ou les moteurs.	Il n'y a pas de frontière entre les logiciels et les idées, puisque les logiciels sont des programmes, les programmes des algorithmes et les algorithmes des idées.
Les CONTRE vivent dans un monde totalement déconnecté des réalités de l'entreprise.	Les POUR sont mercantilistes.
L'essence du logiciel est plus proche du brevet que d'une œuvre de l'esprit.	Le brevet freine l'innovation et va à l'encontre de la logique scientifique de partage des découvertes.

[17] Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce, 15 avril 1994.

Le débat économique À l'étude

POUR	CONTRE
Le logiciel est devenu une industrie à part entière.	Difficulté de recherche documentaire pour les offices de propriété intellectuelle.
Le brevet confère une exclusivité temporaire d'exploitation de l'invention et permet une valorisation des actifs immatériels de l'entreprise.	Le succès du logiciel libre n'aurait jamais été tel si les algorithmes de base avaient été monopolisés par un grand groupe.
Situation actuelle qui favorise ceux qui savent contourner l'exclusion...	Un frein à un certain modèle économique.
... et qui défavorise l'Europe face aux USA et au Japon.	Une multiplication du contentieux (procès à répétition favorisant les plus grandes entreprises).

Source : Cigref

En conclusion, pour les utilisateurs, le brevet peut représenter un coût supplémentaire. En effet, les éditeurs qui ont lourdement investi dans des procédures pour obtenir un brevet, répercuteront leurs dépenses sur le coût des licences[18]. Par ailleurs, il paraît peut probable que le brevet s'accompagne d'une amélioration de la qualité du logiciel[19].

Mais les entreprises membres du Cigref pourront aussi trouver un avantage dans ce brevet. En effet, les entreprises qui réalisent de nombreux logiciels en interne pourront les breveter. Grâce à ces outils, elles obtiendront un avantage concurrentiel en se réservant certaines fonctionnalités.

L'œuvre d'employés

Classiquement, l'auteur est le propriétaire de son œuvre, et l'existence ou la conclusion d'un contrat, par exemple de travail, n'emporte aucune dérogation à la jouissance du droit. Il faut donc un dispositif contractuel précis et explicite pour transmettre à l'employeur les droits en cause.

La loi du 3 juillet 1985 prévoit un régime dérogatoire en matière de logiciel, dans son article 45, article repris et complété par la directive de 1994, intégré en droit français dans l'article L.113-9 du Code de la propriété intellectuelle qui dispose :

« Sauf dispositions statutaires ou stipulations contraires, les droits patrimoniaux sur les logiciels et leur documentation créés par un ou plusieurs employés dans l'exercice de leurs fonctions ou d'après les instructions de leur employeur sont dévolus à l'employeur qui est seul habilité à les exercer. »

[18] Un brevet européen coûte entre 30 000 et 45 000 €. Ce coût élevé est dû aux coûts de traduction de la demande. Il coûte 10 000 € aux USA et 15 000 € au Japon.

[19] Bernard Lang, directeur de recherche à l'Inria, estime, de façon peut-être excessive, que le brevet favorisera les « *bogiciels* », contraction des termes bogue et logiciel (colloque Afdit - 17 juin 2002).

Domaine de l'article L. 113-9 du CPI

Il n'y a donc en principe plus de problème depuis cette loi transférant à l'employeur le droit d'exploitation des logiciels. Mais certains cas résiduels continuent de susciter des difficultés.

Logiciel réalisé par des stagiaires, intérimaires ou salariés en régie

Ce sont des personnes qui restent unies par leur contrat de travail à un tiers (université, école, entreprise d'intérim, SSII...). Les droits sur les développements réalisés reviennent donc en toute logique à leur l'employeur.

En pratique, il est toujours préférable de prévoir contractuellement la cession de l'œuvre. Dans ce cas, il faut veiller au respect des conditions de l'article L. 131-3 du CPI.

Si le prestataire est en régie, deux cas peuvent être distingués. Ce salarié travaille sur une partie spécifique du logiciel. Dans ce cas l'œuvre peut être qualifiée de collective et l'entreprise peut alors être considérée comme l'unique propriétaire. Ce schéma augmente cependant le risque de voir cette entreprise sanctionnée sur le fondement du délit de marchandage.

Dans le second cas, le salarié en régie apporte un savoir-faire que l'entreprise n'a pas. La dévolution des droits doit alors être contractuellement prévue, puisque sa création appartient normalement à son employeur. On remarquera en outre que cette clause favorise l'exclusion du délit de marchandage, puisqu'elle accrédite l'idée que la prestation est représentative d'un savoir n'existant pas en interne.

Les créations en dehors du temps de travail

Le problème est souvent posé. Qu'en est-il du salarié qui développe chez lui un logiciel à partir de l'ordinateur portable mis à sa disposition par son employeur, ou encore, du développement que le salarié installe sur son poste de travail ou même installe sur le poste de ses collègues de bureau ? En matière de brevet, la réponse est réglée par le droit (invention de mission...). Il n'y a cependant rien de tel pour le logiciel ; cependant la jurisprudence va adopter un raisonnement similaire à celui prévu en matière de brevet. Le salarié ne recevra toutefois aucune indemnité. Ici encore il est préférable de prévoir une clause dans le contrat de travail, puis à chaque réalisation.

Les créations commencées avant l'embauche

C'est au contrat d'embauche de prévoir la titularité des droits, sinon, c'est une copropriété entre l'employeur et l'employé.

Il est donc fortement conseillé de prévoir une cession contractuelle. La cession de droits d'auteur doit cependant répondre à certaines exigences énoncées à l'article L. 131-3 du CPI.

Cependant, en ce qui concerne la réalisation d'un logiciel commandé par l'employeur, rappelons que l'auteur sera l'employeur, sauf clauses contraires selon l'article L. 113-9 du CPI.

Le logiciel réalisé par plusieurs entités qui collaborent

Il faut se poser la question de sa qualification conformément à ce que prévoit l'article L. 113-2 du CPI. Il est toujours souhaitable de qualifier cette œuvre de collective, ce qui permet d'attribuer l'ensemble des droits à la personne à l'initiative et sous le nom de laquelle l'œuvre est publiée. À défaut, elle peut être qualifiée d'œuvre composite ou d'œuvre de collaboration. Dans ce type d'œuvre, la gestion des droits est complexe, puisque la règle de l'unanimité s'impose. Il faut éviter autant que possible une telle qualification. Il n'y a en effet, en pratique, qu'un seul exploitant qui doit pouvoir bénéficier de l'exclusivité de la cession. Et malgré le problème des évolutions et modifications, il est toujours préférable d'éviter le système de collaboration. Au besoin, et si l'importance du projet le justifie, les entreprises pourront créer un *joint-venture*.

L'ensemble de ce qui a été doit clairement apparaître dans le contrat de licence ou de cession de logiciel. Ainsi il faut bien distinguer les règles qui gouvernent la forme de celles qui gouvernent le fond.

La notion d'exercice des fonctions ou d'instructions de l'employeur

Cette notion prête elle aussi à confusion. En matière de droit des brevets, cette difficulté a été écartée, mais la logique suivie en cette matière n'a pas été reprise ici. En effet, le droit des brevets distingue entre les inventions de mission, permanentes ou occasionnelles, mission correspondant aux fonctions effectives du salarié et les inventions hors mission qui, tantôt ne sont pas attribuables et demeurent propriété du salarié, tantôt sont attribuables à l'employeur, si l'invention a une relation avec l'exécution du contrat de travail, l'activité de l'entreprise ou a bénéficié du concours de l'employeur. L'article L. 113-9, dans sa version initiale, ne visait, pour son application, que les logiciels créés dans l'exercice des fonctions, c'est-à-dire qu'il devait y avoir une mission d'écriture de logiciel dont l'employé était en charge. Ainsi, les tribunaux ont considéré que l'employeur avait pu obtenir les droits car l'employé avait « transcrit » un logiciel à l'aide des équipements de l'employeur.

La loi de 1994 a ajouté la notion de logiciels créés « d'après les instructions de l'employeur ». Hors de la perception d'un logiciel créé dans les fonctions de l'employé ou sur instruction de l'employeur, les logiciels réalisés par les préposés resteront propres à ces derniers, sans droit d'attribution au profit de l'employeur.

En toute hypothèse, il convient d'être fortement attentif aux questions de preuve car, comme en matière de brevet, et en cas de contestation, c'est à l'employeur qu'il revient de démontrer que le salarié était en charge de telles fonctions ou avait reçu de telles instructions, puisqu'il s'agit de déposséder l'auteur de droits sur son œuvre reconnus par l'article L.111-1 du code.

Régime de l'article L.113-9 du CPI

Dévolution de principe des droits patrimoniaux

Les droits patrimoniaux dont il s'agit portent sur les logiciels, sur « leur documentation », notion qui est plus large que le « matériel préparatoire », et concernent aussi sans doute toutes les créations du salarié, accessoires au logiciel, par exemple les manuels d'exploitation, les différents éléments permettant les révisions, etc.

Absence de rémunération spécifique du salarié

Lorsque l'employé aura créé un logiciel dont les droits seront dévolus à l'employeur, en application de l'article L.113-9 du code, cet employé qui, de fait, aura exécuté les obligations dérivant de son contrat de travail, ne pourra prétendre à aucune indemnité ou rémunération supplémentaire. Les dispositions statutaires des fonctionnaires ou des stipulations contraires résultant des contrats de travail, des conventions collectives, des accords de branche, des règlements d'entreprise peuvent, aux termes de l'article L.113-9, modifier le jeu du dispositif. L'employé pourra ainsi recevoir, par exemple, une rémunération supplémentaire ou encore conserver tous ses droits patrimoniaux, ou certains, sur les logiciels créés par lui.

Inversement, un contrat de travail peut-il étendre le champ de la dévolution à des logiciels créés hors fonction ou hors instructions ? À cette question, comme en matière de brevet, il faut percevoir ce texte comme une disposition de droit social fixant un régime plancher, non susceptible d'être davantage préjudiciable au salarié.

Les droits moraux

La dévolution ne doit concerner que les droits patrimoniaux, les droits moraux étant incessibles. Toutefois, l'auteur, salarié ou non, ne peut exercer de droit de repentir ou de retrait, ni protester d'une méconnaissance du droit au respect de l'œuvre,

pour autant que les altérations réalisées ne mettent pas en cause son honneur ou sa réputation.

En revanche, les deux autres droits moraux sont maintenus au profit des auteurs : droit de paternité et de divulgation. Cela signifie que les salariés, même dans le cadre de l'article L.113-9 du code de la propriété intellectuelle, pourront, s'ils le souhaitent, les exercer. En pratique, cela revient pour l'auteur à exiger que son nom apparaisse sur chaque exemplaire de l'œuvre. Mais en pratique toujours, les employeurs ne sont pas enthousiastes à satisfaire à cette demande en raison de ce que, pour des logiciels de qualité, ils peuvent craindre que les concurrents tentent de débaucher les créateurs. D'autre part, des raisons de bon sens font qu'il n'est souvent pas facile de respecter cette obligation pour des raisons techniques, notamment lorsque de gros logiciels ont été conçus par d'importantes équipes de salariés.

L'auteur du logiciel a enfin un droit de divulgation qui lui permet de refuser de communiquer son œuvre à son employeur. Il peut alors y avoir conflit entre l'obligation d'exécution de la prestation de travail résultant du contrat et l'attribut de personnalité reconnu à l'auteur. Cependant, en tant que droit subjectif, l'utilisation abusive de ce droit peut être sanctionnée. Par ailleurs, le droit de paternité et le droit de divulgation peuvent conventionnellement faire l'objet d'aménagements.

4.1.1.3 Les noms de domaine[20]

Le contentieux du nom de domaine a été et restera certainement encore longtemps l'un des premiers contentieux de l'internet. Près de deux mille décisions d'arbitrage, des procès aux quatre coins du « village planétaire », plus d'une centaine de décisions de jurisprudence lui sont déjà consacrées en France. On ne compte plus les marques prises en otage sur le réseau par un « réservataire » plus rapide que leur titulaire légitime et victimes de ce qu'on appelle le « *cybersquatting*[21] » ou les exemples de conflits d'intérêt.

Les questions sont nombreuses :

- Le nom de domaine est-il créateur de droit ?
- Quelle est la qualification juridique du nom de domaine ?
- Le nom de domaine peut-il être cédé ou vendu ?

[20] Voir aussi le rapport Cigref « Géopolitique de l'internet », septembre 2003.

[21] « *Cybersquatting* » : réservation abusive d'un nom de domaine par une personne sans droits, titres ou intérêts légitimes, en violation des droits des tiers, notamment des titulaires de droits de propriété intellectuelle, dans la perspective d'une spéculation.

- Que se passe-t-il lorsqu'il y a des conflits de droits légitimes ?
- Le nom de domaine fait-il partie du patrimoine de l'entreprise ?

Le projet de loi pour la confiance dans l'économie numérique tente, au moins pour l'espace .fr, d'appréhender un certain nombre de ces questions.

Le dépôt du nom de domaine

Le nom de domaine est un espace d'adressage sur l'internet. Il possède à la fois une fonction d'accès et une fonction d'identification.

Pour le dépôt d'un nom de domaine dans la hiérarchie .fr, il faut s'adresser à l'Afnic, et respecter les règles techniques, administratives et la charte de nommage mise en place par cet organisme. Le nom de domaine doit être soit le nom de l'organisme, soit un sigle, soit une marque déposée par celui-ci. À l'intérieur de la charte, les noms de domaine sont attribués selon la règle du « premier arrivé, premier servi », c'est-à-dire que le premier à demander l'enregistrement d'un nom de domaine en bénéficie s'il n'est pas déjà attribué.

Pour déposer un nom de domaine dans la hiérarchie .com, .net ou .org, il faut s'adresser à l'Internic. Là aussi, les noms de domaine sont attribués selon la règle du « premier arrivé, premier servi ». En revanche, il n'est pas exigé que le nom de domaine soit une marque, un sigle ou le nom du requérant.

Le statut juridique du nom de domaine

Deux thèses s'affrontent : l'une qui considère que le nom de domaine n'est l'expression que d'un élément de protection préexistant (marque, raison sociale, enseigne, nom patronymique, etc.) et d'autres qui pensent que le nom de domaine devrait avoir une protection en propre. Le problème est qu'aucun texte ne permet de mettre fin à ce point d'achoppement, qui est laissé à la libre appréciation des juges.

En l'état de la jurisprudence, un nom de domaine serait valorisable pour une entreprise, faisant partie de son patrimoine. Pour preuve, les quelques décisions prises à l'occasion de procédures de liquidations judiciaires où les noms de domaines sont intégrés dans les éléments d'actifs de la société liquidée et qui sont souvent vendus. Le fait par ailleurs de voir les entreprises ou des États dépenser des sommes considérables dans l'acquisition de noms de domaine démontre de la valeur économique des ceux-ci. La Nouvelle-Zélande a par exemple déboursé fin 2002 la somme de 500 000 dollars pour acquérir le nom de domaine newzealand.com.

La protection du nom de domaine

La règle du « premier arrivé, premier servi » occasionne un lourd contentieux dans les noms de domaine génériques (.com, .org…). L'enregistrement d'un nom de domaine est en effet réalisé sans que soit prise en compte l'antériorité des éventuels dépôts de marques. Aussi de nombreux noms de domaine correspondant à des marques sont-ils enregistrés au détriment ou à l'insu des titulaires des marques, alors qu'il conviendrait préalablement de vérifier que le nom de domaine demandé ne porte pas atteinte à des droits antérieurs détenus par des tiers.

Les droits opposables à un nom de domaine sont les suivants :

- une marque enregistrée ;
- une marque notoire ;
- un nom commercial ;
- une dénomination sociale ;
- un autre nom de domaine ;
- un patronyme.

Les actions possibles :

- action extrajudiciaire, auprès de l'OMPI[22], pour les cas de *cybersquatting* ;
- action judiciaire devant le TGI[23] ou le TC[24], sur le fondement de la contrefaçon de marque, de la concurrence déloyale, du parasitisme ou de la fraude.

Ces actions peuvent aboutir à un transfert du nom de domaine ou à son annulation pure et simple.

En matière de nom de domaine, le piratage est l'enregistrement et l'usage d'un nom de domaine propriété d'un tiers dans l'intention de nuire.

La preuve de la mauvaise foi du réservataire peut être rapportée par tout moyen. Ainsi, peuvent constituer des indices de mauvaise foi le fait de réserver un nom de domaine puis de le monnayer, ou alors de ne pas avoir effectué de recherches d'antériorité.

Le dépôt d'un nom de domaine ne génère aucun droit privatif. Il peut donc s'avérer utile de déposer la marque correspondant au nom de domaine choisi, notamment pour les zones internationales. « Comment protéger efficacement son nom de domaine ? Déposez une marque », déclare sur ce sujet un avocat du cabinet Bensoussan. Le dépôt des marques

[22] Organisation mondiale de la propriété intellectuelle. Centre d'arbitrage situé à Genève.
[23] Tribunal de grande instance.
[24] Tribunal de commerce.

s'effectue auprès de l'INPI[25]. La marque déposée doit être disponible, ce que l'on peut vérifier par le biais d'une recherche d'antériorité.

Conseils en matière de noms de domaine :

- définir une stratégie de protection des signes distinctifs de l'entreprise ;
- mettre en place une surveillance des marques et des noms de domaine ;
- pré-constituer des preuves du *cybersquatting* ;
- mettre en demeure le titulaire du nom de domaine litigieux ;
- agir à bref délai à compter de la connaissance des faits.

L'enjeu du nommage

Le système de nommage de l'internet est un des enjeux de pouvoir sur l'internet aujourd'hui. Il est également un des éléments fondamentaux du développement du commerce électronique. Mais son enjeu reste méconnu, en particulier des Européens car il est difficile à comprendre et à appréhender. Il touche à de nombreuses problématiques d'ordre économique, juridique, technique et politique.

