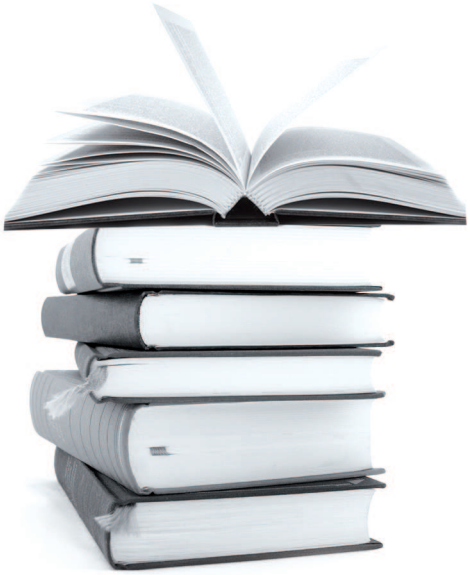
tome VIII

les assises
de la sécurité et des systèmes d'information

réalisé par

hapsis



Le Livre Bleu

Secret et Confidentialité à l'ère du numérique

Monaco du 5 au 8 octobre 2011

le cercle
européen de la sécurité et des systèmes d'information

Face à la menace,
vous n'êtes pas seul...

Sécurité des systèmes d'information :
enjeux, perspectives, retours d'expérience.

Face à la complexité croissante des « cyber-menaces », il est devenu essentiel de mettre en commun expériences, réflexions, compétences pour relever les défis stratégiques de demain en matière de sécurité des systèmes d'information.

Le Cercle, communauté d'utilisateurs et de décideurs du secteur, fédère des professionnels et compte plus de 1000 membres actifs : responsables, directeurs de la Sécurité des Systèmes d'Information, experts en sécurité, présents chaque année aux Assises.
Il vise l'élargissement des compétences et permet les échanges sur tous les enjeux liés aux risques, solutions et moyens de protection des patrimoines numériques des entreprises et institutions. Sa mission consiste également à détecter des solutions innovantes et à en favoriser le développement.
Prenez part aux rendez-vous du Cercle : un levier pour renforcer votre réseau, approfondir votre réflexion sur la stratégie des Systèmes d'Information et faire les bons choix.

Pour plus d'informations : 01 41 93 07 07 - www.lecercle.biz

comexposium
un événement
les assises
de la sécurité et des systèmes d'information

SOMMAIRE

1. INTRODUCTION 2

2. LES ENJEUX ET LA DIALECTIQUE 4
   - 2.1. Préambule 4
   - 2.2. L'ère numérique : de l'âge de pierre à l'âge du silicium ? 6
   - 2.3. Distinguer secret et confidentialité ? 7
   - 2.4. Les 3 sphères : professionnelle, privée, publique 9
   - 2.5. Les 3 générations : baby boomers / génération X / génération Y 10
   - 2.6. Gestion de la confidentialité et sécurité / sûreté 12
   - 2.7. Quelle place pour la cyber-éthique ? 14
   - 2.8. L'exemple de la santé 14
   - 2.9. Synthèse 18

3. CADRER LA PROBLÉMATIQUE 19
   - 3.1. Secret et transparence : au cœur de la gestion des organisations ? 19
   - 3.2. Les textes de loi sur le secret et la confidentialité : le trop plein ? 22
   - 3.3. Le rôle des normes internationales : un langage enfin partagé ? 26
   - 3.4. Des référentiels nationaux : au-delà du domaine public ? 28
   - 3.5. Synthèse 31

4. DU PRINCIPE À LA PRATIQUE 34
   - 4.1. Introduction 34
   - 4.2. Quelle importance pour les questions de confidentialité ? 35
   - 4.3. Comment aborder le problème ? 37
   - 4.4. Et pourtant 43
   - 4.5. Pour aller plus loin : la contrainte et les nouveaux usages 49
   - 4.6. Synthèse 54

5. CONCLUSION 55
   - 5.1. À quoi sert la protection des données ? 55
   - 5.2. Un pré-requis : « la transversalité » 56
   - 5.3. Une exigence : « la contextualisation » 56
   - 5.4. Une obligation : « le pragmatisme et la simplicité » 57
   - 5.5. Une vigilance : « l'externalisation des services » 57
   - 5.6. L'équilibre des forces : « des opportunités et des menaces » 58
   - 5.7. L'information, le numérique et le pouvoir 59

6. ANNEXE : L'ÉCHANTILLON 60
   - 6.1. Secteurs d'activités 60
   - 6.2. Entité d'appartenance 60
   - 6.3. Titre et fonctions 61

Le secret
(Auguste Rodin – 1840-1917)

1- INTRODUCTION

Depuis 2004, les enquêtes du Cercle Européen de la Sécurité et des Systèmes d'Information analysent l'évolution des rôles et des activités des professionnels de la Sécurité des Systèmes d'Information (SSI). Véritable observatoire d'une fonction clé des entreprises et des administrations, elles alimentent surtout la réflexion autour de thématiques majeures sélectionnées par le Comité de Pilotage des Assises et formalisées dans les Livres Bleus. Nos travaux se sont, jusqu'alors, déroulés en 3 grandes phases :

Phase d'exploration et d'introspection en 3 étapes :
- le management stratégique des cyber-risques (2004)
- les indicateurs et tableaux de bord en Sécurité SI (2005)
- les grands défis des professionnels de la Sécurité SI (2006)

Phase d'ouverture et de découverte en 2 étapes :
- les pouvoirs en sécurité / sûreté (2007)
- la sécurité globale (2008)

Phase de maîtrise et de professionnalisation en 2 étapes :
- la culture des risques informatiques / informationnels (2009)
- la dimension économique de la Sécurité des Systèmes d'Information (2010)

À l'issue de ces sept années de travail, l'ensemble des documents représente plus de 300 pages d'analyses, de questionnements et de recommandations qui restent, pour beaucoup, d'actualité et peuvent servir de référence toujours utile. Les travaux de nature socio-économique menés en 2009 et 2010 méritent aussi d'être approfondis dans le cadre du groupe de travail sur l'Économie sécuritaire de la SSI mis en place en 2010 au sein du Cercle.

Pour 2011, le Comité de Pilotage des Assises a souhaité qu'une nouvelle approche soit retenue et qu'un thème à la fois historique et d'actualité soit traité :

« Secret et confidentialité à l'ère du numérique »

Le sujet est vaste et complexe. Il déborde largement du cadre strict de l'entreprise et de la fonction SSI, qui nous intéresse en premier lieu. Les dimensions sociologique et stratégique prennent une importance accrue au regard des questions techniques, juridiques, humaines et organisationnelles.

L'actualité récente (par exemple les affaires HSBC, Wikileaks, Bercy et News of the World) nous indique que le secret (bancaire, défense, diplomatique, des correspondances, etc.) n'a pas / plus de sens pour certains, ni la même portée. Qu'est-ce qu'un secret ou qu'une donnée confidentielle au XXIème siècle ?

La globalisation et le mode de fonctionnement des entreprises comme des administrations, d'une part renforcent l'exigence de transparence (source de confiance des citoyens, usagers, consommateurs, partenaires, etc.) et d'autre part, obligent à renforcer les contrôles face à des menaces de plus en plus complexes, virtuelles et quasi-anonymes. Quel équilibre peut-on établir entre ouverture et repli sur soi, entre transparence et cloisonnement ?

Pour couronner le tout, l'influence de la génération Y (personnes nées entre 1975 et 1995) n'est pas sans poser de nouveaux défis. Les plus âgés d'entre eux, souvent technophiles, ont acquis des responsabilités. Nombreux sont ceux qui, désormais, ne font plus la différence entre les espaces privé et professionnel. Que penser d'un jeune médecin qui souhaite disposer de résultats d'analyse ou de l'IRM d'un patient sur sa tablette, à son domicile ? Quelle réponse lui apporter ?

Bien sûr, le marché tente d'apporter des solutions. La cryptographie d'hier se doit d'évoluer et ne sera, de toute façon, jamais la panacée. Doit-on « bunkeriser » dans le « cloud » ? Ne faut-il pas mieux tout « surveiller » (logiques du SIEM[1] et du « DLP[2] ») ? Mais le remède n'est-il pas pire que le mal ? Et répond-il vraiment au véritable problème, qui reste souvent comportemental voire éthique ?

Chercher à répondre à ces questions ne peut s'effectuer sans une grande humilité, ni sans rappeler le cadre général surpassant et englobant le monde des entreprises / administrations comme des systèmes d'information et de communication. Il tient en quelques mots clés sur lesquels nous reviendrons : globalisation, complexité, confiance.

« En abordant un sujet brûlant, le Livre Bleu des Assises 2011 sort du cadre strict de la Sécurité des SI des entreprises et des administrations.

C'est une évolution essentielle où la psycho-sociologie prend une part importante. Il nous faut désormais appréhender des paradoxes majeurs qu'ils soient individuels ou collectifs sur l'ouverture et le cloisonnement, la transparence et le secret, la liberté et la responsabilité. »

Gérard Rio
Fondateur des Assises de la Sécurité et des Systèmes d'Information

Le Livre Bleu des Assises 2011 reprend une structure habituelle en trois points :

• Un chapitre introductif positionne les enjeux et détermine la dialectique générale dans une optique historique et sociologique.
• Un chapitre central cadre la problématique dans son ensemble en termes politiques et de management, aux plans juridiques et méthodologiques et synthétise les questions clés pour les DSI / RSSI.
• Un troisième chapitre apporte des éléments de réponses en matière de SSI sur la base des résultats de l'enquête annuelle du Cercle.

Nous nous appuierons aussi sur quelques ouvrages de référence, des études et articles spécialisés et sur les avis de personnalités et d'experts. En particulier, les fondamentaux juridiques du secret et de la confidentialité seront traités par Maître Éric A. Caprioli et Isabelle Cantero.

« Poursuivant notre quête de professionnalisation du secteur de la SSI, nous espérons que ce 8ème volet du Livre bleu des Assises vous permettra de mieux appréhender la gestion des informations confidentielles au sein de vos organisations.

Nous remercions tous ceux qui participent à l'enquête annuelle du Cercle, devenue au fil des ans un véritable outil de benchmarking, et qui apportent à nos travaux des éléments concrets et proches du terrain. »

Bonne lecture !

Pierre-Luc Réfalo
Directeur Associé, Hapsis

[1] Security Incident and Event Management
[2] Data Loss Prevention

2- LES ENJEUX ET LA DIALECTIQUE

2.1. Préambule

2.1.1. La science du secret

Le thème du secret et de la confidentialité renvoie immédiatement aux fondements historiques de la Sécurité des SI, à savoir la cryptographie (*secret* est issu du grec *kryptos* qui signifie aussi *caché*). Prenons cependant garde à bien distinguer la science (cryptologie) de la technique (cryptographie), le mécanisme (chiffrement ou décryptement) de la méthode (cryptanalyse).

On constate en effet parfois des abus de langage menant à l'incompréhension, ou encore des erreurs sur l'usage des termes. Certains barbarismes parfois utilisés, comme le chiffrage ou l'*encryptio*n, ne facilitent pas non plus la compréhension de tous.

La question du vocabulaire est donc essentielle pour ne pas voir l'idéal de protection du secret se perdre dans les méandres de la pensée. Dans son ouvrage « La science du secret[3] » – dont nous recommandons la lecture – Jacques Stern[4] présente un aperçu historique et une vision stratégique des enjeux et des usages de la cryptologie. Il indique en particulier que :

• La cryptologie constitue un paradigme pour toutes les sciences dans la mesure où le monde et l'univers ne sont qu'une grande énigme qu'il convient de déchiffrer avec les bonnes clés.
• Elle a évolué en 3 étapes passant de l'âge artisanal (jusqu'à l'entre-deux-guerres), à l'âge technique (avec la mécanisation puis l'informatisation), puis à l'âge paradoxal (depuis l'avènement de la cryptographie asymétrique dans les années 70)[5].
• Répondant historiquement aux besoins de confidentialité, il ne faut pas oublier que la cryptographie aborde également les questions d'identité, d'authenticité, d'intégrité.
• La cryptographie est une arme dont les travaux et les développements sont liés à l'effort de guerre.
• Elle côtoie les concepts de connaissance, de vérité et de preuve et mène tout droit aux confins de la logique, des mathématiques et de la philosophie.

2.1.2. L'art de communiquer... en toute confidentialité

Le développement de la cryptographie civile a été rendu nécessaire par le déploiement de moyens de communication et de services en ligne exigeant des mesures de protection appropriées :

• Échanges et transactions bancaires
• Téléphonie mobile
• Télévision numérique
• Commerce électronique
• Etc.

Ainsi, la démocratisation de l'informatique et l'avènement de l'Internet représentent pour l'humanité une nouvelle (r) évolution dans l'art de communiquer. Bâtis au fil des siècles et des millénaires, les moyens de communication entre les individus et les organisations ont progressivement réduit les barrières du temps et de l'espace. L'ère numérique les a totalement abolies, souvent pour le meilleur, parfois pour le pire.

---

[3] Éditions Odile Jacob - 1998
[4] Cryptologue et Directeur du Département d'Informatique de l'ENS de 1999 à 2007
[5] « La cryptographie a d'abord été un art. Elle est ensuite devenue une technique. Aujourd'hui, c'est une science. » Jacques Stern - La cryptographie fait partie de notre vie quotidienne - Futura-Science - 2007

Dans son ouvrage – dont nous recommandons aussi la lecture – « La grande conversion numérique[6] », Milad Doueili[7] présente une vision de « non informaticien » sur le développement du numérique et ses impacts sociétaux, économiques, politiques, etc. Il indique en particulier que :

• La prééminence des discours juridiques et technologiques dans les débats sur la gestion de l'environnement numérique, révèle une absence qui ne saurait être comblée que par une voix culturelle, au sens large.
• L'identité numérique est polyphonique et peut être gérée techniquement (il cite OpenID) en laissant aux individus la possibilité de maintenir plusieurs présences différentes au sein du réseau, avec leurs propres authentifications, droits, privilèges.
• Les réseaux sociaux, à l'image de l'agora grecque, proposent des « *centres* » de discussion publics (qui s'interpénètrent) s'appuyant sur quelques principes : un point d'entrée unique et familier, une hiérarchie de droits et de privilèges (entrer, lire, écrire, commenter, etc.), des règles de contrôle (modération, propriété intellectuelle), des outils de gestion (présence, intimité) pour les membres et une charte devant être acceptée pour être admis.

Les questions de sécurité sont abordées de manière assez originale lorsqu'il définit le « *numéricien lettré* » qui le devient, selon lui, par accident. Ce sont ceux qui « *sont chargés de réparer et d'entretenir plusieurs ordinateurs pour les membres de leur famille, pour leurs amis. Toujours de garde quand il y a un problème, ils passent souvent l'essentiel du dîner [...] à configurer pour un voisin un réseau sans fil protégé, à mettre à niveau une machine, ou à éliminer les logiciels espions de l'ordinateur infecté d'un beau frère. Bref, ils sont les membres non reconnus d'un service de secourisme autogéré, qui s'efforce de protéger contre les cyber-délinquants et leurs flux incessant d'attaques toujours plus sophistiquées.* »

2.1.3. Questions clés

L'approche culturelle et sociologique du numérique et la dimension quasi philosophique de la cryptographie nous amènent à poser d'entrée 4 questions clés :

• Les **sphères professionnelle, privée et publique** s'interpénètrent de plus en plus et de plus en plus profondément : comment gérer les situations conflictuelles en termes de gestion et de protection de l'information en développant, en particulier, une cyber-éthique ?
• L'importance de la **génération Y** (voir chapitre 2.5) au sein des entreprises et de la société conduit certainement à un rééquilibrage des pouvoirs entre technophobes et technophiles : peut-on traiter la confidentialité de manière pertinente et différenciée selon la génération des acteurs concernés ? Si oui, comment ?
• Les limites technologiques en termes de prévention / protection deviennent de plus en plus évidentes : **le contrôle et la surveillance**, vont-ils se généraliser telles des « invasions barbares[8] » virtuelles ? Faute de mieux...
• La fonction SSI, dont il faut rappeler les origines informatiques en relation avec le monde de l'assurance (donc de la gestion des risques), est plus que jamais **prise en étau** : d'un côté, par les questions de conformité (par exemple CNIL et PCI DSS (Payment Card Industry - Data Security Standard)), de l'autre, par le contexte de guerre économique et de cyber-guerre (illustré par exemple par les affaires EDF/Greenpeace, Sony ou Bercy). Le terme même de Sécurité des SI doit-il être abrogé pour intégrer une bonne fois pour toute la protection des informations ? Ou doit-il se recentrer sur les questions liées aux infrastructures dans une optique purement opérationnelle ?

---

[6] Éditions Seuil - 2008
[7] Titulaire de la chaire de recherche sur les cultures numériques de l'Université de Laval à Québec
[8] On comprendra le concept d' « invasion barbare » comme étant une solution / pratique qui peut être pire que le mal qu'elle combat, mais pourtant nécessaire et aussi, pourquoi pas, porteuse de progrès.

