cigref
Réseau
de Grandes Entreprises

PROMOUVOIR LA CULTURE NUMERIQUE

COMME SOURCE D'INNOVATION ET DE PERFORMANCE

Gouvernance juridique de l'Entreprise Numérique

Octobre 2012

Le CIGREF, réseau de Grandes Entreprises, a été créé en 1970. Il regroupe plus de cent très grandes entreprises et organismes français et européens de tous les secteurs d'activité (banque, assurance, énergie, distribution, industrie, services...). Le CIGREF a pour mission de promouvoir la culture numérique comme source d'innovation et de performance.

Titre du rapport : Gouvernance juridique de l'Entreprise Numérique

Equipe du CIGREF

Jean-François PÉPIN – Délégué général
Sophie BOUTEILLER – Directrice de mission
Anne-Sophie BOISARD– Chargée de recherche
Josette WATRINEL – Secrétaire de direction
Frédéric LAU – Directeur de mission
Matthieu BOUTIN – Chargé de mission
Marie-Pierre LACROIX – Chef de projet
Josette LEMAN – Assistante de direction

Remerciements :

Nous remercions les membres du groupe de travail qui ont contribué à la réflexion :

Catherine PELLETIER - AGIRC ARRCO	Jocelyne VIAZZO – GROUPEMENT DES MOUSQUETAIRES
Nathalie BADAOUI - AREVA	Anastasios IKONOMOU - VALLOUREC
Nathalie JOSSEAUME - AXA GROUP SOLUTIONS	Teresa SANTAMARIA - VEOLIA ENVIRONNEMENT
Chantal PEYRAT - DASSAULT AVIATION	
Isabelle GLACHANT - EURO DISNEY	
Nathalie MASSE - EURO DISNEY	Ainsi que le Cabinet d'Avocats Caprioli & Associés
Grégory SILVAIN - EURO DISNEY	Eric A. CAPRIOLI
Delphine BAZIN-GIRARDET - GEODIS	Pascal AGOSTI
Marc MENCEL - NEXTER GROUP	Isabelle CANTERO
Isaure DE CHATEAUNEUF - SAINT GOBAIN	François COUPEZ

Pour tout renseignement concernant ce rapport, vous pouvez contacter le CIGREF aux coordonnées ci-dessous :

CIGREF, Réseau de Grandes entreprises
21, avenue de Messine 75008 Paris
Tél. : + 33.1.56.59.70.00
Courriel : contact@cigref.fr

Sites internet :
http://www.cigref.fr/
http://www.fondation-cigref.org/
http://www.histoire-cigref.org/
http://www.collection-cigref.org/
http://www.entreprises-et-cultures-numeriques.org

SYNTHÈSE

Le développement de nouvelles pratiques dans l'entreprise, induites par la transformation numérique, bouleverse les conditions de travail en interne, et les relations de l'entreprise avec les parties prenantes (clients, fournisseurs et autres partenaires). Amenée à s'ouvrir sur l'extérieur, l'entreprise doit se protéger juridiquement en mettant en place un certain nombre de mesures. Par ailleurs, le droit a évolué ces dernières années, pour prendre en compte les nouvelles tendances technologiques, et ainsi encadrer les nouvelles pratiques qui se sont développées dans les entreprises.

Face à cela, les dirigeants ne sont pas toujours armés. C'est pourquoi, le CIGREF et le cabinet Caprioli & Associés ont élaboré le présent document, qui recense les nouveaux principes juridiques apparus avec les pratiques du numérique, et les ont confronté aux expériences vécues dans l'entreprise.

Cette publication, **à destination des dirigeants,** aborde les sujets suivants :

- Les délégations de pouvoirs
- Les contrats avec les fournisseurs et les prestataires
- La dématérialisation des documents et des échanges
- Droit des logiciels et des bases de données
- Protection du patrimoine informationnel
- Sécurité des usages numériques
- Les outils de travail collaboratifs
- Le Cloud Computing
- La continuité d'activité
- Développement durable et SI

Les principaux messages clés, que nous pouvons retenir, sont les suivants :

- Les délégations de pouvoirs :
    - Calquer les délégations de pouvoirs sur l'organisation managériale existante
    - Sensibiliser les acteurs de l'entreprise sur la valeur juridique de tout courrier électronique
- Les contrats avec les fournisseurs et les prestataires :
    - Mettre en place des *Requests For Information* préparatoires
    - Mettre en place des comités de pilotage animés par la DSI
    - Prévoir une clause de médiation dans tous les contrats
- La dématérialisation des documents et des échanges :
    - Définir le processus dématérialisé : séquencer le cycle de vie du document, tant d'un point de vue technique, que juridique et métier

- Droit des logiciels et des bases de données :
  - Réaliser une cartographie des applications et des flux associés
  - Intégrer les règles contractuelles en matière de Propriété Intellectuelle dans les contrats de travail des salariés
  - Mettre en place une politique Open Source (gestion des logiciels libres, licences interdites…)
  - Estimer la valeur des bases de données
- Protection du patrimoine informationnel :
  - Sensibilisation à la fonction de Correspondant Informatique et Libertés
- Sécurité des usages numériques :
  - Développer des chartes bien rédigées pour les usages numériques
- Les outils de travail collaboratifs :
  - Mise en place de chartes d'utilisation des réseaux sociaux
  - Mise en place d'une politique de communication
- Le Cloud Computing :
  - Assurer la réversibilité des données
  - Garantir la position géographique des données
- La continuité d'activité :
  - Rédaction de clauses de réversibilité, de disponibilité, de force majeure, de responsabilité
- Développement durable et SI :
  - Rédaction d'une charte de développement durable

SOMMAIRE

INTRODUCTION

A l'heure actuelle, les entreprises ne se contentent plus de faire appel aux systèmes d'information (SI) afin de parfaire leur fonctionnement ou encore dans le but d'optimiser leur rentabilité : les systèmes d'information sont désormais devenus le système nerveux de toutes les entreprises, quels que soient leur taille et leur secteur d'activité. Les applications utilisées par les métiers en interne sont légions. Leur configuration et développement, leur maintenance corrective et évolutive et leur migration doivent être assurés par la Direction des Systèmes d'Information (DSI). Dès lors, tout événement susceptible d'influer sur ces systèmes d'information et sur la masse considérable d'informations qui y circule peut potentiellement avoir des conséquences qui rejaillissent sur l'ensemble de l'activité de l'entreprise. Or, ces événements peuvent prendre les formes les plus diverses : agressions d'ordre externe ou interne telles que les hypothèses les plus évidentes de piratage informatique ou de fraude mais également de non respect des règles internes, d'ajout de nouvelles fonctionnalités ou d'introduction de nouvelles technologies ou encore de l'impact de nouvelles réglementations.

La gouvernance des systèmes d'information implique de tenir compte de l'ensemble de ces facteurs, et de prendre les décisions qui s'imposent afin de répondre aux objectifs de l'entreprise, tout en réduisant les risques les plus divers et en optimisant le fonctionnement du système.

Dans ce nouveau contexte, la principale mission du DSI consiste à aligner les prestations informatiques sur les stratégies « métier » de l'organisation dans le cadre d'une politique d'amélioration globale et durable de la qualité de service.

En effet, le DSI doit non seulement appréhender les besoins présents et futurs de son organisation afin de mettre en place des systèmes d'information permettant à l'entreprise de fonctionner de façon optimale et pérenne, mais il doit aussi définir et mettre en œuvre la politique informatique en accord avec la stratégie générale de l'entreprise. A ce titre, il est chargé de déterminer, mettre en place et gérer les moyens techniques et humains nécessaires aux systèmes d'information et planifier leur évolution dans le cadre d'un schéma directeur. Cela recouvre principalement l'architecture des systèmes, les développements entrepris, la gestion des bases de données, la sécurité de fonctionnement de l'ensemble (disponibilité, intégrité, confidentialité et traçabilité). Le DSI prescrit des orientations dans le but de conseiller au mieux la direction générale dans le domaine des technologies de l'information. Par ailleurs, il assure la gestion des équipes nécessaires à la mise en place et à la maintenance des systèmes d'information. En outre, il doit anticiper les évolutions imposées par la stratégie de l'entreprise, tant celles concernant les impacts techniques et technologiques que juridiques. Il est le responsable du choix des outils, des matériels et des logiciels, ainsi que de l'évolution des systèmes d'information de l'entreprise. La tâche peut

être relativement délicate dans le cadre de groupe de sociétés où le DSI est confronté à des solutions techniques souvent hétérogènes et à des règlementations très différentes.

Afin d'atteindre ces objectifs, chacun des flux d'information et chacun des éléments du système doit être valorisé dans toutes ses composantes : évaluation du coût de production de cette information, de sa valeur pour la société ou ses concurrents, mais également du coût qui serait induit par sa non disponibilité, sa modification, sa divulgation à des tiers ou à des concurrents, ou encore sa destruction ou son altération. Cette valorisation assure la meilleure visibilité possible nécessaire à la prise de décision. Ces exigences de sécurité, qu'elles soient légales ou imposées par des régulateurs dans des domaines spécifiques (secteur financier ou des communications électroniques par exemple), impactent en effet directement le coût pour l'entreprise que vont revêtir la collecte, l'utilisation/traitement, mais également la conservation de chaque donnée concernée.

Par ailleurs, la connaissance des risques pesant sur les SI et les informations qui y sont contenues (risques juridiques notamment) ainsi que leur évaluation, pourra permettre aux DSI de les gérer en permettant la flexibilité, la réactivité ou, plus généralement, la qualité de service qui sont demandées au système d'information.

Ainsi, plus la valorisation des SI et des informations qu'ils contiennent sera pertinente et l'évaluation des risques qui en découlent précise, plus le DSI disposera d'une marge de manœuvre lui permettant de diminuer les risques de tous ordres pesant sur l'entreprise (risque financier, risque d'image, risque contractuel, etc.).

La protection du système d'information d'une entreprise repose donc principalement sur l'anticipation des atteintes qui pourraient lui être portées, alors qu'en parallèle, la valorisation du patrimoine immatériel traité par ce système d'information devient incontournable, ne serait-ce que pour évaluer les moyens à mettre en œuvre pour le protéger.

Or, les débats sur la propriété intellectuelle applicable aux logiciels, les règles restrictives applicables à l'utilisation de certains logiciels dits pourtant « libres » (en fonction de la licence qui leur est applicable), la « notification des incidents de sécurité », le « *green computing* » ou encore les services toujours plus innovants proposés par les prestataires de l'entreprise (virtualisation, outils de travail collaboratif, *cloud computing*, SaaS, etc.) incitent le DSI à prendre en compte, dans le cadre de son activité quotidienne, des problématiques toujours plus diverses.

Ces sujets ont d'ailleurs constitué un catalyseur incontestable pour la mise en place des mesures organisationnelles d'analyse et de gestion des risques, nécessaire à une véritable gouvernance juridique des systèmes d'information.

Si le DSI doit élaborer toute une stratégie concernant la gouvernance des SI, il doit également intégrer la dimension juridique. Ce sont ces éléments juridiques que le présent document se propose de présenter afin de contribuer à la Gouvernance du SI[1].

[1] D'autres sujets, comme le traitement des données à caractère personnel, auraient mérité de plus larges développements ; il a été décidé de le traiter à l'occasion de problématiques plus générales, ex : à propos de la sécurité du patrimoine informationnel, des notifications des failles de sécurité ou du cloud computing.

LES DÉLÉGATIONS DE POUVOIRS

Le chef d'entreprise, pourtant tenu de veiller personnellement au respect de la règlementation applicable dans l'entreprise, ne peut pas toujours en pratique s'en acquitter de façon optimale, en raison par exemple de la taille de l'entreprise, du nombre considérable d'activités, de l'existence de plusieurs établissements ou encore d'une gestion trop importante de son personnel. De ce fait, les tribunaux ont admis que le chef d'entreprise, appelé le **délégant**, puisse confier, par le mécanisme de la délégation de pouvoirs, une partie de ses droits et obligations à un salarié, appelé le **délégataire**. Outre la lettre de mission et l'organigramme de l'entreprise, les délégations de pouvoirs jouent donc un rôle juridique essentiel, car elles se présentent comme un mode de répartition et de transfert de responsabilité pénale.

Or, en matière de management du système d'information, le DSI doit disposer de pouvoirs étendus. C'est pourquoi les obligations et le périmètre de responsabilité du DSI doivent être clairement établis et précisés.

De plus, le DSI lui-même est amené à prévoir des délégations de ses propres pouvoirs. On parlera alors de « *subdélégation ou de sous-délégation de pouvoirs* » ou de délégation en cascade.

Par ailleurs, le régime juridique de la délégation (et de la subdélégation) de pouvoirs dépend, en absence de disposition légale, de l'interprétation des tribunaux. Or, si l'on s'intéresse au domaine des systèmes d'information en particulier, force est de constater que les tribunaux ne se sont jusqu'ici presque exclusivement prononcés dans la perspective des infractions pénales liées à la sécurité physique des salariés.

Conformément à la jurisprudence : « *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* » (Cass. crim., 11 mars 1993, Bull. crim. n°112). Le dirigeant sera donc exonéré de sa responsabilité pénale à condition qu'il n'ait pas participé personnellement à la réalisation de l'infraction, qu'il parvienne à justifier de l'existence d'une délégation de pouvoirs valide, et qu'il démontre que, dans un domaine de responsabilité susceptible de transfert à d'autres que lui-même, il a donné délégation à un préposé compétent de prendre des décisions, lui a fourni des moyens nécessaires à cette mission et s'est mis en situation de contrôler que la délégation fonctionne normalement.

Par ailleurs, l'admission de délégation de pouvoirs ne remet pas en cause la responsabilité civile prévue par le Code civil de l'employeur en tant que « *commettant* » (Cass. Crim. 23 janvier 2001, TPS 2001 n° 210) qui reste responsable des agissements de son « *préposé* » (le

salarié). En effet, la responsabilité civile de ce dernier étant fondée sur l'article 1384 al. 5 du Code civil, la délégation consentie à un salarié ne l'exonère nullement et il se verra donc dans l'obligation de verser des dommages et intérêts pour réparer le préjudice subi. L'affaire Escota c./ Lucent Technologie illustre cette responsabilité civile de l'entreprise retenue sur le fondement de l'article 1384, al.5 du Code civil dans une espèce où le salarié avait utilisé son poste de travail mis à sa disposition par l'entreprise pour créer des pages personnelles ayant causé un préjudice à la société Escota.

En effet, l'efficacité de la délégation est subordonnée à des conditions tenant, d'une part, à la personne du délégataire et, d'autre part, à l'objet même de la mission qu'elle comporte. Et, en cas d'action contre le délégant, celui-ci devra rapporter la preuve que ces conditions avaient effectivement été réunies.

CONDITIONS DE VALIDITÉ DE LA DÉLÉGATION DE POUVOIRS

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

- **Il est indépendant dans la mise en œuvre des tâches déléguées**

En effet, de façon logique, car l'indépendance va de pair avec la responsabilité. Lorsque le chef d'entreprise ou un supérieur hiérarchique (comme un DSI) s'immisce dans l'exécution des tâches en rapport avec la mission du titulaire de délégation de pouvoirs, ce dernier ne peut se voir reprocher une faute dans l'accomplissement de sa mission (Cass. soc. 21 novembre 2000, Dr. social 2001, p. 209). Cela ne signifie pas, bien évidemment, que le délégant ne puisse être sanctionné par le délégataire s'il a pris une décision préjudiciable à l'entreprise.

- **Il est pourvu des compétences nécessaires**

En l'occurrence, il ne s'agit pas uniquement de compétences techniques mais de toutes les compétences utiles à l'accomplissement de ses missions, et donc notamment de connaissances juridiques. Le DSI doit donc connaître les principes juridiques et maîtriser les conséquences des textes réglementaires et des interprétations jurisprudentielles applicables aux domaines sur lesquels il intervient et qu'il n'aurait pas lui-même valablement délégué. Notons que cette capacité peut d'ailleurs ne pas découler automatiquement de sa qualification professionnelle et peut nécessiter une formation spécifique en fonction de la nature des prescriptions applicables (Cass. crim. 25 juillet 1991, jurisdata n° 1993-004783).

- **Il est investi de l'autorité nécessaire**

Cela signifie qu'il doit être pourvu d'un pouvoir de commandement suffisant pour obtenir des salariés placés sous sa surveillance l'obéissance nécessaire au respect de la loi (Cass. crim. 21 janvier 1911, Bull. crim. n° 54). Cela signifie également que ces salariés doivent avoir été informés de cette autorité (élément important dans les situations de subdélégations où

le délégataire n'aurait pas de positionnement clair dans la hiérarchie de la société). Dans le même sens, le délégataire ne peut être qu'un préposé (un salarié) de la société et non un prestataire externe par exemple. Il ne doit pas non plus occuper un poste à titre temporaire.

Dans le cadre du système d'information, cela implique que le DSI doit être en mesure de faire respecter par tous les salariés les modalités d'utilisation dudit système (ex : par l'intermédiaire d'une charte informatique, intégrée au règlement intérieur de l'entreprise).

- **Il dispose des moyens nécessaires**

Ces moyens se traduisent en terme humains, financiers, matériels ; ils ont pour but de lui permettre d'exercer efficacement les pouvoirs qui lui ont été délégués (Cass. crim. 26 mars 2008, JCPE 2008, 1813 obs. E. Fortis). L'adéquation de ces moyens s'évaluera en fonction du budget alloué au DSI compte tenu des besoins exprimés en matière de mesures visant à encadrer les risques pénaux de l'entreprise.

Ainsi, un salarié dépourvu de compétences en matière de sécurité relatives à des lignes électriques de 20.000 volts, à qui la délégation n'attribuait aucun pouvoir précis de sanction et en l'absence de moyens financiers et matériels, peut valablement refuser une délégation de pouvoirs en matière de sécurité (Cass. crim. 13 septembre 2005, n° 05-80.035).

- **Il ne peut y avoir cumul des délégations sur un même pouvoir**

L'autorité déléguée doit revêtir un caractère exclusif, c'est-à-dire qu'elle doit être concentrée sur une seule tête pour un même secteur de l'entreprise. Ainsi, pour que la délégation des pouvoirs du chef d'entreprise au profit du DSI soit valide, il ne faut pas que le chef d'entreprise ait pu accorder une délégation de pouvoir sur tout ou partie du champ de compétence du DSI à une autre personne (Directeur des Services Généraux, etc.).

Les tribunaux censurent donc notamment les délégations de pouvoirs qui auraient été données « *à deux préposés au moins* » (Cass. crim. 23 novembre 2003, Bull. crim. n° 295, RJS 2005, n° 330).

Ainsi, la codélégation ou délégation multiple (pouvoirs divisés et délégués entre plusieurs salariés intervenants dans le même secteur de l'entreprise) n'est possible que si elle n'est *« ni de nature à restreindre l'autorité des délégataires ni à entraver les initiatives de chacun d'eux* » (Cass. crim. 6 juin 1989, n° 88-82266, Bulll. crim. n° 243).

De façon similaire, la hiérarchie dans l'entreprise et sa raison d'être doivent toujours être respectées. La délégation n'est donc pas valide si elle conduit à déléguer l'intégralité des pouvoirs du chef d'entreprise voire du DSI (cela reviendrait à modifier l'ordre général du pouvoir au sein de l'entreprise - Cass. com. 11 juin 1965, n° 63-10.240, Akoun c/ Piloy, Bull. civ. III n° 329). D'autant que la délégation ne peut pas porter sur les tâches de nature

personnelle qui ne peuvent être exécutées que par le DSI (Cass. crim. 19 août 1997, n° 97-83.944).

Les sous-délégations, lorsqu'elles sont prévues, doivent respecter strictement les mêmes règles.

MODALITÉS DE LA DÉLÉGATION

- **La délégation doit être certaine et dépourvue d'ambiguïté**

Pour cela, elle n'a pas nécessairement à être nominative (Cass. crim. 2 mars 1988, n° 87-81528), mais elle doit résulter d'éléments clairs et précis qui peuvent être factuels ou tirés du contexte (Cass. Crim. 30 avril 2002, n° 01-84405). Ainsi, seront exclues les délégations purement formelles prévues notamment dans l'organigramme de l'entreprise, mais sans prolongement réel dans le fonctionnement de celle-ci (Cass. crim. 20 mars 2007, n° 0585153). L'exigence de précision, à défaut de laquelle la délégation risque de se retourner contre le délégant (Cass. crim. 7 novembre 1994, Dr. Pén. 1995, n° 41), résulte d'ailleurs en une exigence de limitation dans le temps et en une limitation de son champ d'application (Cass. crim. 20 octobre 1999, n° 98-83562). En effet, dans la mesure où la délégation est censée être un outil facilitant l'exercice du pouvoir au sein de l'entreprise, et non pas un moyen de dénaturer l'organisation décisionnelle de celle-ci, sa durée doit nécessairement être limitée dans le temps.

- **La validité de la délégation de pouvoirs n'est pas nécessairement subordonnée à la rédaction d'un écrit**

Il reste que l'écrit est toutefois fortement recommandé dans la mesure où il constitue une preuve, notamment sur l'étendue des pouvoirs transférés au délégataire. Il peut prendre la forme d'une délégation de pouvoirs expresse et spécifique ou d'une simple clause dans le contrat de travail du salarié délégataire (Cass. crim. 14 mars 2006, n° 05-85.889). Cet écrit doit être explicite et doit bannir les formules vagues et hypothétiques (Cass. crim. 22 novembre 2005, n° 0582082). Si aucun écrit n'est rédigé, la validité de la délégation de pouvoir peut être prouvée par tous moyens (faisceau d'indices s'appuyant sur les déclarations, le comportement du délégataire, etc.) à partir du moment où cette délégation est, là aussi, certaine et sans ambiguïté.