En partenariat avec l'Isoc, le Medef et la CCI de Paris, le Cigref s'est d'ailleurs lancé en 2002 dans l'organisation d'une manifestation annuelle européenne traitant sur une journée de l'actualité du nommage sur l'internet. Une seconde édition a eu lieu en juillet 2003 et une troisième édition en juillet 2004 à Paris.

Au niveau national, on peut citer parmi les évolutions récentes, la décision de L'Afnic en 2004 d'assouplir les conditions d'attribution du .fr : dorénavant toute personne identifiable à partir de bases de données publiques en ligne pourra enregistrer le nom de domaine de son choix.

Au niveau européen, les principaux enjeux portent principalement autour du .eu et la régionalisation de l'Icann.

Au niveau mondial, force est de constater que les choses bougent lentement : aujourd'hui, l'Icann[26] est dominé par les États-Unis. Une réforme a été engagée pour une plus grande efficacité, à un meilleur coût, dans le traitement des dossiers. Elle portait sur les structures (une meilleure représentation des utilisateurs et des différentes régions du monde) et les processus.

[25] Institut national de la propriété intellectuelle.
[26] Internet corporation for assigned names and numbers.

La redéfinition du rôle, des pouvoirs et des compétences de l'Icann fait l'objet de discussions dans le cadre du Sommet mondial de la société de l'information, qui a débuté à Genève en décembre 2003 et se clora à Tunis en 2005.

Parmi les autres enjeux du SMSI on peut citer :

- pour les pays développés en priorité : le spam, la sécurité, la propriété intellectuelle, la protection des données à caractère personnel, l'e-*government*, la gouvernance d'internet
- pour les pays en développement : l'accès aux réseaux, l'accès aux savoirs, l'éducation, la réduction de la fracture numérique, la liberté de la presse et les droits de l'Homme, le logiciel libre.

4.1.2 Valeurs informatiques et libertés

Le recours de plus en plus systématique aux nouvelles technologies de réseau a des incidences considérables sur le rapport salarial. Progressivement, l'information dont disposent les entreprises est numérisée quelle que soit la nature de cette information. Dès lors qu'elle est informatisée et susceptible d'accès par l'intranet ou l'internet, des risques d'accès indus sont démultipliés.

4.1.2.1 La protection des données personnelles

Pour l'entreprise, les NTIC vont poser des problèmes nouveaux en matière de sécurité dès lors que se trouvent externalisées des informations sur toute la vie de l'entreprise, notamment ses fichiers de personnels. Pour le salarié, la différence de nature entre les NTIC et tout ce qui a précédé réside en la capacité nouvelle de la technologie de conserver toutes les traces laissées par la personne connectée. Ainsi, un message électronique que le salarié avait cru supprimer peut avoir été sauvegardé sur un serveur de messagerie ou sur un support magnétique de sauvegarde.

Les trois principes essentiels

Faisant suite au rapport de Gérard Lyon-Caen, professeur de droit du travail et auteur de nombreux ouvrages, la loi du 31 décembre 1992 relative aux libertés individuelles dans l'entreprise est la plus importante sur ce sujet : légalisant pour l'essentiel la très dynamique jurisprudence de la Chambre sociale de la Cour de cassation, elle a confirmé que dans l'entreprise d'aujourd'hui le salarié-citoyen avait cédé la place au citoyen-salarié.

1. Le principe de loyauté

« Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été préalablement porté à sa connaissance » (L.121-8 du Code du travail). Un oubli de cette information préalable rendrait inopposable au salarié l'éventuel contrôle effectué, tout comme la règle qui suit :

« Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou techniques permettant un contrôle de l'activité des salariés ».

Comme l'a remarqué la cour d'appel de Paris dans un arrêt du 31 mai 1995, « le détournement de finalité constitue un manquement à l'obligation de loyauté ». En l'espèce, l'absence d'un agent SNCF n'avait pu être contrôlée que par l'intermédiaire du système de réservation « Socrate », pas conçu pour cela.

2. Le principe de proportionnalité

« Les méthodes et techniques d'évaluation des salariés doivent être pertinents au regard de la finalité poursuivie » (L.121-7). Ce texte permet notamment d'écarter certains logiciels de contrôle de productivité.

Ce n'est pas seulement l'employeur qui est visé : « Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché » (art. L.120-2).

3. La conjugaison des principes de loyauté et de proportionnalité en matière d'informations nominatives : la loi « Informatique et libertés »

Pour contrôler ces flux informationnels dont la teneur peut parfois relever de la vie privée, le législateur a voté, le 6 janvier 1978, la loi dite « Informatique, Fichiers et Libertés », loi créant notamment la Cnil[27], chargée de ce contrôle. Le premier article de cette loi fondatrice énonce :

« L'informatique doit être au service de chaque citoyen. Elle ne doit porter atteinte ni à l'identité humaine ni aux droits de l'homme ni à la vie privée ni aux libertés individuelles ou publiques. »

L'Union européenne va s'intéresser par la suite à ce sujet et élaborer la directive 95/46 du 24 octobre 1995.

[27] Commission nationale informatique et libertés.

Début 2004, la France était le seul État à n'avoir pas encore transposé la directive européenne du 24 octobre 1995 et risquait de ce fait d'être l'objet d'une action en manquement. D'où la transposition en droit interne. Le projet de loi a été adopté en 2e lecture à l'Assemblée nationale le 30 avril 2004. Cette loi nouvelle apporte quelques changements significatifs qui méritent d'être connus par les entreprises.

Les changements majeurs apportés par le projet de loi

Deux modifications affectent essentiellement le comportement des entreprises à l'égard des traitements de fichiers informatisés. Ce sont d'une part la modification des régimes existants de déclaration et d'autorisation des traitements informatiques, et d'autre part l'élaboration de règles pour les transferts de données à caractère personnel vers des États n'appartenant pas à l'Union européenne. Par ailleurs, et de manière subsidiaire, la loi nouvelle prévoit diverses modifications pouvant avoir un impact pour les entreprises.

Le texte réserve les contrôles préalables au seul traitement des textes présentant des risques effectifs d'atteinte aux droits et libertés, avec suppression de la distinction entre secteur public et secteur privé. Il maintient cependant l'autorisation préfectorale pour la vidéosurveillance sur la voie publique et dans les lieux et établissements ouverts au public. Les procédures seront plus rapides. En effet, la Cnil pourra, sauf pour les fichiers relatifs à la souveraineté et à des missions d'intérêt public, décider directement, au lieu de transmettre un simple avis à l'administration. Les procédures déclaratives auprès de la Cnil sont simplifiées pour les traitements ne présentant pas de risques.

Parallèlement les pouvoirs d'investigation, d'injonction et de sanction de la Cnil augmentent considérablement et pour la première fois, elle est dotée de pouvoirs effectifs en ce qui concerne le transfert de données vers des États extérieurs à l'Union européenne ne présentant pas un niveau de protection suffisant. Elle pourra ainsi signaler une difficulté à la Commission européenne, suspendre ou interdire un transfert de données. Elle sera donc plus efficace, en opérant un contrôle *a posteriori* plus sélectif.

Pour la Cnil, au-delà de la réduction du volume de papier qu'elle brasse, l'enjeu est de s'alléger de l'accessoire pour se concentrer sur l'essentiel : conseil du Gouvernement et du Parlement au sujet de la montée en puissance de l'administration électronique ou de l'usage de la biométrie ; contrôle des fichiers de sécurité, qui contiennent encore trop d'approximations ; information des citoyens sur leurs droits – y compris face au développement de fichiers de « mauvais payeurs » ou de « clients à risques ».

Les nouveaux régimes

La loi de 1978 distingue selon la nature publique ou privée du traitement de données personnelles. Ainsi, l'article 16 de la loi actuelle prévoit une simple déclaration des traitements mis en œuvre par les organismes privés, alors que l'article 15 impose aux organismes publics une demande d'autorisation préalable à la Cnil (dont l'avis défavorable ne peut être outrepassé que par un décret pris en Conseil d'État). Sept régimes distincts de déclaration et d'autorisation sont prévus aux articles 22 à 31 du projet de loi pour remplacer le régime actuel.

Les transferts de données hors d'Europe

La directive 95/46 prévoit, dans ses articles 25 et 26, un régime particulier concernant ces transferts. Ceux-ci ne sont en effet autorisés que si l'État tiers à l'Union assure un niveau de protection adéquat apprécié eu égard à la nature des données, la finalité du traitement, les pays d'origine et de destination finale, et enfin la législation en vigueur et les mesures de sécurité qui sont respectées dans le pays destinataire.

La loi de 1978 avait confié la tâche normative sur ce sujet au Conseil d'État, qui devait organiser par décret un régime de transfert de données à l'étranger. Le projet de loi quant à lui reprend les articles de la directive dans un douzième chapitre.

L'efficacité de ce dispositif n'est toutefois qu'apparente, de nombreuses dérogations étant prévues. Ainsi, alors même que la protection n'est pas adéquate, les données pourront être transférées si :

- la personne a consenti au transfert de ses données dans un pays n'offrant pas un niveau de protection adéquate ;
- ou si le transfert est nécessaire à la réalisation d'un contrat entre la personne concernée et le responsable du traitement ;
- ou si le transfert est nécessaire à l'exécution d'un contrat ou de mesures précontractuelles, dans l'intérêt de la personne concernée, entre le maître du fichier et un tiers.

En pratique ce schéma peut paraître insatisfaisant. Aux États-Unis par exemple, l'absence de texte législatif ne doit pas être assimilée à une absence de régulation. Le respect des droits et libertés de la personne est affirmé dans des réglementations sectorielles et, surtout, se concrétise à travers des « codes de bonne conduite » auxquels les entreprises américaines sont tenues de se conformer, sous peine de sévères condamnations par les tribunaux.

Les changements secondaires du projet de loi

Le renforcement des pouvoirs de la Cnil

La loi actuelle permet à la Cnil d'exercer deux types d'actions dont la portée est très relative. Elle ne peut, en effet, qu'adresser des avertissements aux responsables des traitements ne respectant pas les dispositions légales d'une part, et dénoncer au Parquet les infractions à la loi qu'elle constate d'autre part.

Le projet de loi offre quatre nouveaux pouvoirs prévus aux articles 45 à 47 du projet :

- prononcer des injonctions de cesser un traitement illicite ;
- retirer, le cas échéant, l'autorisation de mise en œuvre du traitement illicite ;
- ordonner l'interruption du traitement de données pendant trois mois ;
- prononcer des sanctions pécuniaires.

L'étendue de ces pouvoirs doit toutefois être relativisée puisque les trois premiers pouvoirs ne peuvent être exercés qu'à l'encontre des traitements de police et de justice. Le pouvoir de sanction pécuniaire quant à lui peut apparaître comme une arme redoutable contre les entreprises mettant en œuvre des traitements illégaux. La Cnil peut, en effet, infliger des amendes allant jusqu'à 150 000 euros, voire 300 000 euros en cas de réitération, ou 5 % du chiffre d'affaires.

Ces sanctions peuvent cependant paraître faibles compte tenu des bénéfices que les entreprises peuvent espérer obtenir de ces informations d'une part et, d'autre part, peuvent paraître insuffisantes compte tenu du faible nombre d'agents travaillant à la Cnil, ce qui fait qu'en pratique les traitements illégaux ne sont pas souvent sanctionnés.

Le principe de licéité et de loyauté

Ce principe implique que les données à caractère personnel :

- doivent être collectées pour des finalités déterminées, explicites et légitimes ;
- ne doivent pas être traitées ultérieurement de manière incompatible avec le respect des libertés individuelles ;
- doivent être adéquates, pertinentes et non excessives au regard de ces finalités.

Ce principe n'apparaît pas clairement dans le texte actuel, c'est la jurisprudence de la Cnil qui le fera émerger. Le projet de loi quant à lui consacre à ce principe l'article 6.

En pratique, le problème se pose en termes de marketing. Ce principe apparaît pour les internautes comme un élément qui

influe sur la confiance qu'ils peuvent avoir dans les transactions au même titre que la sécurité de celles-ci. En effet on remarque depuis un an que les internautes souhaitent savoir pour quelles utilisations les données personnelles sont collectées. Cette exigence du consommateur est d'un enjeu important puisqu'elle permet de gagner sa confiance. Ainsi, les mentions légales relatives à ce type de collecte doivent apparaître clairement. Celles-ci pourront par exemple, être matérialisées par une case à cocher pour l'utilisateur et par l'adoption d'une charte par l'entreprise visible sur son site pour que les informations puissent être traitées en toute transparence.

4.1.2.2 La cybersurveillance

Rien de plus légitime pour un employeur que de chercher à éviter les actes de malveillance ou de contrôler l'accomplissement par les employés du travail prescrit. Cela passe par la surveillance des allées et venues (physiques ou virtuelles). Ce droit peut d'ailleurs se transformer en devoir s'il ne veut pas, le cas échéant, lui-même civilement répondre en tant que commettant des errements de certains de ses subordonnés.

Surveiller l'activité, certes, mais toute l'activité ? Sur le lieu de travail, n'y a-t-il pas place pour des activités personnelles ? Le salarié ne peut-il pas « *vaquer librement à des occupations personnelles* » (définition du non-travail effectif), mais sur du matériel de l'entreprise ?

La problématique du secret de la correspondance

Il peut paraître surprenant de mêler vie privée et travail au moins pour deux raisons. La première c'est qu'il ne paraît pas normal que pendant le temps de travail, temps que l'employé doit utiliser pour accomplir la tâche qui lui a été assignée par son employeur, cet employé accomplisse des actes touchant à sa vie privée tel que la rédaction de messages à caractères autre que professionnel. La seconde réside dans le fait que l'employé va utiliser son outil de travail à des fins personnelles. Plus grave encore cette utilisation peut avoir un coût pour l'entreprise, ce coût pouvant être facilement calculé en volume de bande passante du réseau de l'entreprise utilisé à ces fins par exemple.

Mais le travail d'aujourd'hui n'est plus manuel mais cérébral. Dès lors, on ne peut plus contrôler aussi facilement la productivité et surtout on ne peut pas forcer quelqu'un à penser ! Il ne faut donc pas interdire ou limiter excessivement l'utilisation de cet outil pour les salariés.

La recherche d'un équilibre entre vie privée et vie professionnelle

Cette matière est nouvelle et les fondements ne sont pas encore stabilisés. Pour tendre vers cet équilibre, Hubert Bouchet, lorsqu'il était vice-président délégué de la Cnil, proposait diverses recommandations.

- Une corrélation entre productivité et liberté du salarié : il faut surveiller ce qui est utile et nécessaire, sans excès. Pour cela l'administrateur réseau peut contrôler les volumes échangés.
- Un pouvoir réel de l'administrateur réseau : l'administrateur réseau, de par sa fonction, peut être sommé par sa hiérarchie de communiquer des contenus. Les risques de dérive sont donc importants. C'est pourquoi ses pouvoirs doivent lui permettre de résister à la pression hiérarchique. D'autant que, par comparaison avec la téléphonie, les salariés n'ont pas toujours conscience que si avec le téléphone ce qui été dit n'était pas enregistré, il en va différemment avec l'écrit, même électronique.
- L'adoption d'une charte et la désignation d'un « correspondant informatique et libertés » : dans chaque entreprise, il est souhaitable qu'il y est un référent informatique et libertés, avec un interlocuteur entre l'employeur et les salariés.
- Utilisation du réseau pour la négociation sociale : il faut trouver un équilibre entre vie privée et travail.

Le contrôle des connexions à l'internet

Une interdiction générale et absolue de toute utilisation de l'internet à des fins autres que professionnelles ne paraît pas réaliste dans la société de l'information et de la communication.

Un usage raisonnable, non susceptible d'amoindrir les conditions d'accès professionnel au réseau, et ne mettant pas en cause la productivité, paraît admis par la plupart des entreprises. Aucune disposition légale n'interdit évidemment à l'employeur d'en fixer les conditions et limites, lesquelles ne constituent pas, en soi, des atteintes à la vie privée des salariés.

À ce titre, la mise en place de dispositifs de filtrage de sites non autorisés, associés au pare-feu (sites diffusant des produits à caractère pornographiques, pédophiles, incitation à la haine raciale, révisionnistes, etc.) peut constituer une mesure de prévention dont il y a lieu d'informer les salariés.

De même, la possibilité pour les salariés de se connecter à l'internet à des fins autres que professionnelles peut s'accompagner de prescriptions légitimes dictées par l'exigence de sécurité de l'entreprise, telles que l'interdiction de

télécharger des logiciels, l'interdiction de se connecter à un forum ou d'utiliser le « *chat* », l'interdiction d'accéder à une boîte aux lettres personnelle par l'internet compte tenu des risques de virus qu'un tel accès est susceptible de présenter. Une charte ou un document de sensibilisation peuvent être communiqués au salarié, voire annexés au contrat de travail.

Un contrôle *a posteriori* des données de connexion à l'internet, de façon globale, par service ou par utilisateur, ou un contrôle statistique des sites les plus visités, devrait dans la plupart des cas être suffisant sans qu'il soit nécessaire de procéder à un contrôle nominatif individualisé des sites visités.

Les modalités d'un tel contrôle de l'usage de l'internet doivent, conformément à l'article L.432-2-1 du Code du travail, faire l'objet d'une consultation du comité d'entreprise et d'une information des utilisateurs, y compris lorsque le contrôle est dépourvu d'un caractère directement nominatif.

Lorsque l'entreprise met en place un dispositif de contrôle individuel destiné à produire, poste par poste, un relevé des durées de connexion ou des sites visités, le traitement automatisé d'informations nominatives ainsi mis en œuvre doit être déclaré à la Cnil. La durée pendant laquelle les relevés ainsi établis sont conservés doit être précisée. Une durée de conservation de l'ordre de six mois devrait être suffisante, dans la plupart des cas, pour dissuader tout usage abusif de l'internet. Le dossier de déclaration doit en outre comporter l'indication et la date à laquelle les instances représentatives du personnel ont été consultées sur de tels dispositifs.