2.2. L'ère numérique : de l'Âge de pierre à l'Âge du silicium ?

L'humanité a traversé des phases successives qui nous ont amenés à devenir des « homo numericus » pour qui perdre son smartphone est plus dommageable que perdre sa carte bancaire[9]. Impossible de communiquer : Inimaginable !
La communication entre les individus s'inscrit dans une longue histoire nous emmenant aux confins de l'humanité. Nous en rappelons ci-dessous les évènements clés.

Date	Apparition / Invention	Origine / source	Objet / application
300 000 av JC	Langage	Homo Sapiens	?
50 000 av JC	Protolangue	Homo Sapiens	?
18 000 av JC	Dessins	Lascaux	Chamanisme ?
3 400 av JC	Écriture	Mésopotamie	Agriculture
650	Imprimerie	Chine	Textes sacrés
1642	Machine à calculer	Blaise Pascal	Finances publiques
1791	Télégraphe optique	Claude Chappe	Journalisme
1834	Machine à carte perforée	Charles Babbage	Mathématiques
1837	Télégraphe électrique	Samuel Morse	Transports
1876	Téléphone	Alexandre G. Bell	Communications orales
1888	Film cinématographique	Louis Leprince	Reportages actualités
1890	Ordinateur mécanique	Hermann Hollerith	Recensement de la population
1919	Ordinateur mécanique	Frederik R. Bull	Statistiques
1926	Télévision	John Baird	Diffusion d'images animées
1936-56	Ordinateur électrique	Armée US	Défense
1960	Ordinateur à transistor	IBM	Défense / Universités / Recherche
1969	Réseau ARPANET	DARPA (USA)	Défense / Universités / Recherche
1970	Ordinateur à circuit intégré	IBM	Informatique d'entreprise
1973	Ordinateur individuel	IBM	Professionnel et personnel
1982	Protocole TCP IP	IETF	Communications en réseau
1983	Téléphone portable	Motorola	Téléphonie mobile
1984	Ordinateur personnel	Apple	Professionnel et personnel
1991	Langage Web	CERN	Information / commerce en ligne

On constate, dès l'origine, une relation étroite entre « communiquer » et « calculer ». N'oublions pas la fameuse exclamation de Pythagore (580-495 avant JC) : « *Tout est nombre !* ». Sans calcul, sans mathématique, sans numérique, ni « 0 », ni « 1 », pas de communication à la vitesse de la lumière.

On note également une forte accélération de l'innovation depuis le milieu du XIXème siècle, à la suite des développements de l'énergie électrique. Cependant, depuis près de 20 ans, les innovations se situent sans doute plus au niveau de la miniaturisation, du marketing et des usages que de la technologie proprement dite.

Ainsi, tous les domaines de la société ont progressivement bénéficié du développement de nouvelles techniques de communication pour nous faire entrer depuis une quinzaine d'années, dans l'ère du numérique.

Les questions de secret et de confidentialité ont nécessairement été présentes au cours de cette longue histoire :

- Pratique des rituels sacrés : communication avec les esprits et les Dieux
- Messages cachés : crédo religieux, diplomatie, plans de bataille, etc.
- Savoir-faire : agriculture, science, industrie, finance, vente, marketing, etc.

Il est d'ailleurs intéressant de noter que les termes « *sacré* » et « *secret* » ont des racines latines et grecques communes renvoyant aux forces divines (lat. sanctus, gr. hiéros) et séparant ce qui est inaccessible à l'homme (lat. sacer, secretus, gr. hagios, kryptos). Ainsi, comme le sacré se distingue du profane, le secret se distingue du public, ou comme nous le verrons plus loin, de la transparence. Ce qui est sacré ne peut donc être communiqué ou divulgué à celui qui ne peut ou ne saurait le comprendre. Parti de l'oralité en passant par l'écrit, que devient le secret dans l'ère numérique ? Et qu'est-ce qui distingue aussi secret de confidentiel ?

L'ère numérique dans laquelle est entrée l'humanité à la fin du XXème siècle est porteuse d'espoirs et de progrès gigantesques, mais elle perturbe aussi les équilibres historiques du partage et de la protection de l'information.

La confidentialité concerne l'écrit et l'oral comme le numérique. Même si le poids de ce dernier est devenu très important, il ne faut cependant pas négliger les autres !

2.3. Distinguer Secret et Confidentialité ?

Le thème du Livre Bleu des Assises 2011 nous oblige à rappeler les définitions[10] des mots clés en distinguant les noms – le secret ou la confidentialité – des adjectifs – être secret ou confidentiel.

[9] Une étude, réalisée par Redshift Research en mai 2011 et commandée par Intel, montre que 6% des personnes interrogées en France préfèrent se passer de leur partenaire pendant une semaine plutôt que de leur téléphone portable.
[10] Extraites de Larousse.fr, L'Internaute-Encyclopédie, Futura-Science.com, etc.

Terme	Définitions	Synonymes
Secret (nom)	Qui n'est connu que d'un très petit nombre de personnes et ne doit pas être divulgué aux autres. Une information, ou un savoir qui se trouve soit caché soit inaccessible. Qui est hautement confidentiel, caché à tous.	Discrétion, confidence
Confidentialité (nom)	Propriété de ce qui est confidentiel. Fait de garder quelque chose privé et secret vis à vis de tout le monde sauf ceux qui sont autorisés à le voir.	Confidence, secret, énigme
Secret (adjectif)	Ce que l'on tient caché. Qui se dissimule. Qui n'est pas apparent, qui ne se manifeste pas.	Intime, personnel, confidentiel, privé, masqué, discret, énigmatique, réservé, caché, insaisissable, dissimulé, inavoué, caché, voilé
Confidentiel (adjectif)	Qui se dit, se fait en confidence, contient des informations qui doivent rester secrètes. Caractère d'une information qui ne doit pas être rapportée publiquement. Qui ne s'adresse qu'à un petit nombre de personnes. Qui se communique sous le sceau du secret.	Secret, peu connu, dissimulé, insaisissable, privé, personnel, intime, officieux, impénétrable

De toute évidence, les deux termes sont très liés voire synonymes. Cependant, leur usage dans la vie courante, comme dans l'espace professionnel, est très varié et a donné lieu à de nombreuses expressions.

- Au niveau de la nation :
  - Secret d'État
  - Secret Défense
  - Services secrets, agent secret, top secret
  - Voire fonds secrets
- Au niveau privé :
  - Secret de famille : non-dits sur un passé, sur des événements vécus au sein d'une même famille
  - Secret de polichinelle : connu de tous sans pour autant être partagé
  - Secret maçonnique : où quête de vérité et ésotérisme côtoient tant de fantasmes
  - Sceau du secret
- Au niveau professionnel, le secret se décline en :
  - Secret de fabrique
  - Secret bancaire
  - Secret médical pour les professionnels de santé
  - Secret des correspondances : à l'origine pour les opérateurs de la poste et du téléphone
  - Secret de la confession pour les prêtres
  - Secret des sources pour les journalistes
  - Secret de l'instruction pour les forces de police et la justice, etc.

Faute de compréhension claire et partagée, en particulier sur les définitions et le vocabulaire à utiliser, la profession risque de ne jamais répondre à l'enjeu majeur qui est de protéger le patrimoine informationnel / immatériel.

N'oublions pas également que dans la guerre économique du XXIème siècle comme depuis la nuit des temps sans doute, la rumeur, la manipulation, la désinformation sont aussi des armes largement répandues et qu'elles sortent du cadre de notre problématique. Encore faut-il le rappeler !

> ***La confidentialité et le secret ne se distinguent-ils pas dans la mesure où la première doit être maintenue dans la durée, alors que le second peut être « levé » et aurait intrinsèquement une durée de vie limitée ?***

> ***« Il n'est point de secrets que le temps ne révèle.»***
>
> Jean Racine (1639-1699)
> Britannicus - 1669

2.4. Les 3 sphères : professionnelle, privée, publique

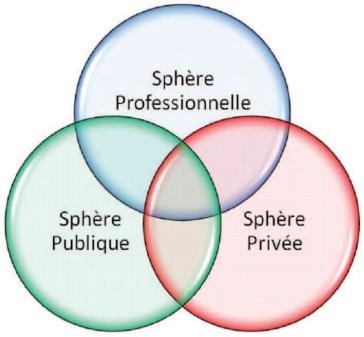
Les infrastructures des SI et l'usage des moyens de communication dans les entreprises comme pour les administrations, ont profondément évolué depuis une dizaine d'années.

D'une part, les pratiques d'externalisation donnent un accès aux sites et aux données de l'entreprise / organisme à des tiers multiples comme les prestataires informatiques, des partenaires, des sous-traitants (par exemple, les services de relation client).

Le développement du « *cloud computing* » conduit les entreprises à ne même plus savoir où sont ou seront précisément stockées leurs données au sein de multiples datacenters externalisés. Quelles données sont / seront hébergées ? Pendant quelle durée ? Quelle est leur classification ? Les données confidentielles voire du domaine du secret ont-elles leur place dans « les nuages » ? Ne serait-ce que la messagerie d'entreprise ou des données à caractère personnel ?

D'autre part, la démocratisation de l'Internet (Web 2.0, réseaux sociaux, e-commerce, etc.) et des outils de mobilité (portables, smartphones, tablettes) abaisse les frontières entre le monde de l'entreprise et l'univers de ses collaborateurs, des clients, des partenaires et des fournisseurs, etc.. L'information est de plus en plus volatile, stockée sur des équipements de plus en plus petits et performants mais également de moins en moins onéreux. Peut-on contrôler efficacement les échanges d'information sensible entre l'ensemble des acteurs internes / externes du monde de l'entreprise et des administrations ? L'exercice semble périlleux voire utopique.

Enfin, pour aller plus loin encore, les individus utilisent désormais aussi leurs outils personnels sur leur lieu de travail pour communiquer avec l'extérieur. Une réflexion sur l'usage professionnel de ces dispositifs personnels est même engagée (« *Bring you own device* »), source d'économie pour l'entreprise certes, mais quid de la responsabilité individuelle et collective ? De toute évidence, le public / privé s'immisce de plus en plus dans la sphère professionnelle.



La mixité et la superposition des 3 sphères créent des zones de conflit et de tension où les questions de confidentialité, de secret, d'intimité et de transparence sont délicates à appréhender.

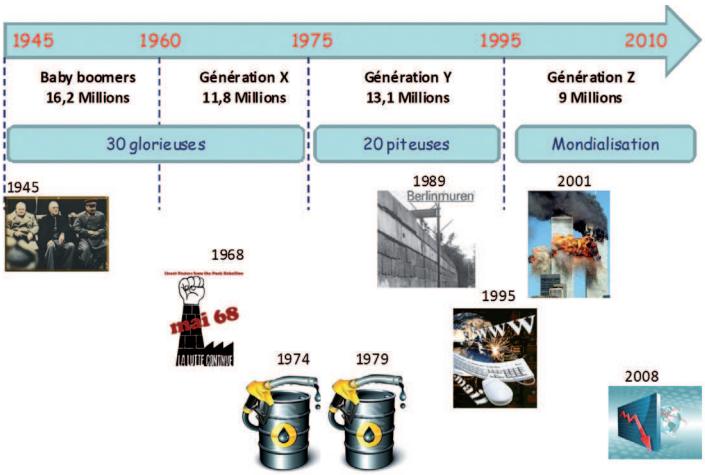
> ***La maîtrise de l'information numérique s'inscrit désormais dans une approche plus stratégique, la technologie submergeant le droit en entremêlant fortement les intérêts collectifs et personnels et opposant parfois ceux du salarié, du client, du fournisseur, du citoyen, du parent, du consommateur...***

2.5. Les 3 générations : Baby boomers / Génération X / Génération Y

Les points précédents ont mis en évidence l'évolution des usages des outils de communication et leurs impacts sur le monde de l'entreprise. Ils s'inscrivent aussi dans l'évolution même de la société.

D'un point de vue sociologique, le marché du travail est confronté à la coexistence de trois générations qui ont vécu différemment l'émergence du numérique. La question n'est pas de les opposer, car des disparités existent aussi fortement au sein d'une même génération. Cependant, force est de constater qu'elles n'ont pas le même vécu et surtout pas la même relation au numérique, à ses apports, ses contraintes ou ses dangers.

Les frontières définies entre les 3 générations varient d'un pays à l'autre, en fonction de l'évolution de la natalité et des comportements. Aussi, les dates indiquées ci-dessous, s'appuient sur celles les plus communément proposées par les sociologues. On notera qu'il y a parfois des zones de superposition et qu'ainsi, certains se situent quelque part, « entre deux » générations sociologiques.



2.5.1. Les baby boomers

Les baby boomers (nés entre 1945 et 1960) ont profité de l'après-guerre et du plein emploi. En Occident, ils seraient particulièrement idéalistes et égocentriques. Ils ont notamment été marqués par trois évènements clés (personnes nées entre...) :

- La conférence de Yalta et la partition de l'Europe
- La décolonisation et les guerres d'indépendance
- L'aspiration à la liberté exprimée en France par les évènements de mai 1968

Peu sont ceux qui ont découvert l'informatique à leur entrée dans le monde professionnel. Les plus jeunes d'entre eux ont parfois pu partager un PC sous MS DOS au milieu des années 80. Ils découvrent aussi Internet pendant leur vie active. Pour les plus anciens, c'est pendant leur retraite !

Ayant bénéficié des « 30 glorieuses », ils sont, pour les générations suivantes, en grande partie responsables de la situation de crise actuelle (sauvegarde de la planète et déficits publics).

2.5.2. La génération X

Cette génération (personnes nées entre 1960 et 1975) découvre le chômage de masse. Elle a notamment été marquée par trois événements clés :

- Les chocs pétroliers de 1974 et 1979
- La guerre froide jusqu'à la chute du mur de Berlin en 1989
- L'innovation technologique et l'avènement d'Internet au début des années 90

Cette génération intermédiaire a vécu « un creux de vague » sur le plan professionnel, trouvant difficilement des emplois stables et bien rémunérés. Ils sont moins fidèles que leurs parents à leur entreprise. Si le numérique fait partie de leur existence, nombreux sont ceux qui conservent de fortes réticences sur ses abus au quotidien (par exemple avec le danger de la cyber-surveillance).

De nature angoissée, elle est caractérisée par l'augmentation des divorces et par un sentiment fort que rien n'est impossible. Il suffit d'y mettre du temps et de l'argent.

2.5.3. La génération Y (ou Net Generation ou Digital Natives)

Cette génération (nés entre 1975 et 1995) est aussi appelée *Net Generation* dans la mesure où ses membres grandissent dans un monde où l'ordinateur et Internet sont de plus en plus accessibles. Ils ont surtout été marqués par cinq évènements clés :

- L'immigration de masse (et le multiculturalisme) initiée dans les années 80
- La bulle Internet de la fin des années 90 et son explosion en 2002
- Les attentats terroristes du 11 septembre 2001
- Les questions écologiques et de sauvegarde de la planète
- La crise financière de 2008 et ses impacts socio-économiques

Le succès de la notion de génération Y dans les entreprises prend appui sur le déphasage entre les besoins et les attentes des jeunes de cette génération et le mode de fonctionnement de l'entreprise instauré par les générations précédentes. L'ordre des priorités s'inverse : les amis passent avant la famille qui passe avant les responsabilités professionnelles. La hiérarchie s'efface au profit du « réseau ». La liberté de communiquer dans un monde ouvert se heurte au cloisonnement et aux contraintes d'un règlement intérieur.

Ce fossé générationnel s'explique par une accélération du changement, l'apparition des NTIC et une hiérarchisation différente dans les transmetteurs de valeurs. L'Église, l'armée, voire la famille sont moins influents que ne le sont Internet, la télévision, voire les réseaux relationnels. Les pairs sont devenus plus importants que le père ! Là où l'employeur s'immisçait dans la vie de famille pour les générations précédentes (Comité d'entreprise par exemple), c'est la vie privée qui rentre dans l'entreprise avec la Génération Y, avec une conscience des risques portant sur leur activité professionnelle assez réduite.

> ***L'importance accrue de la Génération Y au sein des entreprises est-elle source de risques en termes de confidentialité et conduit-elle à une révision fondamentale des droits et devoirs relatifs à l'usage des outils de communication ?***

2.6. Gestion de la confidentialité et sécurité / sûreté

2.6.1. Gestion des risques

Gérer les risques s'intègre historiquement et avant tout dans une logique économique et assurancielle. Or, la dimension économique de la Sécurité des SI reste peu appréhendée par les professionnels. Comme l'attestent les résultats de l'enquête 2010 du Cercle[11], nous avions constaté que :

- Seulement 37% des répondants affirment consolider leurs dépenses en Sécurité SI.
- Les impacts économiques liés aux atteintes à la confidentialité sont pourtant évalués par 73% des répondants dont 18% « systématiquement » et 29% « souvent ».
- Le plus gros impact économique concerne une atteinte à la confidentialité pour 11% des incidents constatés (contre 45% pour un accident / panne matérielle).

Au-delà de l'économie, gérer les risques c'est aussi respecter des principes fondamentaux et simples desquels nous excluons celui de la précaution, tant il participe à la quête du « risque zéro », sans doute encore plus risqué que le risque lui-même !