La délégation de pouvoir est un outil nécessaire dans la gestion opérationnelle d'une entreprise. Pour être valable, elle doit être précise (par exemple : mesures de sécurité liées au système d'information), limitée à certains domaines et doit également répondre à des conditions strictes imposées par les tribunaux, telles que son caractère certain, dépourvu d'ambiguïté et opportun, la limitation de sa durée et de son champ d'application, les compétences et l'autorité nécessaires du délégataire, les moyens suffisants mis à sa disposition.

Constat :

L'envoi de courriers électroniques « engageants juridiquement » est répandu dans l'entreprise.

Actions recommandées :

- **Sensibiliser tous les acteurs de l'entreprise sur la valeur juridique de tout courrier électronique**
- **Calquer les délégations de pouvoir sur l'organisation managériale de l'entreprise**
- **Encadrer les situations de faits existantes afin d'unifier comportements et responsabilité juridique**
- **Formaliser une cartographie des fonctions avec les délégations de pouvoir et leurs mises à jour.**

LES CONTRATS AVEC LES FOURNISSEURS ET LES PRESTATAIRES

Certains aspects juridiques des contrats conclus avec les prestataires de services informatiques et notamment ceux relatifs à l'externalisation informatique (ou *outsourcing*) doivent faire l'objet d'une attention particulière de la part des DSI. Rappelons que le recours à des prestataires consiste à sous-traiter, en partie ou en totalité, le développement et/ou l'exploitation du système d'information de l'entreprise. De ce fait, en confiant une partie du système d'information à des prestataires externes, souvent expérimentés pour chaque type d'intervention, il devient possible pour l'entreprise de se concentrer uniquement sur son activité principale. L'entreprise gère les coûts d'exploitation et les frais de charges sans avoir besoin d'investir en hommes et en matériel, en bénéficiant uniquement du service dont elle a besoin (*Software as a Service* - SaaS par exemple).

CADRE JURIDIQUE

Les contrats informatiques représentent et encadrent des réalités techniques très diverses et plus ou moins complexes : achat de matériels, de progiciels, de bases de données, études, développement informatique, maintenance, hébergement, exploitation, assistance technique …

Dans la mesure où les entreprises éprouvent le besoin de disposer d'un outil informatique fiable, sécurisé et efficace, elles doivent avoir les moyens de mesurer la qualité de service et le suivi des prestations. De nombreux points doivent être étudiés à savoir la bonne formulation des résultats attendus, les modalités du pilotage du prestataire, le dimensionnement des équipes et compétences mises à disposition, l'auditabilité du prestataire (qualité de service), ses assurances, son niveau de responsabilité financière. Le recours à ce type de prestation relève d'une décision stratégique de la direction générale ou de la direction informatique. Elle est susceptible de comporter des risques. Ainsi, conformément à l'article 35 de la loi « Informatique, Fichiers et Libertés » de 1978 modifiée en 2004, il convient de vérifier que le sous-traitant présente des garanties suffisantes pour assurer la sécurité et la confidentialité des données. Cela se traduira par des clauses contractuelles sur les point précédemment évoqués ((ex : modalités d'audit, garanties accordées, …) dans le cas où des données à caractère personnel lui seraient confiées.

Le contrat d'externalisation doit s'accompagner (souvent en annexe) de dispositions contractuelles relatives au niveau de services que le prestataire s'engage à respecter dans le cadre de l'exécution des prestations. L'objectif de l'engagement de niveau de services (convention de services ou *Service Level Agreement* « SLA ») est de déterminer le niveau de performance requis par le client et le volume des garanties apportées par le prestataire. Il convient, au sein du SLA, de mesurer les délais d'intervention dans le cadre de la maintenance, les délais de prise en compte de demandes spécifiques, la performance de la

sécurité du système en matière informatique ou dans le cadre de l'externalisation des systèmes de communications électroniques....

En outre, le contrat d'externalisation informatique doit reposer sur des règles juridiques claires. En effet, ce n'est qu'au terme d'une phase préalable au cours de laquelle l'entreprise aura exprimé ses besoins et le prestataire en aura pris connaissance de manière relativement poussée que ledit contrat pourra – éventuellement - être établi. Les besoins et attentes du client, ainsi que ses objectifs et performances à atteindre, seront exprimés dans un document, le cahier des charges, qui évoquera les obligations contractuelles du prestataire, les critères de responsabilité du prestataire ainsi que les garanties de niveaux de services.

Un audit technique permettra au prestataire d'obtenir une description technique complète du système, de ses performances et de déterminer les moyens qui seront mis en œuvre dans le cadre des opérations d'externalisation. Un audit juridique (en amont) pourra également être réalisé, notamment pour clarifier les droits de propriété intellectuelle dont l'entreprise dispose sur les différents éléments (logiciels, progiciels, applicatifs) de son système.

CA Poitiers, 25 novembre 2011, MAIF c/IBM, disponible sur le site legalis.net

De nombreuses affaires judiciaires traitent de la dérive des coûts lors des projets informatiques.

Si les juges de première instance entendent protéger les clients dans ce cas, les juges d'appel reconnaissent moins facilement la responsabilité du prestataire.

En ce sens, la Cour d'appel de Poitiers, par une décision du 25 novembre 2011, a infirmé le jugement du 14 décembre 2009, rendu par le Tribunal de grande instance de Niort et qui avait prononcé la nullité d'un contrat d'intégration de progiciel entre la MAIF et IBM aux torts de cette dernière. Les juges de première instance ont estimé qu'IBM était coupable de dol, pour avoir fait croire à la MAIF que le projet était réalisable dans les conditions prévues dans le contrat initial du 14 décembre 2004.

En l'espèce, la MAIF souhaitait mettre en place un système de Gestion de la Relation avec ses Sociétaires (GRS) basé sur le logiciel Siebel. Elle décide de lancer un appel d'offres destiné à faire jouer la concurrence à l'issue duquel la Société IBM est retenue. Le donneur d'ordre commande alors une étude préparatoire afin de parfaire l'analyse de ses besoins et de son environnement. A la suite de cela, un contrat d'intégration est conclu entre la MAIF et IBM par lequel cette dernière s'engageait à fournir sur la base d'une obligation de résultat, une solution intégrée conforme au périmètre fonctionnel et technique convenu entre les parties, en respectant le calendrier impératif fixé et pour le prix ferme et définitif de 7 302 822 euros HT. Or, dès le mois de février 2005, la MAIF constate un retard sur le

calendrier fixé initialement entre les parties. Au mois de septembre 2005, elle demande alors par voie de lettre recommandée un dédommagement financier suite aux retards accumulés ainsi qu'un plan d'action afin d'arrêter les accumulations. Les deux parties s'entendent finalement sur un règlement amiable consistant au report du pilote initialement prévu pour avril 2006 à début 2007 et en une majoration de 3,5 millions d'euros de la charge financière. La signature de ce règlement à l'amiable n'a finalement pas eu lieu car IBM a constaté que le projet n'était pas *« techniquement réalisable dans les conditions initialement envisagées ».* Un nouveau protocole d'accord est alors signé le 22 décembre 2005 à l'initiative d'IBM. Toutefois, malgré la signature de ce protocole, les relations entre les parties se détériorent, la MAIF reprochant à IBM le manque de visibilité du scénario proposé. En juin 2006, la MAIF finit par décliner l'offre de 15 millions d'euros proposées par IBM qu'elle juge exorbitante au regard du prix forfaitaire initialement prévu. IBM demande alors le règlement des factures impayées mais la MAIF refuse.

C'est dans ces conditions qu'IBM a saisi le Tribunal aux fins d'obtenir le remboursement des factures impayées ainsi que le versement des dommages et intérêts pour rupture abusive et unilatérale de leur contrat. La MAIF de son côté, a formé une demande reconventionnelle en nullité du contrat informatique pour vice du consentement et en réparation du préjudice subi. Elle reproche à la SSII d'avoir sous-évalué le calendrier et sous-estimé le budget nécessaire dans le seul but de remporter l'appel d'offres. En effet, elle estime qu'IBM savait pertinemment qu'elle ne tiendrait pas ses engagements et considère que ce comportement est représentatif d'une réticence dolosive conformément à l'article 1116 du Code civil.

En première instance, le Tribunal de grande instance de Niort a prononcé la nullité du contrat d'intégration et des deux protocoles d'accord, pour dol, en retenant qu'IBM avait surpris le consentement de la MAIF en lui faisant croire que le projet était réalisable dans les conditions initiales alors qu'IBM savait parfaitement depuis le début que l'accomplissement du projet était impossible. Le tribunal avait condamné IBM à restituer à la MAIF les sommes versées au titre de leur relation contractuelle, excluant les sommes dont la MAIF a conservé le profit. De plus, IBM était condamné à verser des dommages et intérêts à la MAIF pour un montant total de 9,5 millions d'euros. Le jugement était assorti de l'exécution provisoire.

Mais le 25 novembre 2011, la 1ère chambre civile de la cour d'appel de Poitiers a infirmé le premier jugement du Tribunal de grande instance de Niort, opérant un total revirement.

La Cour d'appel réfute ici la thèse selon laquelle, le prestataire, IBM, se soit rendu coupable de manœuvres frauduleuses destinées à obtenir un appel d'offres et donc, de tromper son client, la MAIF.

Concernant tout d'abord le dol, invoqué par la MAIF, l'arrêt exclut toute réticence dolosive d'IBM au motif qu'il « *n'est pas établi qu'IBM a dissimulé de surcroit volontairement à la MAIF des informations majeures relatives au calendrier, au périmètre, au budget du projet* ».

La Cour retient que le projet a été ajusté par des avenants successifs acceptés par la MAIF en toute connaissance de cause, reconnaissant bien là que le projet initialement convenu n'était pas réalisable. La MAIF ne pouvait soutenir avoir été trompée et la Cour rejette le moyen tiré du dol.

Dans un second temps, la MAIF reprochait à IBM de s'être contentée de laisser prospérer les dérives et difficultés et ajoute qu'elle n'a disposé *« d'aucun conseil, ni de mise en garde relatifs aux risques liés à l'exécution du contrat ».* La cour d'appel de Poitiers constate que la MAIF disposait de la parfaite connaissance technique dans le domaine informatique, grâce à une direction informatique étoffée, et écarte le manquement à l'obligation de conseil. La MAIF ne peut pas, au regard de son service informatique qualifié, être considérée comme étant profane dans ce domaine afin de bénéficier d'une protection juridique accrue.

La Cour d'appel de Poitiers a donc reconnu la validité du contrat et a condamné la MAIF à verser la somme de 4 664 400 millions d'euros à la BNP Paribas Factor au titre d'une facture restée impayée à ce jour et la somme de 450 441,28 euros à IBM.

NÉGOCIATION ET CLAUSES CONTRACTUELLES

La période précontractuelle se caractérise par la liberté de rompre les pourparlers, car l'entreprise et le prestataire n'ont pas encore annoncé publiquement leurs négociations dans le cadre d'instruments juridiques précis tels que les lettres d'intention, *MoU* ou encore les protocoles d'accord. Cependant, il est important de préciser que cette liberté de rompre les négociations est susceptible de constituer une faute sur le fondement du droit commun de la responsabilité civile, à savoir les articles 1382 et 1383 du Code civil. La réparation de cette faute se fera en fonction de l'importance et la singularité du contrat discuté, de l'état d'avancement des négociations, de la durée de celles-ci...

Suite à cette période précontractuelle, le contrat devra jouer un rôle considérable dans la réussite ou l'échec d'une opération d'externalisation. Un soin tout particulier devra être apporté concernant la rédaction de certaines clauses afin d'éviter de potentiels désagréments.

Les clauses relatives notamment à l'obligation d'information, de conseil et de collaboration, doivent prévoir que le prestataire préconise la solution qui lui paraît la plus adaptée, et qu'il avertisse par ailleurs l'entreprise cliente des éléments susceptibles d'avoir des conséquences négatives sur les opérations d'externalisation. A cette obligation s'associe celle de collaboration qui pèse sur l'entreprise et qui consiste à des échanges réciproques d'informations et à s'impliquer activement en interrogeant le fournisseur sur les éléments qui pourraient lui échapper.

L'un des éléments essentiels d'un contrat d'externalisation consiste à permettre le transfert de responsabilité de l'entreprise vers le prestataire externe, sous certaines conditions. Ainsi, les entreprises doivent adopter des clauses de responsabilité adéquates dans leurs contrats informatiques, mettre en œuvre des garanties pour prévoir la réversibilité des données et des fichiers, encadrer les règles de preuve applicables entre les parties (signature électronique, archivage des éléments de preuve – par qui ? -, etc.) ainsi que l'identification des échanges entre l'entreprise et les tiers, veiller à la bonne rédaction des clauses de confidentialité, d'audit de sécurité et d'audit d'intrusion, surtout lorsque des données à caractère personnel sont concernées…, ou logs de sécurité.

Toutes les clauses de prix mais également d'assurance ou de garantie financière (et, en pratique, de limitation de garantie) devront, en outre, être étudiées très attentivement. En effet, la Cour de cassation a tout récemment décidé de confirmer la validité *a priori* d'une clause limitative de responsabilité à propos d'un manquement à une obligation pourtant considérée comme essentielle au contrat. Une clause limitant la responsabilité du prestataire à 200 000 euros (prix de la licence payée) alors que le préjudice était évalué à plus de 70 millions d'euros a ainsi été considéré comme valide.

Cass. com. 29 juin 2010, Faurecia c/ Oracle France, N° de pourvoi : 09-11841, disponible sur le site www.legifrance.gouv.fr

L'équipementier automobile Faurecia avait conclu plusieurs contrats avec la société Oracle concernant l'intégration d'un logiciel de production et de gestion commerciale. Or, seul un logiciel provisoire avait été livré, connaissant de graves difficultés d'application. Pour cette raison, Faurecia avait décidé de ne plus régler ses redevances. La société Franfinance à qui Oracle avait cédé ses créances, l'a alors assigné en paiement des créances de redevances. En contrepartie, Faurecia a assigné son prestataire à la fois aux fins de nullité des contrats pour dol ou en résolution pour inexécution. La Cour d'appel dans une décision du 26 novembre 2008, a, par application de la clause limitative de réparation, limité la condamnation d'Oracle envers Faurecia. Cet arrêt a été partiellement cassé (Cass. com. 13 février 2007, Pourvoi n° 05-17.407). Statuant sur renvoi après cassation, la Cour d'appel, faisant application de la clause limitative de réparation, a condamné la société Oracle à payer la somme de 203 312 euros avec intérêts. La Cour de cassation dans sa décision du 29 juin 2010 a rejeté le pourvoi de la société Faurecia considérant que : « la faute lourde ne peut résulter du seul manquement à une obligation contractuelle, fût-elle essentielle mais doit se déduire de la gravité du comportement du débiteur ». Ainsi, un manquement « essentiel » ne conduit pas à réputer automatiquement non écrite une clause limitative de responsabilité. Celle-ci pourra cependant être écartée en fonction des circonstances de l'espèce.

Enfin, le droit applicable au contrat et le tribunal compétent doivent être âprement négociés par l'entreprise, pour éviter qu'un contentieux éventuel dans le cadre d'un contrat signé un peu rapidement ne se déroule devant un tribunal étranger dans un droit parfaitement maitrisé par le prestataire… mais pas par l'entreprise ! Une solution alternative peut également consister à soumettre les éventuels litiges à un arbitrage.

Par ailleurs, en ce qui concerne plus spécifiquement les contrats de prestations, il est essentiel que les rôles de chacun soient strictement observés et qu'en raison par exemple d'une faute d'un salarié du prestataire dans les locaux du client, ce dernier ne lui inflige pas à une sanction directe. A défaut, une sanction pénale sur le fondement des délits de marchandage et/ou de prêt illicite de main d'œuvre pourrait être encourue (art. L. 8224-1 et L. 8243-1 du Code du travail[2]).

De plus, il convient de souligner l'importance des clauses qui concernent la fin des contrats d'externalisation ou d'*outsourcing*, qui peuvent générer de nombreux problèmes économiques et sociaux si elles ne sont pas ou mal anticipées. En effet, la question de la sortie du contrat doit être réglée dès sa signature. Notons que ces contrats d'externalisation comportant des engagements financiers importants et étant conclus pour des durées de plus en plus longues, il existe un risque certain de créer une dépendance du client vis-à-vis du prestataire. Dans le but d'éviter cette dépendance, l'entreprise doit organiser contractuellement la reprise en interne de la fonction externalisée ou les conditions de transfert de cette fonction à un autre prestataire. C'est pour répondre à cet objectif que les contrats d'externalisation prévoient une clause de réversibilité, puisque celle-ci permet au client de prévoir les conditions dans lesquelles il pourra reprendre en interne la fonction externalisée ou encore, de transférer, à un autre prestataire, la gestion de cette fonction. Quelles que soient les raisons pour lesquelles le contrat a pris fin (arrivée du terme, résiliation anticipée, résiliation pour faute), cette possibilité doit toujours être offerte au client. Quant au prestataire, il doit absolument rendre la réversibilité techniquement réalisable. Pour ce faire, il lui incombe de mettre en œuvre des solutions standards non susceptibles de porter atteinte à la réversibilité.

La clause de réversibilité revêt un caractère fondamental en matière d'externalisation dans la mesure où elle met en confiance les entreprises qui souhaitent engager une démarche d'externalisation puisqu'elle leur permet de choisir un prestataire sans que ce choix soit définitif.

NB : Une bonne pratique pourrait être de se référer à l'eSCM-SP (pour *eSourcing Capability Model for Service Providers*), volet "Prestataire" du référentiel eSCM (pour *eSourcing*

[2] L'article L. 8224-1 prévoit une peine de trois ans d'emprisonnement et/ou une amende de 45 000 euros, soit 225 000 euros pour une personne morale. L'article L. 8243-1 prévoit quant à lui une peine de deux ans d'emprisonnement et/ou une amende de 30 000 euros, soit 150 000 euros pour une personne morale.

Capability Model), qui a été conçu en 2002 par l'Université Carnegie Mellon. eSCM-SP est un référentiel de bonnes pratiques avec trois objectifs :

1. Fournir aux prestataires des directives pour les aider à améliorer leur aptitude tout au long du cycle de vie du *sourcing*,
2. Fournir aux organisations clientes un outil d'évaluation objectif de l'aptitude des prestataires, et
3. Donner aux prestataires un standard leur permettant de se différencier de leurs concurrents.

Bien entendu, il s'agit d'un référentiel standard à adapter à chaque besoin de l'entreprise mais il peut servir de base de réflexion.

Constat :

Un contrat bien négocié est équilibré, conçu comme un outil de pilotage et de management du projet informatique.

Recommandations :

- **Mettre en place des RFI (*Request For Information*) préparatoires, des contrats d'études spécialisées pour un projet**
- **Ordonner le contrat avec une table des matières, une liste des annexes et des définitions précises ; prévoir un cahier de recettes et de jeux de test précis**
- **Prévoir des fiches de suivi contractuel à l'issue de la signature et prévoir l'allocation des ressources internes**
- **Mettre en place des comités de pilotage animés par la DSI, faire des comptes-rendus systématiques et validés par chaque partie**
- **Prévoir la mise à jour et la transmission pour chaque contrat des conditions générales d'achat des prestations informatiques**
- **Prévoir une clause de médiation dans tous les contrats**

LA DÉMATÉRIALISATION DES DOCUMENTS ET DES ÉCHANGES

La dématérialisation concerne toutes les activités stratégiques de l'entreprise (quels que soient sa taille et son secteur d'activité) et constitue une étape clé dans l'évolution de la gestion des entreprises privées comme des autorités administratives, en présentant des enjeux économiques, sociaux, juridiques et technologiques majeurs.

ENVIRONNEMENT JURIDIQUE DE LA DÉMATÉRIALISATION

La dématérialisation consiste à mettre en œuvre des moyens électroniques pour effectuer des opérations de création, de traitement, d'échange, de stockage et d'archivage d'informations sans support papier. En pratique, les documents concernés sont nombreux : contrats et actes en matière commerciale, sociale, en comptabilité … Mais ce sont surtout les documents de gestion qui sont le plus concernés par la dématérialisation : commandes, livraisons, facturations, déclarations fiscales et sociales, bulletins de salaire, notes de frais, …. Parmi les procédures dématérialisées couramment utilisées par certaines entreprises, on peut citer les téléprocédures administratives (télé-TVA, téléCarteGrise, candidatures aux appels d'offres des marchés publics…), les opérations bancaires telles que les virements ou les paiements par carte, mais aussi les relevés de comptes via l'internet, etc.

L'entreprise est souvent tentée par un passage au « tout électronique » ou plus exactement au « plus électronique », au vu de ce que permettent les outils technologiques. Reste que le lancement d'un projet de dématérialisation des documents ou des procédures, qu'il soit de taille restreinte ou impactant l'ensemble d'une entreprise ou d'un groupe, ne peut faire l'économie d'une analyse préalable des conséquences juridiques de cette dématérialisation… et des impératifs qu'il convient de respecter.

Cette étude juridique ne peut se faire que par le biais de l'étude préalable de l'existant (procédures suivies, liste des documents générés et/ou conservés, etc.) afin d'en analyser les conséquences et les opportunités juridiques. La difficulté de ce type de projet est que chaque document est susceptible de recevoir plusieurs qualifications juridiques différentes (voir, pour une vue plus exhaustive de la problématique, la quatrième édition du « *Vade mecum juridique de la dématérialisation des documents* », de la Fédération nationale des Tiers de Confiance, publié en juin 2011, disponible en téléchargement sur le site de la Fédération Nationale des Tiers de Confiance, http://www.fntc.org/ et sur le site http://www.caprioli-avocats.com) comme c'est le cas de la facture à la fois document fiscal, comptable et commercial et dont les régimes juridiques diffèrent selon l'angle retenu.