Le contrôle de l'usage de la messagerie[28]

L'utilisation de la messagerie électronique professionnelle pour envoyer ou recevoir, dans des proportions raisonnables, un message à caractère personnel correspond à un usage généralement et socialement admis.

D'ailleurs, compte tenu des termes de l'arrêt de la Chambre sociale de la Cour de cassation en date du 2 octobre 2001, une interdiction ne permettrait pas à l'employeur de prendre connaissance dans des conditions régulières du contenu de celles des correspondances qui relèveraient de la vie privée des personnes.

Arrêt Nikon : « *Le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors, sans violation de cette liberté fondamentale, prendre connaissance des messages*

[28] On pourra consulter sur ce sujet le rapport du Cigref : « Impacts et usages de la messagerie électronique ».

personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail, et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur. »

Il doit être généralement considéré qu'un message envoyé ou reçu depuis le poste de travail mis à disposition par l'entreprise revêt un caractère professionnel, sauf indication manifeste dans l'objet du message ou dans le nom du répertoire où il pourrait avoir été archivé par son destinataire. Cela lui conférerait alors le caractère et la nature d'une correspondance privée, protégée par le secret des correspondances.

Des exigences de sécurité, de prévention ou de contrôle de l'encombrement du réseau peuvent conduire les entreprises à mettre en place des outils de mesure de la fréquence ou de la taille des fichiers transmis en pièce jointe aux messages électroniques ou encore des outils d'archivage des messages échangés. Dans cette dernière hypothèse, le message électronique bien qu'étant effacé du poste de l'émetteur et du poste du récepteur sera néanmoins conservé. L'emploi de tels outils de contrôle ou de sauvegarde doit être porté à la connaissance des salariés ainsi que la durée de conservation du message « sauvegardé ».

Lorsque l'entreprise met en place un dispositif de contrôle individuel poste par poste du fonctionnement de la messagerie, le traitement automatisé d'informations nominatives ainsi mis en œuvre doit être déclaré à la Cnil. La durée pendant laquelle les messages sont conservés doit être précisée. Le dossier de déclaration doit en outre comporter l'indication et la date à laquelle les instances représentatives du personnel ont été consultées sur de tels dispositifs.

Les fichiers de journalisation

Les fichiers de journalisation des connexions destinés à identifier et enregistrer toutes les connexions ou tentatives de connexion à un système automatisé d'informations constituent une mesure de sécurité, généralement préconisée par la Cnil dans le souci que soient assurées la sécurité et la confidentialité des données à caractère personnel, lesquelles ne doivent pas être accessibles à des tiers non autorisés ni utilisées à des fins étrangères à celles qui justifient leur traitement. Ils n'ont pas pour vocation première le contrôle des utilisateurs.

La finalité de ces fichiers de journalisation, qui peuvent également être associés à des traitements d'information dépourvus de tout caractère nominatif mais revêtent un caractère sensible pour l'entreprise concernée, consiste à garantir une utilisation normale des ressources des systèmes d'information et, le cas échéant, à identifier les usages

contraires aux règles de confidentialité ou de sécurité des données définies par l'entreprise.

Ces fichiers de journalisation, lorsqu'ils sont associés à un traitement automatisé d'informations nominatives, n'ont pas, en tant que tels, à faire l'objet des formalités préalables auprès de la Cnil. Afin de garantir ou de renforcer l'obligation de sécurité, ils doivent être portés à la connaissance de la Cnil au titre des mesures de sécurité entourant le fonctionnement du traitement principal dont ils sont le corollaire.

En revanche, la mise en œuvre d'un logiciel d'analyse des différents journaux (applicatifs et systèmes), permettant de collecter des informations individuelles poste par poste, destiné à contrôler l'activité des utilisateurs, doit être déclaré à la Cnil.

Dans tous les cas de figure, les utilisateurs doivent être informés de la mise en place des systèmes de journalisation et de la durée pendant laquelle les données de connexion permettant d'identifier le poste ou l'utilisateur s'étant connecté sont conservées ou sauvegardés. Cette information réalise l'obligation légale à laquelle est tenu le responsable du traitement, est de nature à prévenir tout risque et participe de l'exigence de loyauté dans l'entreprise.

Une durée de conservation de l'ordre de six mois ne paraît pas excessive au regard de la finalité des fichiers de journalisation.

Aucune disposition de la loi du 6 janvier 1978 ne prive le responsable de l'entreprise de la possibilité d'opposer les informations enregistrées dans les fichiers de journalisation associés à un traitement automatisé d'informations nominatives à un salarié qui n'en n'aurait pas respecté les conditions d'accès ou d'usage (Cour de cass. - Chambre soc. n° 98-43.485 du 18 juillet 2000).

Le cas de l'administrateur réseau

Un arrêt de la cour d'appel de Paris en date du 17 décembre 2001 apporte un éclairage nouveau sur l'utilisation de la messagerie électronique après l'arrêt Nikon, considéré par la doctrine comme un arrêt de principe en matière de surveillance des courriers électroniques :

« La préoccupation de la sécurité du réseau justifie que les administrateurs de réseaux informatiques fassent usage des possibilités dont ils disposent pour mener à bien des investigations et prendre les mesures que cette sécurité impose, de la même façon que La Poste doit réagir à un colis ou à une lettre suspecte. En revanche, la divulgation du contenu des messages ne relève pas de ces objectifs. »

L'administrateur réseau, parce qu'il contrôle tout ce qui circule sur le réseau, a accès à des informations qui peuvent être

sensibles : messagerie, connexions à l'internet, fichiers de « *logs* » ou de journalisation, y compris celles qui sont enregistrées sur le disque dur du poste de travail. Un tel accès n'est contraire à aucune disposition de la loi du 6 janvier 1978.

De même, l'utilisation encadrée de logiciels de télémaintenance qui permettent de détecter et réparer les pannes à distance ou à prendre le contrôle, à distance, du poste de travail d'un salarié (« prise de main à distance ») ne soulève aucune difficulté particulière au regard de la loi à condition que les mesures de sécurité nécessaires à la protection des données soient mises en œuvre.

Toutefois, aucune exploitation à des fins autres que celles liées au bon fonctionnement et à la sécurité des applications des informations dont l'administrateur réseau peut avoir connaissance dans l'exercice de ses fonctions ne saurait être opérée, d'initiative ou sur ordre hiérarchique.

De même, l'administrateur réseau, tenu au secret professionnel, ne doit pas divulguer des informations qu'il aurait été amené à connaître dans le cadre de ses fonctions, et en particulier lorsque celles-ci sont couvertes par le secret des correspondances ou relèvent de la vie privée des utilisateurs, et ne mettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt de l'entreprise. Il ne saurait non plus être contraint de le faire.

Il faut en déduire dans ces conditions que seul le contrôle contradictoire en présence du salarié des messages ne portant pas la mention « personnel » est possible... Cette seule solution n'est évidemment pas satisfaisante pour l'employeur en cas de constatation ou de suspicion de faits graves nécessitant des mesures non contradictoires. L'employeur, alerté par l'administrateur réseau grâce à un contrôle statistique ou à un filtrage par mots clés, pourra à l'évidence accumuler les indices lui permettant de solliciter en justice, sur requête, l'autorisation de faire saisir les traces informatiques des messages du salarié enregistrés sur la mémoire du disque dur.

Le recours à la justice de l'employeur se fonde alors sur l'avertissement donné par l'administrateur réseau et la révélation d'indices graves, sans toutefois que ce dernier ne puisse révéler le contenu des messages. Le juge saisi sur requête appréciera alors les faits incriminés en vertu de son pouvoir d'appréciation souverain.

4.1.2.3 La valeur juridique des courriels

Le courriel ne constitue pas une preuve

Le courriel est souvent la seule matérialisation d'une négociation en ligne ou d'un accord conclu autour d'un site web ou d'une place de marché. Il est aussi très souvent admis comme matérialisant l'accord de l'internaute.

Or le courriel n'est pas, en tant que tel, recevable à titre de preuve, car il identifie mal celui dont il émane, et n'est que très rarement stocké dans des conditions de nature à garantir son intégrité.

Certaines solutions existent néanmoins qui permettent de garantir non seulement l'identité des personnes mais aussi d'autres impératifs tels que l'authentification, l'intégrité, la confidentialité, la datation :

- la loi du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information, admet la validité des conventions de preuves entre les parties ;
- les décrets publiés en mars 2001 organisent la signature électronique afin de sécuriser ces correspondances.

La signature électronique consiste à lier un document numérique à son auteur en utilisant une clé de codage, cette clé étant préalablement authentifiée par une autorité de certification.

Pour l'instant, ce système de cryptage est réservé aux chefs d'entreprise et la loi impose que le logiciel nécessaire à l'identification soit vendu par un organisme de certification habilité par l'État.

Le procédé de la signature électronique a été considéré comme fiable par le législateur : désormais, les tribunaux lui confèrent la même valeur qu'à la signature manuscrite.

D'un point de vue juridique donc, le courriel signé électroniquement peut tout à fait être produit en justice, mais au titre de la constitution d'un faisceau d'indices, pas en tant que preuve.

***Une des réponses des entreprises : les* disclaimers**

« Ce message et toutes les pièces jointes sont établis à l'intention exclusive de ses destinataires et sont confidentiels. Si vous recevez ce message par erreur, merci de le détruire et d'en avertir immédiatement l'expéditeur. »

Ces messages d'avertissements fleurissent à la fin des courriels. Le phénomène est trop massif pour qu'il ne retienne pas l'attention du juriste. Tous les internautes en reçoivent et tous les internautes en émettent, presque à leur insu, puisque ce sont bien souvent les systèmes de messagerie des

entreprises qui incluent automatiquement ces « *disclaimers* » lors de l'envoi d'un message.

- Cette pratique présente-t-elle un intérêt juridique quelconque ?
- L'omission d'un tel message d'avertissement lors de l'envoi d'un message fait-elle courir un risque à son expéditeur ?

Une enquête réalisée en 2002 sur la pratique du « *disclaimer* » dans les entreprises membres du Cigref révèle que la quasi-totalité des banques et assurances ont mis en place un « *disclaimer* », l'industrie et les services étant quant à eux un peu plus en retrait.

La technique de mise en œuvre est majoritairement celle de l'insertion automatique *via* les passerelles SMTP. Le libre choix de l'utilisateur en signature d'un courriel est peu courant.

Rappelons tout d'abord qu'aucun texte de droit français, loi ou règlement, n'oblige l'expéditeur d'un courriel à inclure dans celui-ci un tel message d'avertissement. Le droit refuse en effet de légitimer les déclarations unilatérales d'irresponsabilité.

Il n'y a donc que le principe de précaution qui conduise les entreprises à insérer de façon automatique de tels avertissements dans les messages.

Si la loi ne l'impose pas, la pratique est-elle néanmoins de nature à prévenir un risque juridique ? À y regarder de plus près, on peut distinguer différentes finalités qui président à l'inclusion des « *disclaimers* ».

Corriger une erreur de destination

En premier lieu, certains de ces messages visent à réparer l'erreur humaine de l'expéditeur : à savoir le message adressé à la mauvaise personne. Ainsi, on demande souvent la coopération du destinataire fortuit pour la réparation de l'erreur d'envoi :

« Si vous n'êtes pas destinataire de ce message, merci de le détruire immédiatement et d'avertir l'expéditeur de l'erreur de distribution et de la destruction du message. »

Rien n'oblige le destinataire à répondre à cette sollicitation, si ce n'est la correction. De plus, la présence d'un avertissement sur la nature confidentielle d'un message électronique ne dégagera pas l'expéditeur de sa responsabilité si l'erreur qu'il commet dans l'envoi entraîne une violation d'un engagement de confidentialité auquel il était tenu. On peut d'ailleurs se demander si un courriel non protégé par un dispositif de cryptage est bien le moyen adéquat pour transmettre un document de nature confidentielle.

Dans la plupart des cas, celui qui aura reçu par erreur le message effacera celui-ci comme n'importe quel autre « *spam* ». Mais si à la faveur d'une erreur d'envoi, une entreprise vient à recevoir des informations stratégiques sur l'un de ses concurrents, pourra-t-elle en tirer profit ? L'utilisation de ces informations pourrait-elle engager sa responsabilité délictuelle alors qu'elle ne les a pas acquises frauduleusement ? Très certainement cet agissement pourrait être sanctionné au titre de la concurrence déloyale. Cependant, la société victime de cet agissement sera confrontée à la difficulté d'en apporter la preuve et particulièrement de prouver que son concurrent a exploité un message qui lui avait été adressé par erreur.

Rappeler les sanctions encourues

D'autres messages d'avertissement se font plus dogmatiques et font office de rappels à la loi. Ainsi, il y est parfois mis l'accent sur le caractère pénal de la violation du secret des correspondances :

« Ce message est à l'intention exclusive de son destinataire. Sa prise de connaissance par une personne autre que son destinataire est punie par la loi. »

En effet, l'article 226-15 du Code pénal punit d'un an d'emprisonnement et de 45 000 euros d'amende le fait de prendre frauduleusement connaissance de correspondances adressées à des tiers.

Ici encore, aucun texte ni principe juridique n'impose à l'expéditeur d'un message d'insérer ce type d'avertissement. Le fait que l'avertissement ne soit pas présent ne permet pas à la personne qui prendrait connaissance frauduleusement d'un courriel d'échapper au délit d'atteinte au secret des correspondances. « Nul n'est censé ignorer la loi ». Ce vieil adage a toujours cours. Nul n'a donc besoin de rappeler la loi.

Précisons que l'article 226-15 du Code pénal n'aura vocation à s'appliquer que pour le cas où une personne prend connaissance d'un courriel de façon frauduleuse, par exemple par l'ouverture du message dans la boîte de son destinataire légitime. La personne qui prend connaissance d'un message qui ne lui était pas intentionnellement destiné, mais dont elle était bien destinataire par erreur, n'est évidemment pas concernée par cette infraction.

Dénier l'engagement de la société

Autre forme de « *disclaimer* », celui qui s'apparente à une « dénégation de volonté ». On pourra lire, accompagnant les courriels reçus :

« L'internet ne permettant pas d'assurer l'intégrité de ce message, le contenu de ce message ne représente en aucun cas un engagement de la part de notre société ».

Compte tenu du nombre des messages que les salariés d'une entreprise peuvent envoyer par jour, sans que les organes de direction puissent en contrôler le contenu, il peut être en effet de bonne politique de prévoir que ceux-ci n'engagent pas la société ès qualité, et que, par exemple, un courriel ne puisse constituer une offre ou l'acceptation d'un contrat.

D'un point de vue strictement juridique cependant, il est pourtant loisible à tout émetteur d'un courrier électronique d'en dénier la « paternité » même en l'absence d'un tel avertissement. Pour qu'un courriel puisse valablement engager son émetteur, ou la personne morale qui l'emploie, encore faut-il que celui qui s'en prévaut puisse faire la preuve qu'il émane bien de la personne à laquelle il prétend l'opposer. Or, une simple adresse électronique ne permet pas d'identifier de façon fiable une personne, et donc de lui imputer un engagement. Il n'en serait autrement que si le message était signé électroniquement, à l'aide d'une signature électronique sécurisée au sens du décret n° 2001-272 du 30 mars 2001 relatif à la signature électronique.

Que retenir de cette pratique ? Elle est certainement un nouvel exemple de l'emprise du droit dans notre société. Ces « *disclaimers* », qui n'ont pas de valeur juridique en tant que tels, sont recommandés dans la mesure où :

- dans d'autres pays, sous l'empire d'autres législations, leur valeur juridique pouvant être différente, il s'agit, par prudence, de « se caler » sur les règles de la législation la plus restrictive ;
- ils permettent d'informer les utilisateurs sur les « règles du jeu » ;
- ils permettent de sensibiliser les utilisateurs sur la nature non sécurisée des échanges sur l'internet ;
- ils ont une valeur dissuasive et permettent de présumer la bonne foi de l'expéditeur.

4.2 Négocier ses contrats informatiques

Le contrat informatique présente plusieurs particularités qui le distinguent des autres contrats :

- Il constitue un « mode opératoire » qui fusionne les aspects juridiques et opérationnels. Il doit donc être rédigé dans un langage accessible et s'imprégner de la culture propre au projet. Il doit être le fil conducteur du projet.

- Il doit « vivre » et, à ce titre, il convient d'anticiper les scénarios susceptibles de se produire. L'élaboration d'une matrice des risques, en concertation avec les opérationnels concernés, doit permettre d'identifier, pour chaque risque répertorié, une solution pragmatique susceptible d'être mise en œuvre.
- Il doit encore intégrer la notion d'évolutivité propre aux technologies. Il ne faut surtout pas enfermer les contractants dans un périmètre figé, sous peine de s'exposer à une succession d'avenants et de lourdeurs juridico-administratives.
- Il doit s'imprégner de la notion de partenariat, notion inhérente à ce type de projet. La collaboration est souvent la clé du succès.

Les contrats informatiques correspondent à des réalités très variées en raison de la complexité technique de la matière et de la diversité des besoins à satisfaire. Chaque contrat a une rédaction qui lui est propre et il n'est pas toujours facile de déceler les pièges que les juristes ont prévus dans leur rédaction. De ce fait, les contrats informatiques doivent être examinés avec le plus grand soin.

4.2.1 Les difficultés rencontrées

La négociation des contrats informatiques est délicate. Les enjeux sont importants, tant financiers que fonctionnels. Dans cet exercice délicat, les relations entre la direction des systèmes d'information et la direction juridique sont essentielles car les pièges sont nombreux, faits de clauses léonines perçues comme étant autant de facteurs de déséquilibre entre le client et le fournisseur de services ou de produits.