Gérer un risque c'est d'abord l'identifier et l'évaluer. Ce n'est qu'ensuite que des mesures (de sécurité / sûreté) qui réduisent sa potentialité / faisabilité comme ses conséquences / impacts doivent être mises en place. Les questions de confidentialité n'échappent pas à la règle. Il convient donc toujours de trouver un équilibre cohérent entre les mesures :

- De prévention / protection
- De régulation / sanction
- De détection / réaction

Cependant, à la différence d'autres domaines de la Sécurité des SI, l'information n'est pas traitée uniquement sous une forme numérique. Pour être cohérent, il faut donc associer aux mesures juridiques (lois, chartes, clauses, engagements et accords de confidentialité, etc.) et informatiques (chiffrement, authentification et gestion d'habilitations), des moyens humains et matériels (accueil, gardiennage, vidéo-protection, destruction de supports, détection d'intrusion, etc.), le tout associé à des comportements adéquats (discrétion, vigilance, observation, alerte, etc.).

C'est ici que les synergies entre les directions et les métiers (utilisateurs / usagers), la DSI, la sécurité et la sûreté, les services généraux, le juridique et les RH doivent jouer pleinement. Ensemble, ils doivent œuvrer à la **création d'une véritable culture du risque numérique**. Transcendant la sensibilisation et la formation, l'acculturation[12] s'inscrit dans une approche socioprofessionnelle et à finalité résolument économique.

2.6.2. Sécurité et Sûreté

Le rappel de ces évidences, toujours utile, nous amène alors à nous poser la question du champ d'action de la Sécurité SI dans le cadre de la gestion de la confidentialité. Ainsi, des directions et des équipes ont été mises en place dans plusieurs secteurs afin de s'occuper de « sûreté de l'information » ou de « sûreté du patrimoine informationnel ». Cette démarche a sans doute été contrainte par une séparation historique entre le « numérique » et le « matériel » d'une part, et entre la gestion des risques accidentels (en particulier pour la Sécurité des SI) et celle de la fraude / malveillance (souvent en lien avec la sûreté) d'autre part.

Si la « sécurité » traduit une « *situation dans laquelle quelqu'un ou quelque chose n'est exposé à aucun danger, à aucun risque* »[13], en particulier d'agression physique, d'accident, de vol, de détérioration, la « sûreté » définit « *l'état de quelqu'un ou quelque chose qui est à l'abri, n'a rien à craindre* ». Comme pour le secret et la confidentialité, la sécurité et la sûreté se rejoignent, se complètent et parfois se recoupent.

Dans la pratique, on assimile souvent les questions de sûreté à la malveillance plus qu'aux accidents. Dans le transport aérien par exemple, la sûreté (traduite en *security*) s'exerce lors de l'embarquement (fouilles, scans, contrôles d'identité) alors que la sécurité (traduite en *safety*) se concrétise par les consignes à appliquer en cas d'accident ou de crash (à bord et par les hôtesses). Pourtant, sécurité et sûreté se recouvrent lorsqu'elles s'adressent globalement à la protection des personnes et des patrimoines.

[11] Livre Bleu des Assises 2010 : « Dimension économique de la Sécurité des SI »
[12] Acculturation : processus par lequel un individu ou un groupe d'individus acquiert une culture qui lui est étrangère.
[13] www.larousse.fr

L'enjeu représenté par le secret et la confidentialité n'oblige-t-il pas l'ensemble des professions de la gestion des risques et de la sécurité / sûreté à œuvrer de concert dans tous les secteurs d'activité sans exception ?

2.7. Quelle place pour la cyber-éthique ?

Peut-on répondre à ces défis autrement que par l'instauration d'une réelle confiance numérique et en développant une forme de cyber-éthique ?

Qu'est-ce que l'éthique et comment s'intègre-t-elle dans le monde du numérique ? De toute évidence, l'éthique est loin d'être toujours restée identique à elle-même. Au contraire, elle a connu de nombreuses et importantes transformations au cours de son histoire. L'éthique occidentale a elle-même connu plusieurs grandes périodes, de l'Antiquité au Moyen-Âge, des Lumières à Internet. Approche collective ou individuelle ? Centrée sur les droits ou les devoirs ? Vision philosophique ou démarche pratique ?

Notre époque vit un fort développement de l´éthique appliquée en rapport avec des préoccupations environnementales et sociales. Dans les activités professionnelles, la déontologie (éthique collective au sein d'une profession) établit avant tout des codes de comportements. Dans le domaine du numérique justement, plusieurs applications pratiques de l'éthique sont en cours : développement durable (green IT), protection de la vie privée (privacy), intelligence économique (*business intelligence*).

À ce titre, nous recommandons la lecture du document publié par le CIGREF avec le Cercle d'Éthique des Affaires en 2006 : « Déontologie des usages des Systèmes d'Information ». L'enjeu de la démarche est clairement d'aller au-delà du droit sur les « *risques liés à des usages juridiquement non conformes.* » Il convient donc de définir des règles du jeu en transposant en « *règles et contrôles internes les contraintes juridiques qui pèsent aujourd'hui sur l'usage des Systèmes d'Information et qui peuvent amener les entreprises à être sanctionnées de ce fait.* » Une annexe de 15 pages aborde la question du secret professionnel sur lequel revient Maître Éric A. Caprioli au chapitre 3.2. S'adressant aux grandes entreprises et cherchant avant tout à sensibiliser les acteurs, l'ouvrage semble cependant « enfermer » les organisations dans un cadre juridique et organisationnel, selon une démarche de « conformité ».

La cyber-éthique ne doit pas être limitée aux questions juridiques et réglementaires dans une logique de conformité. C'est une démarche éducative de longue haleine associant intelligemment les mots clés : usages, risques et acculturation.

2.8. L'exemple de la santé

2.8.1. Le contexte

Aujourd'hui, le secteur de la santé est un bon exemple de la prise en compte de la Sécurité des SI à tous les niveaux décisionnels et opérationnels. Les actions, initiatives et projets, intégrés dans la direction de la loi HPST (Hôpital, patients, santé et territoires) que sont le Dossier Médical Personnel, la Télésanté, la Carte CPS, l'Hôpital numérique et les futurs Espaces Numériques Régionaux de Santé, sont associés à une prise en compte quasi-vitale des risques liés aux SI.

Nous reprenons ci-dessous, une synthèse des avis et positions de personnalités et de professionnels publiés dans le recueil « Sécurité et Confidentialité des Systèmes d'Information » paru en mai 2011 avec la contribution de Nora Berra, Secrétaire d'État chargé de la Santé dans le cadre de la conférence HIT 2011 à Paris. Maître d'œuvre de l'ouvrage, Jean-Pierre Blum, Président de l'IISIST[14] et du Pôle Santé des Assises, mentionnait dans son éditorial que « *c'est la première fois que l'ensemble des décideurs, politiques, administrations centrales, collèges des DSI et des RSSI, accepte de livrer, dans un même temps, leurs visions sur la sécurité des systèmes d'information de santé.* »

Le recueil propose une quarantaine de tribunes dont nous avons extrait des passages clés complétés par quelques avis complémentaires.

2.8.2. Les positions institutionnelles

Pour **Nora Berra – Secrétaire d'État chargée de la Santé**, « *Les informations de santé touchant par essence à l'intime, la garantie de la confidentialité des données personnelles de santé doit être au cœur de la sécurité des systèmes d'information.* »

Selon **Annie Podeur - Directrice de la Direction Générale de l'Offre de Soins**, « *La confidentialité des données médicales pose la question du partage de l'information : ce que l'on partage et avec qui, dans un objectif constant, celui de la confiance des patients.* »

Pour **Jacques Lucas – Vice-président chargé des SI de santé du CNOM**[15], « *À la qualité déontologique, respectant le droit des patients, à la confidentialité et au secret qui protègent leurs données personnelles de santé, se superpose la qualité des exercices médicaux. Ces deux aspects se complètent et ne s'opposent pas. Les médecins doivent s'impliquer dans la définition de la politique de confidentialité de l'établissement, comme dans les formations des professionnels de santé et les auxiliaires avec lesquels ils exercent. La "sécurité déontologique" est une première marche fondamentale dans la sécurité de l'information dans son ensemble.* »

De son côté, **Pierre Lasbordes - Député de l'Essonne**, Président de la Commission Télésanté missionné par le Premier Ministre, rappelle que « *La dernière recommandation de [son] rapport*[16] *insistait plus particulièrement sur cette nécessité d'informer et de générer l'intérêt et la confiance dans l'utilisation de la télésanté, d'où la nécessité de garantir des critères de confidentialité et de responsabilité.* »

Enfin, le Sénateur **Alex Turk - Président de la CNIL**, insiste pour sa part sur les enjeux liés à l'usage des cartes CPS « *Le décret "Confidentialité" du 15 mai 2007, impose l'utilisation de la CPS ou d'un certificat logiciel équivalent pour identifier et authentifier toute transmission ou accès aux données de santé, y compris au sein d'une même structure. L'on sait pourtant que la généralisation de la carte CPS n'est pas effective à ce jour dans de nombreux établissements de santé, faute de moyens financiers et techniques, alors même que son utilisation est obligatoire depuis le 15 mai 2010.* »

Ces positions, centrées sur les questions de confidentialité (objet de notre travail), ne doivent pas faire perdre de vue que la continuité de l'activité et des services médicaux reste autant sinon plus critique. En effet, la Sécurité des SI ne doit pas aller à l'encontre de la sécurité de la prise en charge des patients, finalité ultime des établissements de santé et des soignants.

---

[14] Institut International des Systèmes d'Information de Santé et de la Télésanté
[15] Conseil National de l'Ordre des Médecins
[16] La télésanté : un nouvel atout au service de notre bien-être – 15 octobre 2009
[17] Carte des Professionnels de Santé

2.8.3. Points de vue de fonctionnels

Les points de vue des acteurs fonctionnels de la Sécurité des SI apportent des éclairages complémentaires.

Pour **Éric Grospeiller - Fonctionnaire SSI des Ministères de la Santé et des Affaires Sociales**, « *dans le monde de la santé, la disponibilité revêt un caractère vital. Il est possible que certaines mesures de confidentialité soient des freins à cette exigence. Il convient donc de pouvoir temporairement dégrader la confidentialité sans pour autant la supprimer. On passe alors d'une confidentialité à priori (mesures maximales), à une confidentialité à posteriori (contrôle des actes). Le renforcement des moyens de contrôle intègre alors les mesures de traçabilité.* »

Selon **Patrick Pailloux - Directeur Général de l'ANSSI**[18], « *le schéma de confidentialité du DMP est particulièrement ambitieux. Comment gérer 60 millions de clés de confidentialité tout en autorisant, en cas d'urgence, le bris de glace (passe-partout pour les professionnels de santé) ? Car la disponibilité des données peut être plus importante que leur confidentialité lorsque le personnel médical doit faire face à un pronostic vital.* »

En termes de gouvernance, **Pascal Forcioli – Directeur Général adjoint de l'ARS**[19] **du Nord-Pas-de-Calais, plus particulièrement chargé de la Sécurité et de la Télésanté**, considère que « *le choix du RSSI est stratégique. Il faut privilégier la désignation d'un professionnel qui ne soit pas seulement un technicien compétent, mais aussi – et surtout – un manager, prosélyte et pédagogue.* »

Christian Huart - Sous-directeur en charge des SI de l'ARS de Picardie, rappelle aussi que « *la réglementation impose de respecter intégrité, intégralité, haute disponibilité, authentification, identification de l'information sur la base de comportements respectueux des chartes internes. Il s'agit bien de continuité d'activités médicales, nécessitant un haut niveau d'exigences sur la disponibilité des dispositifs qui les supportent.* »

Vision complémentaire, pour **François Tesson - RSSI du GCS**[20] **e-Santé Pays de la Loire**, « *la pyramide des âges des médecins en activité indique que dans les 3 ans à venir*[21]*, les membres de la génération X seront au cœur de la révolution numérique. La confidentialité des données médicales est ancrée dans leur quotidien principalement par l'application du code de déontologie. Mais la numérisation des usages vient bouleverser son application. Par contre, l'usage numérique fait partie, au moins dans leur vie privée, de la culture de la génération Y. Ne serait-il pas opportun et plus efficace de former cette génération à appliquer les mesures de sécurité sur la protection des données numériques sensibles pour assurer le passage vers les NTIC de leurs pairs ?* »

2.8.4. Visions des Établissements de santé

Il nous faut aussi confronter ces positions avec celles des acteurs de terrain, au sein même des établissements de santé.

Pour **Serge Bernard - Directeur Général du CH Régional d'Annecy**, « *des actions de sensibilisation et de ''culturation'' doivent être conduites au sein des établissements et figurer dans les plans de formation des établissements. Elles doivent réunir les professionnels toutes catégories confondues et donner lieu à des exercices pédagogiques au sein des équipes de soins et de tous services. Les clés du changement sont celles des portes qui s'ouvrent vers l'extérieur !* »

---

[18] Agence Nationale de la Sécurité des Systèmes d'Information
[19] Agence Régionale de Santé
[20] Groupement de Coopération Sanitaire
[21] La démographie médicale à l'horizon 2030 - dossiers Solidarité et Santé – DREES 2009

Mylène Jarossay - DSI adjointe et RSSI de l'Institut Curie – Centre René Huguenin, estime qu'« *avant même de poser un problème aux RSSI, le développement du numérique est en soi déjà un challenge pour les DSI qui doivent produire un SI efficace, complet, consolidé et toujours accessible malgré ou grâce aux nouveaux usages. Le RSSI doit revoir en profondeur ses méthodes de sécurisation, mais avant lui, le DSI doit redéfinir ce qu'est son système d'information, où il se niche, et où sont les enjeux. Les RSSI gagnants seront ceux qui sauront transformer les nouveaux contextes de sécurité en atout, qui sauront faire de la délocalisation de l'information une parade, une astuce plutôt qu'un risque.* »

Guillaume Deraedt - Responsable de la SSI du CHRU de Lille, indique de son côté que « *les métiers de l'urgence requièrent une disponibilité optimale associée à des plans de continuité d'activité, rapides à mettre en place, et éprouvés. Les patients souffrant de longues maladies sont singulièrement soucieux de la confidentialité de leurs données. Le RSSI aspire à changer la vision d'une sécurité technique contraignante en une démarche qualité permettant un espace numérique performant de confiance. Le RSSI est aujourd'hui un pilier du déploiement de nouvelles fonctionnalités, de l'ouverture vers les Espaces Numériques Régionaux de Santé et le Dossier Médical Personnel.* »

Enfin, **Vincent Trély - DSIO du Centre Hospitalier du Mans** considère que « *la confidentialité des informations concentre la majorité des questions, parce que dans le monde de la santé et de l'hôpital, elle va de soi... Le médecin a prêté serment et le patient ne doute pas du rapport de confidentialité avec son praticien. Le système d'information n'a donc pas droit à l'erreur, puisqu'il fait aujourd'hui en quelque sorte «partie du médecin» et de son rapport avec le patient. La confidentialité est donc vue comme « l'enjeu majeur ». Ceci étant dit, lorsque l'on explique ce que signifient disponibilité (et surtout conséquences d'indisponibilité...) et intégrité (et surtout conséquences de la fausse information), tout redevient important !* »

2.8.5. L'implication d'un assureur

Éric Doyen, RSSI de Generali, indique pour sa part que « *la sécurité SI collabore avec les métiers via un réseau de correspondants, experts métiers et ambassadeurs de la protection de l'information. Il encadre les démarches propres à la réduction des risques par la mise en place de processus et de mesures de sécurité adaptées. Concernant plus particulièrement la confidentialité des informations, et étant dans le monde de l'assurance, les directions sont bien sensibilisées à la protection des informations, en particulier pour les données à caractère médical (cadre de la convention AERAS - accès à l'Assurance et à l'Emprunt des personnes présentant un Risque Aggravé de Santé). Nous associons des mesures de protection de la confidentialité de ces données au plan logique mais également au plan physique avec la mise en place de zones spécifiques dédiées et protégées nommées zones "AERAS".* www.aeras-infos.fr ».

« En présence des maîtres de cette école et de mes chers condisciples et selon la tradition d'Hippocrate, je jure et je promets d'être fidèle aux lois de l'honneur et de la probité dans l'exercice de la médecine.

Je donnerai mes soins gratuits à l'indigent et n'exigerai jamais un salaire au-dessus de mon travail.

Admis à l'intérieur des maisons, mes yeux ne verront pas ce qu'il s'y passe, ma langue taira les secrets qui me seront confiés et mon état ne servira pas à corrompre les mœurs ni à favoriser le crime.

Respectueux et reconnaissant envers mes maîtres, je donnerai à leurs enfants l'instruction que j'ai reçue de leur père.

Que les Hommes m'accordent leur estime si je suis fidèle à mes promesses.

Que je sois couvert d'opprobre et méprisé de mes confrères si j'y manque.