Confronté d'une part, aux offres de dématérialisation des prestataires et d'autre part, aux demandes internes des métiers cherchant à simplifier leurs procédures et à réduire leurs coûts, le DSI est souvent conduit à s'assurer de la maîtrise du processus par ses équipes et de leur valeur juridique eu égard au cadre législatif existant. Quelques principes demeurent

valables dans la plupart des documents dématérialisés. Ainsi, pour qu'une valeur juridique puisse être attribuée aux informations et aux opérations dématérialisées, la garantie de l'intégrité des documents (ou la fidélité et la durabilité des copies numérisées) apparaît souvent comme la pierre angulaire des exigences législatives et réglementaires. En revanche, si elle n'est pas exigée dans l'ensemble des cas**, l'intégrité des documents et des traces informatiques** permettra de disposer de preuves solides et peu discutables en cas de contentieux.

En plus de la garantie d'intégrité, un grand nombre de documents (factures, contrats, etc.) nécessite également la garantie de l'identification de leur auteur afin qu'ils puissent acquérir ou conserver une valeur juridique équivalente à celle des documents papier. Cette identification de l'auteur sert le plus souvent à marquer son consentement à l'acte (contrats), mais elle peut également être utilisée à des fins de preuve de la traçabilité pour limiter les fraudes (factures transmises sous forme électronique).

Instaurer la confiance et la sécurité dans le cadre d'un processus de dématérialisation induit donc le respect de règles juridiques et des exigences techniques associées.

Juridiquement, en matière de dématérialisation, les règles peuvent également apparaître comme différentes car elles dépendent en pratique de la branche du droit régissant la matière concernée. Ainsi, en droit administratif (droit applicable par exemple dans les rapports entre l'Etat et une entreprise) ou en droit commercial, les preuves sont libres en cas de contentieux, indépendamment de leur forme.

A l'inverse, en droit civil, pour les actes dépassant une certaine valeur (1 500 euros) ou s'il n'y a pas eu d'accord antérieur entre les parties quant aux moyens de preuve utilisables entre eux (convention sur la preuve), l'écrit devient nécessaire pour prouver les engagements souscrits.

ECRITS ET SIGNATURES SOUS FORME ÉLECTRONIQUE

La loi n° 2000-230 du 13 mars 2000 (JO n° 62 du 14 mars 2000, p. 3968) portant adaptation de la preuve aux technologies de l'information et relative à la signature électronique a intégré les écrits sous forme électronique dans le système juridique français, affirmant, dans le Code civil, l'équivalence de force probante entre les écrits sous forme papier et les écrits sous forme électronique.

L'article 1316-1 dispose, en effet, que : « L'écrit sous forme électronique est admis en preuve au même titre que l'écrit sur support papier, sous réserve que puisse être dûment identifiée la personne dont il émane et qu'il soit établi et conservé dans des conditions de nature à en garantir l'intégrité ». Dans les faits, l'intégrité de l'acte (c'est à dire la non altération du contenu pendant toute la durée de vie de l'acte depuis son origine) est souvent assurée par

certains procédés de signature (la signature numérique, fondée sur un certificat à clé publique, émanant d'une infrastructure à clé publique).

De plus, l'article 1316-4 al.1 du Code civil vient définir la signature de manière fonctionnelle : « La signature nécessaire à la perfection d'un acte juridique **identifie celui qui l'appose**. Elle **manifeste le consentement** des parties aux obligations qui découlent de cet acte ». L'article 1316-4, al.2 du Code civil quant à lui, énonce celle de la signature électronique entendue comme « ***un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache***. *La fiabilité de ce procédé est présumée, jusqu'à preuve contraire, lorsque la signature électronique est créée, l'identité du signataire assurée et l'intégrité de l'acte garantie, dans des conditions fixées par décret en Conseil d'Etat.* ». Selon l'article 2 du décret n° 2001-272 du 30 mars 2001 : « *La fiabilité d'un procédé de signature électronique est présumée jusqu'à preuve contraire lorsque ce procédé met en œuvre une signature électronique sécurisée, établie grâce à un dispositif sécurisé de création de signature électronique et que la vérification de cette signature repose sur l'utilisation d'un certificat électronique qualifié* ». En pratique, les procédés utilisés se fondent sur les techniques de cryptographie asymétrique.

L'une des principales erreurs véhiculées depuis plus de dix ans dans le domaine de la dématérialisation consiste à attendre l'arrivée de la signature électronique sécurisée bénéficiant de la présomption de fiabilité. En effet, bien qu'il existe une distinction entre la signature électronique « *simple* » et la signature électronique « *présumée fiable* », les deux types de signature électronique ont la même valeur juridique. **Seule la charge de la preuve est inversée.** Pour une signature électronique présumée fiable, la charge de la preuve de l'absence de fiabilité du procédé utilisé repose sur celui qui conteste la valeur juridique de la signature (et plus généralement l'acte signé). Pour une signature électronique simple, la charge de la preuve de la fiabilité du procédé utilisé pour signer l'acte en cause repose sur celui qui se prévaut de la signature électronique.

Il faut bien comprendre que tous les types de signatures électroniques « simples » sont valables dès lors qu'elles répondent aux exigences posées par l'article 1316-4 du Code civil, à savoir l'identification du signataire, la manifestation du consentement des parties aux obligations découlant de l'acte et la fiabilité du procédé.

A titre d'exemple, la jurisprudence a eu l'occasion de se pencher sur le cas de la signature manuscrite scannée, en indiquant que « *la signature électronique ne peut résulter d'une simple signature scannée, ce procédé ne permettant pas, en effet, d'identifier de manière fiable et précise l'auteur du message* » (CA Besançon, 20 octobre 2000, JCP éd. G, 2001, II, 10606, p. 1890 et s., note E. A Caprioli, P. Agosti - confirmé par Cass. civ. 2ème, 30 avril 2003, Bull. civ., II, n° 118 p. 101).

Dans les rapports entre une entreprise et un particulier, l'entreprise doit suivre les exigences du droit civil alors que le particulier bénéficie de la souplesse du droit commercial. **En d'autres termes, l'entreprise doit disposer d'un écrit pour l'opposer au consommateur alors que celui-ci peut justifier d'un document quelconque, voire de présomptions devant le juge pour l'emporter. L'entreprise doit donc fiabiliser au maximum les preuves de ses transactions ou en tous les cas prévoir une évaluation juridique des risques avant la mise en œuvre de tout projet de dématérialisation.**

Rappelons que l'article 9 du Code de procédure civile dispose en effet qu'il « *incombe à chaque partie de prouver conformément à la loi les faits nécessaires au succès de sa prétention* ». La préconstitution de preuves est donc essentielle pour l'entreprise.

A côté de ces règles applicables en matière de preuve des engagements souscrits, il existe également des documents pour lesquels l'établissement d'un écrit est exigé à titre de validité : en l'absence d'écrit, le contrat ou la convention est nulle ; ils n'ont jamais existé ! A côté des textes spécifiques par exemple en procédure civile ou pénale qui imposent une telle signature à titre de validité (actes d'appel, etc.), les crédits à la consommation, le Taux effectif Global (TEG), ou encore par exemple les statuts de société doivent également être constatés par écrit à titre de validité. Le législateur a tenu en effet à protéger le signataire en raison de l'importance de l'engagement pris.

Afin de rendre possible la dématérialisation de certains de ces actes, la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique a introduit, dans le Code civil, les articles 1108-1 et 1108-2. Le principe posé par le nouvel article 1108-1 est celui de l'équivalence, là aussi, entre l'écrit établi sous forme papier et celui sous forme électronique, avec un renvoi aux conditions d'équivalence identiques à celles des écrits à titre de preuve : « *Lorsqu'un écrit est exigé pour la validité d'un acte juridique, il peut être établi et conservé sous forme électronique dans les conditions prévues aux articles 1316-1 et 1316-4 et, lorsqu'un acte authentique est requis, au second alinéa de l'article 1317.*

Lorsqu'est exigée une mention écrite de la main même de celui qui s'oblige, ce dernier peut l'apposer sous forme électronique si les conditions de cette apposition sont de nature à garantir qu'elle ne peut être effectuée que par lui-même ».

Reste que pour certains actes d'une particulière gravité (contrat de mariage, adoption, convention préalable au divorce par consentement mutuel, cautionnement non professionnel, etc.), le législateur a spécifiquement interdit le recours à l'électronique (article 1108-2 du Code civil).

Ces exigences, qu'elles concernent la preuve des engagements souscrits ou leur validité, sont des conditions nécessaires et indispensables à la mise en œuvre de la dématérialisation. De plus, il est primordial d'organiser la dématérialisation des informations au sein de l'entreprise dans un contexte de sécurité optimale afin de pallier les risques potentiels

d'interception des données, d'attaques malveillantes ou criminelles, de piratage, de fraude et d'usurpation d'identité. Les fichiers confidentiels (contrats signés), représentant des informations décisives et engageant l'entreprise sont nombreux, d'où l'intérêt d'assurer la confidentialité des échanges et de protéger et garantir l'intégrité des données transmises. Différentes solutions techniques peuvent concourir à la réalisation de cet objectif : mise à disposition de certificat électronique, de moyens de chiffrement, VPN, etc.

COPIES NUMÉRIQUES

Il est important de noter ici que de nombreuses entreprises numérisent leurs originaux papiers et conservent dans leur système d'information des copies numériques. En principe, jusqu'à présent, les entreprises archivaient les originaux papiers (à titre probatoire ou à des fins de contrôle fiscal ou social) et utilisaient quotidiennement les copies numériques contenues dans le système de gestion électronique des documents (GED). La qualification de copie ou d'original est importante car si un original peut être considéré comme une preuve parfaite (sauf dénégation d'écriture), la copie est souvent reconnue comme un commencement de preuve par écrit qui doit être complétée par d'autres éléments de preuve manifestant sa fidélité par rapport à l'original ainsi que sa durabilité conformément à l'article 1348, al.2 du Code civil. De nombreux jugements ont apporté certaines confusions concernant la qualification juridique des copies numériques en se fondant tant sur des exigences propres aux écrits signés (art. 1316-1 et s. du Code civil) qu'aux copies (art. 1334 et 1348, al.2 du Code civil). (Cass. civ. 1ère, 30 septembre 2010, v n° de pourvoi: 09-68555 ; Cass. civ. 2ème, 1er juillet 2010, CCE, Octobre 2010, comm. 105 ; Cass. civ. 2ème, 4 décembre 2008, CCE, Février 2009, comm. 19, note Eric A. Caprioli).

Notification et copie électronique : Cass. civ. 2ème, 4 décembre 2008, n° pourvoi : 07-177622, publié au Bulletin (CCE, Février 2009, comm. 19, note Eric A. Caprioli).

« *Pour débouter la société de sa demande, la cour d'appel, après avoir observé que la preuve de l'envoi de la lettre d'information pouvait être faite par tous moyens, énonce qu'il ne saurait être fait grief à la caisse de n'avoir conservé que la seule copie informatique du courrier en date du 20 janvier 2003 et que le fait de l'avoir édité sur du papier à en-tête revêtu d'un logo diffusé en 2004 ne saurait constituer en soi la preuve de l'absence de réception de l'original* »
Prive de base légale sa décision la Cour d'appel qui n'a pas recherché si le document électronique produit (une copie informatique non signée du courrier) par une CPAM répondait bien aux exigences des articles 1334, 1348 et 1316-1 du Code civil.

ARCHIVAGE ÉLECTRONIQUE ET SÉCURITÉ

En outre, la dématérialisation ne doit pas se limiter à l'établissement des documents et doit également prendre en compte la phase de conservation et de restitution des données et de leur valeur juridique dans le temps. Ainsi, il est fréquemment demandé par certaines entreprises de procéder à un audit juridique dans le but de déterminer la valeur probatoire d'un processus de dématérialisation de « *bout en bout* ». Cet audit prendra notamment en compte l'origine et l'intégrité du document, les modalités de conservation de certaines catégories de données (factures, données comptables, financières, personnelles…) et vérifier la conformité par rapport aux règlementations en vigueur, les durées de conservation et les risques juridiques encourus.

Il est à noter que l'archivage pourra être réalisé de manière fiable et sécurisée en interne ou en externe via un tiers archiveur (concernant les problématiques de contractualisation se reporter au 2°). Pour ce faire, le plus souvent, les personnes en charge de l'archivage prévoient de répondre aux normes applicables en la matière. S'il est vrai qu'elles n'ont la plupart du temps aucune valeur contraignante, elles constituent un état de l'art du marché qui pourrait être reconnu par le Juge (Cass. civ. 3ème, 4 février 1976 ; Bull. civ. III, n°49. V. notamment sur cette question, P. Agosti, *La prise en compte des normes techniques par le Droit*, Global Security Mag, Juin 2009). Les normes les plus représentatives du marché de l'archivage électronique sont les normes :

- ISO 15489 – *Records Management*
- ISO 15801 – *Legal admissibility and evidential weight*
- NF Z 42-013 – Conception et exploitation de systèmes d'archivage électronique

Cette dernière promulguée par l'AFNOR, et dont la dernière version date de mars 2009, a pour objet d'édicter les modalités propres à l'archivage sécurisé des originaux électroniques ou **des copies numérisées d'originaux papier**. La distinction est essentielle et les règles de conservation diffèreront selon la nature juridique du document : une copie numérisée d'original signé papier devra être **fidèle et durable** tandis que l'original électronique devra être **intègre**.

La norme Z42-013 préconise que soit rédigée **une politique d'archivage**[3] lorsque l'entreprise aura clairement précisé ses besoins d'archivage en interne ou vis-à-vis du tiers archiveur. Elle permettra de définir les rôles et obligations de chaque acteur intervenant dans le domaine d'archivage, les procédures à respecter afin de garantir la traçabilité des actions effectuées sur les documents archivés. La réalisation d'audit est également conseillée pour veiller au respect des engagements souscrits dans la politique et dans le contrat d'archivage avec un tiers.

[3] Disponible à l'adresse: http://www.ssi.gouv.fr/IMG/pdf/ArchivageSecurise-P2A-2006-07-24.pdf

La mise en place d'une politique d'archivage n'est cependant pas une obligation juridique au sens strict, même si elle est vivement recommandée pour la bonne gestion de la conservation des données. A partir de cette politique, **des profils d'archivage et des procédures** en découleront. Mais, en détaillant les conditions de sécurité de l'archivage, ce document assurera au mieux sa fiabilité et permettra d'en rapporter la preuve devant le juge et les experts éventuellement désignés par le tribunal.

En outre, la politique d'archivage doit être adaptée à la structure de l'entreprise. De ce fait, elle devra être rédigée en fonction des autres documents de l'entreprise qu'il s'agisse de la politique de sécurité des systèmes d'information de l'entreprise (surtout les grandes entreprises), la politique de confidentialité, la politique de gestion de preuve (pour assurer la preuve de la validité des écrit et des copies numériques dans le temps), les contrats avec les prestataires ; elle doit donc être cohérente avec la politique générale de l'entreprise.

Constats :

Si certains documents, comme les factures, sont déjà largement dématérialisés, d'autres plus spécifiques à l'activité de chaque organisation, ne le sont pas encore pour des raisons pratiques et / ou juridiques.

Recommandations :

- **Analyser de manière très précise le régime juridique des documents à dématérialiser**
- **Définir le processus dématérialisé : séquencer le cycle de vie du document, tant d'un point de vue technique, que juridique et métier (identification du client, signature, information précontractuelle, archivage, …)**

DROIT DES LOGICIELS ET DES BASES DE DONNÉES

Il convient de rappeler et préciser certaines problématiques dans le cadre de la gouvernance du SI.

- **Conformité des droits :** l'entreprise doit utiliser de façon licite les logiciels et les bases de données sur lesquels elle a acquis des droits (ou qu'elle pense pouvoir utiliser librement), qu'elle a conçus par l'entremise de ses salariés et connaître les droits exacts qui lui sont conférés. En cela, elle évitera au mieux les contentieux avec ceux qui la considèrent comme étant contrefactrice.
- **Valorisation du patrimoine informationnel de l'entreprise** : cette notion qui sera développée au § 5 permet à l'entreprise de se prévaloir de droits sur ses développements logiciels ou bases de données. Elle peut ainsi financièrement rentabiliser, valoriser les développements en concédant des licences d'utilisation à ses clients ou encore, en attaquant judiciairement ses concurrents profitant indûment de ses investissements. D'un point de vue financier, ces éléments sont valorisables à l'actif du bilan de l'entreprise, comme les brevets d'invention ou les marques.

LES LOGICIELS

Le logiciel est protégé par le droit d'auteur, codifié dans le Code de la propriété intellectuelle (articles L. 122-6 et s. CPI).

De façon synthétique, la loi reconnaît la qualité d'auteur à toute personne physique qui crée une « *œuvre de l'esprit* » quels que soient son genre (littéraire, musical ou artistique), sa forme d'expression (orale ou écrite), son mérite ou sa finalité (but artistique ou utilitaire). Elle lui accorde un monopole d'exploitation sur cette œuvre, sans formalité préalable de dépôt, pour une durée correspondant à l'année civile du décès de l'auteur et des soixante-dix années qui suivent, au bénéfice de ses ayants-droits. Elle lui accorde également des droits dits « moraux » (respect de l'intégrité de l'œuvre, droit de paternité, de divulgation et de retrait), droits imprescriptibles, inaliénables et perpétuels. Toute cession (ou concession) de droits sur l'œuvre doit avoir été spécifiquement prévue par l'auteur ou son ayant droit, toute utilisation en-dehors de ce cadre étant illicite et pouvant donner lieu, selon le souhait du titulaire des droits, à action en contrefaçon au plan civil ou au plan pénal (puni de trois ans d'emprisonnement et de 300 000 euros d'amende – article L. 335-2 et L. 335-3 du Code de la propriété intellectuelle).

Il n'y a que deux conditions à la protection de l'œuvre : qu'elle soit « originale » (selon la jurisprudence, qu'elle soit « empreinte de la personnalité de l'auteur ») et qu'elle soit formalisée. Ainsi, les créations de l'esprit purement conceptuelles telles qu'une idée ou une

méthode ne sont pas protégeables, les idées « étant de libre parcours ». Une protection de celles-ci aurait inévitablement pour effet de nuire *de facto* à l'innovation.

Par rapport au droit commun du droit d'auteur, énoncé ci-dessus, les logiciels et les bases de données disposent d'un régime juridique de protection sensiblement différent eu égard à leurs spécificités.

Le droit commun des logiciels

Conformément au Code de la propriété intellectuelle, la notion de logiciel est vaste et comprend non seulement l'ensemble des programmes, des procédés et des règles relatifs au fonctionnement d'un ensemble de données, mais également sa documentation.

En pratique, la protection des logiciels a surtout été accordée pour des raisons économiques de protection des investissements réalisés. Les critères du droit d'auteur ne s'adaptant pas parfaitement aux spécificités techniques des programmes d'ordinateur, la Cour de cassation, par plusieurs arrêts du 7 mars 1986 (Cass. Ass. Plén. 7 mars 1986) a modifié l'appréciation du critère de l'originalité pour ne rechercher, à la place de « *l'empreinte de l'originalité de l'auteur* » peu décelable dans le logiciel, la notion plus large « *d'effort personnalisé allant au-delà de la simple mise en œuvre d'une logique automatique et contraignante* » portant la « *marque de son apport intellectuel* » alors que la loi du 3 juillet 1985 a adapté le régime juridique applicable aux logiciels.

En conséquence, les principes suivants sont applicables :

- la protection par le droit d'auteur ne porte pas sur les fonctionnalités, algorithmes (idées et principes de base), interfaces ou langages de programmation, mais sur le matériel de conception préparatoire (maquettes, prototypes...), l'architecture du logiciel, l'enchaînement des instructions, le code objet et le code source, les écrans et modalités d'interactivité, les polices de caractère, les différentes versions, ou encore le nom du programme ;
- **Lorsqu'un salarié développe le logiciel dans le cadre de son travail, il y a dévolution automatique des droits à son employeur, qui est investi des droits applicables à ce logiciel ;**
- Les droits conférés au titulaire se composent de droits moraux réduits (droit de paternité, droit de divulgation, droit au respect de l'œuvre fortement atténué), il n'existe pas de droit de retrait ;
- Les droits patrimoniaux (articles L. 122-3 et L. 122-6 du CPI) sont les suivants : droit de reproduction, droit de représentation, droit de traduction et d'adaptation, et enfin droit de distribution ;

- Il est nécessaire de préciser que le titulaire du droit d'auteur sur le logiciel est libre de concéder des licences d'utilisation ou d'exploitation, ou de céder tout ou partie, à titre gracieux ou onéreux ;
- En application de l'article L. 123-1 du CPI, les droits d'auteur sur logiciel restent valables pendant toute la durée de la vie de l'auteur et jusqu'à 70 ans après son décès ou à compter de la première publication, au profit de ses ayant droits.

En pratique, il s'agira pour l'entreprise, lorsqu'elle développe un logiciel, de s'assurer que le logiciel est bien développé en interne par ses propres salariés (hors stagiaires et prestataires) dans le cadre de leurs missions et pendant leur temps de travail, pour bénéficier de la dévolution automatique des droits patrimoniaux à son profit. Le dépôt régulier des codes sources auprès d'un tiers de confiance (comme l'Agence de Protection des Programmes, Logitas, un huissier de justice…) permettra de se prémunir au mieux contre tout contentieux émanant d'un tiers prétextant une contrefaçon ou revendiquant la paternité.

Si le développement est réalisé par des prestataires externes, la propriété du logiciel appartient de facto et sauf exception au prestataire. Dès lors, il convient avant même de confier le développement logiciel de prévoir par contrat le cadre exact de la cession opérée au profit de l'entreprise cliente : une simple licence d'utilisation pour ses besoins personnels ? Un droit de sous-licence lui permettant de concéder à un tiers, à titre gracieux ou onéreux, une partie des droits concédés (et seulement ceux-là) ? Voire une cession pure et simple de l'ensemble des droits patrimoniaux ? Il conviendra en tout cas de prévoir le cadre juridique applicable à cette cession (ou concession) ainsi que la durée de celle-ci.