4.2.1.1 Le rapport de force entre éditeurs et utilisateurs

« Coupables, mais pas responsables. » Telle est la situation paradoxale des éditeurs après diffusion de logiciels affectés par des bogues. Car nul recours efficace ne s'offre aux sociétés utilisatrices en cas de dysfonctionnement grave des outils informatiques induisant une cessation temporaire d'activité, un manque à gagner ou une détérioration d'image. La responsabilité civile des éditeurs est quasiment nulle. Constat unique dans l'industrie, la responsabilité civile des fournisseurs de progiciels est presque inexistante. Les contrats, aux nombreuses clauses léonines, ne remédient guère à ce vide juridique. Individuellement et selon ses moyens, chaque société tente de se défendre, en engageant des négociations amiables et, rarement, une procédure judiciaire. Mais le rapport de force entre éditeurs et utilisateurs devrait dans les années à venir s'inverser.

Le droit positif ne reconnaît pas le logiciel comme une chose, mais comme une œuvre intellectuelle, exactement comme un livre ou une chanson. Le logiciel est soumis aux dispositions du Code de la propriété intellectuelle et son inventeur au régime des droits d'auteur. Impossible dès lors d'invoquer la responsabilité des fournisseurs pour vice caché. Le droit admet de plus un point extraordinaire : « Un logiciel peut boguer. » L'arrêt puis le redémarrage de l'ordinateur pour cause de bogue bloquant représentent une pratique admise. Nul n'attaque pour cette raison l'éditeur en justice.

4.2.1.2 Des clauses léonines...

Le point de vue des éditeurs : « Une œuvre intellectuelle ne peut pas être parfaite. L'essentiel est de rechercher un bon compromis entre coût et qualité de progiciel et de service. »

Encore faut-il que ce compromis soit jugé acceptable par les utilisateurs. Les contrats pourraient certes combler ce déficit de responsabilité. En pratique, ils le creusent avec des clauses perçues comme léonines par les acheteurs mais imposées par les éditeurs. Les fournisseurs proposent des contrats types non négociables, où sont définis avec précision les contours de leur responsabilité. Les cas de garantie sont réduits, de même que les montants de garantie sont limités à des sommes dérisoires au regard des préjudices subis.

Ainsi, les clauses contractuelles n'établissent la responsabilité des éditeurs qu'en cas de lien frappant de cause à effet entre les failles avérées des progiciels et les dommages directs. Le montant de réparation est plafonné, souvent proportionnel à celui des licences. En cas d'arrêt accidentel prolongé de l'activité, provenant d'un dysfonctionnement du logiciel, ce dédommagement peut se révéler négligeable.

Quant à la garantie pour vice, incluse dans le contrat de maintenance, elle n'est pas légalement imposée. Mais c'est une précaution indispensable. Trop souvent, la garantie néglige l'organisation de l'assistance, alors qu'il faudrait trouver dans les contrats des indications comme les délais d'intervention ou les moyens mis en œuvre.

4.2.1.3 ... Mais des garde-fous érigés par la jurisprudence

Les vendeurs ont une obligation de renseignement, de conseil, voire de mise en garde, au-delà de la simple délivrance de produit. Les fournisseurs sont tenus d'attirer l'attention sur les limites et les conséquences des solutions retenues, d'apporter leur aide dans la formulation des besoins des utilisateurs, d'éviter les dépenses injustifiées et de prévenir des perturbations lors du démarrage des logiciels. À la condition toutefois, très restrictive dans les faits, que le client soit profane. Tout acheteur compétent, qualifié ou assisté d'un expert

extérieur est présumé en mesure d'effectuer un choix raisonné. Le fournisseur se trouve ainsi souvent délivré des devoirs dont le charge la jurisprudence.

Une certaine régulation peut se faire par les acteurs eux-mêmes, qui ont intérêt à travailler en bonne intelligence, dans une logique de partenariat constructive. Dans cet esprit, le Syntec Informatique et le Cigref ont signé en février 2003 une charte commune, pour une déontologie commune au service des technologies de l'information.

Charte
Cigref et Syntec Informatique

Le Cigref et le Syntec Informatique, associations professionnelles de référence dans le secteur des technologies de l'information décident d'unir leurs compétences et leurs efforts pour promouvoir l'usage des technologies et des systèmes d'information comme vecteur de création de valeur pour l'entreprise.

Ensemble, le Cigref et le Syntec s'engagent à promouvoir les orientations suivantes auprès de leurs membres :

- **Connaissance des métiers**

  Affirmer conjointement leurs aptitudes à connaître et à maîtriser l'évolution des différents métiers liés aux technologies de l'information ainsi que favoriser la mise en œuvre des moyens nécessaires pour assurer l'adéquation des offres aux besoins des entreprises.

- **Transparence**

  Faire preuve en toutes circonstances d'une transparence dans la recherche de l'intérêt commun et la mise en place de solutions. Rédiger un guide de bonnes pratiques réciproques dans la relation client - fournisseur et favoriser la résolution des difficultés.

- **Impartialité**

  Mettre en place des structures de recours en cas de litiges et en faire la promotion auprès de leurs adhérents.

- **Indépendance d'opinion et d'expression**

  S'affirmer dans nos métiers respectifs comme les représentants légitimes et les porte-parole libres de nos professions.

- **Qualité**

Les systèmes d'information constituant un actif fondamental des entreprises, mettre en place un label de qualité Cigref-Syntec à partir de la définition, et du suivi d'indicateurs, facteurs de confiance et de progrès.

- **Innovation**

  Développer une vision prospective (et à long terme) de l'impact des systèmes et technologies de l'information sur l'Entreprise et la Société, base d'un développement pérenne et d'une modernisation sociale.

- **Diffusion de l'information**

  Faire respecter les intérêts et les droits de nos professions, tant en France que dans le monde. Faire connaître les progrès que chacun peut attendre de l'usage pertinent des technologies de l'information.

- **Partage des connaissances**

  Développer dans leurs rôles respectifs, et mettre en commun leurs expériences métiers et technologiques pour définir des standards et des règles de l'art de la profession et ainsi tendre vers l'excellence.

- **Productivité**

  Recommander l'utilisation de méthodes, procédures, et outils de mesure garants de la prédictibilité et de l'optimisation des coûts.

- **Suivi**

  Publier chaque année pour leurs membres, un bilan de la mise en œuvre de la Charte

Ensemble, en unissant leurs compétences et leurs maîtrises des technologies de l'information, le Cigref et Syntec Informatique souhaitent ainsi optimiser leur contribution au développement de la société de l'information.

Paris, le 24 février 2003

Jean-Pierre CORNIOU
Président
Cigref

François DUFAUX
Président
Syntec Informatique

Figure 12 : La charte Cigref Syntec Informatique.

4.2.2 La structure du contrat informatique

Les contrats informatiques comportent de nombreuses clauses dont la rédaction protège le fournisseur. Pour rééquilibrer le contrat, l'utilisateur doit être capable d'évaluer les conséquences des limitations voire des exonérations de responsabilité ou d'obligation intégrées par le fournisseur dans le contrat.

Mais les contrats ont chacun leurs spécificités et la valeur de ces clauses est différente en fonction de l'objet du contrat. Ainsi, la négociation portera sur des éléments différents selon que l'on est en présence d'un contrat d'intégration, de maintenance, de licence de logiciel ou encore d'infogérance. Toutefois, un socle commun peut être dégagé de l'ensemble de ces contrats, selon deux parties :

- L'économie générale du contrat :
  - préambule et objet du contrat,
  - langue du contrat,
  - attribution de compétence et loi applicable,
  - définitions,
  - nature de l'obligation des parties,
  - règlement amiable et arbitrage ;
- Les clauses de limitation et d'exonération de responsabilité :
  - Des exemples :

    dommages directs et indirects,

    résiliation,

    force majeure, cause d'exonération ;
  - les garanties :

    les garanties en matière de logiciel,

    la garantie de la titularité des droits,

    la garantie de non-contrefaçon.

4.2.2.1 L'économie générale du contrat

Préambule et objet du contrat

Souvent négligé lors de la négociation du contrat, le préambule présente un intérêt certain puisqu'il témoigne de l'économie générale de celui-ci et de la commune intention des parties.

Ce paragraphe du contrat doit donc, lui aussi, faire l'objet d'attentions particulières, d'autant que les informations contenues ont la même valeur juridique que les dispositions principales. Il est donc largement utilisé par le juge lorsqu'il souhaite interpréter les clauses.

L'objet présente la chose sur laquelle porte le contrat : licence de logiciel, intégration de logiciel, externalisation, etc. Il doit être décrit avec précision afin d'éviter toute ambiguïté.

La langue du contrat

Les logiciels qui circulent sur le marché français sont essentiellement conçus par des sociétés américaines. Ainsi, les contrats passés sont souvent rédigés en anglais, alors même que les parties au contrat sont françaises.

Lorsque le contrat est rédigé en langue étrangère, les parties seront amenées à traduire le contrat en cas de litige judiciaire. Le juge français, s'il est saisi sur le fondement du contrat, doit, en effet, rendre sa décision en français. Cette traduction emporte comme conséquence un alourdissement des frais du procès.

La loi n° 94-665 du 4 août 1994 sur l'emploi obligatoire de la langue française en matière de commerce ne concerne que la protection du consommateur et de l'utilisateur final sur le territoire français. Cette loi ne s'applique donc pas dans les contrats conclus entre professionnels. Les parties françaises sont donc libres de rédiger l'intégralité de leur contrat dans la langue de leur choix, ce que confirme la jurisprudence de la Cour de cassation.

Attribution de compétence et loi applicable

Les parties disposent d'une certaine liberté pour aménager le contentieux susceptible de survenir dans le cadre de leur relation contractuelle. Les cocontractants peuvent purement et simplement éviter le recours au juge et faire appel à l'arbitrage ou à la médiation. En cas de contentieux judiciaire, ils peuvent aménager les règles applicables et s'entendre pour organiser les modalités du recours, en vertu de l'autonomie de la volonté.

S'agissant d'un contrat conclu entre deux sociétés commerciales de droit français qui a vocation à s'exécuter sur le territoire national, l'application de la loi française s'impose aux parties sans possibilité de dérogations contractuelles.

Dans le cas d'une opération qui revêt un caractère international, les parties retrouvent leur liberté contractuelle et peuvent choisir la loi applicable. Ce principe de liberté ne trouve que peu de limites mais le juge pourra cependant invalider le choix des parties s'il lui paraît frauduleux.

Il convient de distinguer la compétence d'attribution de la compétence territoriale.

Pour ce qui est de la compétence d'attribution, le contrat conclu entre deux sociétés commerciales doit envisager la

compétence d'une juridiction commerciale en cas de contentieux judiciaire.

Parallèlement à la nature de la juridiction, les parties désignent le lieu où celle-ci doit être saisie c'est-à-dire la juridiction territorialement compétente. La clause demeurera valable pour la compétence d'attribution alors même qu'elle sera déclarée nulle en ce qui concerne la compétence territoriale.

Le principe de droit civil impose au demandeur d'assigner le défendeur devant le tribunal du lieu du domicile de ce dernier (article 42 nouveau Code de procédure civile). L'article 48 pose une règle qui déroge à ce principe dans des conditions strictes : « Toute clause qui, directement ou indirectement, déroge aux règles de compétence territoriale est réputée non écrite, à moins qu'elle n'ait été convenue entre des personnes ayant toutes contracté en qualité de commerçant et qu'elle n'ait été spécifiée de façon très apparente dans l'engagement de la partie à qui elle est opposée. »

La clarté et la rigueur de cet article invitent les parties à faire figurer cette clause par exemple en fin de contrat, au plus près des signatures et en caractères gras ou majuscules.

Par ailleurs, la clause dite « *de juridiction* » prévoit souvent que la juridiction désignée sera compétente pour le règlement du différend ainsi que pour les mesures conservatoires ou d'urgence. Dans ce cas elle stipule qu'« il est fait expressément attribution de compétence au tribunal de commerce de [ ], même pour les procédures de référé ou par requête. »

Définitions

Cette partie permet de donner un contenu au vocabulaire utilisé. L'utilité de définir certaines expressions (techniques ou juridiques) employées dans la suite du contrat est incontestable dans la mesure où il s'agit pour les parties d'un moyen d'entente et de clarification, par l'accréditation d'un seul sens à un terme.

Dans les accords internationaux, il s'agit d'un moyen de traduction par la mise en place de termes équivalents dans les différentes langues en présence. Les parties s'accordent alors sur un contenu car une traduction directe pourrait être source de méprise.

Mais par le caractère réducteur ou au contraire général d'une définition, les parties peuvent influencer l'objet du contrat. Ainsi est-il fréquent de trouver des clauses types et donc vagues comme :

« Le contrat désigne l'ensemble des dispositions énoncées dans le présent document, dûment signé par les parties, ainsi que *tout avenant ou annexe qui viendraient compléter, modifier*

ou se substituer au présent document, étant précisé que le préambule et les annexes en font parties intégrante ».

À la largesse des termes en italique, il est préférable de lister limitativement les documents et de définir une hiérarchie de ceux-ci tout en laissant la possibilité d'ajouter par la suite des avenants négociés.

Nature de l'obligation des parties

La qualification d'obligation de moyens ou de résultat influe sur la preuve.

L'obligation de moyens est celle par laquelle le débiteur s'est seulement engagé à employer les moyens appropriés afin d'accomplir une certaine tâche. Il n'est cependant pas tenu d'obtenir le résultat en question, même s'il est vrai qu'il est au moins tenu de chercher à l'obtenir.

Ainsi, sur le terrain de la preuve, il appartient au créancier de prouver la faute du débiteur, autrement dit que celui-ci n'a pas mis en œuvre tous les moyens promis.

Pour savoir s'il y a une faute, on a recours à une appréciation en référence à un fournisseur moyen.

L'obligation de résultat a pour objet un résultat précis. Ainsi, le débiteur n'a exécuté son obligation que si le résultat est atteint.

Par conséquent, le créancier peut mettre en œuvre la responsabilité du débiteur par la seule constatation que le résultat promis n'a pas été atteint. C'est une responsabilité sans faute.

Pour s'exonérer le débiteur devra prouver une cause étrangère (c'est-à-dire un évènement extérieur, imprévisible et irrésistible) ou une faute de la victime.

En pratique, il est apparu une troisième catégorie d'obligation, à savoir l'obligation de moyens renforcée.

En l'espèce, la faute est présumée à l'égard du débiteur. Il s'opère donc un renversement de la charge de la preuve puisque le débiteur ne peut se dégager qu'en prouvant qu'il n'a pas commis de faute (il doit donc rapporter la preuve positive de son absence de faute).

En général, dans un contrat, lorsque les termes faisant référence à la nature de l'obligation ne sont pas clairs, il est possible que le juge utilise la méthode du faisceau d'indices. Autrement dit, celui-ci considérera qu'on est en présence d'une obligation de moyens dès lors que le créancier a une participation active dans l'exécution du contrat. À l'inverse, si celle-ci est passive, ce sera une obligation de résultat.

Une autre méthode est d'utiliser le critère de l'aléa. En effet, il est souvent considéré que si la réalisation de l'obligation est entachée d'un aléa alors ce sera une obligation de moyens, mais dans le cas contraire, cela sera une obligation de résultat.

Dans la pratique le DSI a tout intérêt à exiger une obligation de résultat, alors que le fournisseur lui proposera assurément une obligation de moyens. Au cours des négociations, le DSI devra obtenir au minimum une obligation de moyens renforcée, pour faire peser la preuve de l'absence de faute sur le fournisseur.

En effet en pratique, deux hypothèses doivent être distinguées :

- Si le prestataire a accepté une obligation de résultat et que la machine bloque.

  On considère que la faute peut venir soit d'un bogue, soit d'une mauvaise manipulation par le client, soit d'une erreur de communication ou enfin d'une erreur de paramétrage.

  Dans ces hypothèses, il appartient au prestataire de débloquer car le résultat promis n'est pas atteint (c'est une situation difficile pour le prestataire).
- Si le prestataire a accepté une obligation de moyens et que la machine bloque.

  Le client sera alors dans l'obligation de démontrer la faute du prestataire (et dans ce cas, c'est parfois très difficile de le faire pour le client).

En conclusion, si l'utilisateur n'obtient pas une obligation de résultat, la seule voie acceptable pour les deux parties afin de répartir la charge de la responsabilité et donc, rééquilibrer le contrat, est l'obligation de moyens renforcée. Le prestataire est présumé responsable sauf s'il rapporte la preuve positive de son absence de faute.

Exemple de clause :

« *L'éditeur s'engage à exécuter les obligations lui incombant au titre du contrat conformément aux règles de l'art et en professionnel diligent (obligation de moyens). Dans le cadre de l'exécution de ses prestations à l'égard du licencié, l'éditeur ne pourra s'exonérer de son éventuelle responsabilité qu'en apportant au licencié la preuve positive de son absence de faute* (obligation de moyens renforcée). »

Règlement amiable

L'introduction d'une telle clause impose aux parties de rechercher une solution négociée à leurs possibles différends.

Elle les oblige à négocier de bonne foi. En cas d'insuccès de cette procédure, d'autres modes de traitement des conflits entreront en jeu (recours au tribunal ou à l'arbitrage).

Ce type de clause est appréciable mais peut aussi retarder inutilement un recours au juge ou à l'arbitre inévitable. Dans ce cas elle s'assimile à une perte de temps largement préjudiciable.

Certaines actions doivent d'ailleurs être intentées dans un « *bref délai* » or ce bref délai n'est pas interrompu par une tentative de conciliation amiable. Un fournisseur mal intentionné pourra accomplir des actes dilatoires dans l'unique but de rendre caduque l'action devant les tribunaux. Il est donc important de bien vérifier que cette clause ne soit pas une obligation faite aux parties mais une simple invitation à la discussion.

Arbitrage

L'arbitrage et la médiation constituent une alternative au procès soumis aux juridictions de l'État. Mais alors que la médiation consiste en la désignation de personnes privées que les parties chargent d'aider à trouver une solution à leur différend, l'arbitre va trancher le litige qui les oppose.