Je jure ! Je jure ! Je jure ! »

2.9. Synthèse

S'appuyant sur ces rappels et cette dialectique d'ensemble, le Livre Bleu des Assises 2011 cherche à ouvrir le champ de la réflexion des professionnels de la Sécurité des SI. Quelques questions clés méritent ainsi d'être posées :

• Faut-il dissocier les notions de secret et confidentialité dans le monde numérique ? Si oui, comment ?
• Classifier en termes de confidentialité, une information numérique de plus en plus partagée et volatile, a-t-il un sens ?
• Les dirigeants et les managers prennent-ils réellement en compte les évolutions sociologiques et technologiques dans leur gestion de la confidentialité ?
• Les questions psychosociologiques ne doivent-elles pas prendre une importance accrue dans la gestion des risques SI, en particulier dans la gestion de la confidentialité ?
• Quelles sont les véritables risques à couvrir en relation avec les nouveaux usages des systèmes d'information et de communication, en particulier l'émergence du Cloud computing et du Web 2.0 ?
• Comment devra s'adapter, en conséquence, la gouvernance des risques SI ?
• Et enfin, ne doit-on pas dépasser le concept de sensibilisation pour tendre vers une acculturation sur les risques numériques dans chaque contexte spécifique ?

Nous sommes bien conscients que les questions posées n'auront pas une réponse unique, tant elles dépendent du secteur d'activité et de la maturité des organismes et entreprises. Mais elles méritent d'être posées. A lui seul, le secteur de la santé présente des challenges très particuliers touchant chacun de nous, parent ou ami de patient, voire patient potentiel ...

Pour approfondir ces éléments de départ, nous conservons la forme des éditions précédentes et une approche résolument pédagogique, posant plus de questions qu'apportant de réponses et de vérités.

Les chapitres suivants présentent :

• D'une part, un approfondissement de la problématique sous les angles stratégique / politique, juridique / réglementaire et normatif,
• D'autre part, la restitution des résultats de l'enquête annuelle du Cercle traduisant la position d'un échantillon de près de 220 professionnels ayant répondu à 13 questions.

« Garder un secret consiste à ne le répéter qu'à une seule personne à la fois. »

Michel Audiard (1920-1985)
Les 3 mousquetaires – 1953

3- CADRER LA PROBLÉMATIQUE

Sur la base de ce rappel à la fois historique et sociologique, il nous faut maintenant nous recentrer sur le fond de notre problématique. Pour ce faire, nous allons reprendre dans ce chapitre les principes fondamentaux sur lesquels nous devons bâtir l'approche :

- Le développement de la transparence au sein des entreprises et de la société
- Les textes de loi (français) sur le secret et la confidentialité
- Les normes internationales sur la Sécurité des SI
- Trois documents de référence propres au secteur public national

Leur analyse permet de dégager des points invariants et des questions clés qui seront approfondis au chapitre 4 en relation avec les résultats de l'enquête du Cercle.

3.1. Secret et transparence : au cœur de la gestion des organisations ?

Nous ne pouvons pas engager notre réflexion sur le secret et la confidentialité à l'ère du numérique sans nous replacer dans le contexte général des entreprises et des administrations, voire de la société.

Signalons également que nous excluons de notre réflexion les questions relatives au secret d'État et au secret Défense. Si certains membres du Cercle (ministères, administrations, industries sensibles) sont concernés par le sujet, il va de soi que nous sortons ici du cadre de nos capacités d'analyse.

« Cultiver le secret et l'énigme, c'est du passé.
Les mots d'aujourd'hui sont transparence et crédibilité. »

Jean-Claude Trichet
(Président de la Banque Centrale Européenne)
L'Express – 11 octobre 2004

3.1.1. La transparence : symptôme démocratique

En 2001, Denis Kessler (alors vice président du MEDEF) publiait un article[22] au titre évocateur : « L'entreprise : entre transparence et secret ».

Partant du constat que le monde de l'entreprise s'est historiquement construit sur certaines opacités et plus sur le secret que la transparence, de nombreux facteurs sont apparus mettant à mal les pratiques anciennes. Il en cite cinq :

- Le développement des technologies de la communication : « le temps qui sépare l'instant où l'information revêt un caractère privé ou secret et l'instant où cette même information devient semi-publique voire publique se restreint chaque jour davantage. »

[22] Revue « Pouvoirs » N°97 (2001)

• L'évolution de l'organisation des entreprises : le fonctionnement matriciel génère une diffusion plus fluide et déconcentrée de l'information ainsi qu'une forte remise en cause des pouvoirs. Cependant, que ce soit pour des informations sur le personnel ou des données financières, « *il a fallu dresser des murailles de Chine (par exemple pour éviter les délits d'initié) [...] accompagnées par l'adoption de codes de déontologie ou de codes de bonne conduite qui portent précisément sur le secret à observer dans telle ou telle situation.* »
• L'évolution générale du droit : la prolifération de textes relatifs à la transparence sous couvert de lutte contre la corruption. Ainsi, « *le secret a aujourd'hui mauvaise presse en entreprise : secret des affaires, de fabrique, ... comme ailleurs. Il suffit de citer les atteintes constantes au secret de l'instruction, les coups de butoir de la Cour de cassation contre le secret professionnel de l'avocat...* »
• Le passage d'une économie d'endettement à une économie de fonds propres : « *l'information financière avant tout privative devient alors essentiellement publique.* »
• Les exigences particulières des investisseurs institutionnels renforcent encore l'exigence de transparence (notamment lorsqu'ils sont anglo-saxons). La sanction vient alors du marché et « *elle est particulièrement sévère lorsqu'il apparaît que le management a sciemment caché des informations sensibles au marché, ou qu'il a donné des informations erronées.* »

Ainsi, le champ du secret tend à se réduire quasi-mécaniquement sous l'effet d'une démocratisation de la gouvernance et de la pression des marchés.

> ***La transparence érigée comme nouvelle vertu ne risque-t-elle pas de porter atteinte aux intérêts économiques des États (donc des citoyens) et des entreprises (donc des salariés) si les règles du jeu ne sont pas partagées par tous ?***

3.1.2. Le numérique : rupture de l'espace-temps

Dans cette évolution fondamentale, le numérique joue un rôle majeur. Dans un article de la Revue française de gestion[23], Aurélien Colson (professeur de science politique à l'ESSEC), décrit avec pertinence comment cette aspiration démocratique à la transparence est facilitée par l'essor des technologies de l'information.

« L*es mécanismes concrets permettant à l'injonction de transparence de se réaliser sont les fruits des révolutions successives des technologies de l'information et de la communication. Radio et télévision sont désormais presque universellement diffusées. Avec l'Internet, l'essor du haut-débit et la puissance exponentielle des systèmes informatiques, le fait de produire, transporter, diffuser et stocker de l'information ne coûte plus grand-chose. Cela entraîne deux effets supplémentaires.*

D'une part, la segmentation de l'espace s'évapore : les barrières à l'information s'estompent. Ce qui devait rester clos dans un espace contrôlé menace à tout moment de fuir vers l'extérieur. Ce qui était de l'information interne devient plus facilement de l'information externe, publique. D'autre part, le temps s'accélère : la circulation de l'information devient de plus en plus rapide. Ce qui hier mettait du temps à se diffuser au sein d'une population peut aujourd'hui l'être instantanément. »

Concrètement, l'usage généralisé des systèmes de messagerie comme des blogs ou réseaux sociaux (professionnels et personnels) disponibles sur des terminaux multiples et désormais mobiles, facilite la publication instantanée et la diffusion sur le Web, d'un texte, d'une conversation, d'une vidéo ou d'une photo, qui peuvent aussi être manipulés et sortis de leur contexte.

[23] Colson Aurélien, « Gérer la tension entre secret et transparence » Les cas analogues de la négociation et de l'entreprise Revue française de gestion, 2004/6 n) 153, p 87-99

3.1.3. La tension secret-transparence

La transparence généralisée rompt la dissymétrie propre au secret. Elle traduit une forme d'égalité et de réciprocité. Je suis transparent si l'autre l'est aussi. Je garde le secret si l'autre fait de même.

Elle entretient aussi une relation positive et intéressante avec la confiance. Confiance et confidence – c'est-à-dire le fait de révéler une information secrète – ont d'ailleurs la même étymologie[24].

En l'absence de ce système obligatoire de partage d'information, les acteurs seraient tentés de choisir des comportements compétitifs espérant bénéficier d'asymétries d'information.

Pourtant, peut-on imaginer un monde sans secret et totalement transparent ? Évidemment non. Nous sombrerions dans une nouvelle dictature.

Aurélien Colson prend l'exemple intéressant de la négociation qui s'adresse potentiellement à chaque individu au cours de sa vie que ce soit entre salarié / employeur, acheteur / vendeur, parent / enfant, États / ONG, ministre / syndicats, etc. **Le secret conserve en effet un grand intérêt pour tout négociateur !**

Au sein de l'entreprise, celle-ci se doit « *de maintenir la confidentialité sur certains de ses objectifs, de ses choix stratégiques. La sensibilité extrême des marchés à la moindre rumeur justifie que la plus grande discrétion soit de mise sur certaines informations.* »

« Un paradoxe veut ainsi que dans un marché où l'information circule de façon plus transparente, le secret acquiert une valeur plus importante encore qu'auparavant. »

Prenant enfin l'exemple d'une négociation entre Hubert Védrine (alors ministre des Affaires Étrangères) et Madeleine Albright (alors secrétaire d'État des États-Unis), il indique que chaque point de la négociation était classé selon les quatre catégories suivantes :

- *nous sommes d'accord et nous souhaitons le rendre public*
- *nous sommes d'accord mais nous le garderons secret*
- *nous sommes en désaccord et nous le dirons*
- *nous sommes en désaccord mais nous le garderons secret*

« Observez la loi suprême ! Le secret. »

Honoré de Balzac
Les illusions perdues

[24] Confiance est un substantif qui appartient à la famille de foi, qui va donner se fier ou se défier, mais aussi confier. Jusqu'au XVIIème siècle, confiance et confidence sont des doublets, c'est-à-dire qu'ils ont le même sens. À partir du XVIIème siècle, confidence commence à prendre le sens de communication d'un secret.

3.2. Les textes de loi sur le secret et la confidentialité : le trop plein ?

3.2.1. Définitions

Pour faire face aux atteintes à la confidentialité et aux secrets des données, aux fraudes, aux accès non autorisés et à l'espionnage, les entreprises souhaitent mieux protéger l'information industrielle et commerciale. Ces connaissances, de nature technique, commerciale, administrative, financière ou autre, constituent le savoir-faire des entreprises et leur assurent un avantage concurrentiel dont la valeur doit être protégée ; elles constituent leur patrimoine informationnel.

L'un des moyens de protection repose sur **la confidentialité des informations** transmises aux salariés ou aux partenaires. La notion de confidentialité peut être définie comme le « *Caractère de ce qui est confidentiel* » (le terme « confidentiel » étant entendu comme « *ce qui a été communiqué à quelqu'un sous l'interdiction, pour celui-ci, de le révéler à quiconque, qui est livré par écrit ou oralement sous le sceau du secret (en confiance et confidence) ; qui doit être accompli en secret.* ») *(G. Cornu, Vocabulaire juridique, V°Confidentialité).*

L'autre moyen de protection est le **secret professionnel**, une obligation légale sanctionnée pénalement en vertu de l'article 226-13 du Code pénal. Selon ce texte, « *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* ».

Il se définit comme l'« *obligation, pour les personnes qui ont eu connaissance de faits confidentiels dans l'exercice ou à l'occasion de leurs fonctions, de ne pas les divulguer hors les cas où la loi impose ou autorise la révélation du secret ; obligation, sanctionnée par la loi pénale, qui pèse sur les médecins, chirurgiens, pharmaciens, sages-femmes, mais également sur toutes autres personnes, dépositaires par état, profession ou fonctions (temporaires ou permanentes), des informations à caractère secret qu'on leur confie (avocats, notaires, ministres du culte, etc.) et qui dispense de celle de déposer sur les faits appris dans ces conditions » (G. Cornu, Vocabulaire juridique, V°Secret professionnel).*

La consécration du secret professionnel a pour conséquence de faire encourir, outre la condamnation à des dommages et intérêts, des sanctions pénales aux personnes tenues au secret qui auront donné des renseignements, hors les cas où la loi les y autorise ou les y oblige. La condamnation suppose naturellement que soit reconnu l'élément intentionnel du délit (Cour d'appel de Grenoble, ch. corr., sect. B, 9 févr. 2000).

Par conséquent, contrairement à la confidentialité qui est de nature contractuelle, le secret professionnel est d'ordre public et établi dans l'intérêt des clients de certains professionnels qui, pour le bon exercice de leur activité, ont la qualité de « *confidents nécessaires* ». Son but est donc d'assurer la confiance dans certaines professions (avocats, médecin, assistante sociale, notaires, banquiers, ...).

« Mais le secret professionnel couvre uniquement ce qui est secret et seule la révélation d'une «information à caractère secret» est punissable. »

Maître Éric A. Caprioli
Avocat à la Cour

Toute appréhension des secrets de l'entreprise ne constitue pas automatiquement une faute. Non seulement l'entreprise peut être tenue de révéler certains de ses secrets, mais surtout ces derniers ne font pas l'objet d'un droit privatif (CA Paris 3 juillet 1975 ; Cass. Com. 18 janvier 1982, Bull. civ., IV, n° 14). Ainsi, à partir du moment où une information de nature confidentielle a été acquise de manière légitime, elle peut en principe être librement utilisée. L'entreprise conserve cependant le droit de classer certaines de ses informations comme étant strictement confidentielles (politique de confidentialité). Par conséquent, lorsque l'entreprise manifeste sa volonté de conserver secrètes des données et, par conséquent qu'elle en interdit ou encadre strictement l'accès et la divulgation (Politique d'IAM[25] ou de gestion des droits et des accès), le tiers non autorisé commet une faute (concurrence déloyale), voire un délit (abus de confiance, ...) s'il cherche à obtenir les informations protégées.

Enfin, il faut également citer les exigences de la loi n° 78-17 du 6 janvier 1978 « Informatique, Fichiers et Libertés » dont l'article 34 soumet le responsable du traitement des données à caractère personnel à l'obligation de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, afin de préserver la sécurité des données tout en interdisant la communication de ces informations à des personnes non autorisées, et sous peine de sanctions pénales, (Cour d'appel de Rennes, ch. corr., 13 janv. 1992, X c/ Proc. Rép. Guingamp et autres,). Ces obligations sont reprises aux articles 226-21 et suivants du Code pénal.

« En vertu du nouvel article 34Bis de la loi de 1978 (ordonnance n° 2011-1012 du 24 août 2011) les fournisseurs au public de services de communications électroniques sur les réseaux de communications électroniques ouverts au public, doivent notifier à la CNIL les violations de données personnelles. »

Isabelle Cantero
Cabinet Caprioli Avocats

3.2.2. Secret bancaire et secret médical

S'agissant du secteur bancaire, l'article L.511-33 du Code monétaire et financier dispose que « *tout membre d'un conseil d'administration et selon le cas, d'un conseil de surveillance et toute personne qui à un titre quelconque participe à la direction ou à la gestion d'un établissement de crédit ou qui est employée par celui-ci, est tenu au secret professionnel dans les conditions et sous les peines prévues à l'article L. 571-4 du Code monétaire et financier* ».

Par ailleurs, l'article 154 de la loi n°2008-776 du 4 août 2008 de modernisation de l'économie a étendu le secret bancaire aux entreprises d'investissement. Il résulte du texte modifié que les établissements de crédit peuvent, dans les cas prévus par la loi, sans avoir à obtenir le consentement du client, faire circuler des informations normalement couvertes par le secret bancaire. En dehors de ces cas, le consentement du client doit être obtenu. Ainsi, par exemple, la chambre commerciale a jugé, le 18 septembre 2007, que « *l'obligation au secret professionnel à laquelle sont tenus les établissements de crédit leur interdit de fournir à un client qui en formule la demande des renseignements autres que simplement commerciaux d'ordre général et économique sur la solvabilité d'un autre de leurs clients* » (Cass. com., 18 sept. 2007, no 06-10.663.).

[25] Identity and Access Management

Dans le domaine de santé, le droit au secret et à la confidentialité fait partie des droits généraux du malade. De manière plus particulière, de nombreux articles du Code de déontologie médicale concernent directement ou indirectement le secret professionnel applicable au personnel de santé. Par exemple, l'article 4 de ce texte impose au médecin une obligation de secret de tout ce qui est venu à sa connaissance 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* » (art. R.4127-4 du code de santé publique). Dans le même sens, la loi n° 2002-303 du 4 mars 2002 relative aux droits des malades vise notamment à favoriser l'accès du patient aux données médicales, tout en préservant leur confidentialité. À cet égard, elle a introduit l'article L.111-8 du Code de la santé publique qui définit les grandes lignes de l'encadrement de l'activité de l'hébergement des données de santé à caractère personnel et pose les prémisses du dossier médical personnel (DMP), instauré par la loi n° 2004-810 du 13 août 2004 relative à l'assurance maladie.

Chaque hébergeur doit ainsi être agréé pour son activité, son dossier de demande d'agrément mettant l'accent sur les garanties de sécurité et de confidentialité. Ces garanties s'étendent plus particulièrement au respect des droits des personnes concernées par les données hébergées et à la sécurité de l'accès aux informations (art. R.111-14 du Code de santé publique). Dans la continuité de cette réglementation, le décret « confidentialité » (décret n° 2006-6 du 4 janvier 2006 relatif à l'hébergement de données de santé à caractère personnel) codifié aux articles R.1110-1 et suivants du même code est venu préciser les mesures techniques et organisationnelles à mettre en œuvre de sorte que l'échange et le partage des données garantissent la même sécurité et confidentialité aux données que l'hébergement de celles-ci. Ce texte rend donc obligatoire l'utilisation de la carte de professionnel de santé pour l'accès, l'échange et le partage de données de santé à caractère personnel, cette carte permettant notamment d'authentifier son porteur et de « tracer » ses actions.