Ces illustrations démontrent que, pour le DSI, les choix opérés par exemple lors de l'externalisation de certains développements doivent être encadrés juridiquement au plus proche de l'utilisation réellement envisagée. A défaut, en effet, l'entreprise s'expose à devoir négocier après coup le droit d'utiliser le logiciel qu'elle pensait avoir acquis pendant la durée nécessaire à ses plans. La négociation se fera souvent au détriment de l'entreprise cliente.

Le cas des logiciels libres

Par ailleurs, des règles particulières sont applicables aux logiciels dits libres. L'idée fondamentale de ces logiciels est de permettre à chaque personne qui le souhaite de travailler sur l'œuvre,de l'utiliser, la modifier et la distribuer en fonction des possibilités offertes par la licence. Or, de plus en plus de développements sont réalisés par des directions informatiques en incorporant des parties plus ou moins importantes de codes source dits « libres », quand ce ne sont pas les logiciels « libres » qui sont directement utilisés en interne ou revendus avec ou sans compléments propriétaires, que ce soit pour

des raisons de coût, d'efficacité, etc. Notons que le logiciel libre diffère du logiciel propriétaire, puisqu'au lieu de payer des redevances comme dans le modèle propriétaire, dans le libre l'entreprise utilisatrice va recourir à des prestataires de services pour l'intégration ou encore la maintenance et les évolutions. Par ailleurs, l'auteur d'un logiciel libre doit fournir les codes sources de son œuvre, contrairement aux logiciels propriétaires où seuls les codes objets sont fournis aux utilisateurs. Mais pour des raisons de continuité, le contrat peut imposer au prestataire, que les codes sources soient mis en séquestre auprès d'un tiers et accessible en cas de défaillance dudit prestataire.

Le terme de « *libre* » est encore parfois considéré à tort comme signifiant « *librement utilisable, sans limitations* ***et*** *gratuitement* » alors qu'il n'en est rien. Derrière cette appellation unique se cache en effet une multitude de réalités juridiques différentes qui ont un seul point commun : la liberté d'accès au code source, par opposition aux logiciels dits « *propriétaires* ». Mais il ne faut surtout pas s'y tromper : ces logiciels restent régis et protégés par le droit d'auteur. Ils ne sont pas libres de droit ! Certes la licence impose généralement que le logiciel libre soit librement exécuté, copié, distribué, étudié, modifié et amélioré, sous réserve de respecter - le plus souvent - une condition essentielle : **la rediffusion du code source, modifié ou non, doit elle-même *souvent* être libre et gratuite (en dehors des frais limités engendrés par la mise à disposition du code source), afin de protéger les travaux effectués par l'ensemble des programmeurs contre toute appropriation privative.** En pratique, les droits reconnus à la personne qui acquiert ou utilise le logiciel varient d'une licence à l'autre ; de la simple possibilité d'exécuter une ou plusieurs copies du programme à un droit très large permettant jusqu'à la redistribution de copies et l'amélioration et la redistribution du logiciel et de ses codes sources.

C'est en réalité la présence ou l'absence de la clause dite de « copyleft » qui marque le clivage le plus important entre les différentes licences libres, étant entendu de surcroît que la clause de copyleft peut être forte ou atténuée dans ses effets.

Ainsi, une licence avec copyleft imposera à l'utilisateur (pour qu'il ait le droit d'utiliser, copier, étudier, modifier et distribuer l'œuvre) de redistribuer la version modifiée du programme et des sources sous la même licence que le programme original, l'empêchant ainsi de disposer de droits patrimoniaux sur l'œuvre qu'il a modifiée. On parlera ainsi de caractère héréditaire ou contaminant.

Par ailleurs, les logiciels étant protégés par le droit d'auteur, les licences de logiciels libres demeurent soumises aux règles de la propriété intellectuelle et le non respect des obligations de la licence peut être sanctionné pour délit de contrefaçon en vertu de l'article L. 335-3 du CPI.

Et les conséquences peuvent être majeures pour l'entreprise utilisant de tels logiciels sans le savoir ou sans en avoir étudié attentivement les licences alors qu'à l'inverse, de telles licences bien utilisées peuvent se révéler d'un intérêt précieux, y compris économique.

Il conviendra avant tout de ne pas confondre les logiciels « libres » avec les « freewares », qui ne sont que des logiciels utilisables gratuitement dans les limites de leur licence : beaucoup de « freewares » en effet ne se révèlent être gratuits que pour les particuliers ou les Organisations Non Gouvernementales mais payants pour les sociétés commerciales, ce qui les place en situation de contrefactrices si elles les utilisent sans verser le coût convenu[4].

Ainsi, la prise de connaissance attentive des conditions d'utilisation comprises dans les différentes licences libres permet à l'entreprise de se rendre compte que certaines d'entre elles contiennent une obligation de divulgation du code source en cas de redistribution. Cette obligation s'imposera au logiciel produit par l'entreprise intégrant le code source « libre » et doit être respectée (ex : licences GNU-GPL, …).

Dès lors, pour des raisons de sécurité juridique, ces licences doivent faire l'objet d'une analyse juridique rigoureuse aussi bien lorsqu'elles sont utilisées par des prestataires (Société de Services en Logiciel Libre) que par les équipes en interne.

A titre d'exemple, une affaire judiciaire récente portant sur une licence GNU-GPL (licence empêchant la réappropriation ultérieure du logiciel libre par un tiers) met en exergue les risques juridiques susceptibles de se manifester en cas de non-respect d'une licence de logiciel :

CA Paris, 16 septembre 2009 :

Cette affaire, atypique dans le sens où ce n'est pas l'auteur du logiciel libre qui a fait valoir ses droits mais l'utilisateur dudit logiciel, concerne une société informatique (EDU4) qui a été condamnée pour ne pas avoir fourni à son client (l'AFPA) les sources d'un logiciel libre et pour avoir supprimé le texte de la licence GNU-GPL.

La société EDU4, retenue par l'AFPA suite à un appel d'offres important, avait procédé à des modifications sur un logiciel libre. L'AFPA, prenant conscience de l'existence de modifications, les avait demandées à la société EDU4. Cette dernière refusant cependant d'accéder à cette demande, avait finalement fourni des modifications qui ne correspondaient pas à la version initialement livrée.

[4] De façon similaire aux contenus « libres de droit », qui ne sont en fait librement utilisables que dans un cadre très précis (diffusion restreinte, etc.) et rarement gratuitement. Là encore, une étude précise des termes de la licence applicable est un préalable à toute utilisation à titre professionnel.

A ce titre, la société EDU 4 a manqué à ses obligations contractuelles en livrant un produit « *qui présentait pour les utilisateurs des EOF des risques d'atteinte à la vie privée* » et « *qui ne satisfaisait pas aux termes de la licence GNU GPL puisque la société EDU 4 avait fait disparaître les copyrights d'origine de VNC sur les propriétés de deux fichiers en les remplaçant par les siens et avait supprimé le texte de la licence* ». Par voie de conséquence, la Cour a infirmé le jugement en première instance. En outre, l'AFPA était bien fondée, par application de l'article 1184 du Code civil, en sa demande en résolution du marché et la recette de la première phase n'étant pas intervenue, la société EDU 4 n'a pas obtenu paiement de son prix.

La résolution du contrat portait sur un marché global réparti en quatre lots d'un montant global d'environ 11 millions de francs.

Au vu de l'existence de tels contentieux, il apparaît nécessaire pour le DSI d'anticiper dès l'origine leur émergence en traçant le plus précisément possible l'origine et le contenu de chaque développement informatique, les intervenants et l'encadrement contractuel qui leur est applicable (avec adaptation des contrats de travail ou de prestations au besoin) ou encore le type de code à utiliser en fonction des possibilités offertes par sa licence et par l'usage qui sera fait du logiciel final. L'entreprise doit disposer de la liste des licences utilisées dans les développements avec la version. Dans l'hypothèse de la sous-traitance, il importe notamment de préciser, dans le cahier des charges, le type de licence que pourra utiliser le prestataire (LGPL ? Cecill ? GNUGPL ? BSD ?), en fonction des objectifs souhaités et du coût qui en découlera.

En conclusion, il est utile de préciser, même si un débat important a lieu depuis quelques années sur cette question, que **le logiciel n'est pas brevetable en lui-même et ne peut donc être protégé par le droit des brevets français dans la mesure où un programme d'ordinateur n'est pas considéré par la loi comme une invention**. Par exception, il peut être protégé par le droit des brevets s'il est compris dans une invention brevetée ou s'il est susceptible de produire des effets techniques tangibles. Reste que le United States Patent and Trademark Office (USPTO) aux Etats-Unis a une interprétation quelque peu différente tendant à accepter le dépôt de brevets qui porte en pratique sur des méthodes, voire sur des logiciels, le débat étant pendant à la lecture de la jurisprudence (d'où l'émergence de *Patent Troll* pour bloquer – ou protéger des éléments qui ne devraient pas pouvoir être protégeables).

LES BASES DE DONNÉES

L'information est devenue une richesse pour toutes les organisations qu'elles soient privées ou publiques. Avec les technologies et les systèmes d'information, les organisations disposent de très nombreuses bases de données pour leur fonctionnement interne et leurs relations externes.

Compte tenu de l'importance économique et des investissements financiers que peut occasionner la création de telles bases, le droit ne pouvait laisser ces bases de données sans protection particulière. Certes, ces bases étaient déjà protégées par le droit d'auteur, mais les critères classiques (empreinte de la personnalité de l'auteur quant à sa composition, sa structure, son expression) rendaient la protection par ce biais presque illusoire.

Désormais, la loi du 1er juillet 1998 cumule au droit d'auteur (qui existe toujours) une protection spécifique, appelée « *droit sui generis du producteur d'une base de données* ».

Depuis cette loi, la base de données, qui se définit 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* » (art L. 112-3 du CPI) est protégeable si le producteur de celle-ci démontre que sa base résulte d'investissements substantiels (financier, matériel et humain, prenant en compte les moyens consacrés à l'établissement, la vérification, la présentation de la base).

La preuve de cet investissement peut être apportée par tous moyens (livres de comptes, etc.) bien que cela puisse être difficile pour certains projets internes. Ici encore, la protection de la base doit être anticipée et, lors de sa réalisation, la DSI peut utilement être mise à profit pour comptabiliser par exemple les budgets ou le nombre de jours/hommes alloués au développement de la base. Autant de preuves utiles qui pourront ultérieurement servir pour établir la preuve que des investissements substantiels ont effectivement été réalisés… et que la base de données est donc protégée.

Le Code de la propriété intellectuelle accorde une protection qui court à compter de l'achèvement de la fabrication de la base ou de la mise à disposition du public si celle-ci est différée et expire 15 ans après le 1er janvier de l'année civile qui suit celle de l'achèvement (art. L. 342-5, al. 1er du CPI). Toutefois, cette protection peut en pratique être rallongée dans le temps. En effet, si la base de données protégée fait l'objet de nouveaux investissements, une nouvelle durée de protection court pendant 15 ans après le 1er janvier de l'année civile suivant celle de ce nouvel investissement (article L. 342-5, al. 3, CPI).

Le recueil de la preuve des investissements réalisés sur cette base ne doit donc en aucun cas cesser lors de la mise en production de celle-ci, mais doit au contraire se poursuivre pendant toute la vie de la base afin de permettre une protection juridique maximale et une juste évaluation en vue de la réparation des éventuels préjudices subis.

De façon similaire au monopole d'exploitation accordé par le droit d'auteur à une œuvre de l'esprit, le droit sui generis confère au producteur des droits patrimoniaux (droit de représentation et de reproduction) et des droits moraux, sauf exceptions (telles que la copie privée). Dans les conditions prévues à l'art. L. 342-3 du CPI, le producteur de la base peut interdire l'extraction ou la réutilisation par la mise à la disposition du public de la totalité ou

d'une partie qualitativement ou quantitativement substantielle du contenu de sa base (art. L. 342-1 du CPI).

L'extraction est donc une notion essentielle, mais suppose en tout état de cause une appropriation. Cependant, même en absence de cet élément, il est toujours possible d'agir sur le fondement de la concurrence déloyale.

Cass. Com. 23 mars 2010, Lectiel c/France Telecom, N° Pourvoi 08-21.768

En vertu de l'art. L. 112-3 du CPI, pour qu'une base de données puisse être protégée, elle doit « *par le choix ou la disposition des matières* » constituer une création intellectuelle.

Le critère d'un apport intellectuel réalisé a été retenu dans l'arrêt de la Cour de Cassation en date du 23 mars 2010 (Cass. Com. Lectiel c/ France Télécom, n° 354, 08-20.427, 08-21.768). Dans cette affaire, il a été jugé que la société France Télécom est bien titulaire du droit sui generis du producteur de base de données constituée à partir des informations de son annuaire. La Cour précise que la base en question constitue un ensemble structuré, mis en exploitation de manière spécifique par la France Télécom et qui ne se résout pas à l'annuaire qu'elle à l'obligation de tenir et mettre à jour. Cette base n'est pas seulement construite à partir des renseignements fournis par les abonnées mais elle est enrichie d'autres informations, dont plus de la moitié vient de France Télécom, de façon à former un ensemble spécifique pour lequel celle-ci a conçu et défini les opérations utiles en leur affectant les moyens correspondants. Ainsi, les Hauts Magistrats confirment l'arrêt de la cour d'appel de Paris du 30 septembre 2008 qui avait prononcé une condamnation de 3.870.000 € en réparation du préjudice subi par l'opérateur du fait que la société Lectiel a procédé au téléchargement de la base en question.

Le producteur de la base peut également interdire l'extraction ou la réutilisation répétée et systématique de parties non substantielles (article L. 342-2 du CPI). **Il est par ailleurs important de préciser que si le créateur de la base de données est un salarié de l'entreprise, alors, contrairement aux logiciels, aucune cession automatique des droits n'est prévue. Le salarié créant la base demeure seul titulaire des droits de propriété intellectuelle. L'entreprise devra donc se faire céder expressément les droits.**

En cas d'atteinte aux droits des producteurs d'une base de données, la loi du 1er juillet 1998 avait prévu une sanction pénale. Ainsi, l'article L. 343-4 du CPI énonce : « *Est puni de trois ans d'emprisonnement et de 300 000 euros d'amende le fait de porter atteinte aux droits du producteur d'une base de données tels que définis à l'article L. 342-1. Lorsque le délit a été commis en bande organisée, les peines sont portées à cinq ans d'emprisonnement et à 500 000 euros d'amende* ».

Reste que la preuve, non pas des investissements de la société mais du caractère frauduleux des « *emprunts substantiels* » réalisés par son concurrent doit pouvoir être apportée, ce qui

peut parfois être difficile une fois le préjudice réalisé. C'est la raison pour laquelle de plus en plus de sociétés introduisent volontairement des données pièges dans leur base, afin de pouvoir démontrer si celles-ci sont également reproduites, que seule une reproduction à l'identique peut expliquer cette présence. Cela suppose une procédure de préconstitution de preuve de la teneur de la base (horodatage et archivage réguliers).

TGI Paris, 13 avril 2010, Optima On Line / Media Contact Israel, Amen:

Dans cette affaire, deux sociétés ont réalisé et commercialisé une base de données contenant notamment des adresses e-mail d'entreprises françaises.

La première société a accusé la seconde d'avoir copié sa base de données et l'a poursuivi en justice.

Elle a revendiqué tout d'abord la qualification de producteur de la base de données, sur le fondement d'attestations et de factures (600.000 euros/an), ce que le tribunal a reconnu.

Dans un second temps, elle s'est fondée sur des adresses pièges, dont elle avait truffé sa base et qui ont été reproduites dans la base de la seconde société, pour en prouver la copie.

Le tribunal a reconnu en conséquence l'extraction substantielle réalisée et a condamné la seconde société à payer à la société Optima On Line la somme de 150.000 € à titre de dommages et intérêts en réparation des atteintes commises à l'encontre de ses droits sur sa base de données France Prospect, de cesser sous astreinte de 200 € par jour la commercialisation de la base de données contrefaite et de publier le jugement sur Internet.

Constat général :

Protéger le patrimoine informationnel de l'entreprise constitue l'une des missions du DSI où le droit a une place essentielle.

Recommandation :

- **Réaliser une cartographie des applications et des flux associés (pour les logiciels propriétaires et libres)**

Contrats de travail :

Le graphisme ou la documentation liés à un logiciel (charte graphique, page Html), les bases de données ne relèvent pas du droit du logiciel mais du droit d'auteur, du droit des bases de données et/ou des dessins et modèles: ce point est à prendre en considération dans les contrats de travail – infographistes / les contrats avec les prestataires. Dans les équipes Projet, les membres (informaticiens ou équipes) ne relèvent pas forcément des mêmes droits en matière de Propriété Intellectuelle. La cession tacite n'est applicable que pour les logiciels et dans certains cas (dans le cadre de la mission dédiée de l'informaticien).

Recommandations :

- **Ordonnancer l'intégration des règles contractuelles en matière de Propriété Intellectuelle, avec la DRH, dans les contrats de travail des salariés :**
  - **Nouveaux salariés**
  - **Personnes clés (directeurs R&D…)**
  - **Autres.**

Logiciel Libre :

La portée juridique des clauses relatives à l'utilisation des Logiciels Libres est mal connue des opérationnels (développeurs, techniciens, …) et cela peut placer l'entreprise dans une situation de non-conformité juridique.

Recommandations :

- **Définir, mettre en place et faire connaître la politique Open Source de l'entreprise :**
- **Sensibiliser les sous-traitants et les développeurs**
- **Déclarer tout recours à l'utilisation d'un logiciel libre**
- **Documenter les licences interdites**
- **Indiquer la marche à suivre pour recourir à un logiciel libre**
- **Prévoir des revues annuelles des logiciels libres utilisés par l'entreprise**

- **Intégrer des clauses dans les contrats informatiques concernant le recours au Logiciel Libre (information sur les logiciels libres utilisés, responsabilité, jouissance paisible), ces clauses devant être comprises comme un socle minimal incontournable avant le lancement de tout marché**

Base de données :

Les bases de données sont valorisées comme un actif immatériel de l'entreprises, et doivent être protégées en conséquence.

Recommandations :

- **Estimer au plan comptable la valeur des bases de données, en conservant une trace des coûts associés au développement de chacune des bases de données, avec les numéros de facture, montants, personnes travaillant sur la base de données, bulletins de paie, nombre d'heures, …**
- **Déposer la base de données auprès de l'APP, en y intégrant volontairement des erreurs, ainsi que la liste de celles-ci, concomitamment pour démontrer qu'elles sont volontaires et ainsi, en cas de besoin, prouver une contrefaçon**

Méthodes agiles :

Les méthodes agiles sont régulièrement utilisées dans le cadre de développement de projets, pour gagner en flexibilité, souplesse et réactivité. Cependant, les méthodes agiles pour fonctionner efficacement, doivent faire l'objet d'une répartition claire des rôles et responsabilités de chaque partie.

Recommandation :

- **Organiser la coopération entre les parties au sein du contrat : définir une gouvernance claire**

PROTECTION DU PATRIMOINE INFORMATIONNEL

Le patrimoine informationnel est constitué par l'ensemble des informations dont dispose l'entreprise et notamment des données clients et fournisseurs, des logiciels, des bases de données, (cf § 4) du savoir-faire, des brevets, etc. Ces informations sont très diverses. Certaines peuvent rentrer dans une catégorie juridique spécifique et être protégeables à ce titre (secret des affaires, droit d'auteur par exemple sur les logiciels, données à caractère personnel, secret professionnel, noms commerciaux, marques ou encore noms de domaine qui, alors qu'il est souvent vu comme une simple extension de la marque sur Internet, prend une importance économique de plus en plus importante et nécessite une gestion particulière). Toutefois, toutes les informations même celles d'apparence anodine, sont susceptibles d'avoir une valeur marchande ou stratégique pour les entreprises, après compilations, corrélations, recoupements et traitements.

CONSIDÉRATIONS JURIDIQUES SUR LA PROTECTION DU PATRIMOINE INFORMATIONNEL

Certains droits sont protégés par le Code de la propriété intellectuelle (sur le fondement de la contrefaçon) ou le droit de la responsabilité civile (par le biais d'actions en parasitisme ou en concurrence déloyale par exemple). Tous ces droits ont un point commun : quelles que soient l'efficacité et la puissance du droit qui les protège (le droit d'auteur et ses déclinaisons étant le plus efficace), la preuve de la titularité des droits, de la réalité de l'atteinte, du préjudice causé et du lien entre les deux derniers doit pouvoir être rapportée par l'entreprise. Car il ne suffit pas de démontrer l'atteinte, il faut chiffrer aussi au mieux le préjudice subi, élément souvent mal évalué dans les dossiers judiciaires.

La protection du patrimoine informationnel prend forme au travers d'un triptyque où devraient intervenir à égale proportion et à chaque étape de la vie du SI :

- les aspects juridiques (identifier le droit applicable, remplir et anticiper les conditions de son application) ;
- les modalités techniques de protection des contenus s'ordonnant autour de la Politique de Sécurité des Systèmes d'Information (protection des accès et limitation des droits d'accès, traçabilité des opérations effectuées sur le SI, confidentialité, sensibilisation au sujet des règles applicables, contrôle a priori et a posteriori, audits, mise en place le cas échéant de procédés techniques - chiffrement, anonymisation, authentification, contrôles périmétriques, etc. - en fonction des risques identifiés et de la valorisation de l'information) ;
- l'établissement et la conservation d'éléments de preuve (logs et traces informatiques, éléments comptables, factures, preuve des contrats et de leur contenu – telles que les stipulations prévoyant les audits, les clauses spécifiques ayant trait à la sécurité, etc. -, existence de documents juridiques opposables

prouvant la sensibilisation tels que chartes, politique de gestion de traces, d'Identity and Access Management, etc.)

