Cahier introductif

Déontologie des usages des Systèmes d'information

-

Principes fondamentaux

CERCLE ETHIQUE DES AFFAIRES

CIGREF

Editorial

Les technologies de l'information et de la communication sont des outils de vie, elles permettent la connexion des individus dans et hors de l'entreprise. Elles participent à la construction du lien social et sont devenues de ce fait incontournables.

Cependant, l'usage de ces outils ne relève plus de la seule responsabilité des utilisateurs lorsqu'ils sont dans l'entreprise. En effet, leurs dirigeants peuvent voir leur responsabilité civile et/ou pénale engagée en cas d'usages juridiquement non-conformes de leurs Systèmes d'information par leurs collaborateurs.

De ce fait, le risque que le DSI voit sa responsabilité civile et/ou pénale engagée du fait d'usages juridiquement non-conformes par les utilisateurs existe. A cela vient s'ajouter l'environnement juridique complexe auquel l'entreprise doit, en permanence, se conformer.

Il est donc devenu nécessaire, pour l'entreprise et pour la DSI, de se prémunir contre les risques liés à des usages juridiquement non-conformes des Systèmes d'information. Pour ce faire, plusieurs solutions existent, notamment la définition de règles déontologiques acceptables par tous.

Jean-Pierre CORNIOU,
Président du CIGREF

Depuis le milieu des années 1990, l'*éthique managériale* constitue la préoccupation majeure des acteurs du système économique. Cette notion se décline aujourd'hui suivant les principes du *développement durable*, et, pour ce qui nous concerne dans cette étude, de la *déontologie des usages des Systèmes d'information.*

L'éthique, méta règlementaire par définition, apparaît comme un rempart dressé contre les dérives des techniques de l'information et de la communication.

Les *cybernéticiens*, correspondants des déontologues, et nouveaux responsables de ce secteur d'activité majeur pour l'entreprise, participeront à la sécurité du système informatique des entreprises par leur maîtrise des techniques inhérentes. L'importance de leur fonction est capitale : ils ont en main, pour beaucoup, la survie de leurs sociétés.

Le présent rapport répond pour l'essentiel aux préoccupations des intervenants. Que les participants à cette riche étude soient vivement remerciés pour leur contribution active à cette heureuse initiative. Ils en sont les premiers actionnaires.

Michel LE NET,
Président du CEA

Participants

Ce cahier introductif est issu des réflexions du groupe de travail mis en place par le Cercle d'Ethique des Affaires - Cercle Européen des Déontologues (CEA-CED) et le Club Informatique des Grandes Entreprises Françaises (CIGREF), animé par Paul-Olivier Gibert, Directeur de la Sécurité et de la Déontologie du groupe AG2R, avec la participation active des personnes et entreprises suivantes :

Yvan **Biefnot**	CEA – CED	Paul-Olivier **Gibert**	AG2R
Xavier **Brault**	SNCF	Sylvain **Lebarbier**	AG2R
Michèle **Cazauran**	SNCF	Sylvère **Léger**	AGF
Michel **Dalmas**	CARGLASS	Jean **Ragot**	GE HEALTHCARE
Jean-Michel **Dalod**	CETELEM	Bernard **Revillet**	FRANCE TELECOM
Isabelle **Daviaud**	ACCOR	Antoine **Sebaux**	AGF
Patrick **du Besset**	CEA – CED	François **Subrenat**	LVMH
Catherine **Fauvel**	FRANCE TELECOM	Marc **Ulpat**	GE HEALTHCARE

Ce cahier a été rédigé par Sophie Bouteiller, chargée d'études au CIGREF.

Synthèse

Les technologies de l'information et de la communication offrent aux acteurs de l'entreprise de nombreuses potentialités mais les exposent davantage en termes **de risques liés à des utilisations juridiquement non-conformes**. De plus, l'évolution rapide des outils informatiques et de l'environnement juridique dans ce domaine ne facilitent pas la **conformité des entreprises au droit**. Dès lors, comment l'entreprise s'adapte-t-elle à ce nouveau contexte ? Quelles solutions choisit-elle pour garantir un usage juridiquement conforme de son Système d'information ?

Afin de mieux cerner le périmètre des risques liés aux mésusages du SI et d'améliorer leur protection dans ce domaine, certaines entreprises choisissent de se doter de **règles déontologiques spécifiques au Système d'information**. Ces règles de bons usages peuvent être vues comme des **« règles du jeu »** intervenant pour combler les déficits existants entre le contrat de travail, le règlement intérieur de l'entreprise et les lois en vigueur. L'introduction de telles règles n'a pas pour but de moraliser, ni de standardiser les comportements des salariés au regard des usages du SI, mais de **donner des repères sur les conduites que l'entreprise attend des utilisateurs**.

La problématique fondamentale que pose la déontologie des usages des Systèmes d'information peut se résumer comme suit : **il s'agit de transposer en règles et contrôles internes les contraintes juridiques qui pèsent aujourd'hui sur l'utilisation des Systèmes d'information et qui peuvent amener les entreprises à être sanctionnées de ce fait.** La déontologie des usages des SI pose donc la question d'une utilisation des outils informatiques de l'entreprise conforme aux règles éthiques et juridiques définies. Il s'agit :

- D'identifier les enjeux et les risques liés aux usages juridiquement non-conformes des SI,
- De s'interroger sur la manière dont les règles existantes sont traduites en termes d'application concrète et sur les limites de leur champ d'application.

La finalité du cahier introductif est de **sensibiliser toutes les parties prenantes de l'entreprise**, des directions générales aux unités opérationnelles, **aux risques et aux enjeux liés aux utilisations juridiquement non-conformes des Systèmes d'information.**

Executive summary

Communication and information technologies present many potentialities but users are more exposed in terms of **risks linked to usage which does not comply with the laws in force**. Moreover, the rapid evolution of both data-processing tools and the legal environment in this area does not ease **companies' compliance with the law**. Consequently, how do companies adapt their organization to this new context? Which solutions should be chosen in order to ensure a legal use of information systems?

In order to have a better definition of the risks linked to uses of information systems and to improve protection in this area, some companies choose to equip themselves with a **professional code of ethics specific to the information system**. These rules of correct usage can be seen as **"rules of the game"** designed to fill the gaps between the work contract, internal policies and procedures and the law. The aim of these kinds of rules is not to moralize or standardize employees' behaviour but rather **to provide certain benchmarks regarding the behaviour that a company can expect from the users of their information systems**.

The deontology of information system usage brings up a fundamental issue which can be summarized as follows: **the transformation of the legal obligations companies have regarding information systems – which can potentially result in sanctions – into internal rules and controls.** The deontology of information system usage therefore raises the question of a use of the company's data-processing tools which conforms to ethical, moral and legal rules. The issues are:

- Identifying the stakes and risks linked to information systems usage which does not comply with the laws in force,
- Studying how existing rules of conduct are transcribed in practical terms and marking out the limits of the area of application.

The purpose of this introductory document is **to make all the company's stakeholders** – from top management to operational units – **aware of the stakes and risks linked to information system usage which does not comply with the laws in force**.

Sommaire

Editorial 3

Participants 4

Synthèse 5

Executive summary 6

Avant-propos 8

Présentation de la problématique 9

- Introduction 9
- Quelques notions 10
- Relations entre les notions : des frontières perméables dans l'entreprise 11

Enjeux 13

- Multiplicité des enjeux 13
- Axes de réflexion 15

Quelques fondamentaux 17

- TIC, communication et Système d'information 17
- Effets pervers 18
- Lutte contre les menaces et les risques de mésusages 20
- Déontologie et usages des Systèmes d'information 23

Déontologie, intelligence économique et développement durable : quels liens ? 29

- Déontologie et intelligence économique 29
- Déontologie et développement durable 31

Conclusion 32

Annexes 33

- Les conflits de normes 34
- Le secret professionnel 40
- Enquête *Déontologie des usages du SI* : présentation de l'échantillon et de l'enquête, synthèse des réponses 54

Compléments 62

Avant-propos

Les Technologies de l'Information, de la Communication et de la Connaissance (TICC) occupent une place centrale dans l'entreprise. Celle-ci ne peut plus négliger les risques liés à l'usage de ces technologies dont les problèmes de conformité ne sont plus seulement techniques, mais aussi et de plus en plus juridiques. Dès lors, quelles bonnes pratiques mettre en place pour garantir un usage éthique et juridiquement conforme du Système d'information ?

Ce cahier introductif est une première étape dans la réflexion sur la déontologie des usages des SI. Il identifie les enjeux et les risques qui y sont liés, et pose le problème à un premier niveau en suscitant la prise de conscience des entreprises et des utilisateurs des Systèmes d'information. Il a pour objectif de sensibiliser les lecteurs à la problématique. Il n'a pas la prétention d'être exhaustif, il n'est pas non plus un manuel de déontologie. Les points abordés tout au long de ces pages ne couvrent qu'une partie de ce sujet, particulièrement vaste et complexe. Le lecteur trouvera ici les éléments essentiels de la déontologie appliquée aux usages des Systèmes d'information, largement abordés sous l'angle juridique.

Ce cahier introductif se décompose en deux parties :

- Le corps du document s'attache à présenter la problématique et les enjeux qui y sont liés,
- Les annexes sont le résultat de réflexions spécifiques du groupe de travail :
  - La première traite des difficultés auxquelles peut être confrontée une entreprise à dimension internationale qui souhaite être en conformité, au niveau de son SI, avec les textes qui la régissent (lois et/ou références internes, au niveau national, européen ou international) ;
  - La deuxième s'intéresse au secret professionnel appliqué au SI de l'entreprise (qui est soumis au secret et dans quelle mesure peut-on ou doit-on l'opposer ?) ;
  - La troisième présente l'enquête menée, dans le cadre de la réflexion, auprès de 34 grandes entreprises et dont l'objectif est d'évaluer le niveau de maturité de celles-ci en matière de déontologie appliquée aux usages des Systèmes d'information.

En complément, des liens internet accessibles sur le site du CIGREF renvoient vers plusieurs exemples de chartes, appliquées dans les domaines associatif, public et privé. Elles visent à illustrer la mise en œuvre opérationnelle d'une démarche de déontologie appliquée aux Systèmes d'information et à faciliter la compréhension des enjeux et des méthodes relatives à celle-ci.

La finalité de ce « Cahier introductif » est de sensibiliser toutes les parties prenantes de l'entreprise, des Directions générales aux unités opérationnelles, aux risques et aux enjeux liés aux utilisations juridiquement non-conformes du Système d'information. Il s'adresse donc à un large public.

Présentation de la problématique

• *Introduction*

Les Systèmes d'information (SI) permettent aux acteurs de l'entreprise d'accéder aux données nécessaires à l'accomplissement de leurs activités professionnelles, alliant ainsi des objectifs de qualité, d'adaptabilité, de compétitivité, de rentabilité, d'universalité et de rapidité des échanges d'informations.

Cependant, certaines utilisations des outils informatiques mis à leur disposition par l'organisme qui les emploie, qu'il soit public ou privé, exposent bien souvent ce dernier à une multitude de risques. La rapidité des évolutions technologiques et juridiques dans ce domaine ne facilite en rien ce que le législateur exige, avec force, des entreprises : la conformité au droit[1].

Les risques évoqués ici peuvent être lus à plusieurs niveaux :

- tout organisme peut être victime de mésusages de la part des utilisateurs de son (ses) Système(s) d'information (collaborateurs ou clients), et pour lesquels il pourrait voir sa responsabilité civile et/ou pénale engagée (complicité par fourniture de moyens notamment),
- parce que les systèmes de traitements automatisés de données mis en œuvre par elles n'ont pas été suffisamment sécurisés ou parce qu'elles ont omis de procéder aux démarches administratives qui s'imposaient à elles, les entreprises peuvent, là aussi, voir leur responsabilité engagée,
- enfin, les entreprises peuvent avoir elles-mêmes une utilisation illicite de leur SI.

Il importe donc que les organismes, quelle que soit leur forme, et plus particulièrement leurs directions générales et les personnes intervenant sur la conformité juridique du SI (DSI, RSSI, juristes et déontologues), prennent en considération ces risques et les enjeux qui y sont liés.

Pour ce faire, de plus en plus de structures se dotent de règles déontologiques afin de mieux cerner le périmètre des risques liés à leur domaine d'activité, et donc de se protéger plus efficacement. La définition de règles de conduite visant à lutter contre les abus liés aux usages du Système d'information peut apparaître comme une solution permettant d'allier compétitivité, productivité et conformité juridique de l'entreprise.

[1] Voir par exemple les nombreuses lois récentes modifiant en profondeur les obligations des entreprises en la matière. On peut notamment retenir la loi pour la Confiance dans l'Economie Numérique, la loi dite « CNIL 2 », etc...

- ## Quelques notions

Introduction

Déontologie, éthique, morale : quelles différences ? Les frontières entre ces notions sont souvent confuses… Il est donc essentiel de définir les termes afin de mieux comprendre les contours de la problématique et ce qu'elle recouvre.

Définitions[2]

La morale est « *l'ensemble des règles d'action et des valeurs qui fonctionnent comme normes dans une société* ». Elle se situe donc au niveau de la société, elle est extérieure à l'entreprise. La morale présente un caractère relatif, dans la mesure où elle évolue en fonction de l'époque de référence, ainsi que selon la culture et les besoins de chaque société.

La déontologie correspond à « *l'ensemble des règles et des devoirs qui régissent une profession, la conduite de ceux qui l'exercent, les rapports entre ceux-ci et leurs clients ou le public* ». Pour le CEA, il s'agit du « *travail de l'entreprise pour se conformer à des prescriptions internes ou externes impliquant des contrôles de conformité et d'éventuelles sanctions* ». Elle correspond ainsi à cette partie de la morale qu'est l'éthique professionnelle.

L'éthique concerne « *les principes de la morale* », c'est la « *partie de la philosophie qui [en] étudie les fondements* ». Elle tend à s'imposer à chacun, individuellement, au titre de la conscience personnelle. Dans l'entreprise, elle représente l'ensemble des valeurs morales que chacun doit respecter. Pour le Cercle d'Ethique des Affaires (CEA)[3], l'éthique dans l'entreprise correspond au « *travail sur les valeurs de l'entreprise et leur traduction en principes d'action* ».

Le Système d'information est l'ensemble des ressources techniques, organisationnelles et humaines requises par le traitement des informations nécessaires à la stratégie et aux métiers de l'entreprise. Il comporte donc deux dimensions : « *celle de **l'organisation** qui se transforme, entreprend, communique et enregistre les informations, puis celle du **système informatique**, objet artificiel conçut par l'homme qui permet l'acquisition, le traitement, le stockage, la transmission et la restitution des informations au service de la gestion de l'entreprise* »[4].

L'usage, enfin, a pour sens premier « *l'action, le fait de se servir de quelque chose* ». Appliqué aux Systèmes d'information, il s'agit de l'utilisation même du Système d'information et des outils informatiques mis à la disposition des collaborateurs par l'organisme qui les emploie et par l'entreprise elle-même.

[2] Définitions du Petit Larousse, puis du Cercle d'Ethique des Affaires (2005).
[3] http://www.cercle-ethique.net/
[4] C. Rosenthal-Sabroux, professeur en Systèmes d'information (Université Paris – Dauphine)

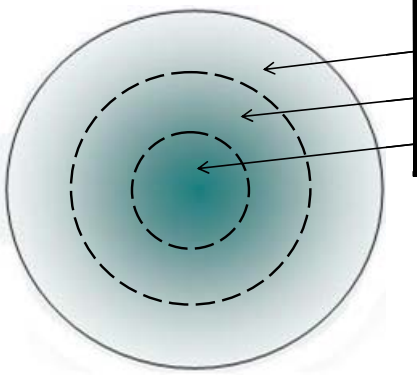
En résumé

La déontologie en entreprise a pour finalité la formulation de règles de conduite inspirées tant des normes externes que des valeurs de l'entreprise traduites en principes d'action. Elle s'appuie à la fois sur des normes impératives telles que les lois et les règlements, sur des règles considérées comme essentielles pour l'ensemble des professionnels d'un même secteur d'activité, ainsi que sur des principes internes à l'entreprise (le plus souvent repris dans des chartes ou des codes de conduite).

• *Relations entre les notions : des frontières perméables dans l'entreprise*

Les interactions entre les notions

Au vu des définitions, la détermination de frontières entre la morale, l'éthique et la déontologie est délicate. Mais tenter de les hiérarchiser peut aider à la compréhension de la problématique globale :

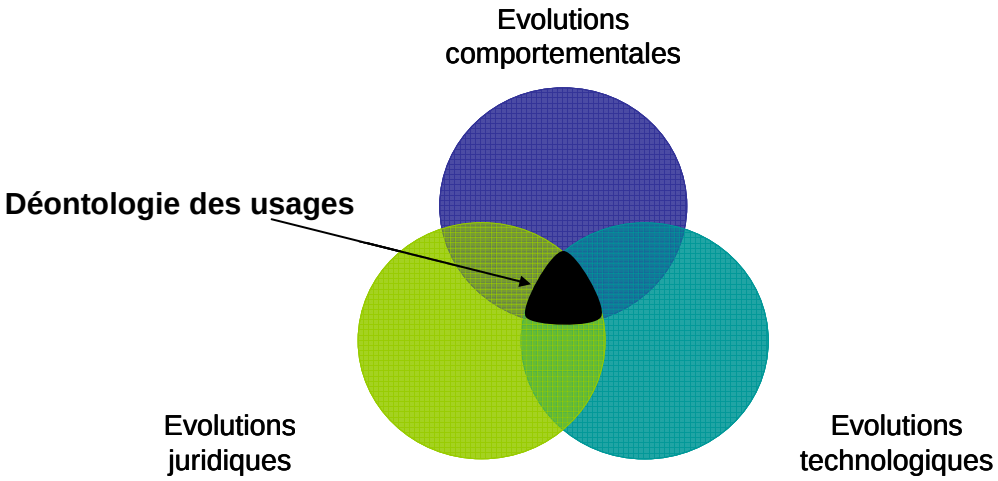


Concepts	Niveaux
Morale	Société
Déontologie	Profession
Ethique	Entreprise

Individu

Une problématique complexe

La problématique est complexe, difficile à cerner, et pour mieux comprendre à quel(s) niveau(x) elle se situe, nous pouvons la schématiser comme suit :



La question de la déontologie des usages des Systèmes d'information revient donc à s'interroger sur une utilisation des outils informatiques de l'entreprise conforme aux règles éthiques, morales et juridiques définies. Il s'agit de réfléchir d'une part, sur la manière dont les règles existantes sont traduites en termes d'application concrète et, d'autre part, sur les limites de leur champ d'application. La déontologie des usages des Systèmes d'information sert ainsi de maillon fondamental entre l'utilisation régulière des outils et le comportement des utilisateurs.