Ainsi, le secret bancaire, à la différence du secret médical, n'est pas absolu mais relatif.

3.2.3. Secret des correspondances

Selon l'article 226-15 du code pénal, l'atteinte au secret des correspondances se définit comme « *le fait commis de mauvaise foi, d'ouvrir, de supprimer, de retarder ou de détourner des correspondances arrivées ou non à destination et adressées à des tiers, ou d'en prendre frauduleusement connaissance.* »

Le terme correspondances doit être compris de façon générale et s'entend de tous messages ou plis fermés ou non adressés par une personne à une autre personne dénommée ; ce qui englobe les messages électroniques et les télécopies. La peine encourue est fixée à un an d'emprisonnement et 45 000 euros d'amende.

L'atteinte à ce secret peut également être commise par un fonctionnaire ou assimilé, avec une aggravation des sanctions à l'article 432-9 du Code pénal qui prévoit une peine de trois ans d'emprisonnement et de 45 000 euros d'amende. À la différence de l'article 226-15, l'article 432-9 ne reprend pas les termes de mauvaise foi pour désigner la teneur de l'élément intentionnel de l'infraction.

3.2.4. Les hypothèses d'atteintes

Le respect de la confidentialité est soumis à des intérêts contradictoires, mais aussi à des exigences contradictoires (protection de la vie privée d'une part, et nécessités de l'administration fiscale d'autre part ; protection des intérêts de l'entreprise d'une part, et la liberté d'expression des salariés d'autre part, etc.).

Le jugement rendu par le TGI de Béthune le 14 décembre 2010 apporte une nouvelle illustration des enjeux juridiques relatifs aux clauses de confidentialité figurant dans les contrats de travail ainsi qu'à leurs conséquences sur la protection des informations et de la réputation de l'employeur.
En l'espèce, l'ancien salarié d'une entreprise a été condamné à un montant symbolique d'un euro (en raison de l'impossibilité d'évaluer le préjudice subi par l'employeur) pour avoir publié sur Internet des contenus dénigrant son ex-employeur en violation d'une clause contractuelle antérieurement signée. Par ailleurs, la question de confidentialité est aussi souvent abordée sous l'angle du règlement intérieur de l'entreprise ou de codes d'éthique (V. TGI Nanterre, 2e ch., 19 oct. 2007).
La violation du secret professionnel comporte des sanctions importantes. D'une part, sur le plan pénal, elle engage la responsabilité personnelle de la personne qui dévoile l'information couverte par le secret. Par exemple, en matière bancaire, la méconnaissance du secret professionnel est sanctionnée par les peines prévues aux articles 226-13 du Code pénal. D'autre part, sur le plan civil, c'est la responsabilité délictuelle et quasi-intellectuelle qui peut être retenue en vertu des articles 1382 à 1384 du Code civil. Par exemple, l'établissement de crédit, civilement responsable de son employé, peut être condamné à payer, à la personne victime de l'indiscrétion, des dommages – intérêts destinés à compenser le préjudice matériel ou moral qu'elle a subi.

Dans le domaine bancaire, la communication à un autre établissement bancaire des informations couvertes par le secret bancaire et en violation de la charte informatique a été réprimée dans une décision du conseil des prud'hommes de Nanterre du 15 septembre 2005 (RD bancaire et fin. 2006, comm. 82, note Éric A. Caprioli).

En matière de santé, les juges ont eu l'occasion de prononcer l'engagement de la responsabilité civile sur le fondement de l'article 1382 du Code civil d'un médecin traitant qui, dans le cadre d'une procédure contractuelle de conciliation, a communiqué des informations d'ordre médical sans l'accord ou la demande de son patient au médecin-conseil d'une compagnie d'assurances. L'immixtion dans un litige opposant le patient avec son assureur ainsi constaté a été aggravé par la violation flagrante du secret médical. Les juges ont estimé que la faute du médecin a causé un préjudice moral certain au patient anormalement dépossédé d'informations médicales, donc d'essence intime, et a eu pour effet de conforter l'assureur dans son refus de prendre en charge le sinistre et finalement de donner une nature judiciaire au litige entre l'assureur et son assuré. Les dommages et intérêts ont été évalués à 3 000 euros. (Cour d'appel de Metz, 13 mars 2002).

Dans le domaine des correspondances, en vertu d'un arrêt de la Cour d'appel de Paris du 17 décembre 2001 : un administrateur réseau et le chef d'un laboratoire de recherche ont été condamnés sur le fondement de l'article 432-9 du Code pénal en raison de la divulgation du contenu des messages électroniques privés d'un chercheur du laboratoire.

3.2.5. Quelles perspectives ?

Le système juridique français comporte de nombreuses qualifications qui peuvent entraîner des sanctions pénales pour la diffusion des informations confidentielles : l'abus de confiance, le vol, le recel, les contrefaçons de droits d'auteur, les atteintes au secret de fabrique ou civiles pour les violations de clauses de confidentialité.

Toutefois, en matière pénale, qui demeure le meilleur endiguement, les affaires Valéo (TGI Versailles, 18 déc. 2007) et Michelin (TGI Clermont-Ferrand du 21 juin 2010) ont largement mis en évidence le manque de moyens juridiques pour sanctionner les cas d'atteinte au patrimoine informationnel de l'entreprise et nous amènent à penser que la qualification d'abus de confiance semble être la seule disposition pénale applicable en matière d'espionnage par un salarié et de divulgation de secrets d'affaires, à l'exclusion de toute autre et notamment du vol de données dématérialisées qui n'a été retenu que par quelques jurisprudences isolées.

Dans le premier de ces litiges, une stagiaire de l'entreprise qui avait reproduit des documents confidentiels sur son disque dur personnel a été condamnée sur le fondement de l'abus de confiance pour des agissements qui étaient manifestement contraires à l'engagement de confidentialité et au règlement intérieur mis en place par l'employeur. Sa peine s'élevait à un an d'emprisonnement dont dix mois avec sursis, accompagné de 7 000 euros de dommages et intérêts.

Dans l'affaire Michelin, un salarié a été retenu coupable d'actes d'abus de confiance sur la base de l'article 314-1 du Code pénal en tant que détenteur à titre précaire des données couvertes par la confidentialité visée dans son contrat de travail qui a fait usage desdites informations à des fins sans rapport avec son activité professionnelle.

Par conséquent, l'État français et ses entreprises gagneraient à ce que soit adopté un cadre juridique spécifique à la protection du secret des informations économiques pour contrer les actes de malveillance et les atteintes au patrimoine informationnel des entreprises. Tel est d'ailleurs le sens de la proposition de loi déposée à nouveau en janvier 2011, suite à l'affaire Renault, par le député Bernard Carayon qui, en renvoyant à l'infraction d'abus de confiance, punit de trois ans d'emprisonnement et 375 000 euros d'amendes le fait pour toute personne non autorisée de « *s'approprier, de conserver, de reproduire ou de porter à la connaissance d'un tiers non autorisé une information à caractère économique protégée ou de tenter de s'approprier, de conserver, de reproduire ou de porter à la connaissance d'un tiers non autorisé une information à caractère économique protégée* ».

Mais finalement, étant donné que le droit pénal n'intervient qu'a postériori, la meilleure des réponses reste encore et toujours l'anticipation de la survenance des risques et la mise en place de mesures techniques, organisationnelles, encadrées par des documents à valeur juridique (contrats, engagement du salarié ou des prestataires, ...).

La sécurité des données de l'entreprise repose sur un travail d'équipe impliquant les directions informatiques, de la sécurité et du juridique.

3.3. Le rôle des normes internationales : un langage enfin partagé ?

Ainsi, depuis près de 25 ans, le monde de la Sécurité des SI est fortement impacté par un ensemble de lois répondant pour beaucoup à la protection des données en termes de confidentialité alors qu'en même temps les obligations de transparence deviennent aussi plus fortes. Tout ceci s'inscrit dans un contexte international qu'on ne peut pas ignorer.

Le monde de la Sécurité des SI a aussi été peu à peu « envahi » par des normes internationales de toutes natures et aux finalités nombreuses. Dès 1996, les normes ISO/IEC 10181 1-7 ont statué sur les 7 grands axes que sont : la disponibilité, l'intégrité, **la confidentialité**, l'authentification, le contrôle d'accès, la non répudiation, l'audit.

> ***Depuis 15 ans, la confidentialité est définie par la norme ISO/IEC 10181-5 comme « le fait de s'assurer que l'information n'est seulement accessible qu'à ceux dont l'accès est autorisé. »***

La confidentialité est présentée ici comme un objectif (et non un état) s'appuyant sur des règles de contrôle d'accès à l'information.

3.3.1. ISO/IEC 27002

La série des normes ISO/IEC 2700x est le fruit de travaux initiés en Angleterre à la fin des années 90. La norme BS 7799 est devenue une norme internationale en 2000 (ISO 17799 puis ISO 27002). Cet ensemble de bonnes pratiques (on en dénombre plus de 130) s'inscrit dans la gestion de la **sécurité de l'information** et non de l'informatique ou des systèmes d'information. La nuance est d'importance. Mais dans le fond, les thèmes abordés s'adressent essentiellement aux systèmes d'information.

L'information y est présentée comme un bien essentiel à tout organisme. Il est donc important qu'elle soit protégée de toute menace interne ou externe. **L'enjeu est d'en préserver** la disponibilité, l'intégrité et **la confidentialité**. Cette dernière demeure ici encore une finalité.

Pour ce faire, l'organisme doit mener un ensemble d'actions et mettre en place les processus requis en termes :

- De politique (règles et directives) et d'organisation (acteurs et processus)
- D'inventaire et de classification des actifs : informations, logiciels, matériels physiques, savoir-faire...) via une fonction de « **propriétaire** »
- De formation et sensibilisation des utilisateurs sur les risques et menaces pesant sur l'information
- De communication
- De gestion et contrôle de l'accès aux données
- De développement et maintenance des systèmes d'information
- De détection et traitement des incidents de sécurité
- D'établissement de plans de continuité de l'activité
- De conformité au regard des lois, des réglementations et de la politique de sécurité

L'ensemble de ces considérations doit être pris en compte dès le lancement d'un projet puis être suivi et contrôlé tout au long de son cycle de vie.

3.3.2. ISO/IEC 27005

À la différence de la norme ISO/IEC 27002, la confidentialité est traitée non pas en tant qu'objectif concret mais dans le cadre des analyses de risques pouvant conduire à une « **perte de confidentialité** ».

En relation avec la norme ISO/IEC 27002, une méthodologie doit être respectée en s'appuyant sur l'inventaire et la classification des actifs. Sont présentés 6 chapitres touchant à la gestion des atteintes à la confidentialité des informations :

- Chapitre 7 : établir le contexte de l'analyse des risques
- Chapitre 8 : définition de l'appréciation des risques
- Chapitre 9 : quatre choix du traitement du risque
- Chapitre 10 : acceptation du risque
- Chapitre 11 : communication du risque
- Chapitre 12 : surveillance et réexamen des risques

On constate donc que cette norme en reste au niveau des principes et ne fournit pas d'élément concret sur les scénarios d'atteinte à la confidentialité des informations.

Il nous faut rechercher dans d'autres travaux ou documents de référence, des éléments de réponses sur le lien entre « atteinte à la confidentialité » et « analyse de risques ».

3.4. Des référentiels nationaux : au-delà du domaine public ?

Il est frappant de constater que des textes, qu'on qualifiera de référence, existent mais qu'ils demeurent parfois méconnus[26]. Nous retiendrons ici trois documents récents particulièrement instructifs :

• La méthode EBIOS (Evaluation des Besoins et Identification des Objectifs de Sécurité) produite par l'Agence Nationale à la Sécurité des Systèmes d'Information.
• Le Référentiel Général de Sécurité (RSG) publié par arrêté du Premier Ministre le 10 mai 2010.
• L'instruction générale interministérielle sur la protection du secret de la Défense Nationale (IGI 1300) signée par le 1er Ministre le 23 juillet 2010.

3.4.1. La méthode EBIOS

Loin de nous l'idée de présenter ou de promouvoir ici la méthode EBIOS. Nous nous focaliserons sur un de ses apports essentiels sous la forme d'une base de connaissances. Elle comble ici un manque important de la norme ISO 27005 à savoir les scenarii de risques ou de menaces à prendre en compte dans les analyses de risques.

Ainsi, sur un ensemble de 51 menaces structurées en 9 catégories, 27 (soit plus de la moitié) sont liées aux questions de confidentialité. Le tableau ci-dessous indique les typologies de menaces proposées par la méthode EBIOS.

Catégorie	Type de menace	Moyens requis
Menaces sur le matériel	Détournement de l'usage prévu d'un matériel	Sans objet
	Espionnage d'un matériel	
	Modification d'un matériel	
	Perte d'un matériel	
Menaces sur les logiciels	Détournement de l'usage prévu d'un logiciel	Sans objet
	Analyse d'un logiciel	
	Modification d'un logiciel	
	Disparition d'un logiciel	
Menaces sur les canaux informatiques et de téléphonie	Ecoute passive d'un canal informatique ou de téléphonie	Sans objet
Menaces sur les personnes	Espionnage d'une personne à distance	Sans objet
	Influence sur une personne	
	Départ d'une personne	
Menaces sur les supports papier	Espionnage d'un support papier	Sans objet
	Perte d'un support papier	

[26] www.ssi.gouv.fr

Catégorie	Type de menace	Moyens requis
Menaces sur les canaux interpersonnels	Espionnage d'un canal interpersonnel	Sans objet
Sources humaines agissant de manière délibérée	Interne et malveillante	Faibles
		Importants
		Illimités
	Externe et malveillante	Faibles
		Importants
		Illimités
Sources humaines agissant de manière accidentelle	Interne sans intention de nuire	Faibles
		Importants
		Illimités
Sources humaines agissant de manière accidentelle	Externe sans intention de nuire	Faibles
		Importants
		Illimités
Sources non humaines	Code malveillant d'origine inconnu	Sans objet

Ainsi, la perte, l'erreur ou la manipulation côtoient le vol, la malveillance et l'espionnage avec systématiquement, une mise en danger des informations sensibles.

3.4.2. Le Référentiel Général de Sécurité

Élaboré par l'ANSSI et publié par arrêté le 6 mai 2010, le Référentiel Général de Sécurité s'adresse à toutes les Autorités Administratives ainsi qu'à leurs prestataires impliqués dans la Sécurité des SI.

Il s'inscrit avant tout dans le cadre de la modernisation de l'État et du développement de la confiance numérique.

Il définit un ensemble de règles et de bonnes pratiques en matière de sécurité des systèmes d'information sur lesquelles nous n'insisterons pas et qui s'inspirent des normes ISO 2700x.

Les questions de confidentialité sont abordées dans le document à trois niveaux :

• En termes d'enjeux : la perte de confidentialité via l'accès par une personne non autorisée à des données confidentielles
• En termes de fonction de sécurité (au même titre que l'authentification, la signature électronique et l'horodatage)
• En annexe, en ce qui concerne la mise en œuvre pratique du chiffrement et des mécanismes cryptographiques

Le chapitre 3.4 consacré à la « confidentialité » reprend les définitions clés et pose les bases des bonnes pratiques opérationnelles du chiffrement. Il est précisé dans son introduction que :

*« **La confidentialité** est « **le caractère réservé d'une information dont l'accès est limité aux seules personnes autorisées à la connaître** ». Le chiffrement ainsi que des mesures de gestion des accès (droits de lecture, écriture, modification) permettent de préserver la confidentialité des données.*

Le chiffrement est un procédé cryptographique garantissant la confidentialité des données chiffrées contre toute personne ne possédant pas la clé de déchiffrement. Il s'agit du mécanisme essentiel de protection de la confidentialité.

Par ailleurs, la confidentialité des informations peut aussi être protégée par des mesures complémentaires de gestion des droits d'accès de chacun, en lecture, en écriture ou en modification, aux données contenues dans le système d'information. Ces droits d'accès sont déterminés, en fonction du strict besoin d'en connaître des usagers et de celui des agents dans le cadre de leurs missions. À cet effet, il est recommandé que des mécanismes techniques soient mis en place pour s'assurer que seules les personnes autorisées puissent accéder aux données en fonction de leur besoin d'en connaître. Il est recommandé également que ces mécanismes soient robustes et implémentés au plus près du lieu de stockage des données.

Dans tous les cas, les mécanismes de chiffrement et les mécanismes techniques de gestion des droits d'accès, dès lors qu'ils font appel à des mécanismes cryptographiques, doivent respecter les exigences fixées dans les référentiels mentionnés au chapitre 3.4.1. »

3.4.3. L'IGI 1300

Bien qu'indiquant en préambule de ce chapitre que nous excluions le Secret de la Défense Nationale de notre analyse, il nous a semblé intéressant de faire référence à un document qui pourrait sans doute être adapté à d'autres contextes.