De plus, parallèlement à la valeur que peut avoir l'information pour l'entreprise, ce qui peut motiver cette dernière à adopter des niveaux de sécurité différents, **il convient également de prendre conscience que certaines de ces informations ne sont traités par le SI de l'entreprise qu'à titre de dépôt** : les clients, les salariés, les partenaires commerciaux, lui ont, dans le cadre de l'activité de la société, confié leurs propres données. **A charge pour l'entreprise, qui en devient responsable, de leur apporter un traitement excluant toute modification non intentionnelle, toute révélation, toute destruction.**

A ce titre, la sécurité de l'information est devenue une problématique incontournable. Elle constitue un pré-requis fondamental du patrimoine informationnel de l'entreprise sur lequel le DSI doit veiller, non seulement vis-à-vis de l'entreprise mais également vis-à-vis des personnes dont les données sont collectées et traitées par le système d'information, que ce soient celles des salariés, des clients ou celles des prospects. On peut voir que la jurisprudence reprend indirectement cette exigence de sécurisation du système d'information.

TGI Versailles, ch. correc., 18 décembre 2007 : affaire Valéo

Dans cette affaire, une stagiaire chinoise avait pris copie d'informations confidentielles se trouvant dans le système d'information de l'entreprise où elle était en stage et les avait transmis à des tiers.
Elle a été condamnée pour abus de confiance (art. 314-1 du Code pénal) à 1 an d'emprisonnement (dont 10 mois de sursis) et 7.000 € à titre de dommages-intérêts (et 1.500 € au titre de l'article 475-1 du Code de procédure pénale)

La société victime demandait pourtant 150.000 € de dommages-intérêts … mais les magistrats ont fortement minoré la somme du fait de la non sécurisation du SI de l'entreprise :
« *S'il ne fait aucun doute que la société VALEO a subi un réel préjudice moral dont le lien de connexité avec le détournement dont s'est rendue coupable Mademoiselle L. est avéré, ce comportement ne doit être considéré que comme une cause partielle de ce préjudice.* ***Celui-ci n'a été que l'élément déclencheur de l'ampleur médiatique de l'affaire et révélateur des failles du système informatique*** *de la société VALEO* ***insuffisamment protecteur et dès lors à l'origine de son propre préjudice.***
L'évaluation des dommages-intérêts à la charge de Mademoiselle L. doit à ce titre se trouver sensiblement minorée et ramenée à la somme de 7000 euros*, outre la somme de 1 500 euros au titre de l'article 475-1 du code de procédure pénale.* »

TGI Versailles, 18 décembre 2007, Communication Commerce Electronique, 2008, comm. 62, Eric A. Caprioli.

AFFAIRE KERVIEL et atteinte aux systèmes de traitement automatisé de données

Le Tribunal de Grande Instance de Paris, le 5 octobre 2010, a condamné Jérôme KERVIEL pour abus de confiance, faux et usage de faux mais aussi pour introduction frauduleuse de données dans un système de traitement automatisé des données (STAD).

Jérôme KERVIEL avait saisi personnellement ou fait saisir par son assistant trader des opérations fictives dans la base ELIOT dédiée au front office. Cette base était accessible tant à sa hiérarchie qu'aux services chargés de son contrôle notamment les services middle-office DLM. La stratégie développée par Jérôme KERVIEL a été de saisir les données fictives à distance suffisante, dans le temps, des arrêtés mensuels afin d'être en mesure, le cas échéant, de les annuler avant qu'elles ne donnent lieu à confirmation, règlement ou contrôle.

Le tribunal a considéré que « *le caractère frauduleux de l'introduction des données est indépendant du caractère innovant et complexe des techniques employées, de l'évidence de la fictivité des opérations sous-jacentes ou du maintien de ces données en base tampon pendant plus de 20 jours pour certaines d'entre elles ». Les délits d'introduction frauduleuse de données dans un système de traitement automatisé apparaissent parfaitement constitués à l'encontre de Jérôme KERVIEL qui a sciemment saisi des opérations sans réalité économique, qu'il a par la suite pour partie annulées, dans le seul but de masquer ses engagements hors mandat et hors limites*. ».

Jérôme KERVIEL a été condamné à 5 ans d'emprisonnement, dont deux ans fermes, et à payer à la Société Générale près de 5 milliards d'euros.

En effet, le Tribunal correctionnel a appliqué dans cette affaire la jurisprudence de la Cour de cassation (Cass. Crim. 7 no. 2001, Cass. Crim. 6 mai 2009) qui pose en principe qu'en cas de délit intentionnel envers les biens (introduction frauduleuse sur un STAD, abus de confiance, etc.), il ne peut y avoir de partage de responsabilité entre l'auteur et la victime de ce délit qui n'aurait commis au pire que des délits non intentionnels (négligences, etc.). Le Tribunal était donc tenu d'ordonner l'indemnisation totale du préjudice financier subi et prouvé par la partie civile (à l'inverse du préjudice moral de l'affaire Valéo), sans possibilité de le réduire.

SÉCURITÉ DU PATRIMOINE INFORMATIONNEL

Sécurité des données à caractère personnel

Lorsque les informations collectées, traitées et conservées par l'entreprise sont des données à caractère personnel, c'est-à-dire qui permettent l'identification directe ou indirecte d'une personne physique, la règlementation applicable à la protection des données à caractère personnel, au plan européen et national, impose aux entreprises d'en garantir la sécurité et la confidentialité.

Compte tenu des risques présentés par un traitement de données à caractère personnel (destruction accidentelle ou illicite, perte accidentelle, altération, diffusion ou accès non autorisés) et de la nature de ces données, les responsables des traitements sont astreints à une obligation légale particulière de sécurité. Cette obligation, issue de l'article 34 de la loi dite « Informatique, Fichiers et Libertés » de 1978 modifiée en 2004, dispose que « *le responsable du traitement* ***est tenu de rendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données*** *et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. […]* ».

Cette obligation est pénalement sanctionnée par l'art. 226-17 du Code pénal : « *Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites à l'article 34 de la loi n° 78-17 du 6 janvier 1978 précitée est puni de cinq ans d'emprisonnement et de 300 000 Euros d'amende* », soit 1.500.000 Euros pour une entreprise. Mais un défaut de sécurisation des données peut également conduire la CNIL à prononcer des sanctions allant de l'avertissement au blocage du traitement, en passant par la demande au juge des référés d'une injonction imposant de mettre en place toute mesure de sécurité nécessaire. En cas de manquements graves aux prescriptions légales, elle peut également prononcer des sanctions pécuniaires (jusqu'à un montant de 150.000 euros ou de 300 000 euros en cas de récidive) et décider de rendre public ces sanctions (préjudice d'image fort).

Au sens de la loi de 1978, le responsable de traitement est considéré comme celui qui fixe la finalité et les moyens du traitement, donc celui qui décide de la mise en place d'un traitement de données en fonction des objectifs de l'entreprise. Il ne fait donc partie que rarement de la DSI, les responsables de traitement dans l'entreprise se trouvant plus fréquemment au sein de la DRH (traitements des données des salariés), de la Direction financière (comptabilité et documents y afférents), de la Direction du marketing (prospection commerciale, etc.), du service client (Gestion de la Relation Client) ou d'autres services opérationnels.

Toutefois, malgré le fait que la DSI ne soit pas souvent directement en prise avec les traitements de données, l'obligation de sécurité de l'article 34 de la loi de 1978 a un impact sur elle en ce qui concerne la mise en place de mesures garantissant un niveau de sécurité approprié, au regard de la sensibilité des données, de l'état de l'art technique et des coûts engendrés.

Pour autant, le responsable de traitement ne peut pas déléguer sa responsabilité au titre de cette obligation à un sous--traitant ou à un sous-traitant de sous-traitant. **Ainsi, il doit lui-même veiller à ce que le sous-traitant (par exemple un prestataire de services) présente des garanties suffisantes en matière de sécurité (article 35 de la loi précitée) en :**

- imposant contractuellement un niveau de sécurité jugé par lui adéquat aux traitements de données envisagés ;
- menant régulièrement des audits de sécurité des prestataires avec lesquels il souhaite travailler ;
- précisant le cadre exact de la prestation convenue et des modalités de traitement des données qu'il demande au prestataire d'opérer ;
- fixant ces éléments dans le contrat liant les deux parties, en prévoyant des pénalités notamment financières en cas de manquement ;
- encadrant les hypothèses où le prestataire peut faire appel à des sous-traitants en prévoyant notamment que, dans cette hypothèse, des garanties identiques et un contrôle strict de sa part soit toujours prévu et rendu possible.

Cette obligation de sécurité se retrouve également renforcée par certaines réglementations spécifiques, par exemple dans le cas de l'obligation au secret professionnel (professions réglementées, milieux financiers) ou de l'application des articles 14 et 37-2 du règlement n° 97-02 du 21 février 1997 modifié relatif au contrôle interne des établissements de crédit et des entreprises d'investissement.

Enfin, l'entreprise n'assurant pas suffisamment la sécurité de son patrimoine informationnel doit faire face à un risque encore plus important, indépendamment du fait qu'une législation impose ou non la protection d'éléments de celui-ci. Ainsi, en cas d'attaque de son SI et de pillage de son patrimoine informationnel, le défaut de sécurisation technique des informations (du SI, etc.) risque d'empêcher la protection juridique optimale de l'entreprise qui ne pourra que partiellement poursuivre l'auteur de l'intrusion : la condamnation de celui-ci pourrait être largement minorée notamment en termes de dommages-intérêts.

Délibération CNIL n°2009-469 du 9 juillet 2009 de la formation restreinte prononçant une sanction pécuniaire à l'encontre de la SCP X.

Une délégation de la CNIL s'était rendue le 15 décembre 2006 dans les locaux de la SCP X. (une étude d'huissiers), afin d'effectuer un contrôle sur place. La délégation s'était attachée à examiner le progiciel de gestion des débiteurs et des créanciers dénommé « PRIAM », base de données alimentée par la SCP dans le cadre de ses enquêtes. Des extractions effectuées et dénommées « adresse.dbf » et « agentdos.dbf » avaient révélé l'existence de nombreux commentaires dans les fiches informatiques des débiteurs, tels que par exemple « idiot fini », « maladie alcoolique et syndrome dépressif », « son fils va faire une cure de désintoxication car alcoolique », « deb en maladie cancer avec métastase », « fréquent séjour prison pr pb drogue », « est en prison pour viol de ses enfants », «vit dans taudis » ou encore « appt très sale ».

En outre, il avait été constaté que l'application « PRIAM » était accessible aux collaborateurs de la SCP, sans qu'un mot de passe ne soit exigé.

Il avait par ailleurs été relevé que les deux études d'huissiers partageant les locaux avaient mis en commun leurs moyens informatiques. Ainsi, le progiciel « PRIAM » s'articulait principalement autour d'une table d'identités commune aux deux SCP (comprenant les données d'identification des personnes enregistrées qu'elles soient débitrices ou créancières : nom, prénom, adresse, qualité, profession, etc.) et de deux tables de gestion des dossiers appartenant respectivement à chaque SCP. Les collaborateurs d'une SCP pouvaient accéder aux informations contenues dans la base alimentée par l'autre SCP, les deux structures ayant parfois des débiteurs en commun.

Enfin, il avait été noté qu'au jour du contrôle, le traitement de gestion des débiteurs et des créanciers n'avait fait l'objet d'aucune formalité préalable auprès de la CNIL.

Suite à une mise en demeure et des promesses de la SCP, un nouveau contrôle sur place a été effectué en janvier 2009. Malgré certains progrès, la procédure de sanction a été engagée en se fondant sur divers points et notamment un manquement à l'obligation de veiller à la sécurité et à la confidentialité des données :

« *La Commission rappelle qu'en application de l'article 34 de la loi n° 78-17 du 6 janvier 1978 modifiée, « le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».*

Dans sa délibération n° 2007-012 du 25 janvier 2007, la Commission avait mis la société en demeure de « définir un dispositif d'accès sécurisé au progiciel « PRIAM » (mot de passe et

journalisation des accès) permettant notamment de garantir que les collaborateurs n'auront accès qu'aux dossiers de l'étude ».

Dans sa réponse du 21 mars 2007, la SCP avait notamment indiqué à la CNIL que l'accès au progiciel PRIAM allait être sécurisé par la mise en place de mots de passe individuels régulièrement modifiés et par la journalisation des accès.

Le rapporteur a relevé que si depuis la mise en demeure de la Commission, chaque salarié de l'étude dispose d'un mot de passe individualisé, pour autant les mots de passe attribués n'avaient, au jour du contrôle sur place, pas été renouvelés depuis plus de 18 mois.

La SCP soutient qu'un renouvellement régulier des mots de passe ne sécuriserait pas davantage les données traitées. Néanmoins, la SCP précise que la rédaction de la charte informatique qui sera mise en œuvre par le nouveau CIL désigné, permettra de définir une politique de renouvellement des mots de passe.

La Commission considère, à l'inverse, qu'un renouvellement régulier des mots de passe est une précaution indispensable pour garantir la sécurité et la confidentialité des données. Le mot de passe est par essence un élément clef de la sécurité du réseau et des données. En cas de divulgation de celui-ci à un tiers, interne ou externe à la société, son renouvellement régulier permet de limiter, dans le temps, l'usurpation. Il en va de même dans l'hypothèse d'une captation, par exemple par un logiciel espion, du couple identifiant / mot de passe à l'insu des utilisateurs et des administrateurs.

En conséquence, la Commission estime qu'à la suite de la mise en demeure, la SCP aurait du mettre en place un renouvellement régulier des mots de passe, et ce a fortiori dans le contexte particulier de partage des locaux avec un autre organisme. La SCP ne s'est donc que partiellement conformée à la mise en demeure de la CNIL. ».

De ce fait, la CNIL a prononcé à l'encontre de la SCP une sanction pécuniaire de 10.000 euros ainsi que la publication de la décision sur le site legifrance.

Disponible à l'adresse http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/227/

Obligation de notification des violations de données à caractère personnel

Confrontés aux risques de fraudes à l'identité et aux exemples médiatiques de pertes ou de vols de données préjudiciables (données patrimoniales, etc.), plusieurs Etats (ex : plusieurs Etats aux Etats-Unis, Allemagne) ont récemment décidé de réagir en renforçant leurs règles en matière de sécurité des systèmes d'information. Celle-ci prend notamment la forme d'une obligation, pour l'acteur économique victime d'une violation de sécurité (vol ou perte d'informations sensibles, etc.), de notifier celle-ci à son régulateur ou directement aux propriétaires de ces informations, afin qu'ils prennent les mesures adéquates en toute

connaissance de cause. Ainsi, les coûts engendrés, qu'ils soient économiques (202 $ par incident et par client selon la « *US Cost of Data Breach Study* » du Ponemon Institute) ou juridiques (actions en responsabilité, actions de groupe aux USA, etc.) sont autant de stimulants à la sécurité. L'Union européenne, suivant ce mouvement de fond, a donc souhaité renforcer l'obligation de sécurisation des données issues de la directive 1995/46/CE (parallèle de l'article 34 de la loi française de 1978) en la complétant d'une obligation de notification au cas où cette sécurité aurait été violée.

Après débats parlementaires, cette obligation a tout d'abord été insérée dans deux directives européennes issues de la mise à jour du « Paquet télécom » (cadre juridique communautaire des communications électroniques) de 2002, les directives 2009/140/CE (obligation se concentrant sur la sécurisation technique des réseaux, qui ne sera pas abordée plus avant ici) et 2009/136/CE modifiant notamment la directive « vie privée et communication électronique » 2002/58/CE. Cette directive sectorielle concerne les entreprises fournissant des réseaux de communications publics ou des services de communications électroniques accessibles au public (fournisseurs d'accès à internet, etc.) et s'applique lorsque la sécurité des données à caractère personnel a été violée.

L'Union Européenne avait toutefois inscrit dans les considérants de cette directive le principe de l'extension à tous les secteurs économiques, à brève échéance (Voir notamment F. Coupez, *« De l'obligation de notification des failles de sécurité,* 01 Informatique n°2033 01/04/2010, P. Agosti et F. Coupez*, Sécurisation des systèmes d'information : la pression juridique s'accroît, les sanctions financières aussi,* www.journaldunet.com*)*, ce qu'elle a fait en rendant public une proposition de règlement européen le 25 janvier 2012 qui intègre cette obligation et l'étendra à tous à l'issue de son processus d'adoption (*Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données*).

En ce qui concerne la transposition française des deux directive précitées, elle a été opérée par l'ordonnance n°2011-1012 du 24 août 2011 renforçant donc notamment les obligations à la charge des fournisseurs de services de communications électroniques afin de pouvoir répondre plus efficacement aux atteintes graves à la sécurité des systèmes d'information.

Cette ordonnance a été prise sur le fondement de l'article 17 de la loi n°2011-302 du 22 mars 2011 portant diverses dispositions d'adaptation de la législation au droit de l'Union européenne en matière de santé, de travail et de communications électroniques (JO du 23 mars 2011 p. 5186) et qui a, entre autres, autorisé le gouvernement à prendre par voie d'ordonnance les dispositions de nature législative nécessaires à la transposition des directives précitées. Le projet d'ordonnance avait auparavant été soumis à consultation publique par le Ministre de l'économie numérique Eric Besson le 3 mai 2011, en parallèle de

la consultation de l'ARCEP, du CSA, de la CNIL et du Conseil National du Numérique, nouvellement créé (voir CCE, Christophe Caron *CNN*, CCE juillet 2011 n°7, Repère).

L'ordonnance transpose les directives 2009/136/CE et 2009/140/CE dans le Code des postes et des communications électroniques (CPCE), le Code de la consommation et dans la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Loi Informatique, Fichiers et Libertés) et dans le Code pénal (Titre 1er). Outre ces dispositions, elle contient également des mesures relatives à la gestion des fréquences radioélectriques destinées à lutter contre les brouillages et à encourager le marché secondaire des fréquences (Titre II). Un titre est consacré à la lutte contre les atteintes à la vie privée et à la sécurité des systèmes d'information dans le domaine des communications électroniques afin de renforcer les systèmes d'information des autorités publiques et des opérateurs d'importance vitale (Titre III). Le titre IV lui clarifie certaines dispositions du CPCE. Il est suivi des dispositions transitoires finales (Titre IV).

Un nouvel article 34 bis de la l**oi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés a ainsi été créé**.

Concernant son champ de compétence, ce nouvel article est applicable « *au traitement des données à caractère personnel mis en œuvre dans le cadre de la fourniture au public de services de communications électroniques sur les réseaux de communications électroniques ouverts au public* » c'est-à-dire sur les réseaux de communication établis ou utilisés pour la fourniture au public de services de communications électroniques ou de services de communication au public par voie électronique. Il est précisé que le texte concerne également les fournisseurs « *prenant en charge les dispositifs de collecte de donnée et d'identification* ». Concrètement, cette obligation concerne les fournisseurs d'accès internet et les opérateurs de téléphonie mobile (Orange, SFR, Bouygues Télécom et leurs MVNO). Cette obligation pourrait également être susceptible de s'appliquer aux grandes entreprises dès lors qu'elles offrent un accès internet à des clients ou des prospects, par exemple via un point d'accès WiFi ouvert au public.

La notification concerne les violations « *de la sécurité entrainant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisé à des données à caractère personnel faisant l'objet d'un traitement dans le cadre de la fourniture au public de service de communication électronique* » mais étant donné que l'on considère ainsi tout ce qui permet directement ou indirectement d'identifier une personne physique, l'application en est *de facto* très large.

Dans une telle situation, la société victime des violations de données à caractère personnel (vol, piratage de ses fichiers, perte, etc.) devra alors avertir sans délai la CNIL.

Il est par ailleurs prévu que l'opérateur avertisse également sans délai la personne intéressée lorsque la violation « *peut porter atteinte aux données à caractère personnel ou à*

la vie privée d'un abonné ou d'une autre personne physique ». A défaut d'avertissement des personnes concernées, la CNIL aura la possibilité d'envoyer des mises en demeure. De plus, le dispositif du nouvel article 34 bis de la loi du 6 janvier 1978 est pénalement sanctionné par l'introduction dans le Code pénal de l'article 226-17-1 : « *Le fait pour un fournisseur de services de communications électroniques de ne pas procéder à la notification d'une violation de données à caractère personnel à la Commission nationale de l'informatique et des libertés ou à l'intéressé, en méconnaissance des dispositions du II de l'article 34 bis de la loi n°78-17 du 6 janvier 1978, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende* ».

Enfin, les fournisseurs de services de communication électronique seront tenus à une obligation de tenir un inventaire répertoriant les violations, les modalités et les effets des mesures prises pour y remédier. Cet inventaire devra être tenu à disposition de la CNIL.

Le décret n°2012-436 du 30 mars 2012, portant transposition du nouveau cadre règlementaire européen des communications électroniques, précise quant à lui notamment les modalités des notifications prévues à l'article 34 bis de la loi n° 78-17 du 06 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Ainsi, ce décret liste les éléments devant figurer dans la notification adressée à la CNIL et dans celle adressée à la personne intéressée. Le décret précise notamment que la notification à la personne intéressée n'est pas nécessaire si la CNIL a constaté que les mesures sur lesquelles elle s'est prononcée ont été efficacement appliquées.

Enfin, le décret définit les mesures de protection appropriées comme « *toute mesure technique efficace destinée à rendre les données incompréhensibles à toute personne qui n'est pas autorisée à y avoir accès* » et donne surtout un délai de 2 mois à la CNIL pour vérifier si ces mesures ont correctement été mise en œuvre et appliquées, une absence de réponse à la fin de ce délai valant non acceptation des mesures et par conséquent obligation de notifier à l'intéressé. La CNIL a également la possibilité de mettre en demeure le fournisseur de procéder à la notification après de la personne intéressée quand la violation est grave.

Dès lors, compte tenu de l'importance stratégique du patrimoine informationnel de l'entreprise et de l'ensemble des textes qui le protège il appartient au DSI de faire mettre en place les moyens d'identification et de contrôle à même de le protéger, notamment par le biais d'un système de management de la Sécurité de l'Information (SMSI : norme ISO 27001). Élément primordial de ce système, la traçabilité est la clé d'une collecte utile de l'information à travers l'ensemble du SI, pour, dans le pire des cas, reconstituer les incidents, en réparer ou en diminuer les conséquences.