Enjeux

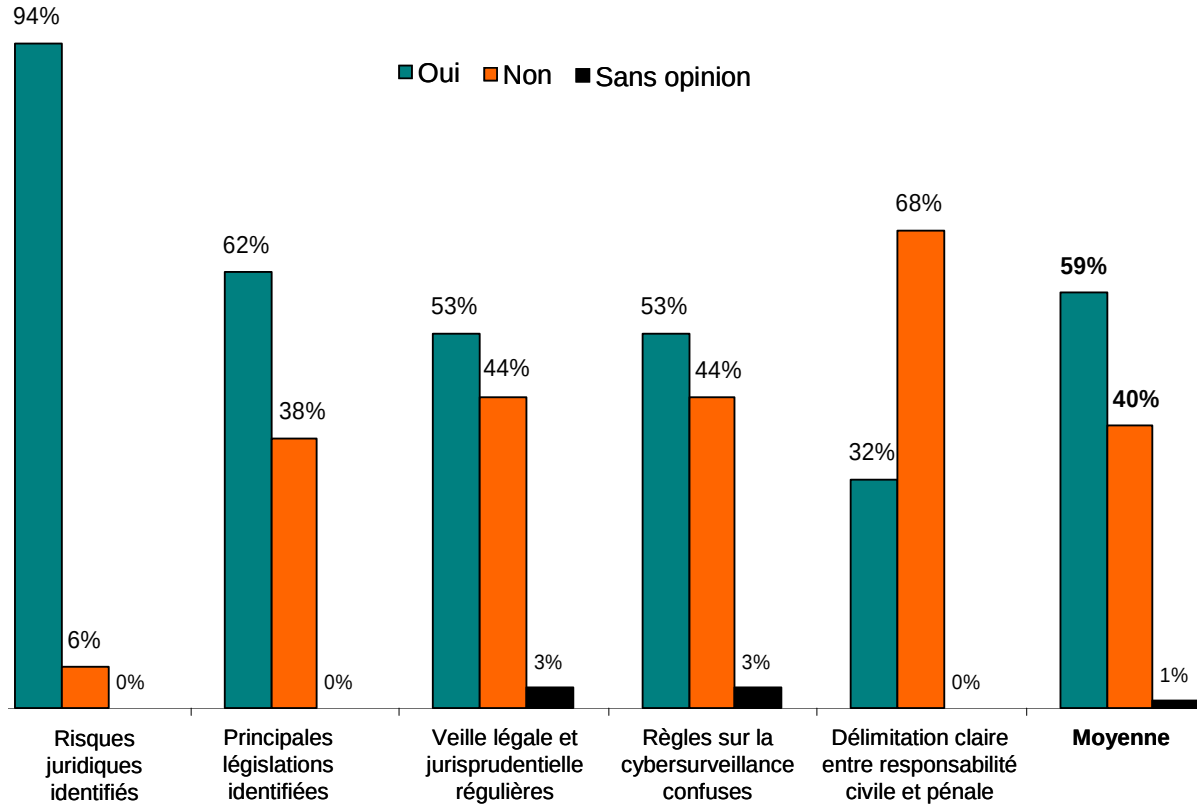
• *Multiplicité des enjeux*

Les enjeux liés aux usages juridiquement conformes des Systèmes d'information sont de tous ordres : techniques, juridiques, économiques, sociaux, voire même environnementaux. Mais ces enjeux sont encore mal perçus par les acteurs, comme le montre le graphique ci-dessous, réalisé à partir de l'enquête (annexe 3).

En effet, en moyenne, 59% seulement des organisations interrogées jugent que les enjeux liés à la conformité des usages du SI sont bien perçus par les personnes en charge de sa sécurité.

Or aujourd'hui, les innovations technologiques et l'évolution des méthodes de travail (connexion à distance, travail collaboratif, visioconférence…) fragilisent le SI et le rendent plus vulnérable. Ceci induit donc de nouveaux risques qu'il est nécessaire de connaître afin de les maîtriser et d'assurer une protection optimale et adaptée du Système d'information.

Perception des enjeux liés à la conformité juridique des usages des SI



Les enjeux pour les entreprises

L'introduction de solutions techniques toujours plus performantes au sein du SI dépend aussi beaucoup de la culture d'entreprise, laquelle peut engendrer des réflexes disparates d'un organisme à un autre. L'apparition de nouvelles techniques de travail, si elle présente des avantages, demande de la flexibilité et une adaptation aux nouvelles contraintes de travail, lesquelles peuvent parfois être contestées. L'entreprise doit donc, dans un souci d'efficience, accompagner le changement. Pour ce faire, elle doit aussi faire face à plusieurs questions essentielles :

- Comment protéger et sécuriser les informations sensibles tant en interne qu'en externe ? Il s'agit ici de répondre aux deux premiers principes de la sécurité de l'information, à savoir **la confidentialité** et **l'intégrité**.

- Jusqu'où et comment l'entreprise peut-elle contrôler les comportements de ses collaborateurs sur le lieu de travail sans porter atteinte au respect de la vie privée ou au secret des correspondances ? Il s'agit là des questions liées à la **cybersurveillance**.

- Comment gérer les habilitations et les droits d'accès pour contrôler l'usage des données et plus largement des outils (qui peut accéder à quoi, qui peut sortir quoi, qui peut insérer quoi dans le SI…) ? On touche ici aux questions de **l'identification** et de **l'authentification.**

- Comment gérer les **conflits de règles** quand, par exemple, une entreprise américaine implantée en France demande des informations sensibles en application de certaines lois fédérales et que la législation française semble y faire obstacle ?

- Comment assurer à la fois plus de transparence (conformité réglementaire, audit des SI, inspection éventuelle de la CNIL ou de l'AMF) et plus de confidentialité (données personnelles, données financières) ? Nous abordons ici la question du recours au **secret professionnel**.

- Qui est responsable de la définition du cadre déontologique de l'entreprise, de sa mise en œuvre, de sa communication, de son respect ?

- Si les rôles sont partagés (DSI, RSSI, Juriste, RH, Déontologue), comment se répartissent les responsabilités entre les différents acteurs ?

Les enjeux pour les Directions des Systèmes d'Information

Au sein des DSI, les questions précédentes nous renvoient à de nouvelles interrogations :

- Comment la DSI gère-t-elle les problèmes de conformité juridique ?

- La politique de protection des données relève-t-elle seulement de la DSI ?

- Comment la DSI gère-t-elle les problèmes relatifs aux usages juridiquement non-conformes ou à risques du SI ?

Face à ces enjeux : la déontologie

Le traitement de l'information est, dans tous les organismes, un processus extrêmement complexe qui demande à être sécurisé. L'information en elle-même représente en effet un actif essentiel à l'activité de l'entreprise dont la protection est une condition vitale.

Des menaces très diverses existent, et toutes ne sont pas forcément d'ordre logique ou physique. La continuité des activités de l'entreprise peut donc être mise en cause et éventuellement générer un grave préjudice, parfois de nature à engager la responsabilité civile et pénale des acteurs de celle-ci. Les traditionnels critères de la sécurité que sont la confidentialité, l'intégrité et la disponibilité se sont vus progressivement accompagnés d'un quatrième critère, la légalité, dont le non-respect peut à lui seul ébranler l'entreprise.

La fraude informatique, les attaques de pirates ou les incendies représentent toujours des menaces réelles au même titre que les tentatives d'espionnage industriel ou de déstabilisation. Toutefois, il est une menace de sécurité qui n'est pas suffisamment, encore aujourd'hui, prise en considération : celle que l'entreprise se crée contre elle-même en refusant ou en omettant de se conformer à un droit qui peut lui échapper.

La déontologie se propose en ce sens de donner à l'entreprise un certain nombre d'outils pour l'accompagner dans la mise en œuvre de procédures rigoureuses, destinées à l'aider à contrôler son degré de conformité aux dispositions légales. Elle rappelle les règles de bon sens qui, sans représenter une conformation au droit *stricto sensu*, ne peuvent que l'aider à se maintenir et à envisager sa pérennité.

• *Axes de réflexion*

Les questions posées appellent des réponses essentielles pour toute entreprise consciente des enjeux, lesquels sont déterminants pour garantir sa sécurité tant en termes d'engagement de responsabilité en cas d'usage juridiquement non-conforme, qu'en termes de sécurité et de protection de son SI.

C'est pourquoi, le groupe de travail a réfléchi sur deux axes définis à partir de ces interrogations, dont le contenu figure en annexe :

- **Les conflits de normes (annexe 1)**, pour mieux comprendre les difficultés auxquelles sont confrontées les entreprises en termes de conformité juridique, en interne comme en externe.

- **Le secret professionnel (annexe 2)**, pour qualifier de manière appropriée les données traitées par l'entreprise et les protéger par un statut particulier qui découle de règles déontologiques spécifiques.

Par ailleurs, l'enquête présentée en **annexe 3** a permis de dégager des étapes incontournables dans la mise en œuvre de règles déontologiques relatives aux usages des Systèmes d'information :

- **Identification des risques liés à un usage non-conforme du SI ou à un défaut de vigilance :** la déontologie offre des moyens permettant d'identifier les mésusages, dont la majorité est commune à tous les SI. Elle peut faciliter la prise de conscience des risques réels liés à ces derniers.

- **Identification des solutions mises en place dans les entreprises :** beaucoup d'organismes ont déjà pris des mesures d'ordre déontologique pour limiter les risques. L'enquête a permis d'identifier les pratiques les plus fréquemment mises en oeuvre et de constater des degrés d'efficacité variables.

- **Identification des relations entre l'éthique de l'entreprise et les usages de son SI :** l'introduction de règles déontologiques incite les utilisateurs, qui ne sont pas toujours volontaires, à changer leur comportement. La communication, la sensibilisation et la formation des collaborateurs doivent donc occuper une large place dans la mise en œuvre de la démarche.

De manière générale, la déontologie des usages des Systèmes d'information repose sur les constats suivants :

- L'outil informatique est devenu nécessaire, mais son utilisation est facteur de risques pour l'entreprise ;

- La loi évolue vers une responsabilisation systématique et accrue de l'entreprise et de ses représentants ;

- La sécurité juridique appelle un contrôle renforcé de l'usage qui est fait de ces outils ;

- Le périmètre de ce contrôle étant juridiquement encadré, il faut trouver un équilibre entre la nécessité pour l'entreprise de s'assurer du respect des règles en vigueur et la garantie, pour le personnel, du respect de ses droits fondamentaux (vie privée, secret des correspondances…).

Dans cette mesure, l'élaboration de règles déontologiques simples en matière d'usages des SI a pour objectif d'aider les acteurs à mieux cerner les actions susceptibles de représenter un risque pour l'entreprise. Mais les règles ainsi élaborées varient selon la taille et le secteur d'activité de l'entreprise. Il convient par conséquent de susciter la prise de conscience, pour définir ensuite les règles de base de la déontologie, les principes fondamentaux.

Quelques fondamentaux

• TIC, communication et SI

Traiter la problématique des usages des Systèmes d'information, c'est avant tout étudier les rapports existants entre les technologies de l'information et de la communication (TIC), les SI et la communication. C'est ensuite identifier les effets pervers et les risques juridiques qui y sont liés. Enfin, pour assurer un fonctionnement optimal, les entreprises doivent faire connaître à leurs collaborateurs les différentes utilisations possibles du Système d'information (ce qui *peut* et *ne peut pas* ou *ne doit pas* être fait). La problématique des usages du SI passe donc aussi par la communication, support indispensable à la diffusion de ces règles, à la sensibilisation et à la formation des utilisateurs.

Les TIC pour mieux communiquer

Les TIC favorisent une meilleure communication, un accès à pratiquement tout, partout, et à tout moment, ainsi qu'une amélioration de la réactivité, et participent éventuellement à la réduction des coûts. Elles transforment les habitudes professionnelles et peuvent être à l'origine de nouvelles pratiques éthiques et/ou non éthiques.

Le SI : une base de communication

Le SI touche toutes les fonctions de l'entreprise, il est présent dans toutes ses strates et est sollicité à chaque instant par les collaborateurs. Il constitue une base de communication interne ascendante et descendante (messagerie, visioconférence, intranet, GED, recherches…).

D'une part, le SI permet à l'entreprise de contrôler les utilisations qui en sont faites (identification des mésusages), mais aussi de détecter les problèmes latents (failles dans le système). Une altération du fonctionnement du système, qu'elle soit due à un mésusage ou à une faille, peut :

- entraîner une atteinte aux données (subtilisation, destruction, modification…), susceptible d'engager la responsabilité pénale de l'entreprise et de ses dirigeants ;
- générer une importante baisse de la productivité (pannes privant les collaborateurs de leur outil de travail, utilisation du SI à des fins personnelles de manière abusive, etc…).

D'autre part, le SI permet à l'entreprise d'informer les collaborateurs et de les mobiliser autour d'un projet fédérateur. Le SI permet « *la connexion des cerveaux en réseau, la mise en commun des connaissances et de l'information* »[5]. Il accélère ainsi le développement de tels projets, et peut servir de support de communication favorisant l'essor de la culture et de l'esprit d'entreprise.

Les effets de l'utilisation du SI

Pour fonctionner de manière optimale, le SI nécessite des échanges et une collaboration à tous les niveaux : l'information doit circuler de manière ascendante et descendante. Son utilisation doit permettre de sécuriser l'information, de favoriser les échanges entre collaborateurs et d'impulser la modernisation de l'entreprise.

[5] J.P. Debeuret dans *Entreprise Ethique*, cahier n°14, p.14

- ***Effets pervers***

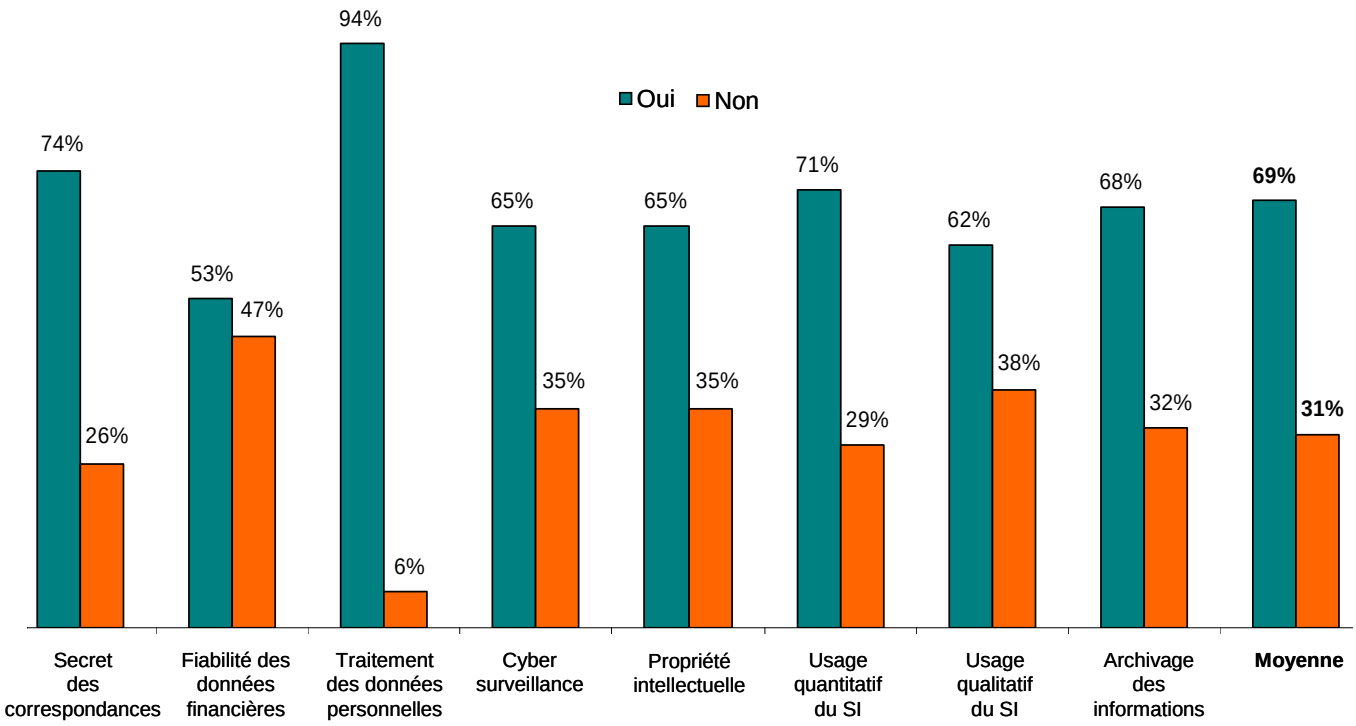
De forts enjeux de pouvoir

A travers son administration et sa gestion, le Système d'information cache de forts enjeux de pouvoir, il transforme le lien social et le rapport à l'information[6]. Ceci peut avoir d'importantes répercussions éthiques. La déontologie est alors une solution qui participe à la gestion de la dimension politique liée au SI. Elle permet de lutter contre les mésusages imputables tant aux utilisateurs qu'à l'entreprise elle-même. Elle permet aussi de protéger/sécuriser le SI en définissant une base de règles de conduite publiée, mise à jour, et accessible à l'ensemble des utilisateurs.

Des mésusages multiples aux conséquences graves pour l'entreprise

Les usages du SI dans un organisme quel qu'il soit sont multiples et le degré de préoccupation de ce dernier varie selon son secteur d'activité. Le graphique ci-après, issu des réponses à l'enquête (annexe 3), illustre les usages à risques identifiés dans la plupart des entreprises et faisant l'objet d'une certaine vigilance.

Risques d'usages juridiquement non-conformes et faisant l'objet d'une vigilance spécifique

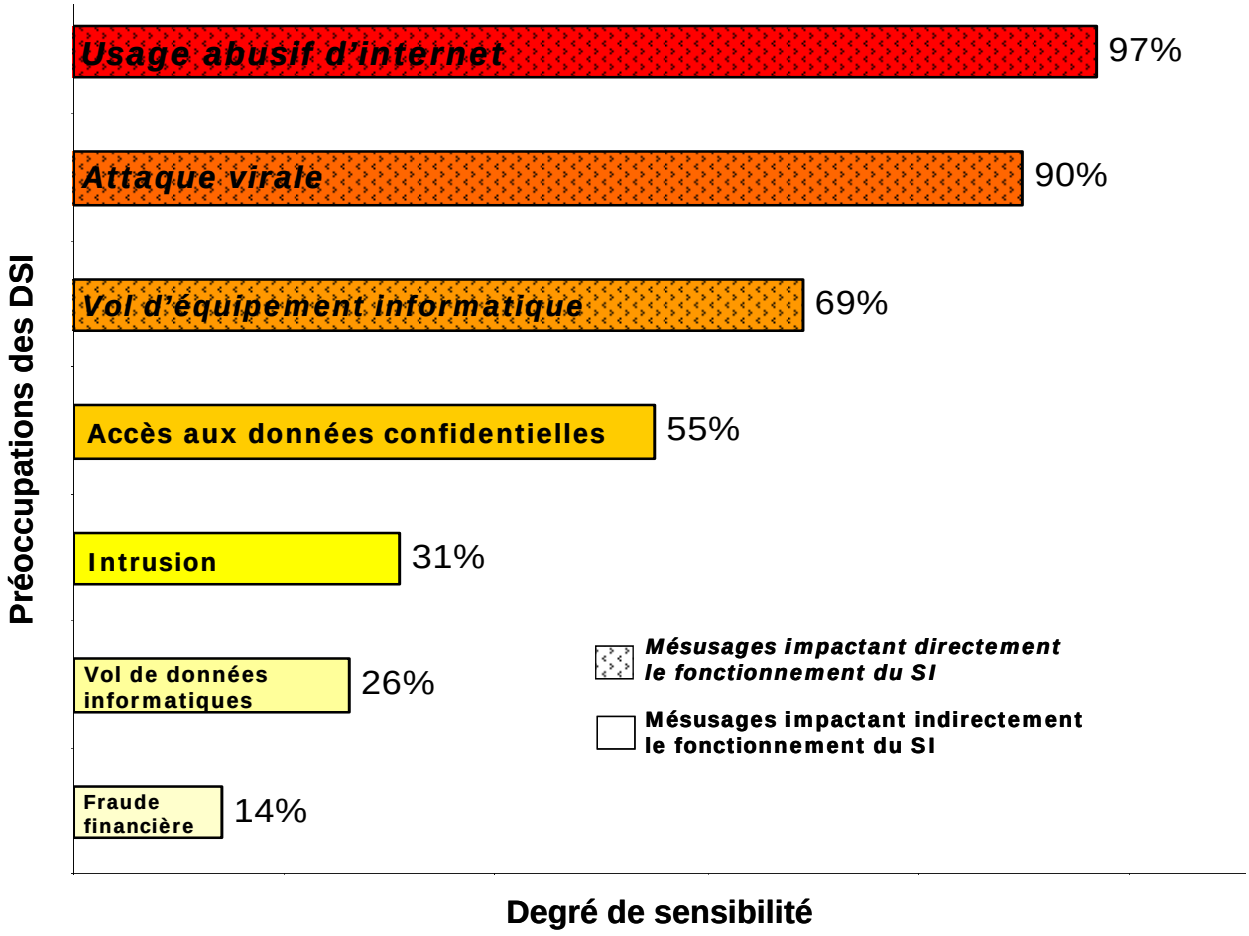


En moyenne, 69% des entreprises portent une attention particulière aux activités susceptibles de générer des risques pouvant engager la responsabilité civile et/ou pénale des dirigeants, et par ricochet celle du DSI qui se trouve de ce fait en situation de risque. Ce constat marque bien le manque de connaissance des enjeux liés aux usages juridiquement non-conformes des Systèmes d'information dans les grandes entreprises et autres organismes.