Ce texte publié le 26 juillet 2010, sous forme d'instruction générale interministérielle, s'adresse à la **protection du secret de la Défense Nationale**.

Au-delà des enjeux nationaux qu'il couvre, il contient des principes et des pratiques applicables dans tout domaine d'activité.

Toute information ou support, dont la diffusion doit être maîtrisée et limitée afin de ne pas nuire à la Défense Nationale, est classifié selon trois niveaux :

Niveau de classification	Définition
Très Secret Défense	réservé aux informations et supports dont la « **divulgation est de nature à nuire très gravement à la défense nationale** »
Secret Défense	réservé aux informations et supports dont la « **divulgation est de nature à nuire gravement à la sécurité nationale** »
Confidentiel Défense	réservé aux informations et supports dont la « **divulgation est de nature à nuire à la sécurité nationale ou pourrait conduire à la découverte d'un secret classifié au niveau Très Secret Défense ou Secret Défense** »

Seules les personnes, dont la fonction ou l'accomplissement de leur mission nécessite la connaissance d'informations classifiées, y ont accès. Elles sont alors soumises à des obligations de confidentialité.

La décision de classifier résulte de l'analyse de « **l'importance de l'information au regard de son contexte** ». Ce choix est important : il faut éviter de sur-classifier, ce qui altèrerait la valeur du secret, ou de sous-classifier, ce qui nuirait à la sécurité nationale.

Notons qu'une **durée de classification** est précisée lors de la classification d'un document. Ce délai peut être réévalué.

Dès lors que l'information est traitée sous forme numérique, des mesures de sécurité sont requises à trois niveaux :

• En termes d'**organisation** : mise en place d'une politique de sécurité qui définit les « principes et exigences de sécurité du système » ainsi que la gestion des incidents
• En termes de **moyens techniques** : « protections techniques du système » ainsi que « la gestion et le contrôle des accès »
• En termes de **défense en profondeur**, basée autour de cinq axes : « prévenir » (éviter l'apparition de failles de sécurité), « bloquer » (empêcher les attaques), « contenir » (limiter les conséquences d'une attaque), « détecter » (pouvoir identifier les incidents) et « réparer » (remettre le système en fonctionnement suite à une attaque).

3.5. Synthèse

Gérer la confidentialité des informations peut sembler une utopie au regard du contexte d'évolution de nos sociétés.

D'une part, la transparence est érigée comme valeur incontournable de la démocratie. **Le secret devient suspect !** Déjà en 1498, Jean de la Véprie énonçait que :

« Secret de deux, secret de Dieu ; secret de trois, secret de tous. »

D'autre part, les entreprises et les administrations se sont ouvertes et interconnectées entre elles, avec leurs clients, usagers, partenaires et fournisseurs. **La fermeture c'est la mort !** En 2004, Alain Juillet alors en charge des questions d'Intelligence économique auprès du Premier Ministre affirmait aussi que « *les secrets d'entreprise sont de plus en plus rares* ».

Tandis que les jeunes générations vivent en connexion permanente avec les nouveaux « Dieux » que sont iPhone et Facebook, l'information prend une valeur nouvelle qu'elle soit vraie ou fausse, privée ou publique, peu importe. Il faut la posséder et la consommer. Revisitant Descartes et son « *Je pense donc je suis* », le XXIème siècle découvre le ***« Je communique donc j'existe ! »*** Mais, un proverbe turc affirme depuis longtemps que « *Tu dis ton secret à un ami, mais ton ami a un ami aussi.* » !

Alors, qu'est-ce que le secret et la confidentialité à l'ère du numérique ?

Un rapport d'information parlementaire a été produit par l'Assemblée Nationale le 22 juin 2011. Son titre : **« Les droits de l'individu dans la révolution numérique »**. Fort de 384 pages, le document aborde l'ensemble des aspects politiques et sociétaux mais aussi très pratiques concernant les citoyens comme les entreprises et les administrations.

Qu'en retenir d'intéressant pour notre Livre Bleu ?
• Une définition du "numérique" : « *L'ensemble des techniques de communication qui utilisent des signaux numériques, notamment dans la reproduction des images.* »
• Un focus très important sur le poids de 2 acteurs clés que sont Google et Facebook et sur la problématique du Cloud Computing
• Un chapitre de 115 pages sur « *Le droit à une protection dans l'univers numérique* »

Les questions de secret et de confidentialité ne sont pas absentes de la dialectique :
• Le secret est abordé une vingtaine de fois dont la moitié sur le thème des réseaux sociaux
• La confidentialité est citée une vingtaine de fois dont la moitié pour les réseaux sociaux

Mais il est particulièrement impressionnant de constater que le terme « *vie privée* » apparaît près de 300 fois dans le document…

Au regard des éléments proposés, nous pouvons établir un premier constat en quatre points :
1. D'un côté, le secret est très présent dans les textes de loi alors que la confidentialité y est quasi inexistante[27]. De l'autre, les normes ISO 2700x n'abordent pas du tout le secret et se concentrent exclusivement sur l'objectif de confidentialité.
2. Une distinction juridique en termes de responsabilité contractuelle / civile ou pénale est possible comme semble l'indiquer Maître Éric A. Caprioli.
3. Une distinction pratique de nature temporelle (un secret peut être levé, sans pour cela rendre l'information publique) pourrait aussi être proposée.
4. Plus simplement, le nombre de ceux qui ont « le droit d'en connaître » n'est-il pas tout simplement très limité pour le secret (quelques-uns), plus large pour le confidentiel ?

Nous pouvons aussi dégager quelques points fondamentaux et des questions clés qui orienteront l'analyse du chapitre 4 reprenant les résultats de l'enquête du Cercle.

3.5.1. Les trois points fondamentaux

Si nous partons de l'hypothèse que notre idéal démocratique ne s'éteint pas, un équilibre doit être trouvé entre la liberté de communiquer, de partager et d'échanger et les exigences de secret / confidentialité dans le cadre de la sécurité numérique.

Ainsi, la confidentialité et le secret doivent être **garantis par la Loi et les règlements** pour pouvoir sanctionner tout abus ou malveillance. Ils doivent aussi être maintenus dans la durée en s'adaptant aux évolutions de la société. De plus, l'usage des politiques, des chartes, des clauses et accords de confidentialité, des codes d'éthiques sur le Web voire des messages d'alerte des courriels doit se développer et se renforcer au regard des enjeux visés. Mais ils ne seront jamais suffisants. En particulier, le concept de Politique de Sécurité du SI couvrant les 4 objectifs DICT[28], ne doit-il pas être revu ?

Par ailleurs, l'**exercice de classification** ne doit pas être négligé et encore moins ignoré. Définir une typologie de données confidentielles selon différents degrés demeure fondamental. Cependant, des difficultés demeurent. Comment sont définis les seuils d'impact en termes de secret / confidentialité ? Par qui ? Comment aller au-delà de la norme de classification ? Et à quoi sert-elle finalement ?

Enfin, garantir le secret et la confidentialité à l'ère du numérique ne peut pas s'opérer uniquement dans la sphère des systèmes d'information et de ses normes.

---

[27] Par exemple, aucune citation avec « confidentiel » ou « confidentialité » n'a pu être proposée.
[28] Disponibilité, Intégrité, Confidentialité, Traçabilité

Plus que jamais les synergies et les travaux doivent se dérouler en **impliquant tous les acteurs concernés au plus près des « propriétaires »**, « dépositaires », « hébergeurs », « utilisateurs », « destinataires », etc. dans une logique de « flux » plus que de « fichier » ou de « traitement ». L'enjeu est bien sûr d'associer systématiquement et intelligemment, sécurité informatique et sécurité physique, mesures techniques, juridiques et comportementales.

3.5.2. Les questions en suspens

Si nous partons de ces trois points pour bâtir la démarche de gestion du secret et de la confidentialité, des questions demeurent néanmoins en suspens.

1. Comment aller au-delà de l'identification et de la classification des informations confidentielles ?

En effet, les processus de gestion des informations sont devenus complexes, nombreux et variés. La confidentialité doit être abordée de l'amont (création) jusqu'à l'aval (archivage / destruction). Les efforts et les coûts pour traiter l'ensemble de la question pourront sembler trop importants pour certains ... Place au pragmatisme ?

Par exemple : Doit-on toujours proposer une classification en fonction de seuils d'impacts (gravité d'une perte ou divulgation) ? Comment sont définis ces seuils en termes médiatiques, financiers, juridiques ? Et par qui ? Qu'est-ce qui distingue alors le secret du confidentiel ? Uniquement le nombre de ceux qui « ont à en connaître » ? Et surtout, comment minimiser la part de la subjectivité ?

2. Comment détecter et inventorier les atteintes aux données confidentielles ?

En effet, autant les vulnérabilités et les attaques logiques se dénombrent par centaines de milliers, autant les atteintes à la confidentialité des données apparaissent marginales telle une partie immergée de l'iceberg, faute d'aller voir sous l'eau ! Comment développer les processus d'alerte permettant d'inventorier et de notifier les atteintes à la confidentialité ?

Ici encore, l'éthique prend une importance fondamentale. Quels sont les outils vraiment nécessaires et comment seront-ils mis en œuvre et exploités (DLP et gestion des traces par exemple). Devra-t-on aller jusqu'aux pratiques de « whistleblowing » américaines ? La notification ou l'alerte devra s'effectuer auprès de qui ? Et surtout comment ?

3. Comment développer une cyber-éthique en termes de confidentialité avec des « règles du jeu » partagées ?

Ceci s'entend aussi bien au sein d'une entreprise ou d'une administration (employeur / salarié) que dans le cadre de partenariats (entreprise / fournisseurs et partenaires), de relations commerciales (client / fournisseur) comme des relations entre États (négociations).

Peut-on imaginer des règles du jeu partagées, formelles, comprises et réciproques partant du principe de Confucius « *Ne fais pas aux autres ce que tu n'aimerais pas qu'on te fasse.* » ?

Ces différents aspects seront appréhendés au chapitre suivant à la lumière des résultats de l'enquête annuelle du Cercle.

« Dire le secret d'autrui est une trahison, dire le sien est une sottise. »

Voltaire (1694-1778)
L'Indiscret - 1725

4. DU PRINCIPE À LA PRATIQUE

4.1. Introduction

Partant des orientations et des questions clés des chapitres précédents, les résultats de l'enquête annuelle du Cercle Européen de la Sécurité et des Systèmes d'Information vont apporter un éclairage plus concret sur la dialectique, centré sur le monde de l'entreprise, des administrations et des services publics.

Nous appliquons ici quatre principes :

Principe N°1 : Exploitation des réponses apportées par un échantillon de 223 professionnels à une série de 13 questions.

Principe N°2 : Analyse des réponses structurée en 4 thématiques.

- Importance accordée aux questions de secret et de confidentialité de l'information
- Typologie des atteintes au secret et à la confidentialité constatées
- Nature et efficacité des moyens mis en place pour protéger l'information
- Perspectives liées aux usages des technologies de l'information

Principe N°3 : Présentation des résultats pour 3 secteurs si les enseignements sont intéressants (écarts significatifs).

- Banques / Assurances
- Industries / Services
- Administrations / Services publics

Les 3 secteurs d'activité	Banques Assurances	Industries Services	Administrations Services publics

Par ailleurs, un « zoom santé » sera également proposé sur certaines questions en mettant à profit la participation d'une quarantaine de professionnels du secteur. Les questions de secret (médical) et de confidentialité (liées à la carte CPS) méritent une attention particulière dans un secteur marqué par de nombreuses initiatives comme la télésanté, l'hôpital numérique, le dossier médical personnel, etc.

Principe N°4 : Conclusions factuelles et peu prospectives laissant aux lecteurs la liberté d'apprécier dans leur contexte particulier, leur pertinence ou leur utilité.

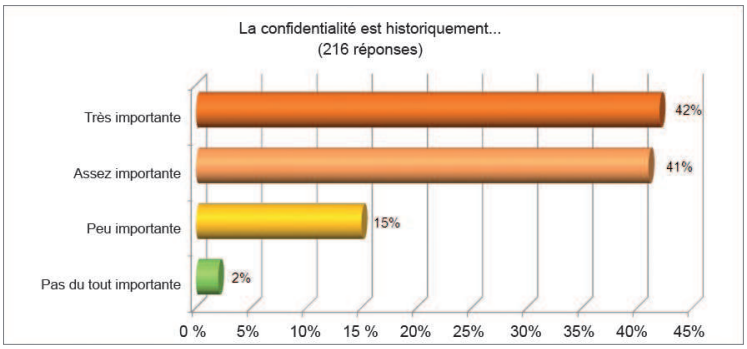
4.2. Quelle importance pour les questions de confidentialité ?

« La règle implicite qui a longtemps prévalu dans le monde des entreprises était le secret. »

Denis Kessler (Ancien vice Président du MEDEF)
L'entreprise entre secret et transparence – Pouvoirs n°97, 2001

Trois questions ont été posées à l'échantillon pour apprécier si les questions de secret et de confidentialité étaient ou deviennent importantes dans leur contexte historique et dans leur domaine d'activité. De toute évidence, le sujet est important pour une large majorité de répondants.

Question posée : Pour vos dirigeants, la confidentialité des informations, au sein de votre entreprise / organisme est de manière générale et historiquement...



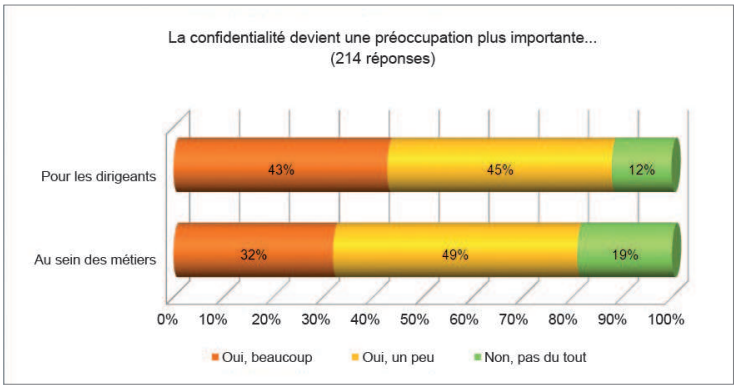
Une analyse par secteur d'activité apporte un éclairage différent et plus intéressant. Les Industries / Services se différencient des deux autres secteurs avec une importance moindre accordée au sujet.

	61 répondants	72 répondants	83 répondants
Très important	52 %	24 %	48 %
Assez important	38 %	47 %	39 %
Peu important	10 %	26 %	10 %
Pas du tout important	0 %	3 %	1 %

Ce constat peut paraître surprenant mais il est pourtant corroboré par de nombreux témoignages indiquant qu'au-delà des grandes entreprises industriels, une majorité d'acteurs des Industries / Services n'accorde pas à la confidentialité une importance majeure, privilégiant la continuité. On peut aussi imaginer que les répondants des Industries / Services appartenant à une DSI parlent exclusivement des données numériques.

La question est cependant de savoir si cette importance évolue dans le temps et pour qui. Est-ce plus marqué pour les dirigeants ou pour les managers au sein des métiers ?

Questions posée : Aujourd'hui, la confidentialité des informations, au sein de votre entreprise / organisme devient-elle une préoccupation plus importante pour les dirigeants / au sein des métiers ?



Ainsi, la préoccupation tend à se renforcer significativement (entre 70 et 90%) avec une perception légèrement différente selon qu'on est dirigeant (perception supérieure) ou au sein d'un métier (perception moins importante).

Nous ne constatons pas d'écart significatif pour les dirigeants selon les 3 secteurs d'activité. Cependant, au sein des métiers, le secteur Industries / Services apparaît ici aussi, en retrait par rapport aux deux autres.

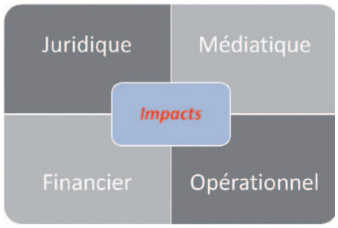
Au sein des métiers			
	60 répondants	73 répondants	81 répondants
Oui, beaucoup	40 %	17 %	39 %
Oui, un peu	43 %	56 %	46 %
Non, pas du tout	17 %	27 %	15 %

La confidentialité présente une importance accrue à la fois pour les dirigeants et les métiers.
Cette vision ne signifie-t-elle pas que, loin de devoir l'élargir ou la renforcer, l'enjeu est de mieux la circonscrire à des environnements / contextes ciblés et des préoccupations plus précises ?

4.3. Comment aborder le problème ?

La question du format de l'information et de son support est essentielle pour des raisons de pertinence et d'efficacité de l'action (avant tout en termes de prévention et protection). Si nous nous adressons ici aux données numériques, nous ne devons pas oublier que les supports sont aussi bien matériels (informatiques ou non) qu'intellectuels (savoir, connaissances).