L'arbitrage présente des qualités certaines : discrétion, rapidité, qualité, liberté des règles applicables, équité…

Autant d'arguments qui font que les parties préfèrent prévoir un tel recours notamment en droit international, pour éviter la compétence d'un juge étranger.

La pratique montre que les partenaires étrangers souhaitent fréquemment recourir à ce mode de règlement, qui évite la compétence du juge français et l'application du droit français.

Cependant, la procédure d'arbitrage se révèle contraignante et coûteuse. En effet, les juges sont désignés et payés par les parties et l'assistance d'un avocat spécialisé est indispensable. Dans ces conditions, le coût est prohibitif au regard du résultat escompté. C'est pourquoi certains contractants préfèrent, si la négociation est ouverte, proposer une clause attribuant, en cas de litige, compétence aux tribunaux et au droit français.

4.2.2.2 Les clauses de limitation et d'exonération de la responsabilité

Ces clauses sont insérées dans le contrat par l'éditeur du logiciel qui cherche à exclure ou limiter sa responsabilité en cas de fonctionnement défectueux du logiciel : la réparation sera limitée contractuellement à un plafond stipulé et à condition que le créancier apporte la preuve du dommage subi.

En pratique, ces clauses peuvent se présenter sous plusieurs formes plus ou moins dissimulées dans le contrat. Elles peuvent affecter aussi bien la mise en œuvre de la responsabilité que ses effets. En matière d'édition de logiciel, la

clause consistera le plus souvent en une limitation du montant pécuniaire de la réparation en cas de défectuosité :

- remboursement des redevances ou minoration des remboursements en fonction de la durée d'utilisation ;
- clause pénale dont le montant sera inférieur au dommage réellement subi ;
- dommage direct qualifié, dans le contrat, de dommage indirect qui ne sera donc pas réparé.

Nous pouvons trouver des clauses du type :

« Le montant de la responsabilité pécuniaire de l'éditeur du fait d'une défaillance ou d'un mauvais fonctionnement du logiciel est limité à hauteur du remboursement du montant des redevances encaissées par l'éditeur au cours [par exemple] des 5 dernières années. »

« Le montant de la responsabilité pécuniaire de l'éditeur du fait d'une défaillance ou d'un mauvais fonctionnement du logiciel est limité à hauteur de la somme de *xxx* euros. »

« Aucune action, quels qu'en soient la nature, le fondement ou les modalités, née du présent contrat, ne peut être intentée par les parties plus de six mois après l'apparition de son fait générateur. » Une telle clause annule quasiment les possibilités d'action, le fait générateur pouvant apparaître avant même la recette ! Il est préférable de prévoir « six mois après la découvert du dommage par le client. »

Le montant de ces clauses doit faire l'objet d'une attention particulière puisque, s'il est trop faible, il peut conduire à une clause d'exonération de garantie.

La qualification du contrat influe sur la validité de ces clauses :

- Louage d'ouvrage ou contrat d'entreprise (avec communication d'un savoir-faire) : la validité des clauses sur la responsabilité est de principe entre professionnels, sauf faute lourde ou intentionnelle de l'éditeur prestataire. Cette qualification est souvent retenue pour les logiciels spécifiques.
- Louage de chose : les dispositions de l'article 1721 du Code civil n'étant pas d'ordre public, il semble possible de stipuler une limitation ou une exonération de responsabilité.
- Vente : n'a été retenue en pratique que pour les progiciels. L'éditeur cherchera à écarter cette qualification car son régime est plus strict que celui du louage d'ouvrage ou de chose.

Néanmoins, si jusqu'à une date récente la jurisprudence s'attachait surtout à la qualification du contrat, on constate désormais que cette distinction n'est plus totalement d'actualité

et la jurisprudence se référera plus souvent à l'objet de la clause du contrat de licence.

Les juges souhaitent limiter la validité de ces clauses notamment en cas de :

- faute intentionnelle ;
- clauses affectant la cause du contrat en touchant aux obligations essentielles de celui-ci ;
- responsabilité délictuelle (le manquement à une obligation contractuelle constitue une infraction) puisque la limitation de responsabilité ne peut jouer qu'en matière contractuelle. Par exemple, une clause qui limiterait ou exclurait la responsabilité de l'éditeur en cas de contrefaçon des droits d'un tiers est nulle.

Dommages directs / dommages indirects

La réparation doit porter sur la totalité du dommage composé de la perte subie et du gain manqué.

Cependant, cette réparation intégrale ne doit s'appliquer qu'au seul dommage réparable. Celui-ci présente quatre caractères : certain, direct, licite et prévisible.

Le dommage direct et licite implique l'existence d'un lien de causalité direct et immédiat entre l'inexécution et le dommage. C'est par rapport à la notion de lien de causalité notamment qu'intervient le problème de la libre détermination par les parties des dommages directs et indirects. En effet, les parties peuvent prévoir dans le contrat que les dommages qui sont normalement considérés comme directs seront qualifiés par eux d'indirects.

Exemple de clause :

« *L'éditeur ne saurait en aucune circonstance encourir de responsabilité du fait d'une défaillance ou d'un mauvais fonctionnement du logiciel au titre des dommages indirects ou imprévisibles au sens des articles 1150 et 1151 du Code civil, qui incluent notamment, mais sans que cette liste soit limitative, tout gain manqué, perte, inexactitude ou corruption de fichiers ou de données, préjudice commercial, perte de chiffre d'affaires ou de bénéfice, perte de clientèle, perte d'une chance, coût de l'obtention d'un produit, d'un logiciel, d'un service ou d'une technologie de substitution.* »

Les parties ont-elles le droit de prévoir quels seront les dommages réparables sans tenir compte de la définition de dommages directs retenue par la jurisprudence ? Il semble, *a priori*, que le juge puisse requalifier de dommages directs des dommages indirects. Cependant cette clause réduisant manifestement le domaine de la responsabilité, il semble qu'elle soit soumise aux différentes obligations et limitations

s'appliquant aux clauses limitatives ou élusives de responsabilité.

Le DSI doit donc être vigilant lors de la signature des contrats et veiller à ce que les clauses qui donnent une liste de dommages qualifiés d'indirects ne visent effectivement que des dommages indirects.

Résiliation

La résiliation unilatérale n'est possible que dans les contrats à durée indéterminée. Si le contrat est à durée déterminée (comme c'est nécessairement le cas dans le contrat de licence de logiciel), la résiliation unilatérale n'est possible qu'avec un recours au juge, sauf clause contractuelle aménageant la résiliation.

En pratique les contrats prévoient toujours une clause de résiliation anticipée. Les parties doivent être vigilantes à l'égard de ces clauses au moment de la négociation afin de tourner la clause en leur avantage.

Ainsi, le fournisseur a tendance à stipuler qu'« en cas de non-respect d'une disposition quelconque » du contrat, celui-ci sera résolu. Le client ne doit pas accepter une telle clause et doit chercher à limiter le jeu de la clause aux seules obligations essentielles du contrat, qui peuvent en outre, et c'est son intérêt, être énumérées (par exemple, non-paiement de la redevance à son échéance, non-respect des droits d'exploitation qui lui sont conférés – on pensera en priorité aux nombre de postes ou de terminaux sur lesquels le logiciel serait installé...). De même, le client doit aménager cette clause pour pouvoir se dégager facilement du contrat en cas de défaillance du prestataire.

Dans les contrats de licences d'origine américaine, on trouve souvent des clauses comme « le titulaire des droits se réserve le pouvoir de résilier le contrat en cas de redressement ou de liquidation judiciaire du bénéficiaire ». L'article 37 de la loi du 25 janvier 1985, devenu L. 621-28 du nouveau Code de commerce, précise que le choix de poursuivre les contrats en cours incombe au seul mandataire judiciaire qui peut avoir été préalablement mis en demeure. Ce dernier peut alors ne pas répondre (et le contrat est alors résilié) ou décider de sa poursuite « forcée ».

Ces clauses n'ont donc que très peu de portée en pratique car sont dénuées d'effet en droit français ; elles peuvent donc être laissées dans le contrat sans grand danger.

Force majeure, cause d'exonération

Cette clause est déterminante dans les contrats dont les prestations s'échelonnent dans le temps. Ainsi, seront particulièrement sensibles les contrats d'infogérance, de maintenance ou encore d'ASP[29]... L'enjeu de cette clause est considérable puisqu'elle va permettre au débiteur d'échapper à la responsabilité d'une inexécution imputable à une cause étrangère (article 1147 du Code civil).

Les juges admettent que les critères d'appréciation de la force majeure peuvent être contractuellement définis puisqu'ils ne sont pas d'ordre public. L'utilisateur aura donc intérêt à strictement encadrer les cas de force majeure.

Classiquement, trois critères cumulatifs sont retenus :

- l'irrésistibilité : elle suppose que l'événement soit insurmontable[30] ;
- l'imprévisibilité : elle s'analyse lors de la conclusion du contrat. À défaut en effet, le débiteur qui n'a pas pris les mesures nécessaires est en faute.
- l'extériorité : si l'événement est imputable à une partie, celle-ci engage sa responsabilité. Ainsi le débiteur ne peut invoquer la défaillance de son personnel, de son matériel ou de la technique utilisée.

Mais la jurisprudence ne considère plus aujourd'hui que ces trois critères doivent être caractérisés pour dégager le débiteur de son obligation. En effet, il suffit que le débiteur se soit trouvé irrésistiblement empêché d'exécuter le contrat. Ainsi, seule la condition d'irrésistibilité doit être caractérisée, les deux autres critères devenant des facteurs d'appréciation de celui-ci.

Les conséquences de la force majeure ne sont pas négligeables puisque lorsque l'impossibilité est temporaire, le contrat est suspendu ; si elle ne vaut que pour l'avenir, le contrat est résilié[31] ; enfin si elle est totale, le contrat sera résolu[32].

La gravité de ces conséquences doit inviter les parties à la plus grande attention quant au choix des critères de la force majeure. Le débiteur aura tendance à faciliter au maximum la mise en œuvre de la force majeure pour se dégager de ses obligations et donc ne retenir que le caractère irrésistible.

---

[29] *Application service provider* ou fournisseur d'applications hébergées.

[30] Si l'événement rend l'exécution plus difficile ou onéreuse, le débiteur est responsable de son manquement ; il n'existe pas de force majeure financière.

[31] C'est-à-dire que le contrat sera annulé sans effet rétroactif et ne vaudra que pour l'avenir.

[32] Conséquence gravissime puisque le contrat est annulé rétroactivement, ce qui signifie que les parties doivent être mises dans l'état où elles étaient avant le contrat, ce qui peut être catastrophique si le contrat a été exécuté pendant une longue période.

Inversement, le bénéficiaire voudra limiter aux cas les plus extrêmes la mise en œuvre de cette cause d'exonération. Ainsi ce dernier aura intérêt à exiger le cumul des trois critères pour mettre en œuvre la force majeure.

La garantie des vices cachés

Cette garantie ne joue que dans le cadre des contrats de vente et de louage. Or la licence de logiciel ne semble pas répondre aux critères légaux de ces contrats. La doctrine considère que la licence de logiciel spécifique est soumise au contrat d'entreprise et considère que les garanties légales sont applicables. Quant aux licences de progiciel, la qualification de contrat de louage peut être admise.

Il est donc important de constater que la qualification de la licence de logiciel influe sur les garanties applicables, la définition du logiciel en droit n'étant pas fixée. De plus, des débats animés divisent les auteurs pour savoir ce qu'est un vice caché dans un logiciel, certains auteurs considérant que tous les vices sont nécessairement cachés puisque la création est immatérielle ; d'autres, pour le même argument, réfutent le caractère caché.

Pour éviter des débats passionnés dont la solution est incertaine, il est préférable de prévoir une garantie contractuelle des vices.

Ainsi, le contrat pourra prévoir une garantie souvent brève mais dont la durée pourra varier en fonction de l'importance du contrat. Pendant cette période, le fournisseur s'engage à corriger les bogues sans conditions (alors que la garantie légale impose une certain gravité et des conditions de mise en œuvre lourde de la garantie), ce qui permet en outre d'éviter le recours au juge, souvent long et coûteux. À l'issue de cette période, le contrat de maintenance pourra prendre le relais.

On trouve ainsi certaines clauses du type :

« L'éditeur garantit que le logiciel fonctionnera de manière conforme à la documentation client ; l'éditeur garantit aussi le licencié, pour une période de *n* jours (période à préciser en fonction de l'importance du logiciel) à compter de la livraison du logiciel, contre tous les vices cachés. »

La conformité

Elle s'analyse comme la garantie des vices apparents. La recette du logiciel sanctionne la conformité de celui-ci par rapport aux attentes du client. Cependant en l'absence de précision du document de référence pour le contrôle de la conformité, c'est la documentation fournisseur qui s'imposera. Il est donc important de définir clairement par rapport à quoi la conformité doit s'analyser, le licencié ayant intérêt à imposer un document qu'il a rédigé comme le cahier des charges.

De même, l'événement qui provoque la recette doit être maîtrisé par l'utilisateur.

Exemples de clauses :

« Le fournisseur garantit au client que les développements spécifiques sont conformes aux spécifications contenues dans la documentation client, annexée au présent contrat.

À ce titre, le fournisseur corrigera gratuitement pendant trois mois à partir du prononcé de la recette définitive toute anomalie par rapport aux spécifications qui lui sera signalée. »

Il faut toutefois veiller à ce que les éléments à fournir au prestataire ne soit pas trop nombreux, ce qui équivaudrait à une limitation de responsabilité comme nous l'avons vu.

Les autres garanties contractuelles

Les parties peuvent prévoir d'autres garanties dans le contrat de licence de logiciel. Ce dernier doit en effet tenir compte d'une possible évolution technique.

Le contrat peut donc comprendre des garanties d'évolutivité du logiciel, d'adaptation, de compatibilité de nouvelles versions avec la configuration du client ou enfin des garanties de performance, le tout en dehors d'une éventuelle maintenance.

La garantie de la titularité des droits

Le danger pesant sur l'utilisateur du logiciel est de découvrir qu'il n'est pas effectivement titulaire des droits donnés en licence, autrement dit de voir sa licence remise en cause par un tiers agissant en contrefaçon.

Cette clause est utile dans les contrats de cession ou de concession de logiciel. Elle se résume souvent en une déclaration de la part du donneur de licence qui ressemble plutôt à un engagement de bonnes intentions. Des clauses du type « L'éditeur est l'auteur du logiciel *xxx* dont les droits sont concédés (ou cédés selon le cas) au client » ne sont pas rares.

Une telle clause paraît peu probante en cas d'action en contrefaçon dirigée contre l'utilisateur. Il est préférable d'exiger du donneur de licence la copie du contrat qui la lie avec la

société américaine lorsque l'on traite avec une filiale, ce qui est souvent le cas.

Il est aussi largement recommandé d'exiger de la part de l'éditeur de déposer le logiciel dans un organisme tel que l'APP ou Logitas qui permet de donner date certaine au logiciel et ainsi de faciliter la preuve de son antériorité. De plus, même si aucune recherche d'antériorité n'est effectuée par ces organismes, ce dépôt permet de présumer du sérieux du donneur de licence.

D'autre part, le donneur de licence est souvent une filiale d'une société mère américaine. Il est donc important de savoir à quel titre agit la filiale :

- si elle agit en tant que commissionnaire, la licence sera concédée par la maison mère contre qui toute réclamation devra être formulée ;
- si la filiale bénéficie d'une licence d'exploitation, elle a le droit de concéder des licences en son nom et sera alors l'interlocuteur de ses licenciés.

La garantie de non-contrefaçon

L'éditeur limite classiquement cette garantie au territoire sur lequel le logiciel a été conçu. Une telle protection est insuffisante et le bénéficiaire de la licence doit demander impérativement à ce que la protection territoriale soit étendue à l'ensemble des territoires sur lesquels le logiciel va être utilisé.

Le contrat de licence précise souvent que « l'éditeur n'accorde aucune garantie d'indemnisation en cas de contrefaçon par le logiciel des droits d'un tiers ». Cette affirmation paraît infondée au regard de l'article L. 335-3 du CPI qui sanctionne pénalement la contrefaçon et, s'il est possible de limiter sa responsabilité contractuelle, il en va différemment de sa responsabilité délictuelle. La jurisprudence annule en effet les clauses exonératoires de responsabilité en matière délictuelle.

En conclusion, il est important de préciser que toutes les clauses qui ont été présentées correspondent aux clauses que l'on trouve le plus fréquemment dans un contrat informatique. Mais la liberté contractuelle permet d'imaginer bien des choses...

4.3 Mettre en place des moyens de prévention adaptés

Comment alors se prémunir contre de tels risques ? « Le pire ennemi, c'est l'utilisateur interne », déclare Joël Rivière, PDG de Lexsi, cabinet de conseil spécialisé dans la sécurité des systèmes d'information. La pierre angulaire de la protection du système d'information et de son responsable reste donc l'établissement d'une charte de bonne conduite, dont chaque

salarié doit être informé. Une protection valable uniquement si les obligations légales ont été respectées et notamment les multiples déclarations à la Cnil.

Rien ne vaut en effet la prévention. Le cabinet d'avocats Alain Bensoussan préconise d'ailleurs la mise en place de « plans de prévention des risques juridiques liés à l'informatique » destinés à alerter les dirigeants sur leur responsabilité civile et pénale.

La cartographie des risques liés au système d'information étant établie, il s'agit pour le DSI d'être vigilant quant à son exploitation. La prévention valant toujours mieux que la réparation, il est conseillé de limiter les risques liés au système d'information par une construction juridique de type contractuel ou assuranciel, et par un suivi en interne, sous forme de tableau de bord, des différentes obligations légales en matière de droit des nouvelles technologies.