[6] Pour plus d'informations sur les enjeux de pouvoir liés au Système d'information, cf. *Les usages du Système d'information, une politique au quotidien* (La recherche au CIGREF, Cahier de recherche n°2, V. Bricoune)

De plus, si le traitement des données personnelles constitue une préoccupation commune à la quasi-totalité des organismes interrogés (94%), l'accès aux données confidentielles représente le risque le plus préoccupant parmi ceux impactant indirectement le fonctionnement du SI.

Préoccupations principales des entreprises, selon les DSI, en matière d'usages des SI par les collaborateurs[7]



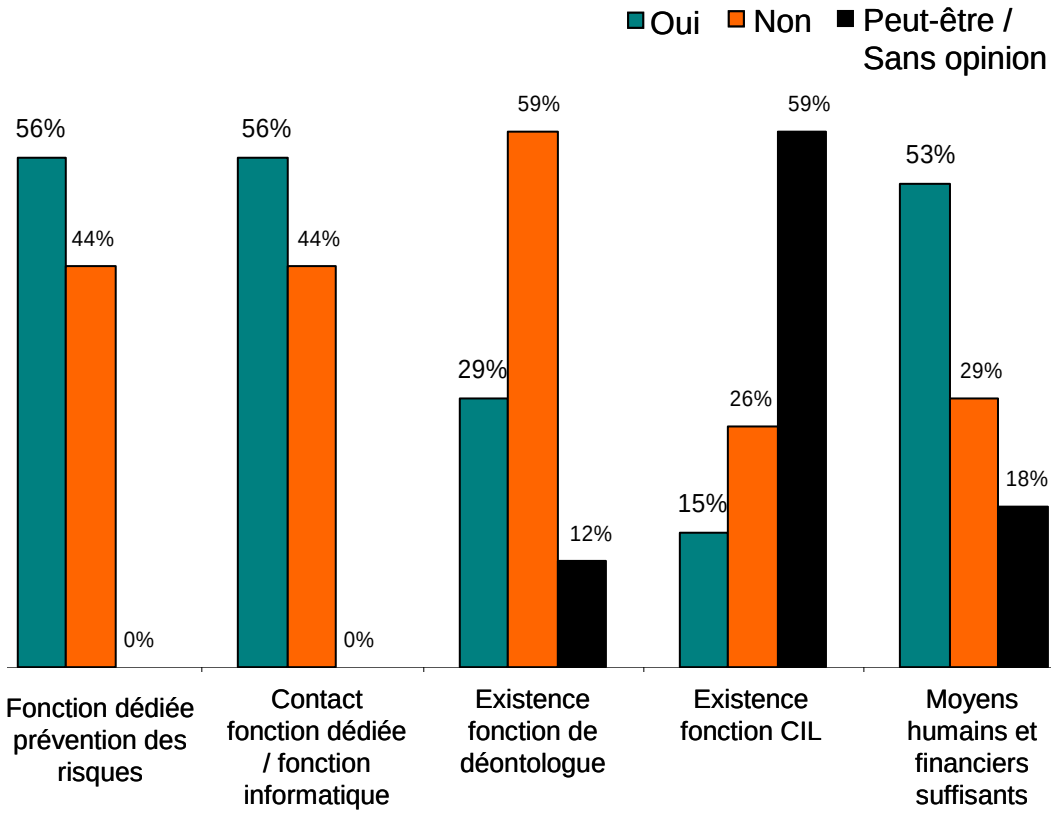
Les conséquences des mésusages ont des répercussions sur l'ensemble des fonctions du SI, c'est pourquoi la problématique de la déontologie prend une importance grandissante.

[7] Source : Médef, *Guide SSI* (mai 2005).

- ***Lutte contre les menaces et les risques de mésusages***

Les risques existent et la majorité des entreprises en sont conscientes… En effet, 56% d'entre elles ont identifié une fonction interne, en contact régulier avec la fonction informatique, dédiée à la prévention des risques de non-conformité (voir graphique ci-dessous issu des réponses à l'enquête). Et un peu moins de 30% d'entre elles ont mis en place une fonction de déontologue pour compléter le dispositif de lutte contre les mésusages.

Solutions organisationnelles retenues ou envisagées pour garantir un usage juridiquement conforme des SI



Identification des menaces « classiques » et définition de règles déontologiques

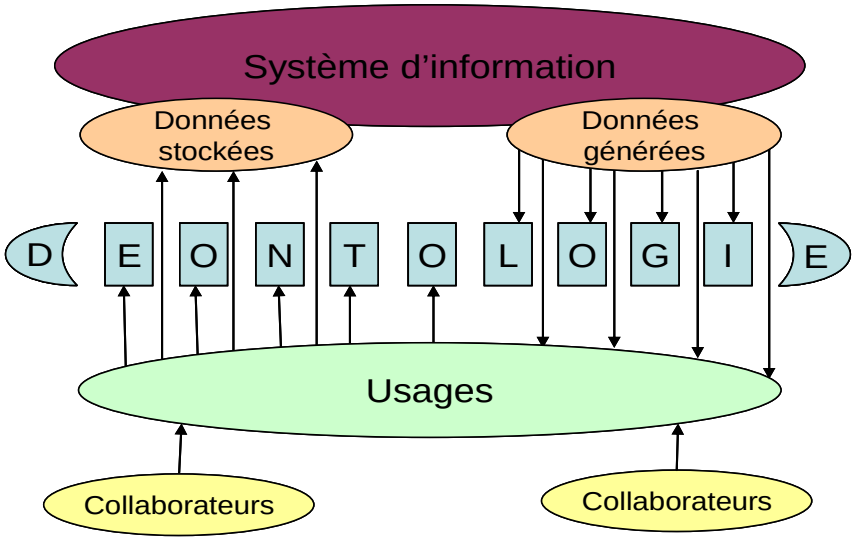
Menaces "classiques"	Dispositions applicables	Peine maximale	Quelques règles déontologiques
Atteinte aux données personnelles	**Art. 226-16 à 226-24 du Code Pénal (voir Loi Informatique et Libertés du 6 janvier 1978, modifiée par la loi du 6 août 2004)**	**Jusqu'à 5 ans de prison et 300.000 euros d'amende**	Déclarer ses traitements ou demander une autorisation et les limiter à ce qui est déclaré, collecter loyalement les données et les sécuriser de manière appropriée, respecter droits des personnes fichées…
Atteinte aux données financières	**Art. L621-15 du Code Monétaire et Financier (modifié par Loi de Sécurité Financière du 1 août 2003)**	**Jusqu'à 1,5 millions d'euros ou 10x le montant du profit réalisé**	Gouvernance d'entreprise transparente, sécurisation des données financières, définition de politiques de sécurité…
Atteintes aux Systèmes d'information de tiers (virus, entraves…)	**Art. 323-1 à 323-7 du Code Pénal (créés par la loi Godfrain du 5 janvier 1988, modifiée par la Loi pour la Confiance dans l'Économie Numérique du 21 juin 2004)**	**Jusqu'à 5 ans de prison et 75.000 euros d'amende**	Sensibiliser les utilisateurs, interdire l'importation de fichiers sur les postes utilisateurs, mettre à jour pare-feu et antivirus, effectuer des tests de vulnérabilité, mettre en place des *pots de miel* (pièges à pirates informatiques), rédiger une charte d'usage…
Contrefaçon d'œuvres audiovisuelles ou de logiciels	**Art. 335-1 et suivants du Code de la PI (peines aggravées par la Loi Perben II, 9 mars 2004)**	**Jusqu'à 3 ans de prison et 300.000 euros d'amende**	Sensibilisation du personnel, restrictions en matière de sauvegarde de données et d'accès à Internet…
Usage abusif d'Internet	**Aucune, seulement atteintes à la productivité, voire à l'image de l'entreprise. Risques de mise en cause en cas d'atteintes au fonctionnement du SI. Risque de complicité en cas d'usage illicite.**	-	Tolérer un usage ponctuel des outils à des fins personnelles, chartes d'usage, filtrage des sites (forums, chats), actions en justice au titre de l'abus de confiance…
Panne du SI	**Aucune, seulement surcoût important lié à la perte de temps. Risques de mise en cause en cas d'atteintes au fonctionnement du SI (pertes de données par ex.).**	-	Prévoir un plan de continuité d'activité, de sauvegarde des données, rédiger et publier une procédure d'escalade du sinistre…

Identification des menaces « nouvelles » et définition de règles déontologiques

Menaces "nouvelles"	Dispositions applicables	Peine maximale	Quelques règles déontologiques
Infractions liées à la loi sur la presse	**Loi sur la presse du 29 juillet 1881**	**Jusqu'à 5 ans de prison et 45.000 euros d'amende**	Conserver tout contenu produit par l'entreprise et communiqué, et les logs de connexion; demander à exercer son droit de réponse sans délai si diffamation ou fausse information…
Courriel indésirable (spamming)	**Art. L34-5 du Code des Postes et des Communications Électroniques (modifié par la LCEN du 9 avril 2004)**	**Sanction possible au titre de la collecte frauduleuse de données ou du détournement de fichiers (jusqu'à 5 ans de prison et 300.000 euros d'amende).**	Ne prospecter par voie électronique qu'après obtention du consentement de la personne, rappeler ses droits d'accès et d'opposition…
Hameçonnage (phishing) ou harponnage (spear-phishing)	**Celles relatives à la collecte frauduleuse de données et à l'escroquerie.**	**Celles relatives à la collecte frauduleuse de données et à l'escroquerie.**	Ne pas divulguer d'informations à une personne non identifiée, et non authentifiée. Culture du secret et de la confidentialité.
Interopérabilité illicite	**Art. L122-6-1-IV du Code de la Propriété Intellectuelle**	**Jusqu'à 3 ans de prison et 300.000 euros d'amende**	S'assurer que les informations ne sont pas déjà disponibles, contacter au préalable l'éditeur du programme, limiter ses actes aux parties essentielles de celui-ci, conserver ces informations secrètes...
Cybersurveillance fautive	**- Loi du 31 décembre 1992 (art. L120-2, L121-8 et L432-2 du Code du travail) - Art. 226-1 et 226-22 du Code Pénal**	**- Rejet de la preuve et requalification du licenciement (sans cause réelle et sérieuse) - jusqu'à 5 ans de prison et 300.000 euros d'amende (divulgation d'informations relatives à la vie privée) - jusqu'à 1 an de prison et 45.000 euros d'amende (collecte d'informations relatives à la vie privée)**	Proportionnalité des moyens employés avec les buts recherchés, information préalable du salarié quant aux modes de contrôle, discussion avec instances du personnel, transparence dans la recherche de preuves...
Violation des correspondances	**Art. 226-15 et 432-9 du Code Pénal**	**Jusqu'à 1 an de prison et 45.000 euros d'amende (3 ans de prison pour un agent public)**	Définition de procédures d'accès à la messagerie en l'absence de l'employé, information, transparence…
Recel de données pédo-pornographiques	**Art. 227-23 du Code Pénal**	**Jusqu'à 5 ans de prison et 75.000 € d'amende**	Filtrage des sites, gestion des accès Internet…

- ***Déontologie et usages des Systèmes d'information***

Les usages du SI impliquent des interactions et des échanges multilatéraux que nous pouvons schématiser comme suit :



La déontologie peut être un moyen de définir un cadre de références contenant la loi mais aussi des règles internes claires, facilement applicables. Pour bien fonctionner, cela nécessite l'adhésion de toutes les parties prenantes.

Les règles déontologiques que l'entreprise s'impose de suivre jouent le rôle de « règles du jeu » venant combler les déficits existants entre les lois, le règlement intérieur et le contrat de travail. Elles interviennent comme un « filtre » permettant de garantir une utilisation adéquate de son Système d'information.

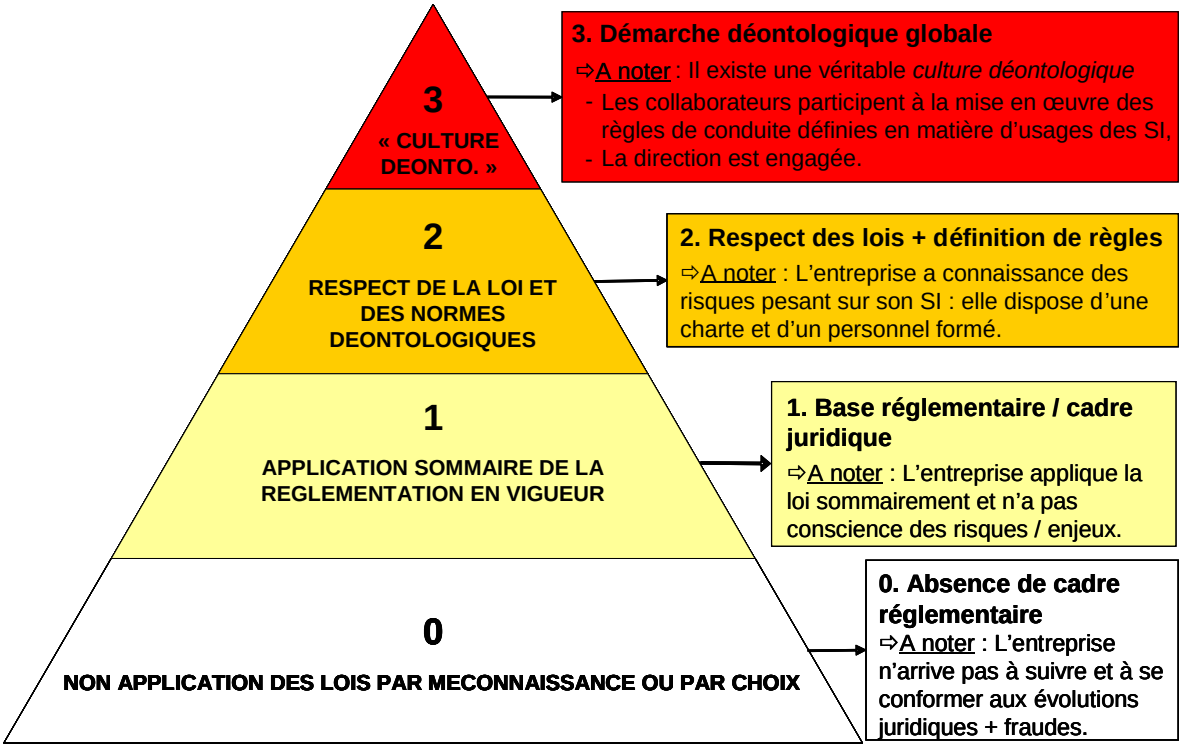
Cadre de références

La question de fond qui se pose alors est la suivante : comment conformer son SI aux réglementations en vigueur par la déontologie ? Une première solution pourrait être de responsabiliser les accédants au SI, ce qui implique pour l'entreprise de connaître les risques et d'avoir une compréhension globale des enjeux.

Imaginer la déontologie comme un cadre de références pour l'entreprise permet de dégager quatre types d'entreprises :

0. Les entreprises qui n'appliquent pas les lois par choix, par méconnaissance ou par manque de moyens,
1. Les entreprises qui appliquent sommairement les lois,
2. Les entreprises qui appliquent les lois, qui ont réfléchi sur la déontologie et qui ont défini des règles internes,
3. Les entreprises qui ont intégré les lois, ont passé le stade de la définition et de la mise en œuvre et dont la priorité aujourd'hui est de sensibiliser les personnels et de s'assurer de leur adhésion aux règles établies.

Typologie des entreprises selon le niveau de déontologie appliquée aux usages du Système d'information



L'adoption de comportements conformes aux bons usages est un préalable essentiel à la protection du SI, et dépasse le simple respect de la réglementation. Certaines entreprises ne pourront probablement pas dépasser le niveau 2 de la pyramide essentiellement pour des raisons de coût, de temps et d'investissement humain nécessaire à la mise en conformité aux diverses réglementations. De plus, la sensibilité des secteurs est variable, et ce paramètre compte aussi pour beaucoup dans le degré de protection du Système d'information.

Il est fort vraisemblable que certaines entreprises se situent au niveau 0 de cette pyramide. En effet, il est probable qu'un certain nombre d'organismes n'appliquent pas la loi par simple méconnaissance de ses dispositions, lesquelles peuvent souvent paraître imprécises, voire obscures (quels types de fichiers déclarer à la CNIL, qu'est-ce qu'une donnée personnelle, pendant combien de temps archiver tel ou tel document ?). En tout état de cause, et dans la mesure où nul n'est censé ignorer la loi, ces entreprises ainsi que leurs dirigeants sont en situation de risque juridique particulièrement grave.

Aucune entreprise ne peut justifier un choix volontaire de ne pas appliquer la loi. En effet, les efforts qu'implique la mise en conformité juridique du SI ne sont en rien comparables aux sanctions prévues par la loi pénale. D'une amende particulièrement lourde, les condamnations prononcées par le juge peuvent effectivement aller jusqu'à plusieurs années d'emprisonnement pour les personnes responsables de tels manquements. Le risque pénal ne peut donc être raisonnablement écarté.

Gérer les contraintes juridiques et les conflits de normes (cf. annexe 1)

Les premières normes juridiques en matière de Systèmes d'information sont apparues il y a une trentaine d'années. Celles-ci restent incomplètes en raison des nombreuses évolutions technologiques et de la construction lente du droit. Si l'entreprise veut être juridiquement bien couverte, il ne lui suffit plus d'appliquer et de respecter les lois en vigueur, il faut aussi qu'elle soit active et qu'elle soit en mesure d'anticiper : adoption d'une charte, mise en place d'une démarche globale, sensibilisation des collaborateurs, veille juridique, etc. Aujourd'hui appliquer et respecter la loi n'est pas aisé… Les conflits de normes nationaux et/ou internationaux sont nombreux, ce qui laisse place à des règles imprécises, voire antagonistes, et donc difficilement applicables.