L'entreprise ne doit toutefois pas perdre de vue que ces outils de traçabilité permettent indirectement un contrôle de l'activité du salarié et ne peuvent donc être déployés hors le respect des principes du droit du travail et des libertés fondamentales (§6).

Constat :

La protection du patrimoine informationnel passe par la maîtrise de la sécurité de l'information, autant en interne que chez les prestataires extérieurs.

En interne, la fonction de Correspondant informatique et Libertés est très importante.

Avec un nouveau règlement européen, accepté le 25 janvier 2012, le détaché à la protection des données à caractère personnel devient le délégué à la protection des données (DPD). Sa désignation deviendra obligatoire dans un certain nombre de cas, notamment pour une entreprise employant 250 personnes ou plus.

Recommandations :

- **Prévoir en amont du choix d'un prestataire technique l'évaluation de la sécurité informatique (à défaut motif d'exclusion) et pas en aval lors d'un audit et calculer des pénalités contraignantes pour le prestataire**
- **Prévoir une sensibilisation à la fonction de Correspondant Informatique et Libertés dont les missions consistent à :**
- **Sensibiliser, réaliser ou faire faire des formations, diffuser des informations relatives à la loi Informatique et Libertés,**
- **Superviser les traitements mis en œuvre,**
- **établir une liste des traitements et éventuellement être chargé d'autres formalités telles que les demandes d'autorisation ;**
- **Détecter les problèmes éventuels liés à la mise en œuvre des traitements**
- **Alerter les autorités de tutelle en cas de problème identifié ou de soupçon sur la conformité d'un traitement.**

SÉCURITÉ DES USAGES DU NUMÉRIQUE

L'entreprise doit assurer au mieux la sécurité de son système d'information.

De plus, la DSI est également confrontée à certains salariés qui font les usages les plus divers des moyens offerts par le SI (mise à dispositions de serveurs partagés, de postes de travail mais également d'ordinateurs portables, d'assistants personnels (Blackberry, iPhone, etc.) ou d'accès distants (via clés 3G, etc). Et certains utilisateurs peuvent vouloir encore les étendre, que ce soit pour des besoins professionnels allégués ou pour des raisons de simple commodité personnelle. Avec l'arrivée de la génération des « digital natives » dans l'entreprise, les frictions de ce type ne feront que croître. S'agissant de l'utilisation des équipements personnels, la décision présente des enjeux importants, ce qui implique une démarche à suivre et une stratégie à adopter. Ces nouveaux usages posent de nombreuses questions juridiques en termes de droit social (discrimination, lien avec le télétravail, consultation des IRP, …), fiscal (subvention aux salariés concernés, …), assurances (du salarié et de l'entreprise), licences d'utilisation non professionnelle. En tout état de cause, la rédaction d'une charte spécifique (ou un nouveau chapitre de la charte informatique) s'impose pour encadrer ces nouveaux usages.

PRINCIPAUX RISQUES À PRENDRE EN COMPTE

La consultation de sites pornographiques n'est plus, depuis longtemps, le seul exemple d'utilisation incorrecte du SI de l'entreprise et il n'est plus rare de voir les DSI confrontées à des hypothèses :

- **De transfert automatique de la messagerie interne** encadrée, sauvegardée et sécurisée, vers un système de messagerie externe de type webmail, à la contenance plus étendue, mais sans aucune garantie de continuité ou simplement de confidentialité ;
- **D'usage dans l'entreprise, voire pour des tâches professionnelles, de moyens informatiques personnels considérés comme plus efficaces par le salarié** (alors que celui-ci n'est pas forcément reconnu par l'entreprise et soulève des problématiques de droit d'auteur (notamment si l'utilisation prévue par la licence est purement personnelle et que le salarié l'utilise à des fins professionnelles) ;
- **D'installation, sans autorisation, de logiciels spécifiques utiles (ou non) pour l'activité professionnelle du salarié,** qui peuvent rentrer en conflit avec les logiciels existants, mettre en danger tout ou partie du SI, voire dont la licence d'utilisation n'est pas respectée ;
- **De désactivation volontaire des systèmes de sécurité type anti-virus ou firewall**, ou encore des systèmes d'indexation ou de sauvegarde automatiques, dans le but d'accélérer les performances de l'ordinateur ;

- **De partage de certains fichiers sur les serveurs partagés de l'entreprise** (dont la sauvegarde régulière à un coût important pour l'entreprise) qui ne sont pas d'ordre professionnel et qui sont parfois extrêmement volumineux ;
- **D'installation et d'utilisation de logiciels Peer to Peer et / ou de téléchargement de contenus volumineux** (démos de jeux, logiciels, vidéos, etc.) et peut-être protégés (musique ou films téléchargés au mépris du droit d'auteur).

Cependant, juridiquement, ces usages qui peuvent s'avérer en tant que tels déjà préjudiciables à l'employeur, sont susceptibles également d'engager sa responsabilité vis-à-vis de tiers. C'est ce qui découle d'une série de réglementations et de décisions de jurisprudence récentes telles que, notamment :

- **La responsabilité de l'employeur du fait des agissements de son salarié** (art. 1384 al. 5 du Code civil), qui s'applique notamment lorsqu'un salarié se sert du SI de son employeur à ses propres fins et pour commettre des actes répréhensibles ou préjudiciables (insultes, propos outrageux ou diffamants, etc.). Ainsi, un employeur a récemment été reconnu responsable du téléchargement et de l'utilisation illégaux par un de ses employés d'une version contrefaite du module d'un logiciel protégé, objet d'un brevet français et international, logiciel déployé sur quarante-neuf ordinateurs du site (CA Grenoble, 7 septembre 2009, n°07/01984).

CA Aix en Provence, 13 mars 2006 , SA Lucent Technologies c/ SA Escota, SA Lycos France, Monsieur Nicolas B.

Cet arrêt met en exergue les conditions de responsabilité de l'employeur confronté aux actes illicites de ses employés commis via les moyens techniques qu'il a mis à leur disposition.

En l'espèce, un salarié de la société Lucent Technologies avait créé, grâce aux ressources techniques de son employeur, des pages personnelles sur l'Internet dénigrant la société Escota.

Bien que ledit salarié ait été licencié, il a quand même été établi que :

- le salarié usait quotidiennement dans le cadre de ses fonctions d'un ordinateur et d'Internet,
- une note de service avait permis au personnel l'utilisation des équipements informatiques pour consulter d'autres sites que ceux présentant un intérêt en relation directe avec leur activité
- enfin, il avait été autorisé à disposer d'un accès à l'Internet, même en dehors de ses heures de travail.

Dès lors l'employeur devait répondre solidairement du dommage causé à autrui par le salarié.

Disponible à l'adresse : http://www.juriscom.net/documents/caaix20060313.pdf

Au contraire, sur le plan du droit du travail, le licenciement pour faute grave a été jugé valable par la Cour d'appel d'Aix-en-Provence. Ainsi,, la Cour a confirmé le jugement qui avait débouté le salarié de ses demandes en indemnités pour rupture abusive de son contrat de travail en considérant « *que les agissements* [reprochés au salarié] *caractérisent la faute car la société Lucent Technologies France ne pouvait conserver à son service, sauf à encourir un risque majeur, un employé au comportement incontrôlable, même pendant la durée limitée du préavis.* » (CA Aix en Provence, 17° ch., arrêt n° 84 du 17 janvier 2005).

- **Droit d'auteur.** Les lois Hadopi 1 (loi « favorisant la diffusion et la protection de la création sur internet » du 12 juin 2009) et 2 (« relative à la protection pénale de la propriété littéraire et artistique sur internet » du 28 octobre 2009) ainsi que leurs décrets d'application, mettent en œuvre la « riposte graduée » afin de lutter contre le piratage des contenus protégés sur l'internet. Or, le concept de riposte graduée se focalise sur la personne du « titulaire de l'accès » à l'internet et lui impose de sécuriser son matériel informatique de sorte qu'il ne soit pas utilisé pour commettre des actes répréhensibles en matière de droit d'auteur. A l'issue de deux injonctions, et outre une amende de 5ème classe (1.500 €, voire 7.500 € pour une personne morale), un juge peut ordonner une coupure de l'accès à l'internet du « *titulaire* », étant entendu que l'exception prévue pour les entreprises a été supprimée. Ainsi, les entreprises titulaires d'un accès risquent dorénavant la coupure du fait des agissements de leurs salariés (l'application aux entreprises n'étant pas expressément exclue). **Par ailleurs, le partage des contenus au sein des infrastructures réseaux est susceptible d'être qualifié d'acte de contrefaçon et d'entraîner la responsabilité de l'employeur (ayant fourni les moyens techniques la rendant possible) notamment si l'on démontre sa connaissance des faits et son incapacité à les faire cesser ou pire, son inaction.**
- L'impossibilité pour l'employeur de se prévaloir de la faute contractuelle du cocontractant du fait de comportements fautifs de ses propres salariés, tel que l'exemple ci-dessous.

CA Paris, sect. B, 4 mai 2007, Normaction c/ KBC Lease France, DMS (Communication Commerce Electronique, 2008, comm. n°30, Eric A. Caprioli)

Une entreprise du secteur industriel conclut un contrat pour la fourniture d'une solution de sécurité intégrant un anti-virus. Infectée par un virus, elle le résilie de façon anticipée, arguant de la totale inefficacité de la solution.

Son contractant, le prestataire, prenant connaissance du rapport des sites consultés par la société du secteur industriel, constate plusieurs connexions à des sites étrangers à son activité et porteurs de contenus pornographiques voire pirates.

Les juges concluent à la résiliation fautive du contrat par le client, condamné à indemniser le prestataire. La raison en est simple : en laissant son personnel se connecter sur des sites étrangers à son activité, l'entreprise cliente est à l'origine de son propre préjudice et ne peut le reprocher au prestataire.

« *Que ces rapports mettent en évidence que la société DMS s'est connectée à un nombre élevé de sites étrangers à son activité tels que Britney Spears (une chanteuse anglaise), Harry Potter, Best Matrix sceen server, Photoshop, Birtney Spears sex xxx, Kazaa, Microsoft Office 2003 Crack best. Exe, XXX hard core pics.jpg exe ;*

Que tous ces sites qui étaient infectés n'avaient aucun lien avec l'activité de métallerie et serrurerie de la société DMS ;

Considérant qu'il ne peut rentrer dans les obligations contractuelles de la société Normaction d'assurer une protection de la société DMS contre des virus contenus dans des sites informatiques étrangers à son activité, voire illégaux tels que les sites qui permettent de télécharger gratuitement des programmes habituellement payants

Considérant que la société DMS, en laissant son personnel se connecter à de tels sites, a rendu, par sa faute, inefficace la protection que la société Normaction s'était engagée à lui fournir de sorte qu'elle ne pouvait invoquer la défaillance de la protection anti-virus comme un juste motif de la résiliation des contrats ».

CONTRÔLE DES SALARIÉS

Face à ces contraintes qui s'ajoutent à son obligation de sécurisation du SI et à sa volonté de préservation du patrimoine informationnel, la DSI doit mettre en œuvre les moyens appropriés de contrôle, de traçabilité et de restriction d'usage du SI sous réserve de la légalité du contrôle de l'activité du salarié.

En effet, à quoi servirait d'avoir une preuve de l'imputabilité à un salarié d'un fait préjudiciable ou fautif si cette preuve ne pouvait être retenue devant un tribunal, le contrôle étant en soi illégal ou faute de respecter un formalisme adéquat observé en amont (lors de la mise en place du système servant au contrôle) ?

Ainsi, il est important de garder en mémoire certains principes fondamentaux :

- La jurisprudence a reconnu que le contrôle de l'activité du salarié par son employeur était parfaitement possible et découlait du lien de subordination entre l'employeur et

le salarié. Ce dernier peut donc donner des directives au salarié, contrôler le suivi de celles-ci et sanctionner les manquements éventuels.

- Pour autant, ce contrôle de l'activité s'inscrit dans un cadre découlant du Code du travail et de la loi « Informatiques, Fichiers et Libertés » :
    - L'employeur ne peut ainsi apporter des restrictions aux libertés individuelles et collectives si elles ne sont pas « *justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* » (art. L. 1121-1 Code du travail) ;
    - Il doit par ailleurs respecter, lors de son contrôle, les principes de transparence, de loyauté et de proportionnalité ;
    - Cela signifie, en synthèse, qu'il doit avertir le salarié de la possibilité et de l'étendue du contrôle, ne pas utiliser de systèmes cachés ou faire preuve de manœuvres et ne pas organiser un contrôle individualisé, précis et systématique. Le principe de proportionnalité impose notamment de mettre en place en pratique **un contrôle général, statistique et anonyme** et de ne passer dans une phase individualisée que ponctuellement, seulement si celui-ci est justifié (ex : alerte de sécurité).
- L'employeur doit remplir les formalités CNIL éventuellement nécessaires (le contrôle se fondant sur des traitements de données à caractère personnel), mais également informer préalablement les instances représentatives du personnel (Comité d'Entreprise, Comité d'Hygiène, de sécurité et des Conditions de Travail, etc.) ;

Par ailleurs, ces formalités doivent être suivies également pour tout projet de mise en place d'outils informatiques, de logiciels ou de systèmes pouvant potentiellement être utilisés pour permettre un contrôle de l'activité du salarié (quand bien même il ne le serait jamais ou seulement à plus ou moins longue échéance).

CHARTE INFORMATIQUE

Pour encadrer au mieux les conditions d'utilisation du SI, l'employeur est amené à établir ou à mettre à jour un document opposable juridiquement aux salariés et détaillant ses droits et obligations en matière de SI. En pratique, celui-ci prend généralement la forme d'une annexe au règlement intérieur de l'établissement (voire elle peut être intégrée dans le règlement intérieur) et peut se retrouver sous des noms différents, le point commun étant en général l'usage du vocable de **« charte »** (« *informatique* », « *d'utilisation des moyens informatiques de l'entreprise* », « *d'utilisation du SI de l'entreprise* », « *d'utilisation des moyens de communication électronique de l'entreprise* », etc.).

Ces chartes ne sont que les premières pierres d'un ensemble plus vaste destiné à tous les acteurs (prestataires, stagiaires, administrateurs, etc.) et doivent être complétées par des livrets de procédures ou « politiques » organisant la traçabilité des incidents, le contrôle et

la conservation des preuves numériques, la gestion de l'authentification et de l'accès au SI, la conservation des messages électroniques, etc.

L'ensemble de ces documents doit bien sûr se fonder sur la Politique générale de Sécurité des SI de l'entreprise, laquelle doit être mise à jour régulièrement et, en tout cas, avant l'élaboration de ces divers documents.

De son côté, la charte précise les principes de confidentialité applicables aux informations numériques et aux moyens d'authentification, les interdictions d'usage du SI à respecter (connexion à certains sites, usage des serveurs partagés, messagerie instantanée, etc.), les modalités d'usage de la messagerie mise à disposition à titre professionnel, de gestion de l'absence ou de l'indisponibilité d'un collaborateur (et donc d'accès à ses fichiers et sa messagerie), le cas échéant, l'usage personnel par le salarié de tout ou partie des outils informatiques mis à sa disposition (et les limites de cet usage), les traces informatiques collectées, les modalités de contrôle éventuel (limites et conditions de l'accès aux fichiers du salarié et à sa messagerie), etc.

Face à l'émergence de la problématique du BYOD ou Bring Your Own Device (parfois françisé en VATA pour « Viens avec ce que tu as ») consistant dans la demande forte des utilisateurs de pouvoir connecter leurs propres outils personnels perçus comme plus performants et plus conviviaux au SI de l'employeur et d'avoir un usage également professionnel de ce moyen, les chartes doivent également prévoir les interactions éventuelles des obligations décrites ci-dessus qu'elles édictent et l'éventuel usage que rendrait possible l'employeur de ces outils personnels. En fonction de la situation (achat d'outils choisis par le salarié, outils achetés sur fonds personnels autorisés dans une faible mesure pour des cas précis, outils achetés sur fonds personnels autorisés dans tous les cas, etc.) la charte devra nécessairement s'accompagner de document juridiques complémentaires (conditions générales d'accès, accord d'entreprise le cas échéant, etc.) de nature à préciser, dans le respect des droits de chacun, l'étendue des contrôles qui pourront être opérés sur ces outils, les possibilités d'éventuels effacements à distance en cas de vol ou de perte, la ségrégation ou non des sphères professionnelles et privées, les questions de filtrage des flux et des données, etc.).

Dès lors, compte tenu de la nature éminemment structurante pour le SI de l'entreprise de nombre de ces documents (politiques, conditions générales d'utilisation et chartes), la forte implication de la DSI dans leur élaboration, leur rédaction, et surtout leur gestion apparaît fondamentale tant dans une approche immédiate (et pratique) que prospective. Ces documents seront également l'occasion d'une stratégie transversale de l'entreprise allant de la direction des ressources humaines aux directions opérationnelles et juridiques et validés le plus souvent par la direction générale.

Enfin, ce type de charte devra également recevoir des dispositions particulières, voire une déclinaison propre spécialement destinée aux utilisateurs disposant de droits d'habilitations dérogatoires, souvent en raison de leur fonction : **les administrateurs, qu'ils soient administrateurs systèmes ou administrateurs de messagerie.** En effet, si des règles particulières peuvent trouver à s'appliquer compte tenu de certains de leurs droits d'accès, il convient surtout de leur rappeler leurs droits et devoirs. Ce rappel paraît nécessaire, ne fût-ce qu'à des fins pédagogiques, la jurisprudence étant particulièrement sévère avec eux.

Ainsi, les tribunaux leur appliquent les mêmes règles qu'aux salariés lambda (devoir de confidentialité, etc.) mais avec une sévérité particulièrement accrue étant donné que les obligations qui pèsent sur les gardiens du SI sont « à la mesure de leurs pouvoirs d'intrusion ».

TGI Rennes, ch. correc., 21 février 2008 : (Communication Commerce Electronique, Juin 2008, Comm. n°85, Eric A. Caprioli)

Le RSSI d'une société a utilisé ses connaissances et droits d'accès pour usurper l'identité des dirigeants de cette société et prendre connaissance de leurs courriers électroniques.

Il a été condamné assez lourdement à une peine de 6 mois d'emprisonnement avec sursis, 1.500 euros d'amende, une interdiction d'accès aux marchés publics pour 3 ans, de 800 euros pour préjudice moral (d'un des dirigeants) et 1.000 pour les frais de justice de ce dernier.

« *qu'il ne peut d'avantage arguer du fait que, administrateur du réseau il avait par nature accès à toutes les données, alors que cet accès est limité aux besoins de la bonne marche du système et de sa sécurité, et ne peut en aucun cas servir des intérêts qui lui sont personnels ; (…)*

Attendu que M. F. exerçait et exerce à ce jour une profession qui place ses partenaires dans un état de réelle dépendance et suppose en conséquence qu'ils puissent lui accorder une totale confiance ;

Que de tels faits, commis dans le cadre d'une profession qui lui conférait des obligations à la mesure de ses pouvoirs d'intrusion, sont d'une particulière gravité ;

Qu'en raison des risques qu'elle génère dans une société de plus en plus informatisée, une telle attitude doit être sanctionnée d'un sévère avertissement ; (…) ».

Recommandations :

- **Définir une charte d'usages des outils numériques en entreprise, dont l'objectif est de fixer quelques règles d'usages éthiques et responsables dans l'entreprise étendue, partagées par tous. Dans ce type de charte :**
- **La Direction s'engage, vis-à-vis des collaborateurs, sur une série de points relatifs à l'emploi des outils numériques et aux bonnes pratiques associées**
- **Les règles définies doivent être cohérentes avec les valeurs de l'entreprise et préciser les conduites managériales à tenir, telles que le respect réciproque, la valorisation de la créativité et le discernement.**
- **Une telle charte doit donc couvrir *a minima* les points suivants :**
  - **Le respect de la vie privée des collaborateurs**
  - **Le télétravail**
  - **Les courriers électroniques**
  - **Les réseaux sociaux et la communication associée**
  - **Le Bring Your Own Device**
  - **La responsabilité des utilisateurs vis-à-vis des informations qu'ils communiquent et publient.**

LES OUTILS DE TRAVAIL COLLABORATIF

Les entreprises sont confrontées à des évolutions managériales et organisationnelles qui les contraignent à adopter de nouvelles habitudes de travail et de nouveaux modes opératoires. Ainsi, pour une plus grande productivité, l'entreprise doit orienter et organiser son système d'information pour accélérer la création et la communication de l'information. C'est dans cette optique que le travail collaboratif s'est développé.

Il recouvre l'ensemble des moyens organisationnels et techniques permettant d'offrir à des groupes de personnes réunies autour d'une action ou d'un projet commun, la possibilité de communiquer, de coopérer, et de se coordonner tels que le partage des fichiers (textes, images, vidéos…) ou la messagerie instantanée.

DÉFINITION DES OUTILS

Le travail collaboratif rassemble de nombreux outils que l'on peut classifier en quatre catégories distinctes :

- **Les outils de communication de base** : Ainsi, le mail ou encore la visioconférence ont pour objectif de faire circuler des informations entre deux ou plusieurs collègues de travail.
- **Les outils de travail partagé** : Le partage d'application, la contribution à des forums ou encore l'édition partagée supposent un degré plus avancé de collaboration entre plusieurs individus. Ils permettent à plusieurs personnes de travailler sur un même document ou sur une même application.
- **Les outils d'accès au savoir (ou de knowledge management)** : tels que les bibliothèques, les wiki, les annuaires électroniques ou encore les FAQ, permettent, lorsqu'un employé a créé ou développé un document ou une expertise, de faire en sorte que tous les autres employés puissent accéder à ces informations, qu'ils en prennent connaissance voire qu'ils l'enrichissent ; ces outils sont centrés sur la gestion des connaissances.
- **Les outils de *workflow* :** On peut citer les outils de gestion des tâches ou les agendas partagés ; ils assistent le chef de projet dans le suivi de son projet et permettent de contrôler et d'accélérer les interactions entre les différents acteurs.