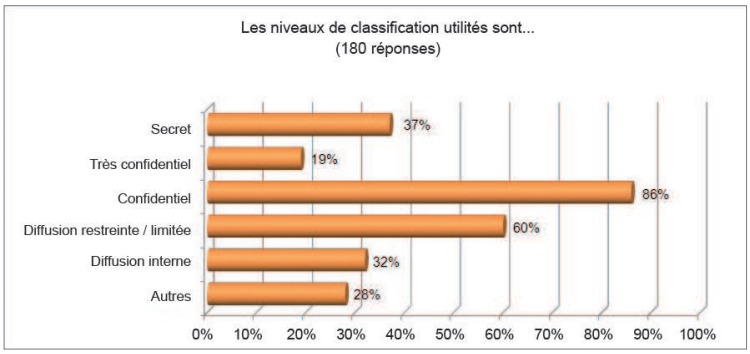
Ainsi, indépendamment de ce support, il est essentiel de pouvoir classifier l'information selon différents degrés qui caractérisent son importance, au regard des impacts (voir schéma ci-dessous) de toute perte, divulgation, vol, accès ou copie illicite.



4.3.1. La classification en question

Classifier les informations en termes de confidentialité n'est pas l'exercice le plus difficile qui soit, mais il faut aussi le faire correctement, efficacement, avec pertinence et de manière utile. Nombre d'entreprises possèdent des politiques et procédures en la matière. Mais pas toutes… En effet, 23% des répondants affirment ne pas posséder de règles de classification en confidentialité.

Question posée : La classification des informations s'effectue au sein de votre entreprise / organisme selon les niveaux…



Pour les autres, les pratiques s'avèrent très variées et il est remarquable que seulement 37% des répondants intègrent une classification au niveau « secret » qui peut être aussi assimilé à « très confidentiel » (19%).

Par ailleurs, 28% des répondants indiquent utiliser d'autres critères que ceux proposés. On peut imaginer le « très secret » gouvernemental, voire le « public » qui n'étaient pas explicitement indiqués.

Une analyse par secteur d'activité apporte un éclairage intéressant et montre quelques différences notables mentionnées dans le tableau ci-dessous.

	61 répondants	73 répondants	82 répondants
Secret	33 %	49 %	31 %
Très Confidentiel	22 %	14 %	21 %
Confidentiel	91 %	95 %	79 %

Ici aussi, le secteur des Industries / Services se distingue avec un usage plus important des classifications « secret » et « confidentiel », alors qu'il apporte une importance moindre au sujet.

Aucune norme de classification ne se distingue concrètement et chacun semble définir ses propres règles en la matière.

Loin d'être un exercice de style, ne doit-on pas exploiter plus largement l'IGI 1300 dans le domaine privé en l'adaptant aux types d'information spécifiques à chaque secteur d'activité ?

Une des questions essentielles réside dans l'usage que l'on fait de la classification des informations. Par nature, celle-ci est indépendante des mesures de prévention ou de protection, mais elle doit aussi être fondamentalement liée aux conditions d'usage et de manipulation de l'information.

À ce titre, il ne peut être fait l'économie de définir les mesures de sécurité appropriées :
• pour chaque niveau de classification : secret, confidentiel, etc.
• pour chaque type de support : numériques, imprimés, intellectuels, etc.
• pour chaque contexte de gestion : création, stockage, accès, échange, impression, destruction, copie, archivage, etc.

Et n'oublions pas que le **marquage** des documents / supports contenant l'information classifiée comme l'**habilitation** des personnes la détenant ou y accédant sont deux aspects essentiels de la protection.

On voit alors que les conditions d'une gestion rigoureuse de la confidentialité nécessite d'une part de bien se concentrer sur les informations les plus importantes (en termes d'enjeux pour un dirigeant ou un métier), et d'autre part d'impliquer voire de responsabiliser individuellement chaque acteur concerné, pour qu'il ne soit pas lui-même une source de vulnérabilité par des comportements inappropriés.

4.3.2. Une boîte à outils à l'efficacité incertaine...

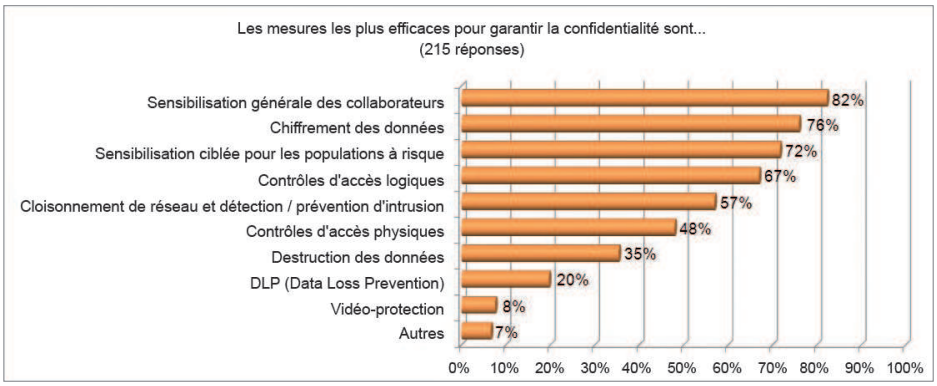
Les mesures de prévention et de protection visent à réduire les risques et les impacts de toute atteinte à la confidentialité. Si historiquement, la cryptographie a répondu au besoin de protection de l'écrit puis des communications orales, la discrétion voire le silence ne demeurent-ils pas les meilleurs garants du secret sous toutes ses formes ? Dans le numérique, cela signifierait une limitation drastique de la communication, du partage et des échanges. Le prix à payer ...

« C'est lorsqu'on procède par ce qu'on appelle "la sécurité par l'obscurité", c'est-à-dire que l'on met en œuvre un algorithme qu'on ne publie pas, qu'on garde secret, que l'on risque de se trouver confronté à des problèmes. »

Jacques Stern
Ce qui est secret est vulnérable – La Recherche, 2008

Désormais, tout se combine et le numérique est devenu le média le plus simple et le plus rapide pour communiquer et échanger que ce soient textes, vidéos, sons et images. Cependant, les mesures appropriées ne peuvent pas être uniquement de nature technologique et informatique, mais aussi comportementale et organisationnelle. Le schéma ci-dessous présente la position des répondants.

Question posée : Parmi les mesures suivantes, quelles sont, selon vous, les plus efficaces pour garantir la confidentialité des informations ?



La combinaison de la sensibilisation (générale et ciblée) avec des techniques de base (chiffrement et contrôle d'accès) apparaît comme la solution la plus pertinente et la plus efficace.

D'autres mesures techniques, nécessitant cependant des procédures qui peuvent être très contraignantes et coûteuses (gestion des correctifs, habilitations, gardiennage, etc.), complètent ce 1er arsenal. Mais elles n'apparaissent qu'en 2ème niveau.

Une analyse par secteur d'activité apporte un éclairage différent sur quelques réponses proposées avec des écarts significatifs.

	61 répondants	73 répondants	81 répondants
Sensibilisation générale des collaborateurs	86 %	78 %	80 %
Chiffrement des données	87 %	88 %	58 %
Sensibilisation ciblée pour les populations à risque	72 %	78 %	65 %
Contrôles d'accès logiques	75 %	66 %	62 %
Cloisonnement de réseau détection/ prévention d'intrusion	69 %	44 %	59 %
Destruction des données	41 %	51 %	17 %
Sensibilisation générale des collaborateurs	86 %	78 %	80 %

On retiendra que :

• Les réponses apportées pour les actions de sensibilisation sont globalement homogènes
• Les Banques / Assurances priorisent moins les mesures proposées et portent une plus grande importance aux outils techniques
• Les Banques / Assurances et les Industries / Services ciblent les actions de sensibilisation sur les populations à risque
• Les Administrations / Services publics apportent une importance moindre au chiffrement et à la destruction des données

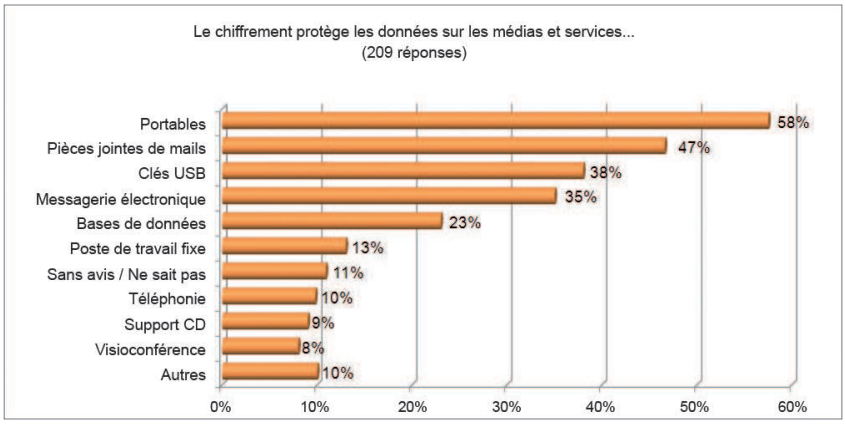
Le secteur de la santé considère les contrôles d'accès logiques comme plus efficaces (79%) par rapport aux autres secteurs, sans doute en raison des enjeux liés à la Carte CPS et au DMP.

4.3.3. La clé du chiffrement : pour quels usages ?

Parmi les mesures proposées, le chiffrement est un élément clé de la protection de la confidentialité et du secret. Néanmoins, son usage qui s'est très élargi au-delà des mondes étatique, militaire, industriel et bancaire, pose la question de son adaptation à des environnements plus ouverts (complexité de la gestion des clés, obligations légales, etc.) et de son acceptation par les utilisateurs (performance, ergonomie, etc.).

Le chiffrement répond à de nombreux besoins potentiels de protection des données comme l'indiquent les résultats présentés au schéma ci-dessous.

Question posée : Quel usage faites-vous du chiffrement aujourd'hui, en termes de médias ?



Sans surprise, les équipements de mobilité (portables, clés USB) et la messagerie arrivent en tête. Les autres usages étant globalement ponctuels ou marginaux. Pour Jacques Stern, « *Les algorithmes de cryptographie ne sont qu'un élément de la chaîne permettant la transmission sécurisée de données. À l'heure actuelle, ils ne constituent pas le maillon faible de cette chaîne : lorsqu'ils sont publics, leur fiabilité est largement éprouvée. Les fonctions de hachage demandent cependant un effort de recherche pour continuer de garantir à l'avenir le contrôle d'intégrité. Quant à la menace d'un ordinateur quantique capable de venir à bout des algorithmes, elle reste très hypothétique.* »[29]

Une analyse par secteur d'activité apporte un éclairage différent sur quelques réponses proposées.

	60 répondants	72 répondants	77 répondants
Portables	68 %	71 %	38 %
Pièces jointes de mails	47 %	53 %	42 %
Clés USB	45 %	43 %	27 %
Messagerie électronique	38 %	35 %	34 %
Bases de données	32 %	18 %	20 %

On retiendra :

• Des écarts peu significatifs entre les Banques / Assurances et les Industries / Services à l'exception des bases de données

• Un usage moindre du chiffrement au sein des Administrations / Services publics et des Industries / Services pour les bases de données

Le secteur de la santé apparaît encore plus en retrait dans l'usage du chiffrement pour les portables (21%) mais est plus avancé pour la messagerie électronique (51%), sans doute en raison des usages spécifiques de ces outils.

[29] Jacques Stern, Ce qui est secret est vulnérable – La Recherche, 2008

4.4. Affronter la réalité

L'importance accordée à la confidentialité des données et l'ampleur des mesures mises en œuvre n'évitera jamais qu'une erreur, une négligence, une attaque bien menée ne conduisent à une perte ou une divulgation aux conséquences plus ou moins graves.

Quelques études et publications indiquent les points clés à ne jamais perdre de vue. Selon une note blanche de la DCRI (Direction Centrale du Renseignement Intérieur) de 2009, sur une période de 3 ans, plus de 3000 entreprises françaises ont été visées à des fins d'intelligence économique.

- Quelles sont les cibles ?
  - Les entreprises de toutes tailles dont les PME représentent près des trois quarts.
- Quelles sont les informations visées ?
  - Les données financières, le savoir-faire et les secrets industriels
- Quels sont les modes opératoires ?
  - Souvent légaux, ils s'appuient sur l'intrusion physique ou logique et les manipulations (visiteurs autorisés et intrusions consenties (17%), atteintes aux savoir-faire (12%), risques informatiques (11%), atteintes physiques sur sites (11%), exploitation des vulnérabilités humaines (5%))

Une étude plus récente de Verizon nous indique qu'en 2010, le nombre de pertes de données est équivalent à celui des 6 années précédentes cumulées. On objectera ici que « *plus on cherche, plus on trouve* » ! Mais aussi que les obligations de notification des atteintes aux données personnelles en vigueur, notamment aux États-Unis et désormais en Europe, ont un réel impact. Dans le rapport de 2011, on constate une inflexion à la baisse du nombre d'enregistrement de données personnelles compromis, en même temps qu'une augmentation des compromissions : plus d'attaques, plus simples, plus ciblées et avec moins d'impacts ?

Enfin, selon une étude de KPMG[30] les secteurs les plus touchés par les atteintes aux données sont par ordre d'importance, les services financiers, la santé et l'assurance. On objectera ici que « *on ne trouve que là où on cherche* » ! Bizarrement, le secteur industriel est absent de ce bilan…

4.4.1. C'est le monde réel

L'actualité sur ce type d'évènement est désormais quasi quotidienne. Elle ne représente sans doute que la partie immergée de l'iceberg, tant une certaine forme d'omerta règne toujours sur le sujet[31]. Toute publicité sur une divulgation volontaire ou non, comme le vol ou la disparition de données confidentielles aura un impact immédiat sur l'image de l'organisme ou de l'entreprise concerné. Quelques exemples marquants méritent pourtant d'être rappelés.

En 1996, le Docteur Gubler, ancien médecin de François Mitterrand, publie un ouvrage intitulé « *Le grand secret* », consacré à la découverte, à l'évolution et au traitement de la maladie du Président. Il sera condamné à quatre mois de prison avec sursis pour « violation du secret professionnel ».

En 2005, le Groupe Valeo déposait plainte contre une stagiaire chinoise pour intrusion informatique et vol de données. Elle sera condamnée et fera 53 jours de détention en préventive. Dans l'industrie d'autres affaires ont défrayé la chronique : Coca Cola / Pepsi (2006), Ferrari / Mac Laren (2007), Michelin / Bridgestone (2008)…

---

[30] Data Loss Barometer – KPMG, 2009

[31] Voir les résultats de l'étude de l'Institut Ponemon en conclusion

En 2008, lors d'un transfert d'informations entre son siège au Royaume-Uni et une filiale en Afrique du Sud, l'assureur Zurich a égaré les données personnelles et bancaires de près de 36000 clients. La Financial Services Authority (UK) sanctionnera Zurich à une amende de 2,3 M£.

En 2008, un ordinateur contenant onze années de dossiers médicaux (plus de 15 000 dossiers) a été volé dans un cabinet médical de l'Oise.

En 2009, une liste de 3 000 noms de ressortissants français possédant des comptes bancaires en Suisse non déclarés à l'administration fiscale était communiquée à Bercy par un ancien informaticien de HSBC.

En 2009 toujours, des collaborateurs d'EDF sont soupçonnés d'avoir commandité depuis 2004, des intrusions informatiques à des fins de collecte d'information sur l'association Greenpeace.

En 2010, le site www.wikileaks.com publie des dossiers confidentiels de nature militaire et diplomatique faisant trembler plusieurs états occidentaux. Certaines informations sont communiquées au site par un informaticien, militaire américain basé en Irak. Les démêlés du fondateur de wikileaks avec la justice suédoise et le système de paiement en ligne Paypal, conduit ses défenseurs à pirater le site en ligne de ce dernier via des cyber-attaques.

En 2010 aussi, l'affaire Bettencourt éclate avec comme point de départ l'enregistrement d'une conversation privée par un employé de maison à l'insu de sa patronne.

En mai 2011, des pirates informatiques ont accédé aux informations personnelles de plus de 77 millions d'utilisateurs du site de jeux en ligne Playstation Network (PSN). Longue à réagir et à informer ses clients, peu précise sur les données concernées (bancaires notamment), Sony est visée par des « class actions » aux États-Unis.

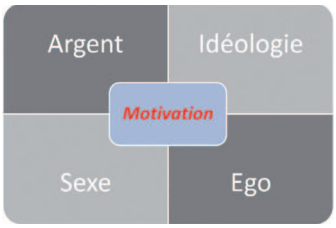
En juin 2011, les exercices du sujet de mathématiques du BAC S sont mis en ligne avant l'épreuve, via une photo prise avec un smartphone dans un site d'imprimerie supposé sécurisé. L'employé, auteur de la photo, comme les internautes ayant publié le document sur un blog, ne se rendaient visiblement pas compte des conséquences de leur acte ...

En juin 2011 encore, un scandale éclate en Angleterre au sujet du recours par le journal News of the World, à des détectives privés et à des téléphones piégés permettant d'accéder aux boîtes vocales de personnes notamment impliquées dans des affaires d'enlèvement d'enfants. Le journal a fermé ses portes. Depuis d'autres révélations sur la cyber-surveillance de personnalités dont des membres de la famille royale, l'affaire dérive en scandale politique et l'empire News Corp est menacé...

Cette longue liste pourrait encore être complétée et nous ne doutons pas que nos lecteurs disposent aussi d'histoires similaires, plus ou moins graves, vécues au sein de leur organisation.