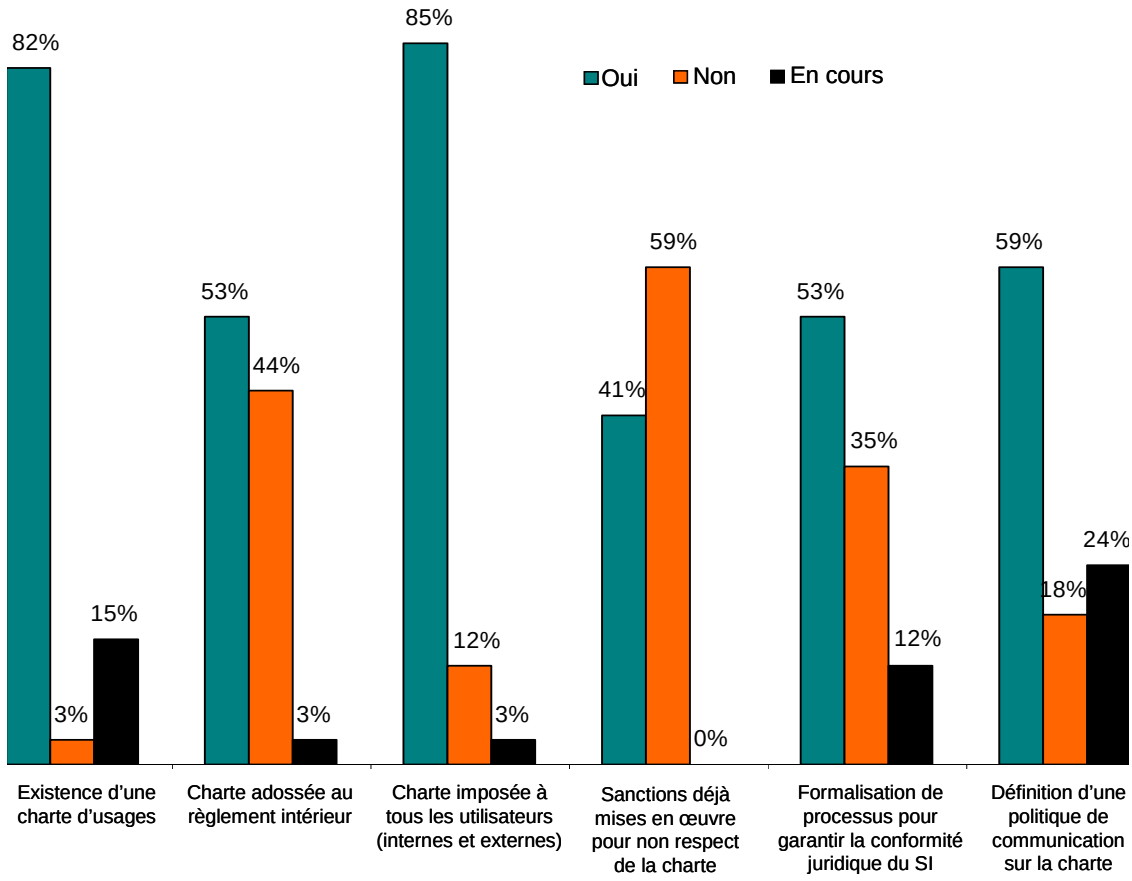
Définir la portée du secret professionnel en qualifiant les données (cf. annexe 2)

La déontologie permet de discerner les règles adéquates en matière de secret professionnel et de déterminer la manière la plus adaptée pour le mettre en œuvre. Car, en effet, traiter de manière massive des données confidentielles et/ou sensibles implique le respect du secret professionnel. Il s'agit d'une obligation légale qui requiert :

- une qualification préalable des données et des personnes soumises au secret ;
- une qualification préalable des circonstances dans lesquelles le secret peut être levé.

Mettre en place une charte et communiquer

Moyens mis en œuvre pour assurer la conformité juridique des usages du SI



La plupart des organismes ont choisi d'agir en se dotant de références internes, inspirées des règles juridiques en vigueur. Ce constat est renforcé par le graphique page 24 (basé sur les réponses à l'enquête, annexe 3) : plus de 95% des entreprises sont déjà dotées d'une charte d'utilisation du SI ou sont en train de le faire.

Cette démarche leur offre davantage de visibilité, une meilleure compréhension des lois et leur permet de mieux les appliquer. Mais ces textes internes ne doivent pas avoir d'autre ambition que celle de garantir un usage conforme et responsable du Système d'information, sans entraver les droits et les libertés des personnes.

C'est pourquoi il est nécessaire de définir des règles d'utilisation : souples mais précises, elles doivent être portées à la connaissance de tous par tous les moyens de communication disponibles. Pour élaborer de telles références, l'entreprise doit faire collaborer plusieurs acteurs : responsables SI, déontologues, responsables RH, juristes, et autres directions le cas échéant, ainsi que les représentants du personnel. Le consensus et l'échange entre tous ces acteurs sont les meilleurs moyens de définir des règles simples, applicables et acceptables par tous. Chacun doit se sentir naturellement concerné et donc s'impliquer volontairement.

La charte de bon usage du SI, même si elle n'a pas une portée juridique systématique et incontestable (dû au fait qu'elle ne soit pas systématiquement rattachée au règlement intérieur – voir annexe 3), est néanmoins devenue un outil incontournable pour responsabiliser les collaborateurs dans leur utilisation du Système d'information. Elle revêt une valeur pédagogique par laquelle l'organisme peut sensibiliser, informer et favoriser la prise de conscience des utilisateurs sur les répercussions négatives susceptibles d'être engendrées par des usages non-conformes.

L'introduction de telles règles n'a pas pour but de moraliser, ni de standardiser les comportements des salariés au regard de l'usage du SI, mais de donner des repères sur les conduites que l'entreprise attend des collaborateurs en matière d'usages du SI :

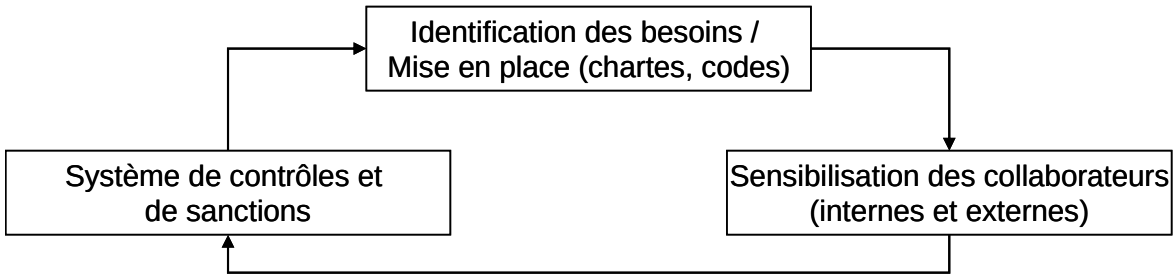
- Responsabiliser les salariés au regard de l'usage du SI de l'entreprise,
- Assurer à la fois la transparence, la confidentialité et le respect de l'espace privé des salariés,
- Sécuriser en interne et en externe la circulation des informations,
- Respecter et faire respecter le droit de propriété intellectuelle,
- Concilier le besoin de sécurité et l'esprit d'entreprise,
- Rendre l'environnement juridique lié aux usages des outils informatiques plus lisible et compréhensible,
- Lister de manière exhaustive les règles d'utilisation des outils liés aux Systèmes d'information.

Démarche

Dans la mesure où les principes éthiques se situent au niveau de l'action, les règles du jeu établies doivent être valables pour tous les acteurs de l'entreprise participant à des projets communs, du top management aux unités opérationnelles. Ces règles peuvent donc également s'appliquer aux acteurs extérieurs à l'entreprise. Selon l'enquête, plus de deux entreprises sur trois font systématiquement appliquer leur charte à leurs collaborateurs internes et externes (prestataires, stagiaires, intérimaires, clients, fournisseurs, voire à d'autres parties prenantes).

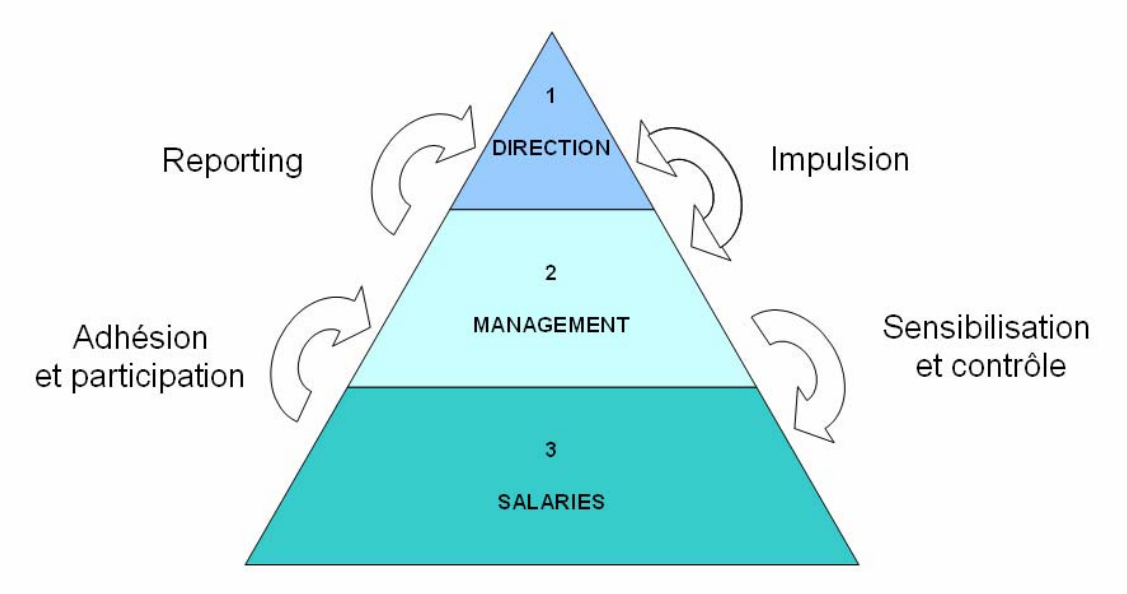
Les entreprises peuvent choisir de donner une dimension juridique à leur démarche en adossant leur charte d'usages, ou certaines de ses dispositions seulement, à leur règlement intérieur. Les règles ainsi établies ont alors force obligatoire et un système de contrôle / sanctions en cas de non respect peut s'appliquer.

Illustration de la démarche



L'entreprise attend de ses salariés qu'ils aient un comportement éthique en matière d'utilisation du SI. Pour ce faire, elle peut adopter une démarche de pédagogie attractive (déclinaison des règles déontologiques sous forme de bande dessinée, quizz et auto-formations sur l'intranet…). Les règles d'utilisation déontologique du SI seront plus volontiers intégrées et acceptées par les collaborateurs qu'elles sont respectées, appliquées et impulsées par la direction.

Impulsion



En résumé

L'entreprise ne peut plus se contenter de respecter et d'appliquer la loi… Comme nous l'avons vu plus haut, l'identification d'une fonction interne, ayant pour attribution spécifique le suivi de la conformité juridique de la structure qui l'emploie, n'est pas unanimement consacrée (moins d'une entreprise sur trois dispose d'un déontologue attitré selon l'enquête).

Cependant, la conformité juridique des traitements de données et le respect des meilleures pratiques en matière de Systèmes d'information est plus que jamais imposée par la loi (protection des données personnelles et financières, responsabilité de l'entreprise pour le fait commis par ses employés dans le cadre de leurs fonctions…). C'est pourquoi, des fonctions spécifiquement dédiées, comme le Correspondant Informatique et Libertés (CIL)[8], devraient émerger peu à peu (15% des entreprises ayant participé à l'enquête ont déjà mis en place une telle fonction et 59% envisagent de le faire).

Dès lors, pour l'entreprise, nommer un spécialiste de la conformité juridique lui permet d'une part de réduire le risque potentiel de non-conformité juridique, et d'autre part de démontrer à toutes ses parties prenantes et aux autorités publiques qu'elle se donne les moyens de cette mise en conformité. Cependant, l'entreprise doit aller plus loin afin d'avoir une visibilité plus nette de son environnement et de garantir une image responsable et éthique à laquelle l'opinion publique est de plus en plus sensible. Ces deux nécessités apportent alors à notre problématique deux nouvelles dimensions : l'intelligence économique et le développement durable.

[8] Cette fonction nouvelle, introduite avec la réforme de la loi Informatique et Libertés en août 2004, existe déjà en Allemagne, aux Pays-Bas, en Suède et au Luxembourg. Spécialisé dans la protection des données à caractère personnel, le CIL doit avoir une double compétence, informatique et juridique. Nommer un CIL n'est pas obligatoire mais fortement recommandé par la CNIL. Pour plus d'information sur le CIL : http://www.cnil.fr/

■ Déontologie, intelligence économique et développement durable : quels liens ?

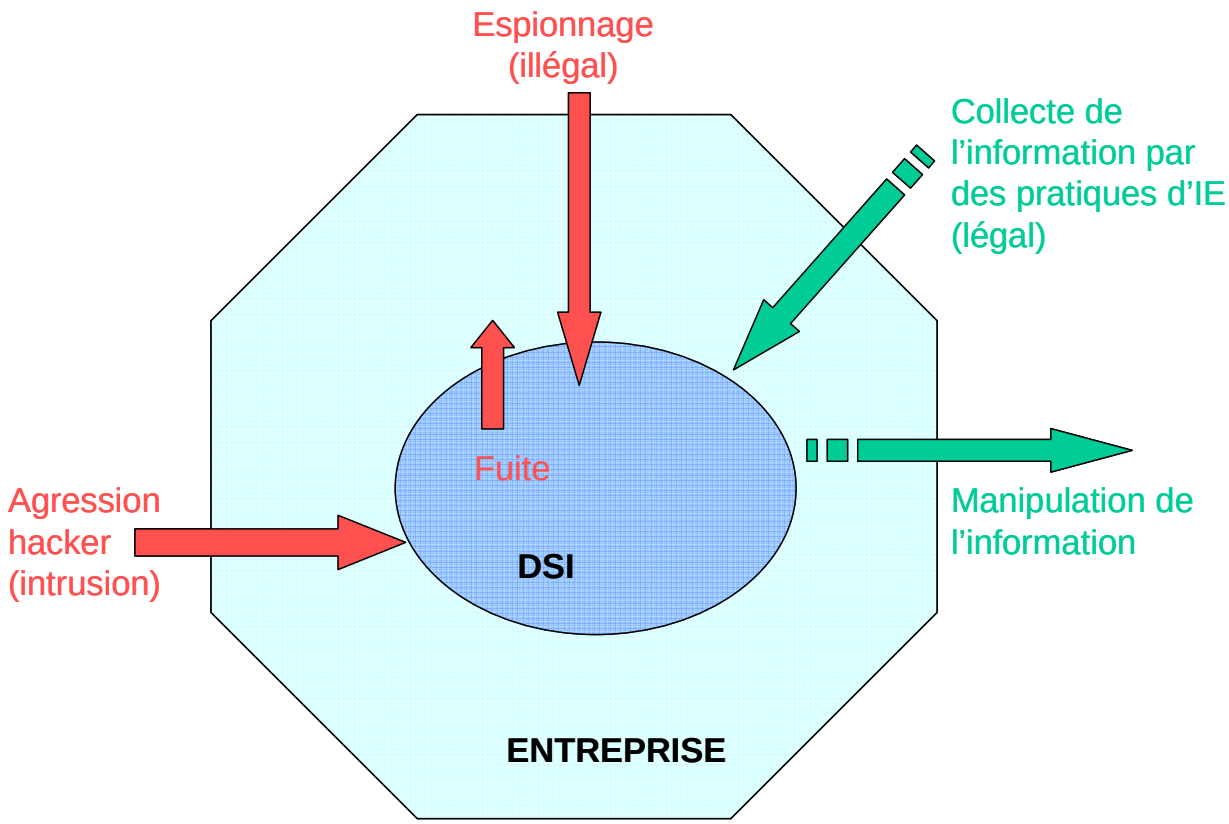
• *Déontologie et intelligence économique*

Aujourd'hui, l'avantage concurrentiel d'une entreprise « *réside dans [sa] capacité à maîtriser l'information (…), à la transformer, la comprendre, l'interpréter et à l'utiliser* »[9].

Une telle démarche implique l'utilisation du SI à tous les niveaux avec un objectif clair d'amélioration des performances globales de l'entreprise. Un bon usage du SI garantit la protection des informations et présente un avantage compétitif indiscutable pour l'entreprise.

Cependant, la question de la déontologie se pose dès lors que les pratiques d'intelligence économique sortent du cadre légal. **La déontologie rejoint donc l'intelligence économique sur la question des pratiques et de la protection du SI.**

Sécuriser et protéger le SI de l'entreprise pour lutter contre les manipulations perverses internes et/ou externes



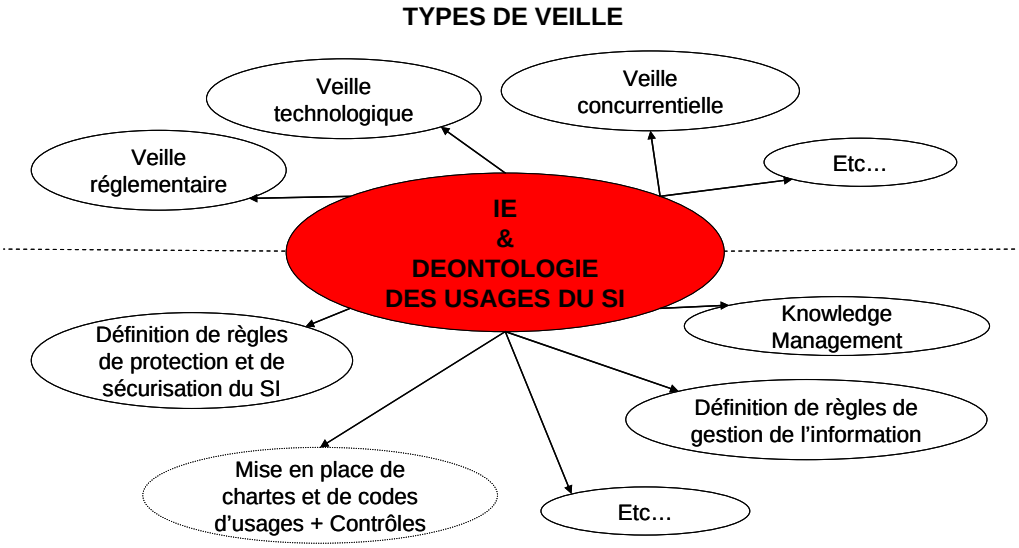
Dans un environnement fortement concurrentiel, la recherche d'informations est perçue comme une activité légitime et normale.

[9] Rapport Cigref, *L'intelligence économique appliquée à la DSI* (mars 2005).

Il est d'usage de « coloriser » l'information afin de mesurer le degré de déontologie, et donc d'exposition juridique, des personnes qui recourent à cette pratique désormais courante :

- *Information blanche :* Information librement accessible qui n'implique aucune violation de règles d'ordre déontologique. Ce type de collecte d'informations représente environ 85% des pratiques (estimation des professionnels).
- *Information grise :* Information obtenue de manière informelle (au cours d'un repas d'affaires, sur un salon, dans un colloque…). Cette pratique, parfois aux confins de la légalité, n'est pas toujours déontologique. Elle éclipse souvent la déontologie au profit de la logique concurrentielle. Cette pratique, si elle peut être contestable, n'est cependant pas répréhensible. Ce type de collecte d'informations représente environ 10% des pratiques (estimation des professionnels).
- *Information noire :* Information obtenue illégalement et résultant de pratiques d'espionnage, de vols… Cette pratique, que l'on peut apparenter à de l'espionnage industriel, implique nécessairement des procédés frauduleux susceptibles d'aboutir à des condamnations civiles et pénales. Le piratage informatique, la corruption ou le « social engineering » en sont quelques illustrations.