Toutefois si les technologies sur lesquelles se fondent ces outils ne soulèvent que rarement de difficultés juridiques (pour l'instant !), leur usage, tant en interne qu'avec des partenaires (publics et privés), ne va pas sans soulever d'intéressantes problématiques juridiques notamment en termes de propriété intellectuelle, de respect des règles d'usage et de confidentialité.

LA QUESTION DE LA PROPRIÉTÉ INTELLECTUELLE

Concernant les problématiques de propriété intellectuelle, celles-ci sont de deux ordres en pratique.

D'une part, le respect des droits de propriété intellectuelle impose **le strict respect des licences d'utilisation des logiciels**, dans l'hypothèse où ils n'auraient pas été développés en interne. Les licences doivent également être respectées, y compris si le logiciel ou la plate-forme est « libre » ou si elle est d'utilisation « gratuite ». Quelle est la licence applicable ? Est-elle libre ou propriétaire ? L'utilisation gratuite est-elle également prévue pour une entreprise ? Telles sont par exemple les premières questions qui doivent être posées et qui doivent trouver leur réponse dans la licence, sauf à risquer une action en contrefaçon (sur ce point, nous renvoyons le lecteur intéressé au § 4). Par ailleurs, une utilisation courante, y compris partagée par nombre d'utilisateurs, ne légalise en rien une pratique interdite et le titulaire des droits pourra y mettre fin quand il le souhaitera (ou agir pour le respect de ses droits).

D'autre part, les outils collaboratifs ont pour nature et fonction d'inciter à collaborer, et donc à partager. Or, ce partage ne peut se faire de façon licite que si l'entreprise détient la propriété intellectuelle **des contenus créés ou mis en commun,** surtout dans l'hypothèse où celle-ci va réutiliser l'ensemble produit à partir de ces éléments partagés pour commercialiser un produit ou un logiciel. L'agrégation au sein du produit d'un élément dont l'exploitation par l'entreprise serait illicite va contaminer l'ensemble du produit, c'est donc un risque qu'il convient d'identifier et de maîtriser dès l'origine. D'où l'importance du rappel préalable aux participants du respect des règles applicables dans l'entreprise.

Rappelons ici une évidence : si l'entreprise décide de faire participer des représentants d'une société prestataire de services (ou un consultant) à son groupe de travail, ces problématiques de propriété intellectuelle devront être tranchées dès l'origine.

Sauf accord particulier en ce sens (et dont les conséquences auront été parfaitement pesées), la propriété des contenus mis en commun par le prestataire de services devront avoir été cédés ou leur droit utilisation concédé à l'entreprise. Par ailleurs, le prestataire devra lui-même respecter les conditions d'utilisation du logiciel ou de la plate-forme tierce de travail collaboratif. De la sorte, la licence négociée par l'entreprise n'inclura pas forcément le droit à ses prestataires de se connecter licitement et / ou sans coût.

Rejoignant la question de la licence d'utilisation, la propriété des contenus créés à l'aide de la plate-forme tierce est également centrale. Certaines d'entre elles prévoient en effet dans leurs licences d'utilisation que tout le contenu produit sur leurs systèmes leur appartient *de facto*, ce qui peut être une vraie source de contentieux pour l'entreprise désirant exploiter le fruit de son travail… réalisé sur cette plate-forme ! Mais, il ne faut pas omettre de traiter la

question de la propriété intellectuelle en indivision des contenus créés par les collaborateurs de plusieurs organisations.

ENCADREMENT JURIDIQUE DE L'USAGE

De plus, les règles internes (charte) n'ayant pas vocation à s'arrêter aux outils collaboratifs, il convient, si nécessaire, de modifier la charte et les procédures existantes afin de prendre en compte l'utilisation de ces outils au sein de l'entreprise. Si l'usage privé de la messagerie interne est tolérée en raison de la discrimination entre messages professionnels et privés que celle-ci permet (entêtes des messages), qu'en est-il des outils de messagerie instantanée ? La charte se doit donc d'être la plus complète possible en envisageant et en résolvant par anticipation ces sources de contentieux.

Mais dans certaines hypothèses, la charte ne peut suffire et l'irruption des réseaux sociaux internes, propres à un service, une direction ou une entreprise, explique la mise en place de documents contractuels (conditions d'utilisation, charte) que l'utilisateur doit connaître avant de participer et qui lui rappelle à la fois les règles internes mais également les règles de bon sens ou de savoir vivre et collaborer sans porter préjudice à son entreprise.

Enfin, le fait de faciliter le partage ne concerne pas forcément que les contenus (documents, logiciels, etc.) mais également et surtout l'information brute. Le travail collaboratif, en permettant l'échange, permet aussi de multiplier les occasions d'échanger des informations, parfois confidentielles. Si l'innovation ne peut naître que dans l'échange, il appartient néanmoins à la DSI de fournir ou préconiser des solutions qui permettent le respect de **la confidentialité** applicable aux informations et donc la conservation de la valeur de celles-ci.

La mise en place de solutions techniques internes mais également la formation des personnels permettraient ainsi d'éviter des hypothèses qui ont pu se rencontrer où les « digital natives » d'une même entreprise, se retrouvant sur un « tchat », un réseau social voire un jeu MMORPG, continuent ou anticipent une réunion de travail et n'en viennent à échanger des informations confidentielles majeures pour l'avenir de la société dans un endroit considéré à tort comme « privé » et « sécurisé ».

Dans la mesure où ils permettent une performance individuelle mais également collective, un partage et un accès à l'information, une capitalisation des connaissances, une diffusion de l'information et, enfin, des économies financières, les outils de travail collaboratif tendent donc à révolutionner les relations de travail dans l'entreprise. Reste que la DSI doit veiller à ce que les moyens techniques adaptés permettent une organisation transversale autour d'outils techniquement et juridiquement maîtrisés.

Finalement, il sera recommandé d'encadrer les relations entre les différentes entités utilisant des outils collaboratifs en prenant en compte les droits et les obligations des utilisateurs, la gestion des droits de propriété intellectuelle (qui a le droit d'utiliser quoi et

qui est propriétaire de quoi ?) et des droit sur les informations échangées, les conditions d'accès et la confidentialité.

Constat :

Si les problématiques sont similaires, d'importantes distinctions sont à opérer selon que l'on considère les comportements sur les réseaux sociaux externes (Facebook, Twitter) et les réseaux sociaux internes, étant entendu que les réflexions juridiques sur les réseaux sociaux internes se sont développés à partir des réflexes existants en matière d'intranet plus classique et des fonctionnalités qui été permises par ce type d'outil.

Recommandations :

- **Mise en place d'une charte d'utilisation pour les réseaux sociaux externes concernant :**
  - **Présence professionnelle sur les réseaux**
  - **Principe de loyauté inhérente au contrat de travail dans le cadre de leur utilisation (pas de diffamations…)**
  - **Qualification des abus et des sanctions attachées**
  - **Propriété des contacts du réseau social d'un salarié d'une entreprise (le problème se posant en cas de départ de salarié, dans le cas de Twitter par exemple)**
  - **Preuve licite des comportements abusifs, etc.**
- **Mise en place de Conditions Générales d'Utilisation pour les réseaux internes (documents qui n'ont pas à être soumis aux différentes formalités normalement requises pour les Chartes mais qui n'en ont pas moins une valeur juridique servant à réguler les abus) :**
  - **Propriété intellectuelle des contenus échangés,**
  - **Droit et régulation sociale applicables à un réseau social interne international accueillant des salariés de nationalités différentes,**
  - **Hébergement technique et traces de connexion,**
  - **Contrôle de l'activité du salarié (et ce que cela entraîne au plan des formalités requises par le droit du travail, etc.),**
  - **Ouverture éventuelle vers des prestataires et clients, etc.**
- **Réaliser un audit juridique préalable à tout déploiement de stratégie de communication sur les réseaux sociaux et de réseau social interne, afin de prendre en compte et de mesurer les impacts potentiels pour la sécurité juridique de l'entreprise.**

LE *CLOUD COMPUTING*

DÉFINITION DU *CLOUD COMPUTING*

Le *Cloud Computing* ou Informatique en nuage se définit au sens du Vocabulaire de l'informatique et de l'internet (J.O. du 6 juin 2010, p. 10453) comme un « mode de *traitement des données d'un client, dont l'exploitation s'effectue par l'internet, sous la forme de services fournis par un prestataire* ».

Il s'agit d'une nouvelle forme d'externalisation informatique qui repose sur l'utilisation de la mémoire ainsi que des capacités de calcul d'ordinateurs et de serveurs informatiques répartis à une plus ou moins grande échelle géographique et liés à un réseau, tel l'Internet. Il peut, en pratique, revêtir de nombreuses apparences en ce qu'il consiste « *en une interconnexion et une coopération de ressources informatiques, situées au sein d'une même entité ou dans diverses structures internes [cloud interne], externes [cloud externe], ou mixtes et dont les modes d'accès sont basés sur les protocoles et standards Internet* » (définition donnée par Syntec). Les « Cloud privés » détenus et gérés de manière privée et dont l'accès peut être limité à une seule entreprise ou à une partie de celle-ci, sont donc plus sûrs en termes de sécurité et de confidentialité, les données restant sous le contrôle de l'entreprise.

Le *Cloud Computing* permet de disposer, à la demande du client, de capacités de stockage et de puissance informatique sans disposer matériellement de l'infrastructure correspondante, impliquant ainsi une totale autonomie et une déconnexion entre l'infrastructure du fournisseur et celle du client. Cela permet à ce dernier d'éviter tout investissement préalable (Infrastructure, Plateforme ou Software as a Service - IaaS, PaaS ou SaaS). Il permet également l'adaptation des ressources, à la demande de l'entreprise. Les utilisateurs peuvent ainsi accéder de manière évolutive à de nombreux services en ligne, en fonction de leurs besoins.

De ce fait, l'accès aux données et aux applications peut se faire à partir de n'importe quel périphérique connecté. Les utilisateurs ne sont propriétaires que des données qui y sont hébergées et non des applications ou de l'architecture qui permet leur utilisation ou leur hébergement. Ils peuvent cependant accéder de manière évolutive à de nombreux services en ligne (stockage de données, traitement de texte, applications de sécurité, etc.) sans avoir à gérer l'infrastructure informatique, ce qui induit bien évidemment des économies budgétaires conséquentes.

De même que **la virtualisation des serveurs** (qui est souvent une technologie mise en œuvre à cette occasion), le *Cloud Computing* est un projet qui conduit l'entreprise à s'interroger sur l'architecture de son système d'information, sur sa capacité à répondre de manière la plus logique et la plus efficace possible à ses objectifs stratégiques. En outre, bien que le *Cloud*

Computing présente de nombreux avantages (tels que la possibilité d'étendre le système d'information d'une entreprise à sa simple demande, le fait de bénéficier d'une capacité de traitement de l'information, de profiter d'un service à moindre coût fondé sur la consommation ou encore de disposer d'une rapidité et d'une simplicité de mise en œuvre du service), l'entreprise doit prendre en compte un certain nombre de contraintes juridiques.

PROBLÉMATIQUES JURIDIQUES

En réalité, les problématiques juridiques ne sont guères différentes de celles abordées au sujet de l'externalisation (sur ce point, nous renvoyons le lecteur intéressé au §0. Guère différentes certes mais exacerbées par l'essence du concept : ce qui est problématique pour l'entreprise n'est pas la perte de l'infrastructure qu'elle détenait antérieurement mais le fait que, le cas échéant, elle risque de perdre le contrôle même des données dont elle doit assurer la sécurité et la confidentialité (sur ce point, nous renvoyons le lecteur intéressé au § **Erreur ! Source du renvoi introuvable.**. En effet, l'utilisation même du terme « Nuage » pour désigner ce nouveau concept n'est pas innocent et l'on comprend que si les données ne seront plus en « dur », présentes dans un endroit particulier, elles seront accessibles de partout… sans que l'on ait, dans tous les cas, la visibilité sur l'endroit exact où elles se trouvent. Au vu du caractère planétaire, disparate et « opaque » du Nuage, il est donc à noter ici que les parties devraient pouvoir identifier tous les serveurs utilisés pour héberger les données du client ou au minimum le(s) pays dans le(s)quel(s) ils sont établis et le type de traitement réalisé (sur quel serveur est la donnée ? qui peut y accéder ? Selon quels droits ?).

Or cette visibilité et cette connaissance apparaissent cruciales, tant au plan juridique qu'au plan financier via les assurances que la société doit souscrire. **En effet, même si ce point est rarement abordé, rappelons que les assurances qui ont été souscrites par l'entreprise pour la prémunir contre les risques (de perte de données, etc.) dépendent directement de l'audit, y compris technique, des infrastructures que l'assureur a prises en compte. Lui enlever cette connaissance et cette visibilité pourrait donc conduire à une remise en cause des assurances souscrites ou à une revalorisation de leur coût.**

Sur le plan juridique, le « Cloud » privé ne soulève pas de difficultés supplémentaires à celles d'un contrat d'externalisation, à partir du moment où le pays dans lequel il est implanté est le même que le pays dans lequel les données étaient antérieurement traitées.

Par ailleurs, les « Cloud » s'étendant sur plusieurs pays, voire en-dehors du cadre et du contrôle strict de l'entreprise, soulèvent notamment des difficultés vis-à-vis de la réglementation applicable aux flux transfrontières de données à caractère personnel hors de l'Union européenne. Si le « Cloud » (et ses solutions de sauvegarde) reste conforme au droit européen, il n'y aura pas de difficultés. Mais en revanche, s'il s'étend vers des pays à bas

coût ou vers les Etats-Unis par exemple[5], même si un seul des serveurs appartenant au Cloud relève de ces pays, et que les données concernées sont en tout ou partie des données à caractère personnel, alors la réglementation s'applique. Or, elle impose une autorisation de la CNIL pour procéder au transfert et surtout un encadrement contractuel très strict s'imposant au prestataire proposant le « Cloud » ainsi qu'à tous ses éventuels sous-traitants et prévoyant des exigences en matière de sécurité et d'audit des infrastructures.

Plus encore que dans les cas « classiques » d'externalisation, l'encadrement contractuel doit être très détaillé et le choix du prestataire envisagé doit être opéré en fonction des assurances et garanties contractuelles qu'il peut apporter sur ces problématiques. La quasi-totalité des risques pèse sur le responsable des traitements. A ce titre, il est dans l'intérêt de l'entreprise de veiller à ce que les agissements du sous-traitant n'engagent pas la responsabilité du responsable des traitements qui pourrait ensuite se retourner contre l'entreprise.

En effet, l'accès aux données étant réalisé au travers de multiples serveurs distants, il existe des risques au regard de la sécurisation des données, risques qui augmentent considérablement avec la mutualisation des serveurs et leur délocalisation. Pour y pallier, il devient donc nécessaire de mettre en place au minimum des **connexions sécurisées et l'authentification des utilisateurs pour accéder aux services souhaités**. En outre, la **traçabilité** de chaque donnée du client et de chaque opération effectuée sur celle-ci constitue une partie essentielle de la sécurité tant technique que juridique.

De façon synthétique, les lieux d'implantation des serveurs, le niveau de sécurité proposé, la pertinence et l'exhaustivité des garanties contractuelles apportées par le prestataire de Cloud doivent être un critère de choix au moins aussi important que le coût proposé pour l'accomplissement de la prestation, compte tenu des risques encourus en cas de traitement de données à caractère personnel.

Reste que si la DSI, la Direction juridique ou encore la Direction des achats sont en général conscientes de ces risques et des nécessaires garanties à obtenir, tel n'est peut-être pas tout à fait le cas dans les services opérationnels. Or, on constate en pratique que, de plus en plus, les décisions de recourir au *Cloud Computing* émanent des métiers eux-mêmes, sans passer par les intermédiaires internes qui pourraient les guider au mieux dans ce choix. Il appartient sans doute aux directions support de l'entreprise de faire œuvre de pédagogie afin de

[5] Nous ne développerons pas ici les cas complexes des Binding corporate rules, des clauses-types européennes ou du Safe Harbor, accord qui permet un flux à destination des Etats-Unis vers des sociétés adhérant à cet accord mais sous réserve et dans le cadre précis de l'engagement qu'ils ont pris. V. Par exemple sur ces questions dans le domaine bancaire, mais les règles s'appliquent aux autres secteurs d'activité, E. Caprioli, *Les flux transfrontières des données à caractère personnel en matière bancaire*, R.D.B.F. Janvier-février 2010, p.72 à 83.

s'assurer que l'utilisation de ces nouveaux concepts puisse se faire dans le respect du droit et de la sécurité informatique et contractuelle de l'entreprise.

Constat :

Il existe un certain flou autour des contrats de *Cloud computing* ; certains prestataires de services ne garantissant ni le lieu d'hébergement, ni la réversibilité. La question du prestataire en Union Européenne qui sous-traite hors de l'Union Européenne n'est pas traitée par le droit. En revanche, le cas direct du prestataire pris hors de l'Union Européenne est traité. Il est souvent impossible de savoir où sont les données sauf à passer par une solution Cloud français ou européen.

Des contrôles de la CNIL peuvent avoir lieu et l'entreprise doit être en mesure de répondre aux questions, notamment concernant la localisation des données. En effet, l'entreprise ne peut pas transférer sa responsabilité pénale à un fournisseur. Il faut donc être intransigeant dans le choix de la solution, car la déclaration est à la charge de l'entreprise et non du prestataire. Ainsi, il sera important de prévoir les différentes formalités déclaratives pesant sur le responsable de traitement.

Sur le plan comptable par exemple, les données ne doivent pas se situer à plus de 600 km de leur centre de traitement.

Recommandations

- **Déterminer quel type de Cloud (privé ou public) sera requis, en fonction du périmètre des données à externaliser, des applications, de leur caractère sensible…**
  - **Prévoir le recours à une solution de Cloud privé (interne ou privatif). Concrètement, les applications virtualisées « privées » seront soit administrées directement par l'entreprise (qui gère seule son infrastructure), soit mutualisées (un prestataire de confiance prend en charge une partie des services externalisés). Ce modèle est censé apporter les avantages du *Cloud Computing* « public » (ex : baisse des coûts liés à la virtualisation des applications dans le cas d'une infrastructure mutualisée) sans en présenter les inconvénients : en mettant l'accent sur la sécurité des données, sur le respect de la gouvernance d'entreprise et sur la fiabilité des services fournis. L'administration fiscale peut ainsi accéder facilement aux données comptables ;**
- **Disposer de clauses avec le prestataire de Cloud concernant les éléments relatifs au contrôle fiscal du système d'information (notamment les questions d'accessibilité au Système d'information).**
- **Ne pas prendre un prestataire qui ne sait pas dire où sont situées les données.**
- **Ajouter une clause de droit applicable permettant d'éviter d'être soumis à des corps de règles extracommunautaires (cette mesure relève de la stricte sécurité**

juridique)

- **Une clause relative à la réfaction des tarifs pourra être intégrée en cas de non atteinte des objectifs.**
- **Déterminer les conditions de la réversibilité ou de la restitution des données. Techniquement, la réversibilité comprend notamment le système avec son architecture technique, là où la restitution concerne seulement les données, dans un format récupérable.**

LA CONTINUITÉ D'ACTIVITÉ

Dans la mesure où une entreprise doit assurer la continuité de son activité pour satisfaire les besoins de ses clients (s'acquitter de ses commandes, leur répondre le plus rapidement possible après le sinistre, …), sa préoccupation, initialement axée sur la sécurité informatique est désormais située sur la continuité d'activité, qui devient une priorité pour le directeur des systèmes d'information (ou dans certaines activités, comme les activités financières, la direction de la conformité).

LES ENJEUX

Les entreprises ne sont à l'abri d'aucun risque technologique, environnemental, sanitaire. En effet, catastrophes météorologiques, coupures de courant de grande ampleur, incendies, inondations, ou encore épidémies sont autant de risques imposant d'élaborer un plan destiné à assurer la reprise et la continuité de l'activité. Face à un événement imprévu, c'est la capacité à réagir vite et efficacement qui permet à l'entreprise de reprendre rapidement son activité normale et respecter les contraintes réglementaires qui pèsent sur elle. Pour réagir à un sinistre en vue de diminuer ses impacts négatifs sur l'activité de l'entreprise, il incombe donc au DSI de prévoir, d'investir et de mettre en place un plan de continuité d'activité (PCA), défini par le Comité de la Réglementation Bancaire et Financière comme un ensemble de mesures visant à assurer, selon divers scénarios de crise, le maintien, le cas échéant de façon temporaire selon un mode dégradé, des prestations de services essentielles de l'entreprise puis la reprise planifiée des activités.

ELABORATION DU PCA

Ce type de plan est, en effet, très fréquent dans le domaine bancaire, mais, étant donné qu'il est inutile et voué à l'échec de prévoir un plan de continuité d'activité qui, à l'heure actuelle, ne s'adresserait qu'à la seule société visée par la réglementation, les régulateurs ont indirectement imposé que les prestataires leur fournissant des services essentiels pour leur activité soient également pourvus de tels plans. Cette « obligation indirecte », qui a pris la forme d'une obligation réglementaire (dite « clause 97-02 » pour les établissements financiers de prévoir un engagement contractuel de leur fournisseurs de services essentiels de prévoir un tel PCA pour leurs prestations), a conduit à décupler le nombre d'entreprises qui en sont dorénavant pourvues.

Et, effectivement, le PCA constitue un excellent moyen de se prémunir des risques encourus par une entreprise et de garantir la pérennité des activités de l'entreprise. En outre, pour les organismes qui accompagnent ou soutiennent financièrement des PME, le PCA constitue également une assurance de continuité d'activité, lesdits organismes étant certains que l'entreprise peut désormais faire face à un quelconque sinistre.