4.3.1 La gestion du risque informatique

Les entreprises considèrent que la politique de sécurité doit répondre à l'ensemble des objectifs suivants :

- authentification : vérifier l'identité de l'utilisateur et acquérir la preuve que l'utilisateur est bien ce qu'il prétend être ;
- contrôle d'accès ;
- intégrité : se protéger contre toute modification non autorisée d'information ;
- imputabilité : possibilité d'attribuer une action à son auteur ;
- confidentialité : empêcher toute divulgation non autorisée d'informations sensibles ;
- non-répudiation : s'assurer qu'une transaction a effectivement eu lieu ;
- disponibilité : garantir le fonctionnement des informations de l'entreprise ;
- audit : contrôler et évaluer la sécurité ;
- assurance : passer par des contrats d'assurance adaptés aux principaux risques ;

La gestion du risque pesant sur le système d'information implique :

- l'analyse des risques et l'évaluation des conséquences ;
- la remontée de l'ensemble des éléments qui permettent de prendre des décisions ;
- l'étude des moyens propres à assurer la sécurité et le respect de leur application ;
- l'établissement d'un plan de secours et de sauvegarde.

4.3.2 La couverture des risques liés au système d'information

4.3.2.1 La solution contractuelle

Outre les aspects fondamentaux des contrats, ce sont surtout les aménagements de la responsabilité des parties au contrat qui retiennent l'attention.

L'aménagement direct de la responsabilité

Quatre moyens peuvent être envisagés. Ces limitations de responsabilité exposent l'utilisateur à un plus grand risque dont le fournisseur se dégage.

- Les clauses de non-responsabilité

Elles ne sont pas interdites (principe de liberté contractuelle...) sauf exceptions légales et jurisprudentielles, comme la faute lourde (le débiteur a conscience qu'il cause un préjudice à son cocontractant ; la charge de la preuve incombe à la personne qui invoque la faute).

- Les clauses limitatives de responsabilité

Elles sont admises sauf interdiction légale, atteinte à une obligation essentielle du contrat (c'est-à-dire que la limitation ne doit pas priver le contrat de sa cause ; cf. arrêt Chronopost, Cass. Com., 22 octobre 1996).

- Les clauses fixant le dommage réparable

Le dommage réparable est défini à l'article 1151 du Code civil. Une difficulté d'interprétation se pose lors de la lecture de cet article : qu'est-ce qu'une perte éprouvée et un gain manqué ? La frontière entre dommage direct et indirect n'est pas toujours très claire... Toutefois, il est important de préciser que le dommage indirect n'est pas synonyme de dommage immatériel ; un défaut de logiciel peut générer un dommage immatériel, comme une perte d'exploitation par exemple.

- Les clauses de renonciation à recours

Dans ce cas, la personne renonce à son droit à agir. Il doit alors informer son assureur de cette clause car, à défaut, en cas de sinistre l'assuré ne pourra pas faire jouer son assurance.

On remarque toutefois que si l'utilisateur renonce à agir contre son fournisseur, il n'a pas nécessairement renoncé à agir contre l'assureur de ce dernier contre lequel il peut agir par recours subrogatoire.

Il est donc très important de savoir à quel droit l'utilisateur a renoncé, et il est conseillé de ne jamais perdre le droit de recourir contre l'assureur.

L'aménagement indirect de la responsabilité

Le contrat doit clairement régler les droits et obligations des parties pour ne pas laisser au juge un trop grand pouvoir d'interprétation du contrat.

Le contrat doit aussi être cohérent avec les documents « paracontractuels ».

Les parties peuvent limiter le nombre d'obligations ou encore leur portée.

Ainsi, une clause prévoyant une correction des bogues mais qui est assortie de conditions trop rigoureuses pour être mise en jeu (délai pour signaler le bogue extrêmement court, informations à apporter trop nombreuses et difficiles à établir...) peut s'assimiler à une non-garantie.

C'est ici que joue la requalification d'une obligation de moyens en une obligation de résultat... ou inversement.

4.3.2.2 La solution assurancielle

L'assurance des systèmes d'information doit être considérée non pas comme une alternative à la sécurité mais comme un complément.

L'indemnisation d'un sinistre n'étant jamais équivalente à la non-survenance d'un sinistre. L'assurance est, par conséquent, l'aboutissement logique de toute étude de sécurité.

Les aspects fondamentaux de l'assurance

L'assurance est une adéquation complexe entre des exigences juridiques et techniques.

Les exigences juridiques imposent une cohésion entre un risque qui doit être aléatoire (incertain et non dépendant de la volonté des parties), une prime qui est calculée en fonction de la valorisation du risque au moment de la souscription et une garantie que doit l'assureur en cas de réalisation de l'événement.

Les exigences techniques imposent en pratique l'organisation d'une mutualisation.

Pour que l'assurance soit valable, l'assuré doit de son côté déclarer les biens à assurer au moment de la souscription et en cours d'exécution du contrat à l'assureur. À défaut, l'indemnisation sera partielle, le contrat pourra même être résilié. L'assuré ne doit donc pas négliger son obligation d'information.

Enfin les courtiers en assurances, qui sont indispensables en matière informatique, sont soumis à une obligation de conseil particulièrement lourde à l'égard de leur client. L'utilisateur, en

cas de difficulté, ne doit donc pas négliger le recours contre son courtier, sa responsabilité étant forte en cas de manquement.

La conciliation entre risque informatique et adéquation de la couverture d'assurance

L'assurance de valeurs immatérielles n'est pas chose aisée. C'est le problème du « *risk management* » : il faut analyser le risque pour trouver des solutions adaptées.

L'analyse consiste d'abord à identifier les risques compte tenu de la rapide évolution des techniques utilisées. Dans un second temps, il faut les quantifier pour voir s'il est ou non financièrement intéressant de couvrir ce risque par le contrat d'assurance ou d'une autre manière.

La couverture sera ainsi adaptée en fonction de certains risques ciblés préalablement. Toutefois, la couverture ne sera efficace qu'avec un contrat dont les clauses à « double lecture » ont été neutralisées, celles-ci étant à l'origine d'incertitudes pouvant jouer à l'avantage de l'assureur.

L'assurance doit donc dépasser la simple couverture du matériel pour couvrir les pertes d'exploitation issues de problèmes informatiques. Il est de ce fait recommandé de veiller à ce que la police d'assurance couvre l'immatériel.

Ainsi le contrôle de la police ne doit pas se limiter à son intitulé, souvent trompeur, « tout risque informatique » ou encore « global informatique », mais il faut analyser le contenu des clauses et bien mesurer leur portée. Le recours à une personne compétente peut être nécessaire.

4.3.2.3 Les solutions alternatives

En dehors de l'appréhension du risque par le contrat ou par la voie assurancielle, l'utilisateur d'un système informatique peut s'auto-assurer ou préférer s'assurer par le biais de captives.

Les captives se définissent par un mécanisme avantageux pour l'entreprise :

- l'ensemble du risque du groupe est mutualisé sur la société mère ;
- la sinistralité est mieux appréhendée puisqu'une fois les causes identifiées, la politique de prévention peut être optimisée ;
- enfin, puisqu'elles sont créées par l'assuré, si le risque ne se réalise pas, l'assuré récupérera sa prime.

4.3.3 Le tableau de bord juridique du DSI

Le cabinet d'avocats Alain Bensoussan, dans son ouvrage « Le tableau de bord juridique des DSI », récapitule l'ensemble des connaissances juridiques que doit posséder le DSI dans le cadre de ses fonctions pour assurer la sécurité juridique de l'entreprise.

Que ce soit au travers de cet ouvrage ou par la constitution d'un tableau de bord personnel et adapté aux situations rencontrées au quotidien, le DSI doit s'efforcer d'acquérir des réflexes dans les différents domaines que sont les libertés individuelles, la propriété intellectuelle, les contrats et les assurances.

Il doit comprendre l'utilité de l'opération et le texte juridique applicable pour pouvoir discuter, si nécessaire, avec la direction juridique.

Un tel tableau de bord comprendrait notamment :

- l'identification des connaissances juridiques à posséder dans le domaine du droit des nouvelles technologies ;
- la vérification de leur validité (lois et règlements en vigueur) ;
- la détermination des opérations à mener pour assurer la sécurité du système d'information.

Par rapport à ce qui a été développé précédemment, voici un exemple de *check-lists* d'opérations pouvant ainsi être constituées par un DSI qui inévitablement, de par ses fonctions, est amené à s'en occuper, seul, ou en liaison avec la direction juridique.

4.3.3.1 Les relations avec les salariés

À l'égard des salariés créateurs

Rédiger une clause de cession des droits au profit de l'entreprise, lui permettant d'être propriétaire de la création et ainsi l'exploiter et la faire évoluer éventuellement. Cet aspect doit être pris en compte par la DRH dans le cadre du contrat de travail du salarié.

À l'égard des utilisateurs de logiciels

Respecter les limites des droits acquis dans le cadre des licences, afin de ne pas s'exposer au paiement d'amendes voire à des peines de prison.

En cas de création d'une base de données

Conserver la trace des frais investis, pour éviter que l'entreprise ne finance une base de données qui ne bénéficierait d'aucune protection juridique.

À l'égard de salariés responsables d'un département

Prévoir des délégations de responsabilité pénale par écrit, afin d'écarter les risques d'engagement de la responsabilité pénale de l'entreprise et des dirigeants. La délégation doit être accompagnée de moyens permettant de remplir correctement la ou les missions déléguées.

À l'égard des salariés amenés à travailler chez le client

Prévoir des clauses contractuelles spécifiques pour ne pas rendre l'entreprise coupable de prêt de main-d'œuvre illicite, voire de délit de marchandage.

À l'égard des salariés travaillant au cœur du savoir-faire de l'entreprise

Prévoir une clause de confidentialité, afin d'éviter la divulgation d'informations stratégiques. Il faudra identifier au préalable les populations « à risque ».

4.3.3.2 La sécurité du système d'information

- Mettre en place des règles de sécurité du système informatique.
- Sécuriser particulièrement les traitements d'informations nominatives.

4.3.3.3 Les démarches auprès d'organismes extérieurs

- Déposer les logiciels créés par l'entreprise auprès de l'Agence pour la protection des programmes (APP).

  L'entreprise est ainsi en mesure de se défendre dans le cadre d'une action en contrefaçon.

- Effectuer la déclaration des traitements de fichiers nominatifs à la Cnil.

  La non-déclaration de traitement automatisé de données est un délit, qui peut engager la responsabilité d'une personne physique ou morale.

- Veiller à procéder à une régularisation de cette déclaration auprès de la Cnil en cas de modifications.

  Il s'agit de prémunir l'entreprise contre le risque de détournement de finalité de traitement informatisé de données, qui constitue un délit sanctionné sur le plan pénal.

  La mise en place d'un responsable des données personnelles pour le compte de l'entreprise permettra d'alléger la charge de travail et la responsabilité du DSI et d'identifier clairement un interlocuteur de la Cnil dans l'entreprise.

- Déposer le ou les noms de domaine auprès d'un bureau d'enregistrement.

  Le nom de domaine est objet de propriété intellectuelle et peut constituer un élément d'actif valorisable.

- Déposer une demande de brevet des logiciels créés par l'entreprise auprès de l'INPI ou de l'OEB s'ils sont indissociables d'un procédé industriel brevetable ou s'ils produisent un effet technique.

L'entreprise bénéficie ainsi d'un monopole d'exploitation et double la protection de la forme du logiciel par une protection du fond du logiciel.

4.3.3.4 Les données nominatives

- Collecter les informations nominatives par le biais de moyens loyaux.
- Interdire la collecte de certaines informations.
- Informer les personnes « fichées » de leurs droits.
- Assurer la sécurité des données nominatives.
- Utiliser les données collectées dans la seule finalité prévue à la déclaration.
- Ne pas entraver l'action de la Cnil.

4.3.3.5 Les contrats

Le rôle du DSI est essentiel. Sans revenir sur les clauses devant faire l'objet d'une attention particulière, le cabinet Alain Bensoussan recommande aux DSI de suivre la *check-list* suivante.

- Savoir distinguer les différents types de contrats.
- Gérer l'avant-contrat.

  Il s'agit d'éviter que l'entreprise ne voie sa responsabilité engagée en cas de rupture brutale des pourparlers.

- Avant la signature du contrat, ne pas sous-estimer la valeur de la proposition commerciale.

  Le DSI doit porter une attention toute particulière à l'utilisation de notions telles que « maîtrise d'œuvre », « obligation de moyens », « obligation de résultat », « solution clé en main »...

  La coordination avec la direction juridique est à cette étape essentielle pour élaborer l'architecture contractuelle et prévoir la rédaction d'un véritable contrat envisageant tous les aspects.

- Avant la signature du contrat, connaître les obligations des parties dans le domaine informatique, l'incidence juridique de certaines notions techniques.
- S'assurer que les risques associés aux produits ou services sont couverts par une police d'assurance appropriée.

5. COMMENT LE DSI PEUT-IL FAIRE DU DROIT UN OUTIL STRATÉGIQUE ?

Par sa connaissance des produits technologiques existant sur le marché, le DSI peut aider techniquement à la mise en place d'un dispositif de *veille juridique*. Mais le DSI est également acteur de l'*intelligence juridique* par le biais du droit des nouvelles technologies.

L'intelligence juridique est une forme poussée et une démarche proactive de la veille juridique. Basée sur la recherche, le traitement et l'analyse des informations juridiques, elle peut aussi impliquer une action de lobbying. Par intelligence juridique, il faut en effet entendre l'organisation des ressources informationnelles en matière juridique en vue de la prise de décisions stratégiques.

Cette approche anglo-saxonne de la connaissance permet de conférer au droit un caractère dynamique, visant à en faire un atout stratégique pour l'entreprise.

Le DSI est personnellement concerné par l'intelligence juridique appliquée aux nouvelles technologies du fait de leur déploiement considérable depuis que l'informatique est devenue communicante. Le droit des NTI peut être exploité, souvent par des processus conventionnels, devenant ainsi un véritable outil stratégique.

Dans les NTIC, passer de l'information à la communication

L'informatique s'est historiquement développée autour de la saisie, du traitement et de la mise à disposition de données. La dématérialisation de l'économie a favorisé le développement de nouveaux services de collaboration et d'échange interentreprises ainsi qu'entre les entreprises et l'administration.

Les textes juridiques les plus récents ont consacré cette évolution vers la transmission des données et des actes juridiques :

- La loi du 13 mars 2000 a intégré la signature électronique dans le Code civil pour en faire le principal moyen de preuve de l'écrit électronique télétransmis.
- La loi du 21 juin 2004 sur la confiance dans l'économie numérique (LCEN) permet, entre autres innovations, de négocier les affaires par voie électronique et de former les contrats en ligne.

Subir le droit ou en tirer parti

Dans sa vie professionnelle comme dans sa vie personnelle, chacun est responsable de ses actes et de ses choix. La première rencontre de l'homme avec le droit peut se dérouler sur le terrain de la responsabilité qui va de pair avec la prise de

risque juridique. Mais dans tout secteur de la vie professionnelle ou personnelle un tant soit peu organisé, les facettes juridiques visibles sont surtout bloquantes. Elles proviennent généralement :

- soit de la mise en jeu du droit pénal (piratage et intrusion dans les systèmes, protection du logiciel...) ;
- soit de l'obligation d'accomplir des formalités administratives (déclaration à la Cnil, autorisations pour la cryptographie, déclarations de système de télétransmission de facture, etc.) ;

Les aspects juridiques sont d'abord contraignants avant d'être positifs et de se prêter à une exploitation opérationnelle. Il en va ainsi lorsqu'il s'agit d'utiliser l'outil juridique comment un moyen de valider, de planifier ou d'organiser les activités professionnelles. Cet espace juridique de liberté repose sur l'emploi d'instruments conventionnels (convention, contrat, protocole d'accord, MOU, politique, charte de bonne conduite ou de bonnes pratiques, etc.)

5.1 Développer la dématérialisation des écrits

Le développement de l'informatique communicante permet à l'entreprise de passer au commerce électronique avec ses partenaires commerciaux ou aux téléprocédures dans ses relations obligatoires avec les administrations. Ainsi est mis en évidence un important besoin de dématérialisation des actes et des procédures qui doit s'accompagner d'une sécurisation des échanges électroniques, le tout modélisé et développé dans un cadre contractuel.

5.1.1 Les incitations des pouvoirs publics à la dématérialisation

Simplifier la vie des entreprises, les aider à franchir le pas vers le commerce électronique et amener les services de l'État et les organismes sociaux à se moderniser, tel est le triple enjeu de la dématérialisation des procédures administratives. Dans cette optique, la dématérialisation *via* internet est tout à fait compatible avec les travaux de normalisation sur Edifact en cours. La dématérialisation constitue un enjeu gagnant-gagnant entre les administrés et les administrations ou organismes sociaux, elle s'inscrit pleinement dans le programme de simplification administrative engagé les pouvoirs publics.

Le développement des téléprocédures

Le plan actuel du gouvernement en matière de NTIC, RE/SO 2007, prévoit la mise en œuvre de deux téléprocédures par an et par ministère d'ici l'année 2005. Comme les systèmes d'information des administrations ne peuvent être profondément modifiés en quelques mois, les services qui font intervenir plusieurs administrations différentes devront être développés à

l'extérieur des systèmes d'information existants, dans un « *middle-office* », à charge pour ce dernier de s'adapter aux contraintes des administrations avec lesquelles il doit échanger des données.

Le plan pour l'administration électronique Adele constate que les services proposés aujourd'hui par les administrations correspondent encore trop souvent aux attentes des administrations plus qu'aux besoins réels des usagers, qu'il s'agisse des citoyens, des entreprises ou des associations[33].

Pour accélérer la mise en œuvre de l'administration de service, centrée sur les besoins des usagers, les pouvoirs publics ont décidé d'intensifier la création de nouveaux services dématérialisés, et d'enrichir ou de faire évoluer les services existants afin qu'ils répondent de mieux en mieux aux attentes de leurs publics. À cette fin, 140 services nouveaux ou enrichis, dont la description figure dans le plan d'action accompagnant le plan stratégique, seront ouverts durant la période 2004-2007.