Veiller pour anticiper les risques d'usages non déontologiques du SI par l'environnement interne et/ou externe

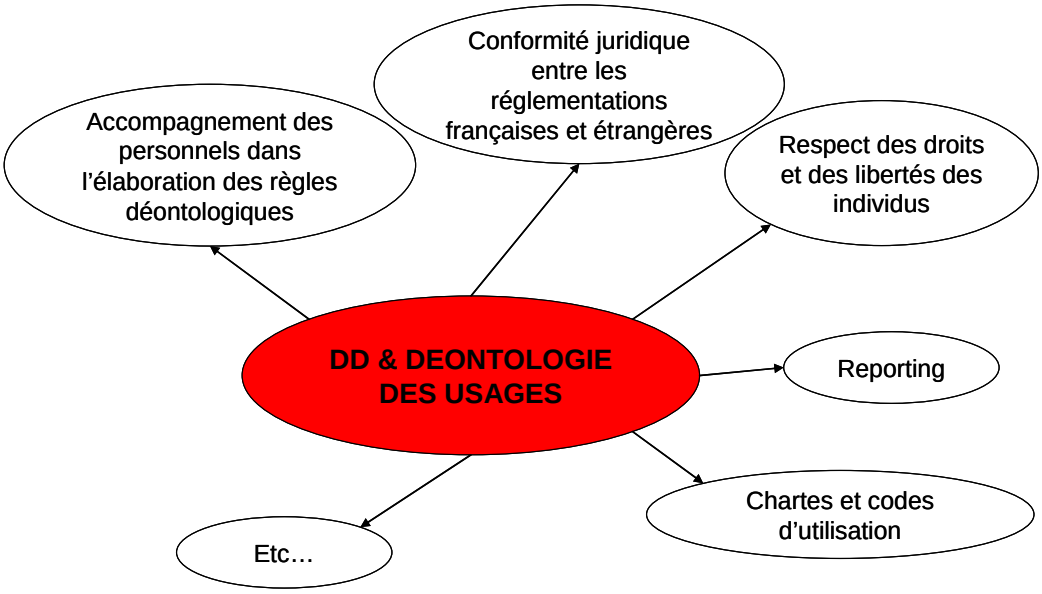


La DSI ne peut plus seulement assurer le bon fonctionnement du SI : elle doit aussi le sécuriser et le protéger pour lutter contre les risques de manipulations non déontologiques. Les DSI doivent être vigilants pour anticiper et alerter leur direction générale sur les éventuels effets pervers liés aux usages du SI par l'environnement interne et/ou externe (attaques, cybercriminalité, fuites d'informations sensibles…). Pour ce faire, plusieurs actions peuvent être mises en place par l'entreprise, sur lesquelles la DSI peut placer des garde-fous afin d'éviter les déviances liées à des pratiques illégales.

• Déontologie et développement durable

Les usages du Système d'information ont des répercussions sur la démarche de développement durable d'une entreprise. En effet, aujourd'hui presque toutes les grandes entreprises ont mis en place une telle démarche. Ce concept est devenu un puissant vecteur de communication car il impacte directement l'image de l'entreprise, à laquelle l'opinion publique est très sensible.

Définir des règles déontologiques pour encadrer les usages et garantir l'image d'une entreprise responsable



La définition de pratiques éthiques de management des hommes et des outils, ainsi que d'achats et d'approvisionnements, s'inscrit pleinement dans une démarche de développement économique, social et environnemental durable, laquelle est encouragée par son impact positif sur l'image de l'entreprise. Mais choisir de se doter d'une charte d'usages dans ces mêmes domaines s'inscrit aussi et surtout dans une démarche déontologique initiée par l'entreprise.

Conclusion

La problématique fondamentale induite par la déontologie des usages des Systèmes d'information peut se résumer comme suit : **il s'agit de transposer en règles et contrôles internes les contraintes juridiques qui pèsent aujourd'hui sur l'utilisation des Systèmes d'information et qui peuvent amener les entreprises à être sanctionnées de ce fait**. L'entreprise se doit donc de réduire le risque de non conformité à ses obligations d'ordre juridique. Cependant, elle doit veiller à ne pas multiplier les chartes qui risqueraient de devenir un régulateur pénal fait pour sanctionner les collaborateurs qui ne respecteraient pas les modalités d'usages. Elle doit s'efforcer de trouver un juste équilibre entre la volonté des collaborateurs de contribuer à encadrer les pratiques et le risque de glisser dans le contrôle permanent des utilisateurs.

Nous avons développé les orientations données par le groupe de travail, après avoir sélectionné quelques **fondamentaux communs à la majorité des entreprises, susceptibles d'inciter certaines d'entre elles, soucieuses des enjeux et de leurs répercussions, à se doter de règles déontologiques**. Les actions déjà entreprises par certaines organisations (cf. page 53) ne sont qu'un début… Toutes envisagent de mettre en place de nouvelles actions dans les années à venir afin de mieux prévenir et gérer les risques liés à des usages juridiquement non-conformes de leur Système d'information (cryptage, archivage des courriels, mise en place de politiques de sensibilisation, etc.).

De plus, les réflexions développées ont permis d'ouvrir la voie à d'autres thèmes qui appellent des réponses opérationnelles et concrètes. En effet, les questions essentielles que se posent désormais certains DSI sont les suivantes :

- Quelles sont les questions à se poser en amont de la mise en place d'une démarche de déontologie ?
- A qui s'adresser pour assurer la mise en place opérationnelle d'un processus déontologique ?
- Sur quel support s'appuyer pour mettre en place une *démarche plan progrès*, démarche d'amélioration continue avec une mise en œuvre par étape, un suivi et un reporting réguliers) dans l'entreprise d'une part, et assurer la conduite du changement d'autre part ?

L'enquête renforce ces points dans la mesure où elle a permis de mettre en lumière un certain nombre de besoins :

- Développer une *charte type* adaptable en fonction de l'environnement et une *charte spécifique « SI »*. Afin de donner une idée précise du contenu de telles chartes, nous vous invitons à visiter le site www.cigref.fr, sur lequel sont présentés plusieurs modèles de chartes reconnues, et spécifiques aux SI,
- Développer un *guide* décrivant clairement les responsabilités, le rôle et le statut du Correspondant Informatique et Libertés (CIL),
- Développer un *kit opérationnel de mise en œuvre* d'une démarche déontologique et préparer un support permettant d'initier une *démarche plan progrès* et d'assurer la conduite du changement : élaboration d'un *kit de communication* et d'un *kit de formation* des utilisateurs.
- Mettre en place une veille juridique et jurisprudentielle.

Dès lors, une poursuite de ces premiers travaux peut être envisagée dans la mesure où un certain nombre de **besoins opérationnels ont été identifiés** au cours de la réflexion sur la déontologie des usages des Systèmes d'information.

Annexes

- ***Annexe 1 : Les conflits de normes***
- ***Annexe 2 : Le secret professionnel***
- ***Annexe 3 : L'enquête « Déontologie des usages des SI » : présentation des participants et synthèse des réponses***

Complément (à télécharger sur le site du CIGREF)

- ***Exemples de chartes***

Nous vous invitons à consulter le site du CIGREF[10] sur lequel vous trouverez trois exemples de chartes appliquées dans les domaines associatif, public et privé. La finalité est d'illustrer la mise en œuvre opérationnelle d'une démarche de déontologie appliquée aux Systèmes d'information.

Vous trouverez :

- La charte de présentation des règles et obligations des utilisateurs en matière d'utilisation du *système de base de connaissances,* élaborée par l'Association Française de l'Audit et du Conseil Informatique (AFAI), en collaboration avec le Cabinet d'avocats Bensoussan. Adaptable dans n'importe quelle structure, cette charte peut évoluer dans sa granularité, son périmètre et sa focalisation. Le Groupe La Poste, par exemple, l'a adaptée afin de pouvoir l'appliquer en son sein.
- La charte du Conseil Général des Hauts de Seine : spécifique à l'utilisation des Systèmes d'information, elle s'applique tant aux agents qu'à la Collectivité.
- La charte d'Air France : annexée au règlement intérieur, elle s'applique à tous les salariés basés en France métropolitaine et outre mer, ainsi qu'aux stagiaires et aux intérimaires

[10] www.cigref.fr

Annexe 1

• Les conflits de normes

Sous le terme de « norme », il faut comprendre un document de référence de toute nature (loi, règlement, code, charte…) et/ou une règle de conduite, générale et obligatoire.

Définition et finalité du document

Définitions

- ***La loi***

La loi est une règle écrite, générale et permanente élaborée par le Parlement, elle est source majeure du droit.

On ne peut y déroger.

- ***Le règlement***

Le règlement est un acte de portée générale et impersonnelle destiné à assurer l'exécution d'une loi ou à disposer dans des domaines non réservés au législatif.

On ne peut y déroger.

- ***Le code***

Le code, au sens juridique, est un recueil systématique de textes (lois et règlements) concernant un secteur du droit.

On ne peut y déroger.

Le code peut aussi désigner des règles internes à l'entreprise qui peuvent recevoir une valeur contractuelle, ou rester des guides non contraignants pour les entreprises ou pour leurs collaborateurs.

- ***Le règlement intérieur***

Le règlement intérieur est un document écrit émanant du chef d'entreprise qui contient exclusivement les mesures d'application de la réglementation en matière d'hygiène et de sécurité, les règles générales permanentes relatives à la discipline et notamment la nature et l'échelle des sanctions, les dispositions relatives aux droits de la défense des salariés susceptibles d'être sanctionnés.

Toute modification à ce règlement (dérogations) doit faire l'objet d'une procédure expresse écrite et communiquée auprès des salariés, de leurs représentants et de l'Inspection du Travail.

- ***La charte***

La charte est un ensemble de conditions à remplir, des contraintes à respecter dans un domaine particulier. Toute modification de ce corpus (dérogations) doit faire l'objet d'une procédure expresse écrite et communiquée auprès des salariés et de leurs représentants.

Finalité du document

Les objectifs du présent document sont de deux ordres :

- Informer le lecteur sur les difficultés auxquelles peut être confrontée une entreprise qui souhaite s'assurer de sa conformité avec les textes (nationaux ou internationaux) qui la régissent,
- Proposer au lecteur quelques pistes pour faciliter sa propre réflexion.

L'environnement des entreprises

L'environnement juridique et réglementaire

L'entreprise évolue dans un environnement juridique qu'elle ne maîtrise pas et auquel elle ne peut pas déroger. En particulier, l'utilisation des technologies de l'information est un domaine faisant l'objet de multiples textes juridiques tant nationaux qu'européens ou internationaux, ainsi que de recommandations de la CNIL (en France) qui n'ont pas la même portée juridique.

En effet, en France, plusieurs textes ont récemment modifié l'environnement légal en matière de Systèmes d'information : la loi pour la confiance dans l'économie numérique du 21 juin 2004, la nouvelle loi informatique et libertés du 6 août 2004 complétée par le décret d'application du 20 octobre 2005. Par ailleurs, le code du Travail (articles L.120-2 et suivants, puis L 432-2 et L 432-2-1) exige des entreprises qu'elles informent au préalable les représentants du personnel avant tout projet important d'introduction de nouvelles technologies lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail du personnel.

Mais, malgré l'abondance de textes, la législation reste silencieuse sur les possibilités d'articulation entre les chartes et/ou les codes de conduite avec le règlement intérieur de l'entreprise. Celle-ci se trouve alors confrontée à d'importants conflits, particulièrement en matière de protection des données sensibles (nominatives et/ou financières). Ce sujet étant la préoccupation essentielle des entreprises, mais non la seule, nous nous sommes attachés à aborder exclusivement ce thème.

Les conflits des références internes et la protection des données

Les entreprises ayant des ramifications internationales ou une activité mondiale se trouvent régulièrement confrontées à d'importants problèmes de conflits de références internes. En effet, ces conflits peuvent apparaître dans deux situations :

- ***Entre une maison-mère et ses filiales :*** une maison-mère étrangère peut imposer l'application d'un code de conduite dans toutes ses filiales ; or, le texte peut ne pas être applicable en l'état dans les filiales et nécessiter des aménagements.
- ***Au sein d'un groupe :*** il peut arriver que l'ensemble d'un groupe suive un code de conduite universellement appliqué, s'appuyant sur des règles internes d'entreprises (les *binding corporate rules :* de portée générale, ce type de règles englobe des règles spécifiques au SI) ; sur un plan juridique, si ces règles ne sont pas adossées au règlement intérieur de chaque entité, alors elles ne feront jamais office de référence que ce soit en France ou dans un autre pays.

De plus, les États ont des législations — a priori — différentes… Des difficultés de conformité juridique peuvent alors naître lorsque ces mêmes entreprises sont conduites à échanger des données par delà les frontières. La loi Sarbanes-Oxley, par exemple, à laquelle certaines entreprises sont soumises, impose de tels échanges de données. C'est pourquoi, la question de la protection des données est si importante, que ce soit en France ou en dehors de ses frontières.

- ***La protection des données en France***

La CNIL a explicité dans un document d'orientation[11] du 10 novembre 2005 la mise en place des dispositifs d'alerte professionnelle (*whistleblowing)* dont la finalité est de renforcer la protection des données sensibles de l'entreprise en favorisant la dénonciation de comportements suspects de collaborateurs. Ce dispositif est applicable à un cadre restreint et sous certaines conditions :

- limitation du dispositif d'alerte aux domaines comptables, financiers et bancaires (lutte contre la corruption),
- définition des catégories de personnes concernées par le dispositif d'alerte par le chef d'entreprise qui fixe également les limites de la procédure,
- création d'une organisation spécifique dans l'entreprise chargée de la gestion du dispositif d'alerte : nomination d'un responsable, définition de son rôle,
- information individuelle et collective des salariés sur le dispositif d'alerte, par tous les moyens,
- information des salariés mis en cause dans le cadre de l'alerte professionnelle par le responsable du dispositif.

De plus, en matière de transferts internationaux de données, et pour conclure sur la protection des données en France, la CNIL a récemment publié un document sur la simplification des démarches des entreprises en matière de transferts de données à l'étranger. Pour plus d'informations sur ce sujet, vous pourrez consulter ce document sur le site de la CNIL : http://www.cnil.fr.

- ***La protection des données en Europe, hors France***

L'intérêt de l'UE pour la protection des données à caractère personnel n'est pas nouveau. En effet, dans un premier temps, l'UE a garanti le droit au respect de la vie privée et familiale avec l'article 8 de la Convention européenne des droits de l'homme (CEDH, novembre 1950).

Puis, le Conseil de l'Europe a adopté en janvier 1981, la Convention 108 relative à la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. La protection des données apparaît comme un droit équivalent à la protection des droits fondamentaux énumérés dans la CEDH. Le niveau de protection des données étant plus ou moins contraignant d'un pays à l'autre, l'UE cherche à harmoniser le cadre juridique.

De plus, la Commission a engagé un dialogue avec les pays non membres de l'Union européenne, particulièrement avec les États-Unis, afin qu'un niveau élevé de protection lors du transfert des données à caractère personnel vers ces pays soit garanti.

[11] Document téléchargeable sur le site de la CNIL à l'adresse suivante : http://www.cnil.fr/index.php?id=1890

La coopération entre la Commission et ces pays tiers a abouti à la mise en place de dispositifs particuliers[12] :

- Les *Safe Harbor Principles* : Au nombre de sept, ils ont été définis par le *Department of Commerce* américain en réponse aux exigences imposées par la Directive européenne de 1995, notamment sur la question du « niveau de protection adéquat ».
- Les *clauses contractuelles types* : Ces 11 clauses contraignantes définies en 2001 par la Commission ont été simplifiées et assouplies en 2004. Le recours à ces clauses permet de garantir la protection des données transférées entre un pays membre et un pays tiers.
- Les *clauses ICC 2004* : Solution alternative aux clauses contractuelles (car plus souple), ces clauses ont été définies par une coalition d'associations professionnelles rattachée de l'*International Chamber of Commerce*.
- Les *Binding Corporate Rules (BCR)*: Ces règles internes d'entreprises sont définies par les maisons-mères multinationales et sont applicables dans toutes les filiales. Cependant, elles doivent être approuvées par plusieurs acteurs, notamment les autorités de protection des données des pays dans lesquelles elles doivent être appliquées, ce qui rend le processus lourd et long. A ce jour, seules trois multinationales se sont dotées de telles règles : Daimler Chrysler, Philips et General Electric.

Dans la pratique, pour tenter d'être en conformité avec tous les textes qui les régissent (internes, lois nationales et/ou internationales), les entreprises optent pour diverses solutions, dont quelques unes d'entre elles, les plus fréquemment utilisées, sont présentées ci-après.

Les solutions les plus fréquemment mises en œuvre par les entreprises

Les codes de conduite et les chartes éthiques

Comme nous l'avons vu un peu plus haut, la réglementation est abondante et complexe. Les entreprises cherchent donc à sensibiliser leurs collaborateurs et à leur fixer des limites dans l'usage des ressources informatiques et Internet en définissant un partage clair des responsabilités en cas d'abus.

Pour ce faire, certaines entreprises ont rédigé des codes de déontologie ou d'éthique afin d'attirer l'attention de leurs salariés sur ces sujets en les illustrant de cas pratiques. Ces règles internes peuvent recevoir une valeur contractuelle, ou rester des guides non contraignants pour les entreprises ou pour leurs collaborateurs.

Beaucoup d'autres ont choisi d'annexer à leur règlement intérieur des extraits de chartes rédigées en interne qui doivent par principe respecter la loi (charte du bon usage des ressources informatiques et Internet par exemple). Dans la mesure où des sanctions disciplinaires sont prévues, une information des salariés est exigée.

[12] *Safe harbor principles* : http://www.export.gov/safeharbor/
Clauses contractuelles types : http://europa.eu.int/eur-lex/pri/fr/oj/dat/2002/l_006/l_00620020110fr00520062.pdf
Clauses ICC 2004 : http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp84_fr.pdf
Binding corporate rules : http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2003/wp74_en.pdf

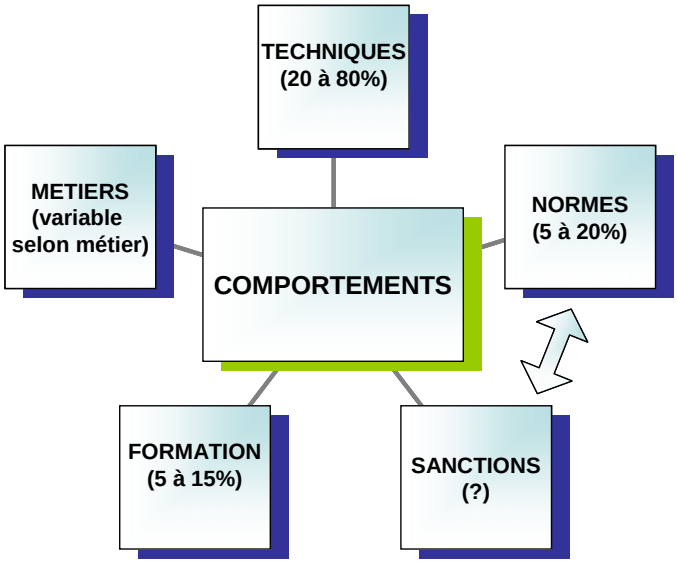
Cependant, ces deux solutions, les plus fréquemment utilisées, ne sont pas les seules et d'autres possibilités restent ouvertes. Dans tous les cas, un accompagnement du changement des comportements est nécessaire si l'entreprise souhaite voir appliquer les règles de conduites responsables qu'elle a définies.

L'évolution des comportements

Plusieurs leviers permettent d'accompagner le changement des comportements des utilisateurs en matière de Systèmes d'information :

- Les **techniques** constituent la méthode la plus efficace et impliquent une modification des comportements dans 20 à 80% des cas : restriction des accès Internet, mise en place de filtres…
- La **mise en place de normes** assorties d'un **système de sanctions** est le deuxième levier le plus efficace. L'adoption d'une charte ou d'un code entraîne une modification des comportements dans 5 à 20% des cas.
- La **formation et la sensibilisation** des utilisateurs est le troisième levier par lequel l'entreprise peut arriver à faire évoluer les habitudes des collaborateurs en matière d'usages du SI (5 à 15%) : auto formation via l'intranet de l'entreprise, affichage, formation avec un consultant, actions de sensibilisation…
- Enfin, chaque **direction métier**, peut faire évoluer elle-même les utilisations faites par les collaborateurs du SI selon les activités qu'elle exerce.

Leviers permettant l'évolution des comportements en matière d'utilisation du SI – Illustration[13]



[13] Les pourcentages sont une estimation issue d'une réflexion entre AGF et Gartner au cours d'un vis-à-vis : l'intérêt est de montrer le degré plus ou moins contraignant des mesures prises en vue de lutter contre les mésusages des outils informatiques à disposition des salariés.