Cependant, l'élaboration d'un PCA doit, pour être efficient, se faire de façon méthodique et rigoureuse. Tout d'abord, la nomination d'un chef de projet indépendant de la direction des systèmes d'information, chargé de réaliser des préconisations organisationnelles et technologiques, s'avère idéale. Par ailleurs, en amont de la mise en place d'un PCA, un audit de vulnérabilité des activités critiques de l'entreprise doit être établi. A ce titre, le responsable PCA doit se poser les questions adéquates, à savoir qu'est-ce qu'il faut protéger (les données ? les collaborateurs ? le système d'information ? la production ?), quelle est la perte maximale de données tolérable, quel est le délai maximum d'interruption…, le but étant de déterminer les éléments et les activités sans lesquels elle ne peut poursuivre sa ou ses missions principales.

Suite à cet audit, un document de synthèse précisant le niveau de criticité des éléments (le niveau d'exigence) doit être établi puis suivi par un cahier des charges qui, pour chaque activité, examine les éléments nécessaires au plan de reprise, en termes d'infrastructure logicielle et matérielle (nombre de serveurs, d'accès réseaux…), d'applications (outils métier…) mais aussi de ressources humaines (effectif à mobiliser au moment du sinistre…). Des niveaux de tolérance sont ensuite déterminés, en termes de temps de reprise pour chaque application et en termes de perte de données. Le PCA doit refléter correctement la prise en compte des risques.

Par ailleurs, le dispositif mis en place doit être capable d'évoluer et de s'adapter aux changements de l'entreprise (en cas de croissance externe par exemple) afin d'éviter de devenir inopérant, d'où l'intérêt de prévoir des mises à jour régulières du PCA en fonction des évolutions du système d'information mais aussi de l'ensemble de l'organisation et des procédures internes de l'entreprise. Le PCA doit également être capable de prendre en compte l'évolution des risques. D'autre part, il est possible de faire appel à un prestataire externe pour mettre en place un PCA. Cependant, pour réussir, même avec un prestataire extérieur, le PCA demeure une décision de l'entreprise en général, de ce fait les processus à mettre en place doivent avoir été acceptés au niveau de la direction générale.

En outre, dans le but de ne pas se lancer dans un PCA utopique, il est souhaitable de soumettre préalablement le PCA à une série de tests visant à cerner les désagréments techniques et humains susceptibles de survenir lors de son activation.

Un PCA efficace doit, en principe, être quasi-transparent pour les utilisateurs et garantir l'intégrité des données sans aucune perte d'information. Ainsi, il participera d'une bonne politique de gestion de risques, en faisant jouer des impacts en matière contractuelle et juridique. Le développement des PCA peut entraîner l'élaboration de nouveaux instruments contractuels, que ce soit de nouvelles clauses (dans les contrats de travail), avenants ou annexes techniques, ou encore un nouveau type de contrat de prestation informatique.

L'étude des impacts du PCA sur les salariés en termes de droit du travail est très importante pour demeurer conformité légale et réduire les risques sociaux en cas de sinistre majeur. Les aspects de droit social sont nombreux : par exemple le travail à distance, les réquisitions de personnel, etc. (pour plus de précisions, voir Eric A. Caprioli, *Grippe A : mettre en place un plan de continuité d'activité,* publié le 25 aout 2009, www.Journaldunet.com ; Eric A. Caprioli, *Aspects juridiques des PCA dans le cadre de la SSI,* www.caprioli-avocats.com ; François Coupez, *Responsabilité juridique et continuation d'activité pendant la Grippe A*, JCP 2009, éd. E, 1963 ; Numéro spécial de la TiPi du cabinet Caprioli & Associés « Pandémie grippale », disponible sur le site www.caprioli-avocats.com).

Dans la mesure où la responsabilité pour un dommage survenu lors d'une interruption d'activité repose toujours sur les dirigeants de l'entreprise, ceux-ci sont en droit de déléguer leurs pouvoirs au profit des personnes compétentes qui doivent intervenir dans le cadre du PCA.

De plus, il est fortement conseillé à l'entreprise de recourir à une police d'assurance adaptée à ce type de dommages ainsi que de mettre en place un code de déontologie et des chartes d'éthique et de communication de cri.

Constat :

La mise en place d'un contrat de PCA avec un prestataire a pour objectif de « prévoir l'imprévisible ».

Recommandations :

- **Veiller à la rédaction de certaines clauses : réversibilité, disponibilité, force majeure, responsabilité**
- **Tenir compte de l'engagement financier du prestataire : engagement de responsabilité significatif en qualifiant les fautes directes et indirectes, le préjudice en traitant le point spécifique de la force majeure**

DÉVELOPPEMENT DURABLE ET SI

Les entreprises doivent tenir compte des aspects environnementaux, d'une part pour respecter les lois et règlements en vigueur et d'autre part, pour se développer de manière durable tout en disposant une image positive sur le marché. La question du développement durable et la mise en place de SI durables sont d'une grande actualité et impactent l'évolution de la mission du DSI qui doit désormais respecter les réglementations existantes et anticiper les futures obligations environnementales. Le caractère durable du développement de nos sociétés modernes, mais aussi des activités des entreprises, est à géométrie variable : économiser l'énergie et les matières premières, recycler les déchets, émettre moins de gaz carbonique (CO2)… Les achats informatiques doivent ainsi intégrer des exigences fortes en termes de garanties environnementales. En ce domaine, le droit pose des règles.

DIRECTIVE ROHS (*RESTRICTION OF THE USE OF CERTAIN HAZARDOUS SUBSTANCES*)

Une des règlementations environnementales de l'informatique « verte » se trouve dans la directive européenne 2002/95/CE du Parlement européen et du Conseil du 27 janvier 2003, relative à la limitation de l'utilisation de certaines substances dangereuses dans les équipements électriques et électroniques (J.O.U.E. L- 37 du 13 février2003, p.19–23). Elle spécifie la teneur tolérée des composants polluants dans les produits électroniques. Cette directive réglemente ou interdit ainsi l'usage de certaines substances dangereuses telles que le mercure ou encore le cadmium. Elle est appelée à évoluer, avec en particulier des seuils de tolérance plus bas.

DIRECTIVE DEEE

Dans le contexte des systèmes d'information, un autre sujet est celui du recyclage des déchets des équipements électriques et électroniques (DEEE) (Directive 2002/96/CE du Parlement européen et du Conseil du 27 janvier 2003 relative aux déchets d'équipements électriques et électroniques (DEEE), déclaration conjointe du Parlement européen, du Conseil et de la Commission relative à l'Article 9. J.O.U.E.- L 37 du 13 février 2003, p. 24–39)

Rappelons que les DEEE, essentiellement composés de métaux ferreux et non ferreux, de matériaux inertes (verre, bois, béton), de plastiques contenant ou non des retardateurs de flamme halogénés et de composants spécifiques qu'il faut isoler (câbles, cartouches et toners d'imprimante…), constituent une source potentielle de pollution et une catégorie de déchets concentrant une quantité importante et croissante de ressources naturelles potentiellement gaspillées si elles ne sont pas recyclées. D'une grande diversité, le volume des DEEE connaît une forte croissance liée à un taux d'équipement de plus en plus élevé et à

l'obsolescence due à l'évolution très rapide des performances technologiques. Ainsi, l'informatique est très polluante en raison du caractère non biodégradable des substances toxiques contenues dans les ordinateurs et les matériels informatiques. Les nombreuses substances chimiques (plomb, mercure…) contenues dans les circuits intégrés sont, en effet, très difficiles à recycler. Par ailleurs, les systèmes informatiques sont à l'origine d'une part non négligeable de la consommation des ressources énergétiques de l'entreprise. L'entreprise par l'entremise de son DSI doit donc prendre en compte cette problématique.

La directive européenne 2002/96/CE du 27 janvier 2003 (réf. préc) avait pour objectif prioritaire la prévention des DEEE ainsi que leur collecte sélective, leur réutilisation, leur recyclage et les autres formes de valorisation de ces déchets, le but étant de réduire la quantité de déchets à éliminer.

Elle vient en complément de la directive européenne 2002/95/CE du même 27 janvier 2003, quant à elle relative à la limitation des substances dangereuses (RoHS) dans les équipements électriques et électroniques (J.O.U.E. L 37 du 13 février 2003, p. 19–23). Cette dernière directive introduit ainsi l'interdiction de l'utilisation de certaines substances dangereuses, quelles soient chimiques ou métalliques, dans les équipements électriques et électroniques.

Ces deux directives (DEEE et RoHS) ont été transposées en France par le décret n° 2005-829 du 20 juillet 2005 (J.O. 22 juillet 2005) relatif à la composition des équipements électriques et électroniques et à l'élimination des déchets issus de ces équipements. Le décret n° 2007-1467 du 12 octobre 2007 (J.O du 16 octobre 2007) a abrogé ce décret et a globalement intégré les anciennes dispositions au sein de Code de l'environnement.

Ces directives DEEE et RoHS ont été renforcées par la directive européenne EUP (European Energy using Products) 2005/32/CE du 6 juillet 2005 qui porte sur l'éco-conception des produits utilisant de l'énergie pour améliorer la performance environnementale des produits tout au long de leur cycle de vie en intégrant des considérations environnementales dès le stade de la conception. Ainsi la consommation électrique des PC, serveurs, écrans et imprimantes est définie avec des objectifs de réduction importants. En revanche, même si le champ d'application de la directive EUP est très étendu, elle ne s'applique pas aux moyens de transport.

Quant à la directive européenne ERP (European Energy related Product) 2009/125/CE (J.O.U.E du 31 octobre 2009) elle a refondu la directive EUP (réf. Préc) et concerne principalement les exigences d'éco-conception applicables aux produits liés à l'énergie. Les 11 règlements d'exécution de la directive fixent et définissent les exigences d'éco-conceptions propres à chaque catégorie de produits concernés. Cette directive a été transposée en France par le décret n°2011-764 du 28 juin 2011 (J.O du 30 juin 2011) qui fixe la procédure de surveillance du marché national des produits ayant un impact sur la consommation d'énergie.

Le décret n°2011-153 du 4 février 2011, portant diverses dispositions d'adaptation au droit communautaire en matière de gestion des véhicules hors d'usage et des déchets d'équipements électriques et électroniques, modifie les articles R 543-173 et R 543-178 du Code de l'environnement. Il introduit les notions de substances ou mélanges dangereux, met en place une obligation pour les producteurs de mettre à disposition les informations nécessaires au traitement des déchets EEE, y compris sur les composants et matériaux présents ainsi que l'emplacement des substances et mélanges dangereux.

Par ailleurs, la directive 2008/98/CE du Parlement européen et du Conseil relative aux déchets, définit et clarifie les notions de la gestion des déchets telles que celles de déchets, producteur, détenteur de déchets, prévention, réemploi, recyclage ou encore de valorisation. La directive définit une hiérarchie dans la gestion de ces déchets et introduit la possibilité de sortir du statut de déchet. L'ordonnance n°2010-1579 du 17 décembre 2010 a transposé les mesures législatives de cette directive et ses mesures réglementaires ont été transposées par le décret n° 2011-828 du 11 juillet 2011 (J.O du 12 juillet 2011), qui a modifié les articles R 543-180 à R 543-206 du Code de l'environnement et a abrogé l'article R 543-201 de ce code. Ce décret renforce notamment les obligations de traçabilité et de transparence des différents acteurs de la chaîne de gestion du déchet ainsi que l'encadrement des installations de stockage des déchets inertes.

De plus, le décret n° 2009-1139 du 22 septembre 2009, relatif à la mise sur le marché des piles et accumulateurs et à l'élimination des piles et accumulateurs usagés (J.O du 24 septembre 2009) a transposé la directive 2008/103/CE du Parlement européen et du Conseil du 19 novembre 2008 modifiant la directive 2006/66/CE relative aux piles et accumulateurs ainsi qu'aux déchets de piles et d'accumulateurs, en ce qui concerne la mise sur le marché des piles et des accumulateurs. Ce décret a modifié les articles R. 543-175, R. 543-176 et R. 543-204 du Code de l'environnement. Si la transposition de la directive RoHs par le décret du 12 octobre 2007 (réf. Préc) interdisait l'usage de certains produits chimiques et métaux dans les équipements électriques et électroniques, le décret du 22 septembre 2009 (réf. Préc) limite cette interdiction aux équipements électriques et électroniques mis sur le marché communautaire après le 1er juillet 2006. Il met également en place des mesures pour faciliter le recyclage des piles et accumulateurs.

Enfin, en ce qui concerne la question des EEE (ainsi que les déchets qui en sont issus), concernant donc directement les équipements informatiques et de communications électroniques utilisés par les DSI, la matière est principalement régie par les articles R. 543-172 à R. 543-206 du Code de l'environnement.

A ce titre, le code établit une distinction entre les DEEE ménagers et les DEEE professionnels. Concernant les DEEE professionnels, l'article R. 543-177 du Code de l'environnement dispose que « *chaque équipement électrique et électronique mis sur le marché après le 13 août 2005 doit être revêtu d'un marquage permettant d'identifier son producteur et de déterminer qu'il*

a été mis sur le marché après cette date », et l'article R. 543-195 du Code de l'environnement précise également que « *les producteurs assurent l'organisation et le financement de l'enlèvement et du traitement des DEEE professionnels mis sur le marché après le 13 août 2005, sauf s'ils en ont convenu autrement avec les utilisateurs dans le contrat de vente de l'équipement* », le cas échéant « l*e contrat de vente de l'équipement électrique et électronique professionnel doit prévoir les conditions dans lesquelles l'utilisateur assure pour tout ou partie la gestion du déchet issu de cet équipement* ». Ces producteurs peuvent pour cela adhérer à un éco-organisme agréé, mettre en place un système individuel de collecte et de traitement (à partir de 2012 les systèmes individuels professionnels devront fournir une attestation de conformité réglementaire) ou prévoir d'autres modalités avec l'utilisateur final dans le cadre de relations contractuelles. S'agissant des DEEE mis sur le marché avant le 13 août 2005, leur enlèvement et leur traitement incombent aux utilisateurs, sauf si les conventions qui les lient aux producteurs en disposent autrement (ou par voie d'avenant à négocier).

Les producteurs encourent, selon l'article R. 543-206 du Code de l'environnement, une amende prévue par les contraventions de 5ème classe (soit 1.500 euros pour une personne physique et 7.500 euros pour une personne morale, montant qui double en cas de récidive) lorsqu'ils mettent sur le marché des EEE qui ne respectent pas les interdictions et/ou limitations liées aux substances toxiques, lorsqu'ils ne contribuent pas à la collecte sélective des DEEE et, enfin, lorsqu'ils ne satisfont pas à leurs obligations d'enlèvement et de traitement des DEEE.

Ils encourent également, selon l'article R. 543-205 du Code de l'environnement, une contravention de 3ème classe (soit 450 euros pour une personne physique et 2.250 euros pour une personne morale, montant qui double en cas de récidive) quand ils mettent sur le marché des EEE qui ne respectent pas le marquage et l'information au consommateur.

Le producteur a le choix de sa solution d'enlèvement et de traitement du moment que ladite solution remplit bien les objectifs du décret et en particulier les objectifs de valorisation. Il incombe aux producteurs de proposer une solution à leurs utilisateurs finaux au moment où ceux-ci désirent se débarrasser de leurs DEEE professionnels. Cependant, il est possible pour un producteur de transférer sa responsabilité à l'utilisateur final via un contrat de vente de l'équipement. Ledit contrat devra prévoir les conditions dans lesquelles l'utilisateur final assure pour tout ou partie l'élimination du déchet.

Le producteur est tenu de déclarer au Registre National des Producteurs de l'ADEME ses mises sur le marché des EEE professionnels ainsi que des tonnages de DEEE qu'il a enlevés et traités. Il incombe également au producteur de mettre en place un outil de suivi des performances (tonnages et valorisation) de sa filière individuelle.

Avec ce régime coercitif de gestion des déchets, la nécessité de concevoir des appareils contenant moins de substances toxiques et pouvant plus facilement se recycler se fait plus prégnante. On assiste ainsi au développement des notions de « Système d'Information durable » ou d'informatique verte (ou « Green IT »).

LE SI DURABLE

Dans le but de diminuer l'impact négatif des activités d'une entreprise sur l'environnement, une des approches du Green IT consiste à recourir à la dématérialisation (voir supra §0 des documents et des échanges (contrats, documents, courriers) dans des conditions juridiquement valables, ce qui permettrait de supprimer les contraintes écologiques liées à la gestion et à la pollution du papier. Cette façon éco-responsable de faire du commerce, de travailler ou d'effectuer des démarches administratives se manifeste donc tant dans le recyclage des matériels TIC en fin de vie que dans l'essor d'une économie purement immatérielle. C'est aussi une manifestation des valeurs de l'entreprise citoyenne.

D'autres moyens, susceptibles pour les entreprises de diminuer l'impact négatif de leur activité sur l'environnement, sont envisageables et très variables. En effet, il est possible de mentionner notamment la mobilité et le travail à distance qui permettent de consommer moins d'énergie et de carburants (télétravail, vidéoconférences, espaces collaboratifs) ou encore la réduction papier (échanges et archivage électronique, charte d'utilisation de TIC et bonnes pratiques en matière d'impression des documents), ces nouveaux moyens devant simplement être encadrées par l'entreprise (charte et autres documents juridiques).

OBLIGATIONS DES SOCIÉTÉS COTÉES ET GRENELLE II DE L'ENVIRONNEMENT

Par ailleurs, l'article L. 225-102-1 du Code de commerce prévoit que les sociétés cotées sur un marché réglementé ont l'obligation de préciser dans leur rapport annuel comment elles prennent en compte les conséquences sociales et environnementales de leurs activités ainsi que les engagements sociétaux en faveur du développement durable (obligation de reporting environnemental), ces informations étant vérifiées par un organisme tiers indépendant. Ces obligations s'inscrivent dans le cadre de la responsabilité sociale de l'entreprise (RSE). Le comportement responsable des entreprises est essentiel pour établir la confiance envers l'économie de marché, l'ouverture commerciale et la mondialisation. Cette obligation de reporting environnemental est désormais étendue, en vertu de la loi n° 2010-788 du 12 juillet 2010 portant engagement national pour l'environnement (JO du 13 juillet 2010), aux sociétés dont les titres sont admis aux négociations sur un marché réglementé ainsi qu'aux sociétés dont le total de bilan ou le chiffre d'affaires et le nombre de salariés excèdent un certain seuil. Un seuil de 500 salariés est fixé par le décret n°2012-557 du 24 avril 2012 (relatif aux obligations de transparence des entreprises en matière sociale et environnementale) à l'article R. 225-104 du Code du commerce, portant à environ 2.500 le nombre d'entreprises concernées. Aux termes cette loi, la mission de vérification de la

qualité du contenu des rapports incombe à un organisme tiers indépendant. Ainsi, la loi Grenelle II renforce considérablement la responsabilité des entreprises vis-à-vis de leurs obligations en matière environnementale et développe l'information des consommateurs/citoyens à travers notamment la rénovation des enquêtes publiques.

Le DSI doit donc prendre en compte ces nouvelles exigences écologiques dans le cadre de la gouvernance des systèmes d'information et les transformer en opportunité commerciale et d'image.

Constat :

Les entreprises prévoient désormais des annexes contractuelles concernant le respect de certaines exigences de développement durable (Charte développement durable) que ses partenaires doivent remplir.

Recommandation :

- **Prévoir la gestion des déchets, le recyclage et les économies d'énergie, etc. dans la charte de développement durable**

CONCLUSION

Le CIGREF – assisté par le Cabinet d'avocats Caprioli & Associés – a exposé, dans le cadre de cette publication, différentes thématiques auxquelles chaque entreprise peut être confrontée. Les recommandations sont issues du Groupe de travail et renvoient aux pratiques que les membres du CIGREF ont mis en place face à ces thématiques et aux problématiques sous-jacentes.

On se rend compte que les différents chapitres étudiés dans le cadre du présent rapport démontrent à quel point le numérique constitue l'épine dorsale de l'entreprise (systèmes d'information principalement mais aussi smartphones, outils informatiques mis à disposition, logiciels, base données). Ainsi, une bonne gouvernance du numérique au sein de l'entreprise assure et consolide sa structure et son développement. Différentes conséquences émergent des recommandations :

- Les contrats avec les prestataires, les licences logicielles, les chartes propres aux outils informatiques ou aux réseaux sociaux, les Plans de continuité d'activité, les chartes de développement durable, ne doivent pas être perçus comme l'apanage des seuls juristes mais au contraire des documents où les différentes directions de l'entreprise (et au premier rang la DSI) doivent être parties prenantes. Il s'agit de faire en sorte que le numérique ne soit pas perçu comme issu d'une réalité opaque mais que son recours soit dument documenté : **l'utilisation du numérique doit s'effectuer sur des bases claires et sécurisées et ne doit pas s'improviser sans au préalable avoir procédé à une analyse technique, organisationnelle et juridique** ;
- L'information constitue une source majeure **du patrimoine de l'entreprise** et son traitement nécessite protection, maîtrise et traçabilité (de sa création ou de son acquisition à la fin de son archivage ou au recyclage des supports qui la contenaient). Il est donc essentiel d'intégrer une gouvernance globale de l'information notamment en ce qui concerne son accès.

Toutefois, d'autres aspects du numérique dans l'entreprise n'ont pas été traités car les technologies en question n'ont pas encore atteint leur maturité, et leur analyse juridique est encore en chantier. C'est le cas notamment des nanotechnologies dont le recours dans certaines entreprises est de plus en plus fréquent ou de l'Internet des objets.

A propos du Cabinet Caprioli & Associés

La société d'avocats Caprioli & Associés se compose d'une dizaine d'avocats et de juristes spécialisés, basés à Nice et à Paris. La plupart des membres de l'équipe enseigne en 3ème cycle d'Universités (Paris II, Nice-Sophia Antipolis) et en grandes écoles (Ecole de formation du Barreau de Paris, ENST).

Plus d'informations : www.caprioli-avocats.com

CIGREF

21 avenue de Messine
75008 PARIS
Tel. : +33 1 56 59 70 00
Fax : +33 1 56 59 70 01

cigref@cigref.fr

www.cigref.fr