Une évaluation annuelle du degré d'avancement des projets sera présentée chaque année par l'Adae, afin d'en rendre compte au Gouvernement, au Parlement et aux citoyens. Les principaux indicateurs seront les suivants :

- le taux de dématérialisation des échanges avec les usagers, c'est-à-dire le pourcentage des échanges entre usagers et administrations effectués sous forme dématérialisée : aujourd'hui 20 % de services nouveaux, l'objectif à fin 2006 étant de la moitié et à fin 2007 des deux tiers.
- le taux de téléprocédures : le pourcentage des procédures par voie dématérialisée est aujourd'hui de 15 %, l'objectif à fin 2006 étant les 2/3 et à fin 2007 de 100 %.
- le taux de dématérialisation concernant les nouveaux usagers de l'administration électronique, nouveaux contribuables, nouveaux chefs d'entreprise : aujourd'hui le taux n'est pas connu ; l'objectif à atteindre fin 2006 est de la moitié et à fin 2007 des trois-quarts.

De la facture EDI au courriel-facture signé

Les textes réglementaires peuvent aussi inciter les entreprises à la dématérialisation. Une illustration désormais classique et bien connue des DSI est celle de la facture.

La facture est un document possédant plusieurs facettes : elle est à la fois une pièce commerciale, comptable et fiscale pour la TVA. La dématérialisation de la facture commencée dès 1990, avec l'EDI et à l'exclusion de la télécopie et du Minitel, est un véritable champ d'expérimentation pour le droit de la

[33] « *Plan stratégique de l'administration électronique (PSAE) 2004-2007* », sur www.adae.gouv.fr.

dématérialisation. Le dispositif réglementaire de la « facture transmise par voie électronique » s'est élargi avec la transposition d'une directive n°2001/115 du 20 décembre 2001 traitant de facturation électronique. L'article 289 du Code général des impôts (CGI) puis l'article 96 F de l'annexe III du CGI maintiennent le dispositif EDI antérieur mais lui ajoutent un nouveau cas, celui de la facture électronique *stricto sensu*, en pratique, un courriel-facture signé.

La réglementation fiscale ouvre un nouveau champ d'application à la signature électronique. En effet, elle n'impose pas qu'une facture soit signée dans le même esprit que le serait un contrat de commerce électronique. Le principe est affirmé par la directive sur la facturation : c'est en vue de sa transmission électronique que la facture doit être sécurisée en authenticité et en intégrité. Il s'agit d'une signature électronique spécifique et non de celle du Code civil qui sert à manifester son accord sur le contenu et à ratifier un acte.

Selon un des décrets d'application (n° 2003-659), la signature à employer doit satisfaire à certaines exigences techniques. Elle doit être propre au signataire, permettre d'identifier le signataire, être créée par des moyens que le signataire puisse garder sous son contrôle exclusif, garantir le lien avec les factures auxquelles elle s'attache de telle sorte que toute modification ultérieure de ces factures soit détectable. La signature électronique doit encore reposer sur un certificat électronique dont le contenu, minimaliste, est précisé.

Une des leçons à tirer du cas de la facture électronique est que la dématérialisation doit se concevoir à deux niveaux : sécurisation juridique d'un écrit électronique et sécurisation technique de sa transmission.

En pratique, on peut signer un document en pièce attachée ou le courriel qui le contient, ou encore les deux, une solution qui n'est pas éloignée d'un recommandé électronique pour la sécurisation des échanges électroniques.

5.1.2 La sécurisation des écrits dématérialisés

Le cas des marchés publics

Le Code des Marchés publics, depuis sa refonte, a inclus un article 56 qui traite spécifiquement de la dématérialisation des marchés publics[34]. Un décret d'application (n°2002-692) précise les conditions techniques des procédures dématérialisées. Au total, c'est une palette complète de la dématérialisation des marchés qui est déclinée où l'on peut relever les besoins les plus habituels en matière de sécurité : l'indentification,

[34] Le nouveau Code des marchés publics a été modifié par un décret n°2004-15 du 7 janvier 2004.

l'intégrité, la confidentialité, l'horodatage, le contrôle d'accès et la vérification des attributs.

Les besoins de sécurité sont regroupés soit individuellement soit collectivement dans de véritables services de sécurisation à créer, par exemple, en ce qui concerne :

- la désignation et l'identification du mandataire parlant au nom des soumissionnaires à chaque transmission électronique ;
- la signature électronique sécurisée pour le soumissionnaire du marché qui souhaite procéder à un double envoi ;
- l'horodatage et la signature électronique sécurisée du soumissionnaire déterminant la date certaine de réception du côté de l'administration ;
- l'accusé de réception électronique de l'administration destinatrice des soumissions ;
- la confidentialité des soumissions pour assurer l'égalité de tous et la concurrence, etc.

La leçon à tirer de la dématérialisation des marchés publics est que la signature électronique n'est que la première phase d'une demande de sécurisation qui ne peut que s'élargir. Les certificats électroniques des diverses classes permettent de travailler avec plusieurs types de signatures électroniques et les spécifications de certificats de signature, certificats d'attributs et des jetons temporels sont disponibles. Mais les applicatifs permettant de gérer cette complexité manquent encore. Il est dès lors nécessaire de suppléer aux carences techniques par un montage contractuel sur papier tant que l'offre de produits et de services ne s'est pas enrichie.

Les pouvoirs publics pourraient apporter leur contribution à cette problématique qui les touche également. Le plan de renforcement de la sécurité des systèmes d'information de l'État prévoit que soient mises en place des procédures de qualification de prestataires privés en sécurité de l'information et des réseaux, notamment le conseil et l'audit. Il prévoit aussi une implication accrue de partenaires privés dans les actions d'évaluation et de certification des produits de sécurité. L'Adae mènera une étude comparative des partenariats public-privé au niveau européen et international. En fonction des orientations prises, elle mettra à la disposition des administrations des clauses types de contrat selon les prestations envisagées et les catégories de marchés publics[35].

[35] Cf. le rapport stratégique de l'Adele précité.

La dématérialisation et la sécurisation par le contrat

Le Droit, même lorsqu'il montre un net caractère technologique, est souvent insuffisant pour organiser le cadre juridique d'application de type NTIC complexe ou innovante. Les partenaires en affaires par échanges électroniques feront naturellement leur propre loi par un dispositif contractuel où ils assembleront les moyens et parades technologiques pour organiser les besoins propres à la dématérialisation et à la sécurisation, tel l'accord d'interchange de l'EDI. L'analyse juridique du dispositif technique ainsi que les dispositions contractuelles complémentaires constituent une sorte de montage juridique nécessaire entre les parties ou devant la justice.

Dans les relations interentreprises, la notion du cadre juridique à créer est généralement mal compris : il s'agit en priorité d'établir un cadre juridique valide et convenable entre les deux partenaires à l'échange. L'action des pirates et des fraudeurs doit naturellement être considérée, mais dans un deuxième temps, car ils ne sont pas invités dans le processus d'affaires. Il faut donc :

- organiser le cadre juridique par un montage contractuel ;
- procéder aux opérations de dématérialisation à droit constant nécessaires ;
- valider juridiquement les contenus électroniques qui se sont substitués à la correspondance commerciale ou administrative par des mesures sécuritaires adaptés ;
- veiller à ce que les transmissions électroniques ne remettent pas en cause les caractéristiques juridique en s'assurant d'une part du maintien de la chaîne de confiance et d'autre part de la traçabilité des opérations et traitements ;
- procéder à un archivage adapté.

Il faut ainsi considérer la Technique et le Droit comme deux disciplines complémentaires en prenant garde aux interférences.

5.2 Distinguer le Droit de la Technique

Les applications des NTIC sont souvent complexes et supposent dans l'entreprise la prise en compte d'un certain nombre de matériels, de logiciels, d'équipements, de produits et services existants. Le DSI doit faire son marché dans ce qui est disponible sur le marché. Le Droit est à cet égard structurant : les exigences légales et réglementaires, puis contractuelles forment autant de critères juridico-techniques permettant au

DSI de faire des choix précis ou au contraire, d'éliminer certains produits.

La dématérialisation des écrits et la sécurisation des échanges électroniques posent une problématique juridique qui est résolue efficacement par des mesures sécuritaires. En effet, les principales garanties offertes par les moyens sécuritaires correspondent également à des attentes juridiques : identification, confidentialité, intégrité, contrôle d'accès, protections diverses, etc. À cause de l'interpénétration du Droit et de la Technique, il faut savoir distinguer dans les notions communes ce qui appartient à l'une et à l'autre, ainsi :

- l'archivage électronique ne correspond pas nécessairement à l'archivage juridique (« la conservation ») ;
- la signature électronique du code civil ne retire rien à l'intérêt et à la pertinence de la signature numérique des techniciens.

D'autant que dans certaines applications, les deux aspects, sécurité technique et sécurité juridique, peuvent être utilisés.

5.2.1 Archivage technique et conservation juridique

Pourquoi pratiquer l'archivage électronique dans les entreprises ? Les réponses sont multiples : préserver le patrimoine de l'entreprise, répondre à des obligations (légales et réglementaires), constituer des preuves, etc. Elles prennent en compte les enjeux techniques, commerciaux ou administratifs qui se présentent à l'entreprise.

Les entreprises s'appuient depuis longtemps sur leur historique soit pour garder la mémoire du passé soit pour servir de socle à leur expansion économique : conserver et retrouver facilement la trace des documents et des communications est vital. Pour le Droit, la motivation est différente. Les fichiers de données et les écrits dématérialisés qui ne sont plus dans une phase active sont archivés pour être en mesure d'apporter la *preuve* en cas de besoin, ce qui est le moyen par lequel les adversaires confortent leurs *prétentions* pour entraîner la conviction du juge. Archivage et preuve (et accessoirement, signature électronique) sont liés dans les NTIC, le Conseil d'État l'a montré en 1998 dans son rapport « *Internet et les réseaux numériques*[36] ».

La conséquence pratique principale porte sur la durée de l'archivage. C'est la survenance de la prescription légale (10 ans pour le commerce, 30 ans pour le civil, etc.) qui met un terme à la durée de conservation légale et non la durée de vie des supports de stockage.

[36] Ce rapport est disponible sur www.internet.gouv.fr/rubrique.php3?id_rubrique=229.

5.2.2 Signature numérique et signature électronique

La signature numérique[37] a été mise au point par les spécialistes de la sécurité pour satisfaire à certains de leurs besoins comme l'identification, l'intégrité et la non-répudiation. Le moyen est efficace et semble appelé à un important déploiement dans les années à venir. Mais il présente le défaut de porter le nom d'un concept important chez les juristes qui y mettent leur propre signification.

Encouragée en cela par une directive européenne, la France n'a pas manqué de se doter d'une législation spécifique en matière de signature électronique intégrée dans le Code Civil. L'instrument répond ainsi à un besoin juridique fondamental : la signature manifeste le consentement du signataire au contenu de l'écrit signé et lui donne une certaine authenticité utile en cas d'administration de la preuve.

Outre cette utilisation typiquement juridique, la signature électronique présente plusieurs utilités dans le cycle de vie de l'écrit sous forme électronique, ainsi :

- la signature électronique valide le passage de l'écrit papier à l'écrit électronique (dématérialisation) et le ratifie en cas de besoin ;
- la signature électronique sécurise la transmission de l'écrit électronique et assure une intégrité nécessaire à sa mise en archive.

Selon les cas, la signature électronique devra assurer la sécurisation juridique ou la sécurisation technique, en s'appliquant soit au courriel, soit à la pièce attachée, soit encore aux deux.

5.3 Anticiper sur la transposition des normes juridiques européennes

Les directives européennes relatives à la société de l'information arrivent dans notre pays à flux continu.

Il peut donc être pertinent pour une DSI ou une direction juridique (DJ) de mettre en place ou de mutualiser une veille juridique orientée vers l'Europe afin d'être en mesure d'anticiper les nouvelles dispositions contenues dans les directives à transposer.

Les directives, l'équivalent de lois-cadres européennes, engagent les États membres, qui doivent les transposer dans leur droit national, dans les délais impartis par la directive elle-même (18 mois en moyenne). Cette transposition est essentielle pour le bon fonctionnement du marché intérieur.

[37] Une signature basée sur des moyens de cryptographie asymétrique (biclé, certificat électronique, AC et PKI) et qui garantit l'identification, l'intégrité et la non-répudiation.

Le terme de *transposition* indique comment les normes européennes pénètrent le droit interne français. Il ne s'agit pas de recopier mot à mot le texte européen en langue française, mais de l'intégrer harmonieusement au droit existant (s'il n'y a pas contradiction) avec une touche plus ou moins appuyée de génie juridique national. Pour prendre un exemple récent, la *directive 1999/93 du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques* a été transposée en droit français par une *Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relatif à la signature électronique*. La valeur ajoutée de la transposition réside dans « l'adaptation du droit de la preuve… » qui sert de pierre d'achoppement à l'*écrit sous forme électronique*. L'écrit électronique est pour le juriste une véritable révolution autrement plus marquante que la signature électronique.

5.3.1 Des délais de transposition incompatibles avec le déploiement des TIC

La plus grande difficulté n'est pas de transposer, mais de transposer dans les temps. Or la France a de médiocres résultats en ce domaine.

La cause principale du déficit de transposition français est d'ordre administratif. Un rapport du Sénat[38] observe que le dysfonctionnement administratif en cause a été repéré depuis longtemps, qu'il a été autrefois souligné par le Conseil d'État, et que pas moins de quatre circulaires du Premier ministre ont tenté d'y remédier ces dernières années. La nature de ce dysfonctionnement est bien connue :

- d'une part, les effets sur le droit interne des projets de directive ne sont pas pris en compte dans les négociations ;
- d'autre part, la coordination interministérielle n'est pas suffisamment efficace, de telle sorte que les désaccords entre administrations aboutissent à des blocages durables.

Le coût de la non-transposition pour la France est élevé, tant au niveau juridique (incertitudes juridiques, contentieux multiples) que politique (risque d'une perte de crédibilité sur la scène européenne). Les plus récents rapports d'information des délégations de l'Assemblée nationale et du Sénat pour l'Union européenne sur la transposition des directives ont dressé le bilan français en s'appuyant sur un document publié chaque semestre, depuis novembre 1997, par la Commission européenne, le « tableau d'affichage du marché intérieur ». Selon ce document, dans la mise en œuvre du cadre juridique

[38] Rapport d'information n° 250 (2001-2002) - Délégation du Sénat pour l'Union européenne, Hubert Haenel.

du marché intérieur, notre pays est celui qui accuse le plus de retard[39].

Le plan d'action présenté par le ministre délégué aux affaires européennes en novembre 2002 a amorcé un mouvement. En dépit de l'arrivée à échéance de plus de 40 nouvelles directives, le déficit de transposition a été réduit à 3,3 % au 15 avril 2003, ce qui a permis à la France de se situer désormais en dixième position dans l'Union européenne. L'effort doit désormais se poursuivre et s'intensifier, pour atteindre l'objectif de 1,5 % et prévenir, dans le futur, toute accumulation de retards.

5.3.2 Les risques mesurés de l'anticipation

Dans le monde de l'informatique communicante, ne pas transposer rapidement peut occasionner un préjudice réel pour l'entreprise.

Le DSI pourrait surseoir à de nouvelles applications ou de nouveaux services faute de régulation juridique, tandis que des entreprises situées dans des pays ayant transposés en temps utiles bénéficient d'un indéniable avantage concurrentiel.

La transposition des directives peut se faire *a minima*, mais elle montre souvent une certaine valeur ajoutée. Aussi le risque n'est pas grand d'anticiper sur la partie « dure » de la directive qui sera de toute façon et quel que soit le débat, incorporée dans le droit national. Il arrive même que les principes de la directive soient très minimalistes. Il en va ainsi pour l'exemple cité plus haut : la directive 1999/93 du 13 décembre 1999 sur le signature électronique ne vise qu'un « cadre communautaire » pour faciliter les échanges internes à l'UE.

Le risque n'est pas très grand d'anticiper sur des règles juridiques qui seront tôt ou tard créées.

Si une personne ou une entreprise se trouvait en grave difficulté pour avoir anticipé face à une autre personne, une entreprise ou les pouvoirs publics, elle pourrait requérir l'aide du juge. Ainsi une *question préjudicielle* peut être posée en ce qui concerne l'interprétation ou la validité d'une règle de droit européen. Le juge national peut ou doit, selon les cas, saisir la CJCE (Cour de justice des Communautés européennes) qui dira de quelle façon il faut interpréter la règle en cause, en lui laissant le soin de trancher le litige. Bien mieux selon une évolution récente, le juge peut reconnaître un *effet direct* à une directive européenne non transposée.

[39] Rapport d'information, Délégation de l'Assemblée nationale pour l'Union européenne sur la transposition de la directive concernant des règles communes pour le marche intérieur du gaz naturel, M. Christian Philip, novembre 2002.

5.4 Prendre la mesure des normes juridiques étrangères

La mondialisation conduit les plus grandes entreprises françaises à déployer leurs relations commerciales à l'international. Parmi les pays cibles pour l'exportation des produits et services figurent les USA. Le poids du leader américain est tel que son système juridique déborde les frontières et s'impose quelquefois dans les sociétés étrangères quand bien même leur siège social serait-il installé en dehors du territoire américain.

En sus de l'obligation de respecter le droit de leur pays d'origine, ces sociétés se voient contraintes de rester « compatibles » avec le droit américain. La question est délicate : doit-on admettre l'application extraterritoriale d'un droit étranger ?

5.4.1 L'application universelle de la loi américaine

Les pratiques commerciales des entreprises américaines mêlent protectionnisme, expansionnisme et rejet du multilatéralisme[40]. Deux approches principales se conjuguent pour expliquer la situation actuelle :

- d'abord, une propension à édicter des lois ou des sanctions économiques à caractère extraterritorial en violation du droit international ;
- d'autre part, le durcissement de l'attitude précédente du fait du développement international du terrorisme et des événements du 11 septembre 2001.