Les étapes à venir

Ce document est une première étape dans cette réflexion complexe aux multiples ramifications. Nous n'avons abordé qu'une infime partie du sujet et d'autres réflexions pourront être conduites, en particulier, sur :

- La séparation des responsabilités entre entreprises et collaborateurs en cas de manquement aux règles établies,
- Les échanges et la conservation des données confidentielles,
- La protection des données aux Etats-Unis,
- Etc.

Pour information

Les entreprises ayant participé à ces réflexions sont : Accor, AGF, France Telecom et GE Healthcare.

Annexe 2

• *Le secret professionnel*

Préambule

Le secret est une notion qui, bien qu'enracinée profondément dans l'Histoire, n'en demeure pas moins aujourd'hui l'une des préoccupations majeures de beaucoup de professionnels. En effet, un nombre grandissant de dispositions de nature législative ou réglementaire, de codes déontologiques, voire même de coutumes, soumettent les membres des professions qu'ils régissent au secret, sanctionné en droit français par des peines relativement lourdes. Concrètement, on peut considérer le secret professionnel comme l'une des facettes les plus communes du secret, exigeant de certains professionnels qu'ils s'abstiennent de divulguer un ou plusieurs types d'informations déterminés, généralement relatifs à leur activité ou à la personne de leurs clients.

Notre objectif est de tenter de comprendre « l'esprit » des quelques normes régissant le secret afin de mieux en discerner la portée ainsi que les limites. Il importe par conséquent d'en rappeler dans un premier temps les fondements historiques.

Fonctions historiques

Historiquement, les médecins furent les premiers à être soumis au secret dans le cadre de leur activité professionnelle, comme en témoignent les propos qu'ils se devaient de formuler lors de leur prestation du serment dit « d'Hippocrate »[14]. Cette exigence était d'ordre déontologique, c'est-à-dire qu'il s'agissait d'une nécessité morale concernant l'ensemble des membres d'une profession. Or, c'est la jurisprudence qui, comme dans la plupart des cas en matière de secret professionnel, est venue en préciser le périmètre. Selon la Cour de cassation[15], l'obligation au secret professionnel est établie pour assurer la confiance envers certaines professions (et s'impose ainsi, en l'espèce aux médecins, de manière générale et absolue comme un devoir de leur état, sauf lorsque la loi en dispose autrement).

Dans la tradition religieuse, les ministres du culte furent eux aussi, à leur tour, tenus de garder le secret sur les révélations qui avaient pu leur être faites à l'occasion de leurs fonctions[16]. La Cour de cassation était alors allée encore plus loin en estimant que les prêtres catholiques étaient soumis au secret pour l'ensemble des informations dont ils avaient eu connaissance, y compris recueillies en-dehors du cadre de la confession. Enfin, les avocats représentent la troisième catégorie de dépositaires historiques du secret. Cette responsabilité était liée aux confidences formulées par leurs clients dans le cadre de l'exercice de leurs droits en justice. Celles-ci sont toutes couvertes par le secret professionnel[17], et persistent même après le décès du client[18].

---

[14] «*Quoi que je voie ou entende dans la société pendant l'exercice de ma profession, je tairai ce qui n'a jamais besoin d'être divulgué, regardant la discrétion comme un devoir en pareil cas* ». Dispositions reprises dans le Code de déontologie médicale à l'article 4 (article R.4127-4 du code de la santé publique) « *Le secret professionnel, institué dans l'intérêt des patients, s'impose à tout médecin dans les conditions établies par la loi. Le secret couvre tout ce qui est venu à la connaissance du médecin dans l'exercice de sa profession, c'est-à-dire non seulement ce qui lui a été confié, mais aussi ce qu'il a vu, entendu ou compris* ».

[15] Cour de cassation, Chambre criminelle, 8 mai 1947: *Bull. crim*. n°124, D. 1948. 109

[16] Cour de cassation, Chambre criminelle, 4 décembre 1891 : *DP* 1892.1.139

[17] Cour de cassation, Chambre civile, 7 juin 1983 : *Bull. civ.* I, n°169

[18] Cour d'appel de Paris, 8 novembre 1971 : *Gaz. Pal*. 1972.1.96

Généralisation des dépositaires sous Napoléon

Prêtres, médecins et avocats étaient déjà reconnus comme étant soumis à une obligation au secret de type professionnel sous l'Ancien Régime. Mais à l'occasion de la codification des lois et de la refonte des institutions sous Napoléon, le Code pénal impérial (« Code pénal de 1810 ») a consacré de manière légale que le secret s'imposait aux professionnels de santé et, de manière plus générale, à toutes les personnes à qui le secret a été confié dans le cadre de leur profession : « *Les médecins, chirurgiens et autres officiers de santé, ainsi que les pharmaciens, les sages-femmes et toutes autres personnes dépositaires, par état ou profession ou par fonctions temporaires ou permanentes, des secrets qu'on leur confie, qui, hors le cas où la loi les oblige ou les autorise à se porter dénonciateurs, auront révélé ces secrets, seront punis d'un emprisonnement d'un mois à six mois et d'une amende de 500 F à 15.000 F* ». La loi ouvrait aux tribunaux l'occasion de délimiter le périmètre des personnes auxquelles s'impose le secret.

Catégories de dépositaires par « état » ou par « profession »

Dans sa rédaction actuelle, le Code pénal dispose qu'est interdite « *la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire* » (article 226-13). Il est très difficile de dresser une liste exhaustive de ces personnes soumises au secret, puisque de nombreux codes déontologiques et dispositions légales font de tel ou tel professionnel un dépositaire potentiel du secret professionnel. La jurisprudence a donc peu à peu été mise à contribution pour définir ces catégories, au-delà des codes déontologiques régissant ces professions[19].

Les banquiers sont régulièrement reconnus comme étant soumis au secret professionnel : il s'agit en effet de protéger leurs clients, auxquels il a toujours néanmoins été reconnu la possibilité de renoncer volontairement à cette sécurité[20]. Selon la jurisprudence, les experts-comptables et commissaires aux comptes, quant à eux, doivent également observer le secret le plus strict dans le cadre des affaires dont ils sont amenés à prendre connaissance dans l'exercice de leurs fonctions[21]. Les notaires[22], les policiers[23], les douaniers[24], les agents de change[25] ou encore les administrateurs de caisses de sécurité sociale[26] sont eux aussi considérés comme étant des dépositaires du secret au sens de la loi.

Enfin, l'obligation née du secret s'impose également aux jurés des tribunaux qui en deviennent dépositaires par état. Cette obligation « *est générale est absolue, car le délibéré est secret par nature*[27] ». Elle s'étend par ailleurs aux magistrats eux-mêmes, puisqu'ils délibèrent avec ces mêmes jurés[28].

---

[19] Les codes de déontologie sont opposables aux membres des professions qui les composent dans la mesure où ils ont été approuvés par décret, ou adopté par les organisations professionnelles disposant du pouvoir réglementaire pour l'ensemble de la profession qu'ils représentent (Voir notamment : Cour administrative d'appel de Marseille, 1er février 1999 : exemple de l'ordre des vétérinaires)
[20] Chambre commerciale, 11 avril 1995 : *Bull. civ*. IV, n°121
[21] Cour d'appel de Limoges, 30 mai 1985 : D. 1985, IR 501
[22] Cour de cassation, Chambre criminelle, 7 avril 1870 : S. 1870.1.277
[23] Cour de cassation, Chambre criminelle, 26 octobre 1995 : *Bull. crim*. n°328
[24] Article 59bis du Code des douanes
[25] Cour de cassation, Chambre criminelle, 1er février 1922 : S. 1922.1.337
[26] Cour de cassation, Chambre criminelle, 30 juin 1955 : *Bull. crim*. n°334
[27] Cour de cassation, Chambre criminelle, 25 janvier 1968 : *Bull. crim*. n°25
[28] Tribunal correctionnel de Paris, 31 mars 1989, JCP 1989.II.21356

Le secret professionnel impose avant tout une obligation de ne rien dire

La révélation du secret est sanctionnée par le Code pénal

- ***Qu'est-ce que le secret professionnel et comment est sanctionnée sa violation ?***

Le secret professionnel tel qu'on le conçoit juridiquement découle de l'article 226-13 du Code pénal qui énonce que « *la révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15.000 euros d'amende* ». La loi ne définit cependant pas juridiquement ce qu'est un secret, se contentant de dire dans quelle mesure sa violation peut être sanctionnée.

- ***A quoi sert le secret professionnel ?***

L'objectif du secret est de garantir au nom de l'intérêt général la confiance qui s'impose dans l'exercice de certaines professions[29], et dans l'intérêt du particulier pour garantir la sécurité des confidences que celui-ci peut faire à certaines personnes du fait de leur état ou de leur profession[30]. Le secret s'impose donc de manière horizontale (entre un professionnel et un client par exemple) et verticale (entre un employeur et son salarié).

- ***A partir de quel moment peut-on être sanctionné ?***

Il suffit que le secret ait été révélé sans autorisation à une seule personne pour que l'infraction soit constituée[31]. Il faut comprendre par révélation « *tout acte volontaire qui a pour conséquence directe ou indirecte de faire connaître à des tiers, en tout ou partie, des faits confidentiels ; que pour être punissable, la révélation doit être faite sans le consentement de l'intéressé à un tiers, et même si ce tiers est lui-même soumis au secret professionnel* [32]».

- ***Le secret de fabrique est une forme de secret professionnel***

Le secret de fabrique recouvre un concept différent, puisqu'il s'agit de protéger un intérêt économique et non un intérêt particulier. Il portera généralement sur un élément nécessaire à la continuité normale de l'activité de l'entreprise. En effet, selon André Bertrand, *un secret de fabrique est un procédé de fabrication offrant un intérêt pratique ou commercial, mis en œuvre par un industriel, mais tenu caché par celui-ci pour s'en réserver le bénéfice*[33]. Sa révélation, qui peut entraîner des conséquences dramatiques pour l'entreprise, est sanctionnée par le double des peines relatives au secret professionnel[34]. Cette disposition concerne tout acteur de l'entreprise responsable de la divulgation du secret, quelle que soit sa position hiérarchique (directeurs, salariés…).

---

[29] Cour de cassation, Chambre criminelle, 15 décembre 1885 : *DP* 1886.1.347
[30] TGI Paris 5 juillet 1996 : D. 1998, *Somm*. 86
[31] Cour de cassation, Chambre criminelle, 21 novembre 1874 : S. 1875.1.89
[32] Cour de cassation, Chambre criminelle, 18 octobre 2000, confirmant la définition donnée par la Cour d'appel de Paris le 16 juin 1999. Même en divulguant le secret à l'intérieur de la sphère bancaire, il y a violation du secret professionnel si cette révélation est faite sans le consentement de l'intéressé.
[33] Bertrand A., *La propriété intellectuelle*, Delmas, page 267.
[34] Article L152-7 du Code du Travail : « *Le fait, par tout directeur ou salarié d'une entreprise où il est employé, de révéler ou de tenter de révéler un secret de fabrique est puni de deux ans d'emprisonnement et de 30.000 euros d'amende. Le tribunal peut également prononcer, à titre de peine complémentaire, pour une durée de cinq ans au plus, l'interdiction des droits civiques, civils et de famille prévue par l'article 131-26 du code pénal* ».

▪ ***L'obligation de discrétion ou de réserve : un secret professionnel "allégé"***

L'obligation de discrétion s'impose par défaut aux agents publics[35]. Dans le secteur privé, et selon le Code du travail[36], seuls les membres du comité d'entreprise et les délégués syndicaux font l'objet de cette obligation pour toutes les informations présentées comme confidentielles par l'employeur (au même titre que le secret professionnel). Les autres salariés verront quant à eux leur responsabilité engagée pour manquement à devoir de loyauté[37] en cas de révélation injustifiée d'informations susceptibles d'impacter l'image ou la réputation de l'entreprise.

La violation d'une obligation de discrétion n'est pas sanctionnée pénalement. Elle engage "simplement" la responsabilité civile délictuelle (dommages et intérêts…) et/ou contractuelle (licenciement pour faute grave ou lourde…) de celui qui a révélé une information confidentielle, violant ainsi son devoir de discrétion.

L'obligation de réserve, quant à elle, se contente d'exiger une retenue de la part des agents publics dans le cadre de l'expression de leurs opinions (politiques surtout). Tout manquement est susceptible de donner lieu à des poursuites d'ordre disciplinaire.

▪ ***Qu'est-ce qu'un secret de défense nationale ?***

Beaucoup d'informations, aussi bien manipulées par l'Etat lui-même que par certaines entreprises entretenant d'étroites relations avec lui, sont dites classées « secret défense ». Il faut au préalable que ces informations aient été comme telles par l'autorité administrative (décret adopté en Conseil d'Etat). En effet, ces « *renseignements, procédés, objets, documents, données informatisées ou fichiers intéressant la défense nationale […] ont fait l'objet de mesures de protection destinées à restreindre leur diffusion*[38] ». Les personnes dépositaires d'un tel secret ont été préalablement accréditées, et sont tenues de le conserver et d'en préserver l'intégrité sous la menace d'une peine de sept ans de prison et de 100.000 euros d'amende.

Par ailleurs, toutes les autres personnes non tenues au secret mais qui ont connaissance de ces informations classifiées doivent le conserver (selon l'article 413-11 du Code pénal, leur est ainsi interdite la divulgation au public, la destruction ou la reproduction, et même la simple possession ; peine prévue : Ces comportements sont punis d'une peine de 5 ans de prison et de 75.000 euros d'amende).

---

[35] Article 26 de la loi n° 83-634 du 13 juillet 1983 : « *les fonctionnaires sont tenus au secret professionnel dans le cadre des règles instituées dans le code pénal. Les fonctionnaires doivent faire preuve de discrétion professionnelle pour tous les faits, informations ou documents dont ils ont connaissance dans l'exercice ou à l'occasion de l'exercice de leurs fonctions. En dehors des cas expressément prévus par la réglementation en vigueur, notamment en matière de liberté d'accès aux documents administratifs, les fonctionnaires ne peuvent être déliés de cette obligation de discrétion professionnelle que par décision expresse de l'autorité dont ils dépendent* ».

[36] Article L432-7 du Code du travail : « *Les membres du comité d'entreprise et délégués syndicaux sont tenus au secret professionnel pour toutes les questions relatives aux procédés de fabrication. En outre, les membres du comité d'entreprise et les représentants syndicaux sont tenus à une obligation de discrétion à l'égard des informations présentant un caractère confidentiel et données comme telles par le chef d'entreprise ou son représentant* ».

[37] Voir article 1134 al.3 du Code civil selon lequel les conventions légalement formées doivent être exécutées de bonne foi. La violation de cette disposition a pu être analysée par la jurisprudence comme un manquement au devoir de loyauté de la part du salarié.

[38] Article 413-9 du Code pénal et suivants

▪ ***L'entreprise face au risque de violation du secret des correspondances***

Beaucoup d'employeurs, soucieux de contrôler l'usage qui est fait des outils qu'ils mettent à la disposition de leurs salariés, s'exposent en effet à ce risque grave. De manière générale, l'atteinte au secret des correspondances peut être caractérisée par plusieurs comportements :

- l'ouverture, la suppression, le retardement[39] ou le détournement[40] de ces correspondances, dans la mesure où ceux-ci sont commis de mauvaise foi[41], peu importe si ces correspondances sont arrivées ou non à destination ;
- l'interception, le détournement, l'utilisation ou la divulgation des correspondances effectuées par la voie des télécommunications, dans la mesure où ceux-ci sont commis de mauvaise foi ;
- la prise de connaissance de toute correspondance de manière frauduleuse.

La violation du secret des correspondances est punie d'un an d'emprisonnement et de 45.000 euros d'amende (article 226-15 du Code pénal).

Le secret protège son propriétaire et s'impose au dépositaire

▪ ***Le secret professionnel protège le propriétaire de l'information confiée***

Selon la loi, une information qualifiée de secrète est confiée initialement par un *propriétaire* (personne qui crée l'information ou qui a l'autorité suffisante pour décider de son utilisation) à une personne qui en devient le *dépositaire* (détenteur d'un bien qui ne lui appartient donc pas, et ce dans un but déterminé). Si le propriétaire y consent, le *dépositaire* peut transmettre le secret à d'autres personnes qui en deviennent à leur tour *dépositaires*. La jurisprudence a souvent précisé qui devait être considéré comme étant un *dépositaire* au sens de la loi (*cf. supra*). Il lui a nécessairement fallu expliquer au préalable en quoi les informations confiées à une personne faisaient d'elle un dépositaire du secret.

▪ ***A défaut d'une réglementation plus large, il faut qualifier l'information de secrète***

La loi pénale est d'interprétation restrictive. On peut déduire de ce principe essentiel qu'aucune information n'est, par défaut, protégée par le secret. Cela implique que pour pouvoir opposer le secret à un tiers ou exiger de celui qui conserve une information qu'il la garde secrète, le *propriétaire* de l'information doit lui conférer ce statut.

[39] A par exemple été assimilée à une atteinte au secret des correspondances le fait, par un employeur, de conserver une lettre destinée à l'un de ses employés (Cour de cassation, Chambre criminelle, 18 juillet 1973 : *Bull. crim*. n°336)

[40] Par détournement, il faut entendre « *tous les agissements malveillants de nature à priver de leurs correspondances ceux qui en sont les destinataires véritables* » (Cour de cassation, Chambre criminelle, 26 octobre 1967 : *Bull. crim*. n°271)

[41] La mauvaise foi est par exemple établie par l'ouverture volontaire d'une correspondance par une personne qui n'en est pas destinataire (Cour de cassation, Chambre criminelle 26 janvier 1981, *Bull. crim*. n°35), ce qui exclut les correspondances ouvertes par mégarde (Tribunal Correctionnel de la Seine, 16 mars 1961 : *Gaz. Pal.* 1961.2.168) ainsi que les correspondances professionnelles (Cour de cassation, Chambre criminelle, 16 janvier 1992 : *Dr Pénal* 1992.170)

De manière générale, des dispositions législatives ou réglementaires déterminent qui doit être soumis au secret professionnel. Bien souvent, des codes déontologiques approuvés par décret ou adoptés par une autorité investie du pouvoir réglementaire définissent les catégories de professionnels soumis au secret professionnel, ainsi que les types d'informations soumises au secret. Parfois, les conventions collectives ou le règlement intérieur prennent le relais, soit pour pallier le silence de la loi, soit pour rappeler ces obligations.

Il peut néanmoins être recommandé aux employeurs d'introduire systématiquement une clause de secret et de confidentialité dans le contrat de travail pour consacrer cet impératif de secret. La rédaction de procédures appropriées est également un moyen de rappeler l'obligation au secret professionnel et de garantir son respect de manière adéquate.

Enfin, dans la mesure du possible, l'adoption de normes professionnelles claires détaillant le périmètre du secret professionnel permettrait non seulement d'uniformiser des pratiques professionnelles parfois confuses au sein d'un même secteur d'activité, et d'autre part de renforcer la légitimité du secret, ce qui représente une étape cruciale dans la perspective de contrôles ultérieurs, notamment en matière de traitements de données personnelles.

- ***Le périmètre du secret ne doit pas être fixé abusivement***

Dans le cadre de son contrat de travail, le salarié devient le dépositaire des secrets confiés par son employeur. Ce dernier doit donc définir quelles informations sont protégées et dans quelle mesure le salarié doit conserver le secret, voire l'opposer. D'une manière générale, le propriétaire d'une information est libre de déterminer si l'information qu'il confie est secrète ou non. De la même manière qu'un tribunal ne pourra pas refuser à une création artistique la protection par le droit d'auteur parce qu'elle est de piètre qualité, la loi pénale ne permet pas aux tiers ou au dépositaire de déterminer qu'une information est trop futile pour être qualifiée de secrète. Il s'agit d'un critère subjectif qu'il convient de respecter.

Toutefois, une limite peut être concédée, notamment au profit des personnes auxquelles le secret est opposé. Si le salarié, dans le cadre de son obligation de secret, doit toujours veiller à le respecter scrupuleusement, il peut être reproché à son employeur de recourir abusivement à l'obligation au secret. Nous pouvons nous permettre cette déduction au regard d'une décision de la Cour administrative d'appel de Marseille[42]. Dans cette décision, relative au périmètre du secret dans la profession de vétérinaire, il a été jugé que « *alors même que la totalité des actes qu'ils accomplissent ne pourrait être regardée comme couverte par le secret professionnel, et que ce secret ne concernerait les actes accomplis qu'en tant qu'ils peuvent livrer des informations sur la personne des propriétaires des animaux soignés, les vétérinaires doivent être regardés comme étant soumis au secret professionnel* ».

En résumé, l'employeur doit qualifier de secrètes les informations qu'il juge bon de protéger de toute divulgation. Il peut s'agir d'informations dont il est lui-même dépositaire (le client lui confie des informations personnelles dont la divulgation est interdite par la loi Informatique et Libertés), ou qu'il a produites (un secret de fabrique dont la révélation mettrait en péril l'avenir de l'entreprise).

[42] Cour administrative d'appel de Marseille, 1er février 1999

Dans ces cas, cités à titre d'exemple, le secret professionnel est non seulement légitime, mais en plus imposé par la loi. Ne pas rappeler que telle ou telle information est secrète expose donc l'entreprise à un risque au regard de la loi, mais aussi la prive de voies de recours qu'elle pourrait engager à l'encontre de celui qui l'a révélée.

Enfin, la volonté de tout qualifier de secret peut parfois être illégitime, lorsqu'elle a notamment pour but de dissimuler des activités frauduleuses. L'opposer à la puissance publique serait alors considéré comme une entrave punissable pénalement. On peut cependant concéder que dans de nombreux domaines s'impose une confidentialité absolue pour toutes les informations traitées par certaines catégories de professionnels (la recherche, l'aéronautique, le nucléaire). Le secret doit par conséquent faire l'objet d'une approche sectorielle pour être pertinente.

Le cas particulier des accès confidentiels au SI

- **Le principe : le salarié utilise les outils de l'entreprise**

Les outils mis à la disposition du salarié sont propriété de l'entreprise. En vertu de cette affirmation, nombre d'employeurs restent convaincus qu'ils peuvent contrôler sans limite l'utilisation qui en est faite. Cette conception, si elle n'est pas totalement erronée, doit néanmoins être nuancée. Le principe est effectivement le suivant : l'employeur est responsable des fautes commises par ses employés dans l'exercice de leurs fonctions[43]. En considération de ce risque, des techniques dites de cybersurveillance ont été adoptées par les entreprises, désormais soumises à un certain nombre de règles issues du Code du travail (proportionnalité[44], information préalable du salarié[45], information préalable des représentants du personnel[46]).

- **La limite : le salarié a droit au respect de sa vie privée sur son lieu de travail**

La frontière entre la mise en place de dispositifs de collecte d'informations relatives à l'utilisation des outils des salariés et les conditions relatives à leur mise en œuvre et à l'utilisation des preuves ainsi produites est particulièrement difficile à définir. Un célèbre arrêt de la Cour de cassation, dit « Nikon[47] », au terme duquel elle a décidé que « *le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur* », mérite d'être retenu.

---

[43] Article 1384 alinéa 5 du Code civil : « *Les maîtres et les commettants, [sont responsables] du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés* »

[44] Article L120-2 du Code du travail : « *Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché* ».

[45] Article L121-8 du Code du travail : « *Aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à un emploi* ».

[46] Article L432-2 du Code du travail : « *Le comité d'entreprise est informé et consulté, préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail du personnel* ».

[47] Cour de cassation, Chambre sociale, 2 octobre 2001 : *La Semaine juridique, entreprise et affaires*, 29 novembre 2001, n° 48

Dans cette affaire, l'employé en cause avait utilisé l'ordinateur de son entreprise à des fins extraprofessionnelles. Pour en obtenir la preuve, son employeur avait accédé à son ordinateur et à un répertoire intitulé « personnel » pour visualiser le contenu de messages émis et reçus par lui.

- **L'exception : l'atteinte au fonctionnement du SI**

A la suite de la découverte de photos érotiques dans le tiroir du bureau de l'un de ses salariés, un employeur avait fait procéder à une recherche sur le disque dur de son ordinateur, ce qui avait permis de découvrir un ensemble de dossiers totalement étrangers à ses fonctions figurant notamment sous un fichier intitulé "perso". Le salarié avait ensuite été licencié pour faute grave. Dans son arrêt, la Cour[48] a donné raison au salarié en estimant que « *sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé* ».

Le contrôle de l'activité du salarié par la vérification du bon usage des outils mis à sa disposition s'avère donc nécessaire, mais la position sibylline de la Cour de cassation ne permet pas à ce jour de déterminer ce qu'est un « *risque ou évènement particulier* ». En tout état de cause, les personnes entrant dans la sphère d'intimité du salarié sont soumises au secret professionnel.

- **La cybersurveillance implique le respect du secret professionnel**

Une catégorie du personnel peut accéder de manière tout à fait légitime à des informations personnelles concernant les salariés, sans pour autant se voir opposer le respect de la vie privée ou l'atteinte au secret des correspondances. Il s'agit des personnes en charge de la sécurité et de la continuité du SI. Dans un arrêt en date du 17 décembre 2001, la Cour d'appel de Paris s'est clairement prononcée en ce sens en rappelant qu'il « *est dans la fonction des administrateurs de réseaux d'assurer le fonctionnement normal de ceux-ci ainsi que leur sécurité ce qui entraîne, entre autre, qu'ils aient accès aux messageries et à leur contenu, ne serait-ce que pour les débloquer ou éviter des démarches hostiles* », et précisant que « *la préoccupation de la sécurité du réseau justifiait que les administrateurs de systèmes et de réseaux fassent usage de leurs positions et des possibilités techniques dont ils disposaient pour mener les investigations et prendre les mesures que cette sécurité imposait* ».

Toutefois, les administrateurs réseaux, compte tenu de leurs pouvoirs, sont soumis au secret professionnel dans le cadre des informations relevées dans l'exercice de leurs fonctions, et par conséquent « *la divulgation du contenu des messages, et notamment du dernier qui concernait le conflit latent dont le laboratoire était le cadre, ne relevait pas de ces objectifs* », ce qui caractérise donc en l'espèce une atteinte au secret des correspondances et une violation de l'intimité de la vie privée de la personne concernée.

La Cour a également relevé le caractère aggravé de cette atteinte, dans la mesure où « *le laboratoire s'était donné à lui-même la règle déontologique de ne pas lire le contenu du courrier électronique, sauf mise en cause de la sécurité du système* », ce qui n'était pas le cas. Le secret peut et doit donc être opposé par le salarié dépositaire à son employeur, dans le cadre des informations obtenues dans l'exercice de ses fonctions.

[48] Cour de cassation, Chambre sociale, 17 mai 2005

Le secret professionnel est également un droit de ne rien dire

De par sa nature même, le secret doit être à tout prix conservé par celui qui en est le dépositaire. Toutefois, dans certaines situations, celui-ci peut être confronté à l'autorité publique qui en exige la communication. Ce cas de figure peut atteindre des proportions particulièrement délicates et complexes lorsque la loi elle-même semble faire obligation au dépositaire du secret de la révéler.

L'opposabilité du secret professionnel à l'autorité publique doit se faire avec prudence

- **L'opposabilité du secret à la force publique n'est pas envisageable**

On entend par force publique l'ensemble des services de l'Etat qui sont chargés du maintien de l'ordre et de la sécurité. Selon plusieurs dispositions du Code de procédure pénale, le procureur de la République, le juge d'instruction ou l'officier de police judiciaire peuvent requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique qui sont susceptibles de détenir des documents intéressant l'enquête, y compris ceux issus d'un système informatique ou d'un traitement de données nominatives, la remise de documents, sans que puisse leur être opposée, sans motif légitime, l'obligation au secret professionnel (voir articles 60-1 et suivants). La loi est hélas muette est ce qui concerne la notion de « *motif légitime* ». Cette tâche délicate revient donc une fois de plus à la jurisprudence. S'il a ainsi, par exemple, été décidé que les officiers de police judiciaire agissant sur les réquisitions du procureur de la République dans le cadre d'une enquête préliminaire (pénale donc) ne pouvaient se voir opposer le secret bancaire[49], celui-ci n'en demeurerait pas moins opposable au juge civil et constitue dès lors un empêchement légitime[50].

De la même façon, le secret professionnel auquel sont tenus les fonctionnaires de l'administration des postes et des télécommunications ne peut être opposé au procureur de la République[51], agissant dans l'intérêt de l'ordre public. Enfin, les organismes de sécurité sociale ne peuvent pas opposer le secret professionnel aux experts commis en justice afin de procéder à des investigations dans les dossiers de la sécurité sociale, et de prendre connaissance des pièces et documents médicaux nécessaires à leur mission[52].

Le refus de répondre dans les meilleurs délais à de telles réquisitions (c'est le cas lorsqu'on oppose le secret professionnel sans motif légitime) est puni d'une amende de 3 750 euros ; la responsabilité pénale de l'entreprise elle-même peut également être mise en oeuvre. Néanmoins, plusieurs catégories de dépositaires du secret peuvent l'opposer à ces autorités qui devront impérativement recueillir leur consentement préalable. Il s'agit des avocats (article 56-1 du Code de procédure pénale), des entreprises de presse ou de communication audiovisuelle (article 56-2), ainsi que des médecins[53], notaires, avoués ou huissiers (article 56-3).

[49] Cour de cassation, Chambre criminelle, 27 avril 1994 : *Bull. crim*. n°152
[50] Cour de cassation, Chambre commerciale, 13 juin 1995 : *Bull. civ.* IV, n°172
[51] Cour de cassation, Chambre criminelle, 5 avril 1962 : *Bull. crim*. n°170
[52] Cour de cassation, Chambre sociale, 31 janvier 1963 : D. 1963.471
[53] Cour de cassation, Chambre criminelle, 20 janvier 1976 : *Bull. crim*. n°23 : les juges ne peuvent prescrire le versement d'un dossier hospitalier aux débats sans violer le secret professionnel, seul le médecin expert commis par eux pouvant prendre connaissance desdites pièces.

▪ **L'opposabilité du secret à la justice est très encadrée**

Depuis plus d'un siècle, la jurisprudence reconnaît régulièrement aux témoins le droit – voire même le devoir – d'opposer en justice les faits dont ils auraient eu connaissance dans le cadre de leurs fonctions et recueilli à titre de confidence[54], ce qui ne les dispense cependant pas de comparaître en justice et d'indiquer si les réponses qui leur sont demandées sont soumises ou non au secret professionnel. A la lueur de la position de la Cour de cassation, il peut être recommandé de conserver, même devant le tribunal, le secret dont on est dépositaire, dans la mesure où la divulgation d'une information protégée peut être de nature à entraîner la nullité de la procédure engagée[55]. Il reviendra en tout état de cause aux tribunaux de décider du caractère secret des informations dont la divulgation a été refusée par le témoin[56].

▪ **L'opposabilité à l'administration financière et fiscale est délicate**

Le secret professionnel peut être opposé à l'administration fiscale pour certaines informations échappant au périmètre d'une inspection éventuelle. Par exemple, en combinant les articles 371 Y annexe II du Code général des Impôts[57] et L86A du Livre des Procédures Fiscales[58], on peut déduire que les documents comptables tenus par les adhérents d'associations agréées doivent comporter notamment l'identité du client et la nature des prestations fournies, cette dernière indication n'étant néanmoins pas exigée des adhérents soumis au secret professionnel en application de l'article 226-13 du Code pénal. Les documents comptables peuvent donc mentionner simplement l'identité de la personne et non la nature des actes accomplis. Ceci est valable par exemple pour les vétérinaires[59], ou encore les médecins[60]. Une limite a cependant été reconnue par la jurisprudence : un médecin qui porterait des mentions soumises au secret professionnel sur ses écritures comptables ne pourrait pas pour autant en interdire la lecture aux inspecteurs du FISC[61].

Il en résulte que le secret professionnel ne peut pas être utilisé pour dissimuler une fraude ou un processus occulte, mais bel et bien pour protéger les personnes concernées par le secret[62]. Pour rappel, le secret professionnel ne peut pas être opposé non plus à l'Autorité des marchés financiers. Cette restriction, découlant de l'article L621-9-3 de la Loi du 1er août 2003 dite « de Sécurité Financière », s'étend notamment aux entreprises de marché, chambres de compensation ou corps de contrôle, et a pour effet explicite de délier les commissaires aux comptes de leur obligation au secret professionnel à l'égard de l'AMF.

---

[54] Cour de cassation, Chambre criminelle, 6 juillet 1894 : *DP* 1899.1.171
[55] Cour de cassation, Chambre criminelle, 15 septembre 1987 : *Bull. crim*. n°311
[56] Voir notamment Cour de cassation, Chambre criminelle, 6 décembre 1956 : *Bull. crim*. n°820
[57] « […] *les ordres et organisations mentionnés à l'article précité s'obligent notamment à faire à leurs ressortissants les recommandations suivantes : […] 2º En ce qui concerne les adhérents non soumis au secret professionnel en application des articles 226-13 et 226-14 du code pénal, mentionner, outre les indications prévues par l'article 1649 quater G du code général des impôts, la nature des prestations fournies* ».
[58] « *La nature des prestations fournies ne peut faire l'objet de demandes de renseignements de la part de l'administration des impôts lorsque le contribuable est membre d'une profession non commerciale soumis au secret professionnel en application des articles 226-13 et 226-14 du code pénal* ».
[59] Cour administrative d'appel de Marseille (précitée), 1er février 1999
[60] Le secret professionnel auquel le médecin est soumis est général et absolu, et que le fait pour un médecin de ne pas inscrire le nom de ses clients en face des sommes perçues à titre d'honoraires ou de refuser de communiquer à l'inspecteur les noms qui y figurent ne rend pas sa comptabilité régulière (Conseil d'Etat, 20 novembre 1959 : D. 1960.157).
[61] Cour de cassation, Chambre criminelle, 11 février 1960 : *Bull. crim*. n°85
[62] Cour administrative d'appel de Nantes, 2 mai 1996 : *Gaz. Pal*. 1997.2.604

▪ **L'opposabilité à la CNIL est possible, mais sous certaines conditions**

L'opposabilité du secret professionnel à la CNIL est une possibilité reconnue par la Loi Informatique et Libertés elle-même. L'article 21 alinéa 3 de la loi prévoit en effet explicitement que « *sauf dans les cas où elles sont astreintes au secret professionnel, les personnes interrogées dans le cadre des vérifications faites par la commission en application du f du 2° de l'article 11 sont tenues de fournir les renseignements demandés par celle-ci pour l'exercice de ses missions* ».

Cette disposition n'était pas prévue littéralement dans la version initiale de la loi, mais elle n'a finalement été que rappelée par la loi du 6 août 2004 dans la mesure où les personnes soumises au secret pouvaient déjà opposer le secret professionnel à la CNIL, ainsi que l'a indiqué le Conseil constitutionnel dans une décision[63] en date du 29 juillet 2004. Dans celle-ci, le Conseil a rappelé que « *l'invocation injustifiée du secret professionnel pourrait constituer une entrave passible des peines prévues par l'article 51 nouveau de la loi du 6 janvier 1978* ». Il s'agit donc d'une limite au caractère opposable du secret professionnel.

Lorsque le secret professionnel est opposé à la CNIL par une personne qui en est le dépositaire au sens de la loi, le procès-verbal dressé par les personnes en charge de la vérification mentionne cette opposition, ainsi que les dispositions d'ordre légal ou réglementaire invoquées par la personne contrôlée, de même que les données qu'elle estime couvertes par ces dispositions[64]. Cette personne devra donc non seulement se référer aux règles propres au secret professionnel de l'article 226-13 du Code pénal qui s'imposent à elles en tant que dépositaire du secret, mais aussi expliquer en quoi un texte la soumet au secret du fait de son état ou de sa profession. Il sera alors nécessaire de s'appuyer sur tout document ayant valeur réglementaire, à savoir la loi elle-même, les codes de déontologie professionnelle, ou encore, dans une moindre mesure, le contrat (qui devra préciser dans quel cadre la personne est soumise au secret). Si la personne ne peut pas justifier son opposition au contrôle, alors cette opposition sera réputée avoir été formée sans motif légitime, et pourra donc aboutir à la mise en œuvre de la responsabilité pénale de la personne pour entrave. Il peut être judicieux pour les entreprises d'anticiper ce type de contrôle en élaborant des procédures internes décrivant quelles seront les personnes habilitées à répondre aux questions des enquêteurs.

L'opposabilité du secret professionnel n'est pas absolue

▪ **Exercice des droits de la défense**

Le secret professionnel peut être rompu dans le cadre de l'exercice de ses droits par la défense. C'est en ce sens que s'est prononcée la Cour d'appel de Douai, dans un arrêt du 26 octobre 1951, pour laquelle on ne peut refuser à qui que ce soit le droit de se défendre. La Cour considère cette liberté comme essentielle et ne pouvant être mise en échec par les règles relatives au secret professionnel. De la même manière, l'avocat[65], ou encore le médecin[66], peuvent briser le secret professionnel en justice lorsqu'ils sont personnellement mis en cause par un client, afin de se justifier de l'accusation dont ils font l'objet.

[63] Décision n° 2004-499 DC du 29 juillet 2004
[64] Article 69 du Décret n°2005-1309 du 20 octobre 2005
[65] Cour de cassation, Chambre criminelle, 29 mai 1989 : *Bull. crim*. n°218
[66] Cour de cassation, Chambre criminelle, 20 décembre 1967 : *Bull. crim*. n°338

Ce droit a également été reconnu, de manière beaucoup plus large, à l'ensemble des salariés qui peuvent produire en justice tout document dont ils ont eu connaissance à l'occasion de leurs fonctions, lorsque cela est strictement nécessaire à l'exercice des droits de leur défense dans le cadre d'un litige les opposant à leur employeur[67].

- **Abus de droit constitutif du délit d'entrave**

Le fait d'opposer abusivement, c'est-à-dire sans motif légitime, le secret professionnel, est passible d'une amende de 3 750 euros (équivaut à un refus de répondre dans les meilleurs délais à l'autorité qui en fait la demande). Dans le domaine de compétences de la CNIL, le Conseil constitutionnel, dans la décision précitée, a affirmé que l'invocation injustifiée du secret professionnel pouvait constituer une entrave passible des peines prévues par l'article 51 de la nouvelle loi Informatique et Libertés. Au titre de cette disposition, « *est puni d'un an d'emprisonnement et de 15 000 € d'amende le fait d'entraver l'action de la Commission nationale de l'informatique et des libertés […] en refusant de communiquer à ses membres ou aux agents habilités […] les renseignements et documents utiles à leur mission, ou en dissimulant lesdits documents ou renseignements, ou en les faisant disparaître* ».

Le recours au secret professionnel devra donc être manié avec précaution pour pouvoir être opposé à la CNIL, c'est-à-dire exclusivement afin de protéger les données sensibles des personnes dont les données sont traitées par l'organisme, et non afin de dissimuler un traitement plus ou moins opaque, faute de quoi le délit d'entrave pourrait fort bien être constitué.