La propension à édicter des lois à caractère extraterritorial est ancienne. C'est un des moyens par lequel les USA tentent d'établir ou de maintenir une position dominante, voire monopolistique, principalement dans les industries aéro-nautiques, des hautes technologies ou de la défense[41]. Le Code de l'OCDE sur les flux transfrontaliers de données, pris dans le cadre de l'accord multilatéral sur l'investissement (AMI) en est une récente illustration. À cette occasion, la France s'était opposée à la transmission des données bancaires pouvant servir à l'application de la législation américaine antitrust.

Depuis les événements du 11-Septembre, le système américain s'ajuste structurellement au déploiement du terrorisme international, tant à l'intérieur qu'à l'extérieur. La sécurité nationale renvoie désormais aussi bien à la projection de

[40] Communication à l'Assemblée Nationale, le 22 octobre 1998 de M. Jean-Claude Lefort, rapporteur d'information sur les relations économiques entre l'Union européenne et les Etats-Unis
[41] Rapport du Parlement européen sur le réseau Echelon dirigé par la NSA (l'Agence nationale de sécurité) sur www.europarl.eu.int.

puissance à l'extérieur qu'à la *homeland security* et à l'action transnationale. Le FBI est devenu l'instance juridique américaine transnationale. Les agences de renseignement militaires, la NSA et le NRO, sont impliquées dans les opérations de protection des systèmes informationnels civils. L'intégration entre le FBI, la CIA et le Pentagone est désormais assurée par le plan Counter-Intelligence 21 (CI-21)[42]. Ce plan donne les bases constitutionnelles à une refonte du renseignement qui prend en compte l'application élargie du droit américain (*American law enforcement*) la collecte du renseignement à l'étranger (*foreign intelligence gathering*[43]) et l'état de préparation de la défense (*defense preparedness*[44]).

5.4.2 Une application volontariste dans le secteur des TIC

Deux exemples permettent d'illustrer l'application extraterritoriale des normes juridiques américaines pour les activités NTIC des entreprises en liaison avec les intérêts américains.

Le 21 CFR part 11

La facilité d'accès, de modifications et d'altérations de tout système informatique nécessite la mise en place de mesures de sécurité pour s'assurer que seules les personnes autorisées sont habilitées à avoir accès et à recevoir des informations leur étant destinées. Aussi un texte réglementaire a-t-il été édicté en août 1997 par la Food and Drug Administration (FDA). L'objectif est de prévenir les fraudes tout en permettant l'accès à toutes les nouvelles technologies électroniques afin de réduire les coûts engendrés par les processus papier.

Parmi les dispositions de ce texte, un règlement *21 CFR Part 11* s'intéresse aux enregistrements électroniques et aux signatures électroniques. Ce règlement reconnaît la validité des documents électroniques en tant qu'éléments de référence sans exiger la forme papier traditionnelle. Les systèmes et applications soumis à ce règlement sont principalement la gestion électronique de document (EDMS) et les systèmes de type MRP/ERP. La réglementation 21 CFR Part 11 définit les critères selon lesquels les dossiers et signatures électroniques sont considérés comme équivalents à des dossiers sur support papier et des signatures manuscrites. Elle s'applique aux dossiers sous forme électronique, qui seront créés, modifiés, maintenus, archivés, récupérés ou transmis dans le cadre des exigences liées à tout dossier décrit dans la réglementation de la FDA. En résumé, le règlement 21 CFR

[42] Cf. http://www.nacic.gov/pubs/online/ci-21.html.
[43] Cf. http://www.epic.org/privacy/terrorism/fisa/.
[44] « *L'hégémonie américaine après le 11 septembre* », Saïda Bédar, Le Débat Stratégique n° 58, septembre 2001.

Part 11 ne pose aucune exigence en matière d'utilisation des enregistrements et des signatures électroniques. Il se contente de préciser les règles conditionnant leur acceptation.

Primitivement, ces règles s'appliquaient aux industries pharmaceutiques et médicales, puis se sont étendues à l'ensemble des industries agroalimentaires, la chimie, les cosmétiques, etc. L'essentiel du texte a été repris par d'autres secteurs économiques. Un texte de niveau fédéral a même été signé le 30 juin 2000 par Bill Clinton : « *Electronic Signatures in Global and National Commerce Act* » (S761).

La loi Sarbanes-Oaxley

Ce texte constitue une réaction étatique aux scandales fiscaux de Worldcom, de Tyco ou d'Enron. La gouvernance et la conformité ne sont pas de nouveaux enjeux pour les entreprises mais la crise de confiance des investisseurs a entraîné de profondes mutations parmi lesquelles des mesures additionnelles de la SEC, du NYSE et du Nasdaq.

Le *Sarbanes-Oxley Act* du 30 juillet 2002 n'implique aucune exigence en termes de logiciel. Le texte a pour objectif, non pas de réguler les technologies, mais au contraire, les processus.

Les entreprises américaines ou étrangères cotées à la bourse américaine ne sont donc nullement obligées d'investir dans l'informatique, mais doivent se doter de moyens prouvant qu'elles suivent de bonnes pratiques.

Parmi ces moyens, l'audit interne, procédure censée contrôler le bon déroulement des processus d'entreprise.

Il se trouve certes simplifié (car automatisé) grâce à des familles de logiciels rattachés au *business process management* (BPM), à la gestion de contenu ou à l'archivage des courriels. Mais il peut aussi être réalisé manuellement. Outre le contrôle interne, la loi instaure un second niveau de vérification : à la demande d'instances extérieures, les entreprises doivent, en effet, prouver que les audits internes ont convenablement été effectués.

Au total, les entreprises visées doivent se préparer à des contrôles internes ou externes, des processus de certification et à des mesures d'autoprotection contre les lanceurs d'alerte (*whistle-blower protection*), des délais de dépôt accélérés de la SEC, l'application du règlement 17 CFR Part 210 sur la conservation des enregistrements, des procédures comptables de l'IASB (International Accounting Standard Board) pour l'Union européenne et spécifications de l'AICPA et du FASB.

En France, la loi de sécurisation financière (LSF) du 1er août 2003, qui s'adresse cette fois à toutes les entreprises, présente de nombreuses similitudes avec la loi Sarbanes-Oaxley. Le

périmètre de la LSF est plus large, mais son niveau de profondeur plus réduit.

5.5 Faire la part de la sécurisation et du respect de la personne

Certains textes légaux sur les TIC, comme le Sarbanes-Oaxley Act ci-dessus, montrent des effets pervers susceptibles de constituer de véritables atteintes aux droits des personnes.

La sécurisation des échanges électroniques est indispensable pour permettre la dématérialisation des actes juridiques à droit constant, comme exposé plus haut. Mais le concept de « sécurisation » est bien plus large car il englobe dans l'entreprise la sécurisation des locaux comme celle des employés. La sécurisation au sens large est nécessaire pour couvrir une large palette de risques allant de l'espionnage industriel à la prévention du banditisme ou du terrorisme.

Les mesures les plus élémentaires de sécurisation consistent à établir avec certitude *qui est qui* et *qui fait quoi* c'est-à-dire, concrètement, à mettre en œuvre des instruments toujours plus puissants pour connaître et vérifier précisément l'identité des personnes ou pour leur imputer des actes ou des événements. Des tendances autant organisationnelles que technologiques s'exercent en ce domaine, comme par exemple :

- la gestion des identités dans l'entreprise ;
- la traçabilité des échanges et des procédures ;
- la cybersurveillance des locaux ;
- la mise en œuvre de mesures biométriques à des fins diverses, etc.

Poussées à leur paroxysme, ces tendances sont susceptibles de porter atteinte aux données personnelles et nominatives des employés, d'empiéter sur les libertés individuelles et la sphère privée (la *privacy* des anglo-saxons).

Le DSI doit déjà veiller au sort des données personnelles et nominatives protégées par la loi Informatique et libertés. Il doit encore anticiper sur les effets pervers des TIC lorsque les applications et services traitent, directement ou indirectement, d'authentification, de sécurisation et de traçabilité, ce qui interfère avec la protection due aux données personnelles et à la vie privée.

Le DSI joue sur ce point un rôle fondamental dans l'entreprise citoyenne et apporte une contribution positive, en marge de l'intelligence économique et de l'intelligence juridique, à la responsabilité sociale et sociétale[45] de l'entreprise.

[45] Sur cette notion, voir l'Observatoire de la responsabilité sociétale de l'entreprise : www.orse.org.

6. CONCLUSION : QUELLE DÉMARCHE D'INTELLIGENCE JURIDIQUE POUR LE DSI ?

La démarche d'intelligence juridique constitue aujourd'hui une démarche managériale innovante et une démarche organisationnelle en profondeur face aux enjeux juridiques de l'entreprise.

Le DSI est à la fois « acteur » de l'intelligence juridique et « client » de l'information juridique : « acteur » puisque, garant du processus et de la fiabilité du système d'information, il garantit sur le plan technique la circulation de toutes les informations, y compris les informations juridiques, et « client » par le biais du droit des nouvelles technologies qui s'impose à lui.

Dans les deux cas, son rôle central transparaît au travers de la mise en cause possible de sa responsabilité sur le plan civil et pénal.

Inversement, le DSI peut de manière positive contribuer à l'aménagement des règles juridiques : par exemple au niveau des contrats par un travail sur les clauses juridiques des contrats informatiques ; ou par exemple au niveau du cadre réglementaire par des actions de *lobbying* et d'influence directes ou *via* des organismes représentatifs.

Le droit est omniprésent. Le DSI, comme tout directeur d'ailleurs, ne peut en faire abstraction, et il ne se résume pas aux contrats informatiques. Ce qui traduit une règle juridique, c'est qu'elle offre une référence et que cette référence est susceptible d'être mise en question devant un juge.

Mais compte tenu de la technicité et de la complexité du droit et de l'informatique, le directeur juridique et le DSI doivent travailler ensemble sur les sujets qui leur sont communs, la propriété intellectuelle, les contrats, les déclarations de traitements informatiques par exemple. Il s'agit au final de connaître le droit de l'informatique pour se protéger d'éventuelles poursuites judiciaires, mais aussi pour asseoir la position concurrentielle de l'entreprise.

Le DSI peut adopter aujourd'hui soit une approche défensive soit une approche offensive du droit des TIC. L'approche défensive consiste à se mettre en conformité avec le droit des TIC ; l'approche offensive consistera dans l'utilisation du droit – bien évidemment dans le respect de la légalité et de la jurisprudence – comme un levier vis-à-vis de ses fournisseurs, de ses concurrents et de ses partenaires. Dans la pratique, il ne faut pas opposer les deux approches mais plutôt les juxtaposer : selon les besoins, le secteur d'activité, le degré de concurrence et le degré de maturité, l'entreprise adoptera des stratégies mixtes, combinant des éléments défensifs et offensifs (cf. infra).

	Approche réactive	***Approche proactive***
Stratégie	Approche par les risques Non implication dans la fabrication du cadre légal Mise en conformité au cadre réglementaire	Approche par les opportunités Influence sur la fabrication des normes et du cadre légal Utilisation du droit comme un levier vis-à-vis de ses fournisseurs, de ses concurrents et de ses partenaires
Domaines d'action	Le traitement des données à caractère personnel La cybersurveillance Les chartes d'usages L'archivage La sécurité La responsabilité Les normes sectorielles (Bâle II)	Le droit des contrats informatiques La propriété intellectuelle Le nommage internet La dématérialisation Influence sur les standards
Méthodes et leviers	Veille ponctuelle en aval Partenariat ponctuel avec la direction juridique Absence de pilotage Absence de contrats cadres ou de clausiers types Mettre en place des moyens de prévention adaptés Arbitrer entre sécurité et respect de la personne	Veille systématique, amont - aval Partenariat systématique avec la direction juridique, direction achats ou recrutement d'un juriste spécialisé Tableaux de bords Contrats cadres et clauses type Brevets et réflexion sur la valorisation des actifs immatériels Anticipation de la transposition des directives Prise en compte des normes étrangères Délégation de responsabilité

Source : Cigref

Figure 13 : Quelle démarche d'intelligence juridique pour le DSI ? (Synthèse)

En définitive, sans être un spécialiste du droit, le DSI doit ouvrir son champ de connaissance, être « bilingue » au sens de Jean-Pierre Corniou, président du Cigref, dans son ouvrage « La société de la connaissance ». L'information qu'a à connaître le DSI n'est plus seulement d'ordre technique ou organisationnelle. Elle renvoie plus largement à l'environnement social et sociétal de l'entreprise.

Annexe 1 : Bibliographie

- **Ouvrages**

Lamy « Droit de l'informatique et des réseaux », éd. 2001

Le droit du travail à l'épreuve des NTIC, *Jean-Emmanuel Ray*, Ed. Liaisons, mai 2001.

Cyberdroit : Le droit à l'épreuve de l'internet, *Christiane Féral-Schuhl*, Dalloz-Dunod, 3e éd. 2002.

Le tableau de bord juridique des DSI, *Cabinet d'avocats A. Bensoussan*, Ed. Gartner, mars 2000.

La cybersurveillance dans l'entreprise - Traquer et être traqué, *Marie-Pierre Fénoll-Trousseau*, Gérard Haas, Ed. Litec, 2000.

- **Revues**

Le Monde Informatique, www.veblmi.com

Le Journal du Net, www.journaldunet.com

01 Net, www.01net.com

Juritel, www.juritel.com

- **Rapports du Cigref**

La sécurité à l'heure d'internet, octobre 2000

Internet dans l'entreprise, avril 2001

Impacts et usages de la messagerie électronique, octobre 2000

Intelligence Economique et Stratégique, septembre 2003

Annexe 2 : Travaux issus de la Charte Cigref - Syntec Informatique

(Communiqué du 31 mars 2004)

La charte Cigref – Syntec informatique, un an après...

Le Cigref, représentant les grandes entreprises de tous les secteurs d'activité, et Syntec informatique, Chambre professionnelle des SSII et des éditeurs de logiciels, rendent publics aujourd'hui quatre guides pour favoriser la réussite des projets informatiques. Résultat d'un an de travaux communs aux deux organisations, ces guides de « bonnes pratiques » font suite à la signature, le 24 février 2003, d'une charte commune de déontologie. Ils adaptent et déclinent les 10 orientations déontologiques de la charte* aux quatre métiers fondamentaux : conseil en organisation et systèmes d'information ; ingénierie et intégration de système ; progiciels ; infogérance et tierce maintenance applicative. Ces textes d'application de la charte explicitent la définition des activités et le périmètre des projets et déterminent les missions respectives des signataires.

La synergie entre l'exigence du client et l'expertise du prestataire

Qualité, productivité et prévention des risques constituent les critères clés pour une maîtrise du cycle de la prestation et de la performance des réalisations. Ces facteurs s'appuient sur la mise en exergue, dès le cahier des charges, d'un tableau de bord définissant les exigences concernant les processus et résultats et identifiant les freins et accélérateurs pour une meilleure perception des contraintes. Ils doivent être appréhendés et suivis conjointement par le client et le prestataire afin d'assurer une transparence dans leurs relations.

La confiance comme vecteur de transparence

Une collaboration, fondée sur une confiance mutuelle et l'acceptation des préoccupations de l'autre partie, constitue un facteur majeur de réussite et de performance durable.
Le client et son fournisseur doivent entretenir des échanges, tout au long du projet, sur l'ensemble des problématiques et contraintes (opérationnelles, techniques, financières...), les cultures d'entreprise, la perception de la qualité de la réalisation. Les démarches positives — telles que le décloisonnement des équipes, l'harmonisation des modes de fonctionnement, la mise en forme d'une communication commune — contribuent à une meilleure compréhension entre direction des systèmes d'information et prestataire.

S'adaptant à l'innovation spécifique aux métiers des technologies de l'information, les propositions préconisées par les experts du Cigref et de Syntec informatique demeurent évolutives et les textes d'application de la charte feront l'objet d'une actualisation régulière.

**** Les 10 points de la charte sont les suivants : Connaissance des métiers ; Transparence ; Impartialité ; Indépendance d'opinion et d'expression ; Qualité ; Innovation ; Diffusion de l'information ; Partage des connaissances ; Productivité ; Suivi de la charte.***

Annexe 3 : Loi sur la confiance dans l'économie numérique – 13 mai 2004

Présentation sommaire du projet de loi

Voir :

http://www.assemblee-nationale.fr/12/ta/ta0285.asp

http://www.senat.fr/leg/tas03-075.html

TITRE Ier - DE LA LIBERTÉ DE COMMUNICATION EN LIGNE

CHAPITRE Ier - La communication au public en ligne

CHAPITRE II - Les prestataires techniques

CHAPITRE III - Régulation de la communication

TITRE II - DU COMMERCE ÉLECTRONIQUE

CHAPITRE Ier - Principes généraux

CHAPITRE II - La publicité par voie électronique

CHAPITRE III - Les obligations souscrites sous forme électronique

CHAPITRE VII - Des contrats sous forme électronique

TITRE III - DE LA SÉCURITÉ DANS L'ÉCONOMIE NUMÉRIQUE

CHAPITRE Ier - Moyens et prestations de cryptologie

- Section 1 - Utilisation, fourniture, transfert, importation ; et exportation de moyens de cryptologie
- Section 2 - Fourniture de prestations de cryptologie
- Section 3 - Sanctions administratives
- Section 4 - Dispositions de droit pénal
- Section 5 - Saisine des moyens de l'Etat pour la mise au clair de données chiffrées
- Section 6 - Dispositions diverses

CHAPITRE II - Lutte contre la cybercriminalité

TITRE IV - DES SYSTÈMES SATELLITAIRES

TITRE V - DU DÉVELOPPEMENT DES TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION

CHAPITRE Ier - De la couverture du territoire par les services numériques

CHAPITRE II - De la liberté concurrentielle dans le secteur des télécommunications

TITRE VI - DISPOSITIONS FINALES