Le secret professionnel peut cependant être légitimement rompu

- **La révélation spontanée du secret professionnel est autorisée dans certains cas**

La loi prévoit la possibilité de révéler le secret sans pour autant que cette divulgation n'engage la responsabilité de son dépositaire. Cette permission de divulguer le secret est prévue à l'article 226-14 du Code pénal qui prévoit trois circonstances spécifiques[68] :

- l'une d'entre elles ne concerne que les médecins, lesquels peuvent porter à la connaissance du procureur de la République les sévices ou privations d'ordre physique ou psychique qu'ils ont constatés dans l'exercice de sa profession et leur permettant de présumer que des violences physiques, sexuelles ou psychiques de toute nature ont été commises. La révélation de telles informations est néanmoins soumise à l'accord préalable de la victime sauf lorsque celle-ci est mineure ;

- la seconde est reconnue « *aux professionnels de la santé ou de l'action sociale qui informent le préfet et, à Paris, le préfet de police du caractère dangereux pour elles-mêmes ou pour autrui des personnes qui les consultent et dont ils savent qu'elles détiennent une arme ou qu'elles ont manifesté leur intention d'en acquérir une* » ;

[67] Cour de cassation, Chambre sociale, 30 juin 2004

[68] Rappelons qu'il est également possible de révéler un secret si son propriétaire a donné son consentement de manière explicite. Il importera donc de s'en préconstituer la preuve, qui ne se présumera jamais, en demandant par exemple à cette personne de rédiger une attestation démontrant son accord de lever le secret, et dans quelles circonstances celle-ci est possible.

- dans le dernier cas, toute personne soumise au secret peut décider de le divulguer auprès des autorités judiciaires, médicales ou administratives pour dénoncer des privations ou des sévices, y compris d'ordre sexuel, dont elle a eu connaissance et « *qui ont été infligées à un mineur ou à une personne qui n'est pas en mesure de se protéger en raison de son âge ou de son incapacité physique ou psychique* ». La Cour de cassation a rappelé sans contredit que ces personnes sont « *libres de fournir leur témoignage sans s'exposer à aucune peine* ».

▪ **La loi n'impose pas la révélation spontanée du secret professionnel**

Peut-on refuser de dénoncer un crime au nom du respect du secret professionnel ? Pour rappel, la non-dénonciation de crime ou de mauvais traitement recouvre deux comportements punis de 3 ans de prison et de 45.000 euros d'amende chacun (article 434-1 du Code pénal). Ces comportements sont les suivants :

- ne pas informer les autorités judiciaires ou administratives d'un crime dont il est encore possible de prévenir ou de limiter les effets, ou dont les auteurs sont susceptibles de commettre de nouveaux crimes qui pourraient être empêchés ;
- ne pas informer les autorités judiciaires ou administratives de privations, de mauvais traitements ou d'atteintes sexuelles infligés à un mineur de quinze ans ou à une personne qui n'est pas en mesure de se protéger en raison de son âge, d'une maladie, d'une infirmité, d'une déficience physique ou psychique ou d'un état de grossesse

Le caractère secret des informations dont la personne est dépositaire peut être opposé dans chacun de ces deux cas, sans qu'elle puisse être poursuivie pour non-dénonciation de crime. Cette possibilité est expressément prévue par la loi, qui exempt même les personnes soumises au secret de l'obligation de dénoncer les crimes commis sur les mineurs de quinze ans (à titre de comparaison, les membres de la famille d'un criminel ne sont pas non plus soumises à l'obligation de dénoncer un crime, *sauf s'il a été commis sur un mineur de quinze ans*. Cette exception ne vaut pas pour les personnes soumises au secret). Les personnes soumises au secret restent néanmoins libres de fournir leur témoignage, dans la mesure où leur conscience les guide.

Conclusion

L'opposabilité du secret professionnel peut être perçue par les uns comme une nécessité absolue d'ordre éthique, et par les autres comme une stratégie subtilement manipulable. Or, le secret professionnel, qui était à l'origine une règle exclusivement déontologique, un rempart éthique pour protéger ceux qui n'avaient d'autre choix que de se confier auprès d'un tiers démontrant son engagement à respecter leur secret, a été érigé au rang de loi.

Hélas, au fil des époques, certains détenteurs du secret consacrés par la loi ont été tentés de détourner ces règles fondamentales du respect des libertés fondamentales de leurs congénères, notamment afin de masquer leurs propres faits, dont ils auraient pu avoir à répondre en justice.

Dans ce dernier cas, et alors que l'invocation de principes d'ordre déontologique semble empêcher leur propre respect, il est fait appel à la sagesse des juges ou aux recommandations d'autorités morales supérieures pour remettre le dépositaire du secret dans le droit chemin. Dans ce cas, pour écarter le détournement des règles d'ordre déontologique dont ils sont les garants, un ultime recours semble pouvoir être invoqué : celui de l'éthique individuelle …

Pour information

Les entreprises ayant participé à ces réflexions sont : AG2R et SNCF.

Annexe 3

- ***L'enquête Déontologie***

Préambule

Contexte

Quelles bonnes pratiques mettre en place pour garantir un usage éthique et conforme des Systèmes d'information ?

L'importance et l'encadrement juridique des technologies de l'information et de la communication impliquent que les entreprises ne peuvent plus négliger les risques liés à l'usage de ces technologies. Au-delà des enjeux techniques, ces risques multiples touchent le fonctionnement global des entreprises et leurs capacités à remplir leurs obligations contractuelles, légales et réglementaires.

Objectif

L'enquête a été diffusée auprès des Directeurs des Systèmes d'Information (DSI), des Déontologues, des Responsables de la Sécurité des (RSSI) et des Juristes.

Les 5 questions qui leur ont été posées avaient pour objectif de nous aider à dresser un tableau des tendances en cours dans les grandes entreprises en matière d'usages du SI.

Pour ce faire, le questionnaire a été orienté de manière à nous permettre de définir :

- le niveau de connaissance des entreprises de leur environnement juridique et des risques liés à un usage non-conforme de leurs Systèmes d'information pouvant engager leur responsabilité, voire celle du sondé,
- les moyens mis en œuvre par l'entreprise pour assurer sa conformité juridique.

Traitement des réponses

Les réponses à cette enquête ont fait l'objet de la synthèse ci-après. Les entreprises qui ont participé à l'enquête sont citées au début du document mais la restitution des réponses est anonyme, présentée sous forme de tableau synthétique.

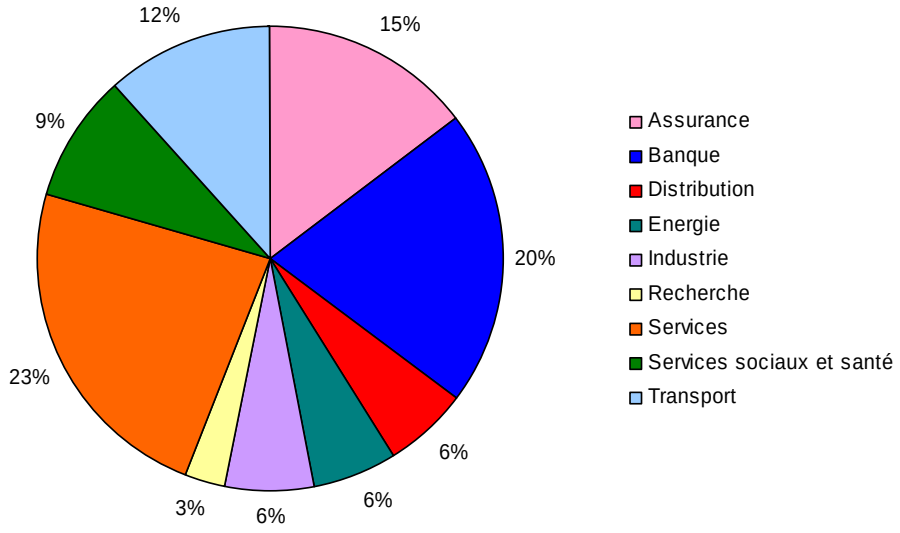
L'analyse des réponses nous a permis de dégager les tendances des grandes entreprises en matière de déontologie des usages des SI.

Présentation des participants

34 entreprises ont participé à l'enquête

Entreprise	Secteur d'activité
AGF	Assurance
Air France	Transport
Alcatel	Services
Amadeus	Transport
Aviva	Assurance
Banque de France	Banque
BNP Paribas	Banque
Canam	Assurance
Carglass	Services / Automobile
CNAM – TS	Services sociaux et santé
CNAV - TS	Services sociaux et santé
CNRS	Recherche
Cofinoga	Banque
France Télécom	Services
Euro Disney	Services
Essilor	Industrie
Euler - Hermès	Banque
General Electric Health Care	Industrie
Groupe Caisse des Dépôts	Banque
Groupe La Poste	Services
Groupement des Mousquetaires	Distribution
Lagardère	Services
LVMH	Distribution / Luxe
Maaf	Assurance
OSEO - BDPME	Banque
RATP	Transport
RTE	Energie
SMABTP	Assurance
Société Générale	Banque
STEF - TFE	Transport
Thomson	Services
Total	Energie
Unédic	Services sociaux et santé
Vedior Bis	Services

Participation par secteur d'activité (en %)



Présentation de l'enquête

Introduction

Informations utiles	***Votre fonction*** ***Votre entreprise / secteur d'activité*** ***Le CA et le nombre de salariés de votre entreprise***

Thème 1

Perception des enjeux	***Selon vous, avez-vous une bonne perception des enjeux liés à la conformité juridique des usages du SI ?*** ***a) « Je suis conscient(e) des risques juridiques liés au SI »*** ☐ Plutôt d'accord ☐ Plutôt pas d'accord ☐ Sans opinion ***b) « Je suis certain(e) d'avoir identifié les principales législations applicables »*** ☐ Plutôt d'accord ☐ Plutôt pas d'accord ☐ Sans opinion ***c) « Le travail de veille légale et jurisprudentielle est assuré de manière régulière et suffisante »*** ☐ Plutôt d'accord ☐ Plutôt pas d'accord ☐ Sans opinion ***d) « Je sais que la cyber surveillance est très strictement encadrée, mais ces règles particulières me paraissent confuses »*** ☐ Plutôt d'accord ☐ Plutôt pas d'accord ☐ Sans opinion ***e) « La délimitation entre ma responsabilité civile et pénale propre et celle de mon entreprise est claire »*** ☐ Plutôt d'accord ☐ Plutôt pas d'accord ☐ Sans opinion
Remarque	

Thème 2

Risques d'usages non conformes du SI	***Parmi les risques suivants, sur lesquels avez-vous travaillé au cours des 18 derniers mois (cocher les cases) ?*** ☐ Secret des correspondances (conservation des logs, accès aux contenus…) : ☐ Fiabilité des données financières (SOX-Act, loi Mer…) : ☐ Traitements de données personnelles (déclaration, sécurité…) : ☐ Cyber surveillance (formalités préalables, proportionnalité et vie privée du salarié…) : ☐ Respect de la propriété intellectuelle (téléchargements, licences de logiciels…) : ☐ Régulation de l'usage quantitatif du SI (durées, taille des fichiers, spamming…) : ☐ Régulation de l'usage qualitatif du SI (filtres, données enregistrables…) : ☐ Archivage des informations selon les dispositions légales et réglementaires : ☐ Autres :
Remarque	

Thème 3

Gestion des risques	***Quelles solutions organisationnelles avez-vous retenues pour garantir un usage juridiquement conforme de votre SI ?*** ***a) « Notre entreprise a identifié une fonction en interne dédiée à la prévention des risques de non-conformité (sanction judiciaire pour manquement à une obligation légale, réglementaire ou professionnelle) »*** ☐ Oui ☐ Non *Si oui, indiquez son rattachement* : *Si oui, indiquez le périmètre de la fonction (modes d'actions et domaines)* : *Si oui, cette fonction est-elle fréquemment en contact avec la fonction informatique ?* ***b) « Nous avons nommé un Déontologue »*** ☐ Oui ☐ Non ☐ Pas encore, mais nous l'envisageons ***c) « Nous envisageons de nommer un Correspondant Informatique et Libertés »*** ☐ Oui ☐ Non ☐ Peut-être ***d) « Mon entreprise se donne les moyens humains et financiers suffisants pour garantir un usage déontologique satisfaisant du SI »*** ☐ Plutôt d'accord ☐ Plutôt pas d'accord ☐ Sans opinion
Remarque	

Thème 4

Moyens mis en œuvre	***Quels moyens ont été mis en œuvre dans votre entreprise pour assurer la conformité juridique des usages de votre SI ?*** ***a) Avez-vous une charte d'usage du SI ?*** ☐ Oui ☐ Non ☐ En cours ▪ *Selon vous, est-elle juridiquement opposable (expliquer)?* ▪ *Comment l'avez-vous intitulée ?* ▪ *Est-elle imposée à tous les utilisateurs du SI : stagiaires, prestataires externes, intérimaires, clients, fournisseurs et autres parties prenantes ?* ***b) Avez-vous déjà sanctionné les manquements à votre charte ?*** ☐ Oui ☐ Non ***c) Avez-vous formalisé un processus, des procédures destinées à garantir la conformité juridique du SI (LCEN, Loi Informatique et Libertés, SOX…) ?*** ☐ Oui ☐ Non ☐ En cours *Si oui, lesquels ?* ***c) Mettez-vous en œuvre une politique de communication ?*** ☐ Oui ☐ Non ☐ En cours
Remarque	

Conclusion

Actions à venir	***Selon vous, quels seraient les prochains chantiers à ouvrir, dans les années à venir, pour vous permettre de prévenir et gérer au mieux les risques liés à des usages juridiquement non-conformes de votre SI ?***

Synthèse des réponses

Thème 1

Perception des enjeux liés à la conformité juridique des usages du SI (en %)	**Oui**	**Non**	**Sans opinion**	**Total**
- Conscient(e) des risques juridiques liés au SI	94%	6%	0%	**100%**
- Certain(e) d'avoir identifié les principales législations applicables	62%	38%	0%	**100%**
- Travail de veille légale et jurisprudentielle régulier et suffisant	53%	44%	3%	**100%**
- Règles sur la cybersurveillance perçues comme confuses	53%	44%	3%	**100%**
- Délimitation claire entre la responsabilité civile et pénale du sondé et celle de l'entreprise	32%	68%	0%	**100%**
Moyenne	**59%**	**40%**	**1%**	**100%**

Thème 2

Risques identifiés d'usages juridiquement non conformes du SI et faisant l'objet d'une certaine vigilance (en %)	**Oui**	**Non**	**Total**
- Secret des correspondances (conservation des logs, accès aux contenus…)	74%	26%	**100%**
- Fiabilité des données financières (SOX-Act, loi Mer…)	53%	47%	**100%**
- Traitements de données personnelles (déclaration, sécurité…)	94%	6%	**100%**
- Cybersurveillance (formalités préalables, proportionnalité et vie privée du salarié…)	65%	35%	**100%**
- Respect de la propriété intellectuelle (téléchargements, licences de logiciels…)	65%	35%	**100%**
- Régulation de l'usage quantitatif du SI (durées, taille des fichiers, spamming…)	71%	29%	**100%**
- Régulation de l'usage qualitatif du SI (filtres, données enregistrables…)	62%	38%	**100%**
- Archivage des informations selon les dispositions légales et réglementaires	68%	32%	**100%**
Moyenne	**69%**	**31%**	**100%**

Thème 3

Gestion des risques, solutions organisationnelles retenues pour garantir un usage juridiquement conforme du SI (en %)	**Oui**	**Non**	**Oui, peut-être / Sans opinion**	**Total**
- Identification d'une fonction interne dédiée à la prévention des risques de non-conformité (sanction judiciaire pour manquement à une obligation légale, réglementaire ou professionnelle)	56%	44%	0%	**100%**
- Contact de la fonction dédiée avec la fonction informatique	56%	44%	0%	**100%**
- Existence d'une fonction de déontologue dans l'entreprise	29%	59%	12%	**100%**
- Existence d'un Correspondant Informatique et Libertés (déjà fait ou envisagé)	15%	26%	59%	**100%**
- Moyens humains et financiers suffisants pour garantir un usage déontologique satisfaisant du SI	53%	29%	18%	**100%**
Moyenne	**42%**	**41%**	**18%**	**100%**

Thème 4

Moyens mis en œuvre pour assurer la conformité juridique des usages du SI	**Oui**	**Non**	**En cours**	**Total**
- Elaboration d'une charte d'usages	82%	3%	15%	**100%**
- Adossement de la charte au règlement intérieur (donc juridiquement opposable)	53%	44%	3%	**100%**
- Imposition de la charte à tout ou partie des utilisateurs (prestataires externes, stagiaires, intérimaires, clients, fournisseurs et autres parties prenantes)	85%	12%	3%	**100%**
- Mise en œuvre des sanctions prévues par la charte en cas de non respect de celle-ci	41%	59%	0%	**100%**
- Formalisation de processus et/ou de procédures destinés à garantir la conformité juridique du SI (LCEN, Loi Informatique et Libertés, Sarbannes-Oxley…)	53%	35%	12%	**100%**
- Mise en œuvre d'une politique de communication sur la charte	59%	18%	24%	**100%**
Moyenne	**49%**	**28%**	**7%**	**100%**

Conclusion

Actions envisagées dans les années à venir pour mieux prévenir et gérer les risques liés à des usages juridiquement non-conformes du SI
- Archivage des courriels - Renforcement de la protection des données personnelles, nominatives et financières + suivi de la propriété intellectuelle - Développement de la gestion du poste de travail pour un usage plus encadré (utilisation messagerie, accès internet…) - Mise en place de politiques de sensibilisation globales et évolutives sur l'utilisation des outils informatiques et du SI, information et suivi sur la charte et renforcement des sanctions en cas de non respect - Cryptage des données - Accroissement du niveau de contrôle des délégations d'accès - Mise en place d'un CIL et communication sur la loi Informatique et Libertés - Structuration des process / des règles / des moyens - Prise en compte des risques liés aux mésusages dans la démarche Contrôle interne - Développement d'un site intranet d'information IT, spécialisé dans l'information juridique - Intégration de points de contrôles déontologiques dans les processus de développement et de mise en œuvre - Mise en place d'un outil de gestion centralisé des identités et des accès pour un meilleur contrôle des usages du SI - Déclinaison de la politique de sécurité sous l'angle juridique - Automatisation du contrôle de conformité des licences logiciel

Axes de développement futurs susceptibles de s'inscrire dans le cadre d'un second groupe de travail
- Développement d'une charte type adaptable en fonction de l'environnement et d'une charte spécifique "SI" - Développement d'un guide décrivant clairement les responsabilités, le rôle et le statut du CIL - Développement d'un kit opérationnel de mise en œuvre d'une démarche déontologique et préparation d'un support permettant d'initier une démarche plan progrès et d'assurer la conduite du changement (kit de communication et de formation) - Mise en place d'une veille juridique et jurisprudentielle

Complément (à télécharger sur le site du CIGREF)

• *Exemples de chartes*

Nous vous invitons à consulter le site du CIGREF[69] sur lequel vous trouverez trois exemples de chartes appliquées dans les domaines associatif, public et privé. La finalité est d'illustrer la mise en œuvre opérationnelle d'une démarche de déontologie appliquée aux Systèmes d'information.

Vous trouverez :

- La charte de présentation des règles et obligations des utilisateurs en matière d'utilisation du *système de base de connaissances,* élaborée par l'Association Française de l'Audit et du Conseil Informatique (AFAI), en collaboration avec le Cabinet d'avocats Bensoussan. Adaptable dans n'importe quelle structure, cette charte peut évoluer dans sa granularité, son périmètre et sa focalisation. Le Groupe La Poste, par exemple, l'a adaptée afin de pouvoir l'appliquer en son sein.
- La charte du Conseil Général des Hauts de Seine : spécifique à l'utilisation des Systèmes d'information, elle s'applique tant aux agents qu'à la Collectivité.
- La charte d'Air France : annexée au règlement intérieur, elle s'applique à tous les salariés basés en France métropolitaine et outre mer, ainsi qu'aux stagiaires et aux intérimaires.

[69] www.cigref.fr