L'enjeu est simplement de montrer ici la réalité du monde qui nous entoure, d'insister sur la multiplicité des modes opératoires et l'importance fondamentale du facteur humain.

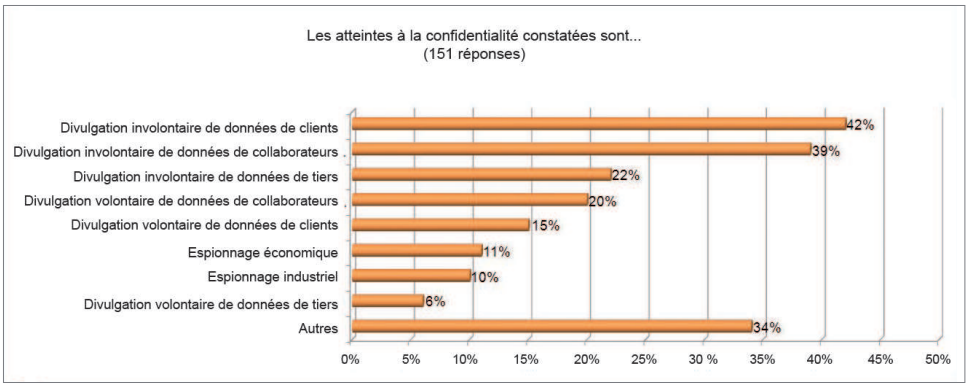
Quelque soit le contexte, il est essentiel de rappeler les quatre grandes motivations des escrocs, pirates, fraudeurs, etc. Des invariants de toute gestion de risque.



4.4.2. Une autre vision du monde...

Nous avons proposé à l'échantillon de l'enquête 8 types d'atteintes à la confidentialité. Et ce n'était pas suffisant !

Question posée : Quels sont les types d'atteintes à la confidentialité des informations dont a été victime votre entreprise / organisation depuis 2 ans ?



Environ un quart des répondants sont victimes d'attaques différentes de celles proposées. Et encore plus significatif aussi, 29% ne savent pas si ces évènements sont une réalité au sein de leur organisation... On notera que :

- Les divulgations involontaires sont les plus fréquentes (66% des répondants en cumulé)
- Les divulgations volontaires sont une réalité (30% des répondants en cumulé)
- Les actes d'espionnage économique et industriel ne sont pas anodins (16% des répondants en cumulé)

Une analyse par secteur d'activité apporte un éclairage différent avec des écarts significatifs pour trois des réponses proposées.

	60 répondants	73 répondants	81 répondants
Divulgation involontaire de données de clients	48 %	33 %	46 %
Divulgation volontaire de données de collaborateurs	10 %	20 %	25 %
Espionnage économique	5 %	22 %	5 %

On retiendra que :

• Les Industries / Services sont, sans surprise, les plus concernés par les actes d'espionnage avérés et relativement moins par la divulgation involontaire de données clients.

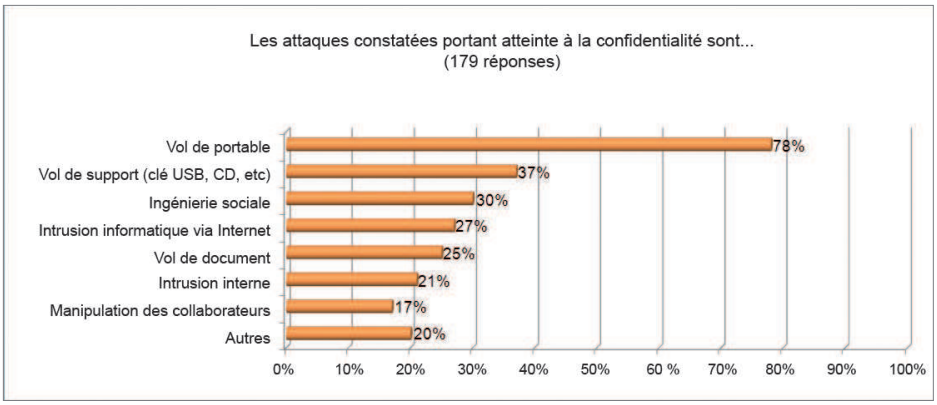
• Les Banques / Assurances possèdent apparemment de meilleurs comportements de leurs collaborateurs en termes de fuites d'information volontaires.

Dans le secteur de la santé, la divulgation involontaire de données « patients » est plus fréquente (55%) que dans les autres secteurs d'activités.

4.4.3. Du vol de portable à l'ingénierie sociale…

Les modes opératoires des atteintes à la confidentialité sont eux aussi variés et nous nous étions concentrés sur les sept qui semblent les plus communs. Une part significative de l'échantillon (16%) affirme ne pas connaître ce type d'évènement et 20% constatent d'autres formes d'attaques dont on peut imaginer que les interceptions / écoutes ou des copies illicites de données font sans doute partie.

Question posée : Quels sont les incidents / attaques portant atteinte à la confidentialité des informations dont est la cible votre entreprise / organisation depuis 2 ans ?



Le vol de portable apparaît très nettement en tête (78%) sachant que le contenant est peut-être autant visé que le contenu. Selon l'Institut Ponemon, environ 80% des portables contiennent des données sensibles (protégées ou non) et 10% sont volés ou perdus au cours de leur cycle de vie.

Enfin, l'Institut indique aussi que l'impact économique de la perte / vol d'un ordinateur portable contenant des données confidentielles non chiffrées s'évalue à environ 50 000 US$.

Au regard de la baisse du coût des équipements, l'information a plus de valeur que la machine. Et n'oublions pas que l'on constate aussi des pertes ou des vols déclarés par des collaborateurs transmettant leur outil de travail professionnel à un enfant ou un ami et pouvant disposer ensuite d'une machine « dernier cri »...

Les autres types d'attaques ont des taux de réponses significatifs mais moindres et on insistera principalement sur l'ingénierie sociale (voir page suivante).

Une analyse par secteur d'activité apporte un éclairage différent avec des écarts significatifs pour deux des réponses proposées relatives au vol.

	60 répondants	73 répondants	81 répondants
Vol de support	47 %	33 %	32 %
Vol de document	12 %	37 %	25 %

On retiendra que :

• Les Banques / Assurances constatent plus de vols de supports numériques au contraire des Industries / Services pour qui les vols de documents sont les plus fréquents.
• Les Administrations / Services Publics se situent globalement dans la moyenne globale.

Zoom « Ingénierie sociale »

par Marion Lemperière (Consultant Hapsis)

Stigmatisée voire diabolisée, l'ingénierie sociale est en réalité utilisée dans des situations quotidiennes, par des gens ordinaires. Cette pratique n'est ni bonne ni mauvaise par nature, c'est son utilisation, à mauvais escient, qui peut la rendre dangereuse. Les méthodes utilisées ne sont pas nées avec l'informatique. De tout temps, des personnes malhonnêtes se sont servies de l'ingénierie sociale pour mettre en œuvre des escroqueries ou des arnaques.

Les définitions de l'ingénierie sociale confirment son caractère universel : « une forme d'acquisition déloyale d'information et d'escroquerie qui exploite les failles humaines et sociales de la structure ciblée, afin d'obtenir d'autrui un bien, un service ou des informations »[32].

Les risques qu'encourent les entreprises via des attaques d'ingénierie sociale sont extrêmement importants comme l'indiquent quelques affaires récentes (Sony, RSA, etc.).

L'ingénierie sociale permet généralement une économie de temps et d'efforts (il est plus rapide et souvent plus facile d'obtenir le code secret d'une personne en lui demandant plutôt qu'en piratant son ordinateur). Contrairement à une attaque technique, les victimes sont manipulées et souvent inconscientes de l'importance des informations qu'elles ont fournies.

Autre point important : chacun peut être visé par une attaque d'ingénierie sociale. Tout individu possède une information qui, un jour ou l'autre, intéressera un tiers, connu ou inconnu. L'escroc jouera alors principalement sur l'enclin naturel ou culturel des personnes à partager de l'information, à rendre service et à obéir à des injonctions. Il pourra alors, en fonction de la cible, prendre le rôle d'un confident, d'un ami ou d'un supérieur hiérarchique.

Contrairement aux attaques techniques, il n'existe pas de processus préétabli pour contrer une attaque d'ingénierie sociale. Un travail de sensibilisation et de formation est nécessaire pour informer les employés sur la réalité de la menace, afin que ceux-ci soient en mesure de prévenir, de détecter et de réagir rapidement en cas d'attaque. Ce sont souvent de simples pratiques quotidiennes qui font la différence : ne jamais divulguer son mot de passe, ne répondre à aucun email d'un contact inconnu, ne divulguer aucune information sous l'insistance d'une personne, même bienveillante comme sur les réseaux sociaux, etc. Les amis de mes amis sont-ils bien mes amis ?

Bien que la formation et la sensibilisation soient essentielles, définir et préciser les directives de sécurité de l'entreprise, classifier l'information et ses modes d'accès, sont également des processus importants, qui permettent d'éviter des fuites de données.

En 2011, le Gartner Group a positionné l'Ingénierie Sociale comme le risque majeur dans le monde IT pour la décennie à venir. Il est sans doute indispensable que les entreprises et administrations mettent en œuvre un véritable plan d'action en la matière.

[32] Définition de l'Ingénierie Sociale, Wikipedia, 2011

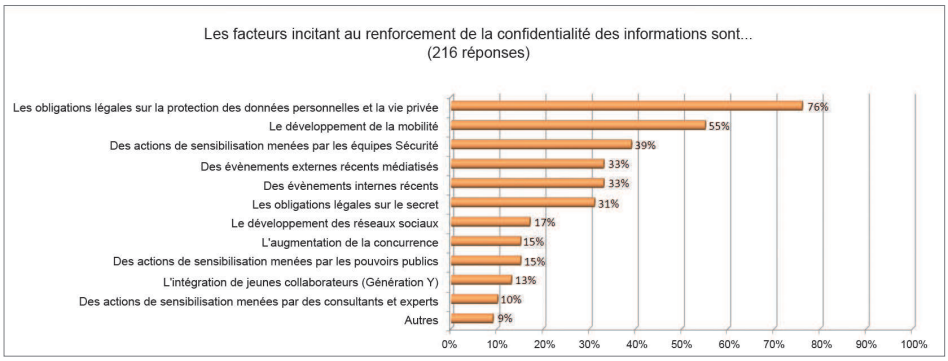
Le secteur de la santé est moins concerné que les autres secteurs par le vol de supports (24%) et par les vols de documents (18%), à l'exception des Banques / Assurances cependant.

4.5. Pour aller plus loin : la contrainte et les nouveaux usages

4.5.1. De l'importance de la réglementation...

Comme nous l'avons abordé au chapitre 3.2, la réglementation est foisonnante, complexe et évolutive. Elle est un levier essentiel de la protection du secret et de la confidentialité. Mais elle ne règle pas tout, loin de là.

Question posée : Quels sont les facteurs clés qui poussent votre entreprise / organisme à renforcer la confidentialité des informations ?



Renforcer la confidentialité des informations n'est pas fondamentalement perçu comme une exigence « business ». Sauf, peut-être, pour les 15% des répondants indiquant « l'augmentation de la concurrence » et les 9% indiquant le choix « autres ».

Les membres de l'échantillon agiraient, dans leur contexte, plutôt sous la contrainte liée à la protection des données personnelles avec comme perspective l'obligation de notifier toute atteinte aux données. L'obligation de secret n'apparaît qu'en 6ème position avec 31% des réponses.

En deuxième lieu, ce sont les usages liés à la mobilité (55%) qui obligent à renforcer la protection des données. Des équipements plus petits et plus performants, plus économiques et plus largement utilisés pour répondre à un des enjeux majeurs : informé et connecté en tout lieu, à tout instant, sur tous les médias (Intranet, Internet, Extranet).

Enfin, cinq des choix proposés, moins porteurs, se situent entre 10 et 15%. Deux d'entre eux, les réseaux sociaux et la génération Y n'apparaissent pas encore significativement comme des facteurs de renforcement de la confidentialité. Pourtant, les risques inhérents à ces deux paramètres ne sont pas anodins.

Une analyse par secteur d'activité apporte un éclairage différent avec des écarts significatifs pour cinq des réponses proposées.

	61 répondants	73 répondants	81 répondants
Protection des données personnelles	79 %	64 %	84 %
Actions de sensibilisation par les équipes Sécurité	54 %	44 %	23 %
Évènements externes récents médiatisés	41 %	30 %	39 %
Évènements internes récents	26 %	44 %	28 %
Augmentation de la concurrence	12 %	30 %	2 %

On retiendra :

• Dans les Banques / Assurances, le poids de la sensibilisation menée en interne et l'exploitation des évènements externes sont plus significatifs.
• Dans les Industries / Services, l'exploitation des évènements internes et le poids de la concurrence sont plus importants.
• Dans les Administrations / Services publics, les obligations légales sur la protection des données personnelles sont majeures au détriment des actions de sensibilisation par les équipes sécurité.

Le secteur de la santé accorde une importance encore plus grande que les autres secteurs aux questions réglementaires (95%).

Inversement, les actions de sensibilisation par les équipes sécurité (21%), les évènements internes (19%) et externes (14%) sont moins considérés (car moins présents et peu identifiés).

Zoom « Génération Y »

par Éléonore Grandemange (Télécom Sud Paris)

La génération Y a grandi à l'ère du numérique. Elle maîtrise donc toutes les subtilités des nouvelles technologies. Cette aisance se révèle être à la fois un atout et un risque pour eux-mêmes et leurs entreprises.

Avec un téléphone greffé à l'oreille et un clavier entre les mains, cette génération a bouleversé les codes de l'entreprise. Un seul mot d'ordre : « communiquer ».

Il n'est pas rare de les surprendre, pendant leurs heures de travail, en train d'envoyer un SMS ou un email personnel, de réserver des billets de trains sur Internet, télécharger des applications sur leur ordinateur professionnel ou de se connecter à des réseaux sociaux. Ces gestes, presque anodins pour la génération Y, peuvent choquer certains de leurs collègues.

Ces pratiques mettent sérieusement en jeu la sécurité des données de l'entreprise. Reprenons l'exemple des réseaux sociaux. Les plus naïfs diront qu'ils bénéficient aux organisations : source de valorisation de produits, promotion d'images ou recrutement. Mais peut-on réellement contrôler l'information véhiculée sur de tels sites communautaires ?

D'après une étude réalisée par le site d'emploi MyJobGroup.co.uk, 55% des salariés britanniques (toutes générations) accèdent à un réseau social sur leur lieu de travail. Régulièrement, des internautes divulguent certaines de leurs informations personnelles (nom, prénom, adresse mail, numéro de téléphone, données bancaires...), mais aussi professionnelles (description de leur poste, de leurs missions, d'un dossier en cours...), de manière consciente ou inconsciente. Mais savons-nous réellement ce que deviennent les données collectées ?

La politique de confidentialité de Facebook indique que les utilisateurs s'engagent à accepter que leurs « *données personnelles soient transférées et traitées aux USA* ». Dans la continuité, la déclaration des droits et responsabilités affirme : « *Nous ne garantissons pas que Facebook soit sûr et sécurisé* ». Rien de très rassurant...

Une utilisation abusive du matériel et des données professionnels sont parfois à l'origine de fuites aux conséquences mal appréhendées. Afin de les limiter, une sensibilisation du personnel à la gestion de l'information semble essentielle et doit être en adéquation avec le public visé. Rien ne sert de redire ce que les chartes affirment, en fonction de la génération, du poste et de l'éducation de chaque employé, une formation plus individualisée et mieux ciblée doit être proposée.

« Sous l'influence du numérique d'Internet, de la téléphonie mobile, la société est en train de changer sous nos yeux sans qu'on en mesure spontanément la profondeur. »

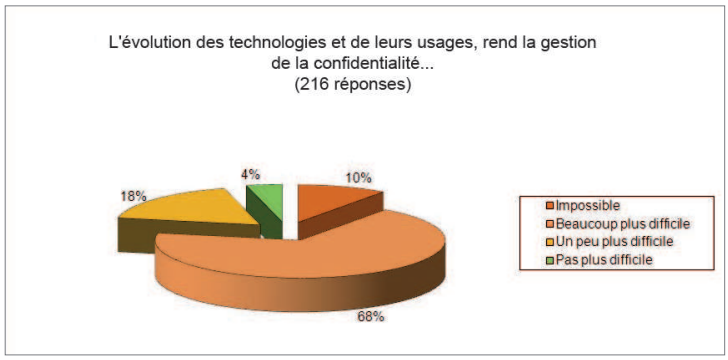
Maurice Levy (PDG du Groupe Publicis)
L'entreprise.com - 2010

4.5.2. Mission : Impossible ?

L'ultime question de l'enquête cherche à mesurer si l'évolution des technologies, essentiellement autour de la dématérialisation (e-business, e-commerce, e-administration), de la mobilité (tablettes notamment), des réseaux sociaux (professionnels et personnels) et du « cloud computing » rend la gestion de la confidentialité plus difficile.

De l'avis unanime, la partie n'est pas gagnée. Pour 10% de l'échantillon, c'est même mission impossible !

Question posée : Selon vous, l'évolution des technologies et de leur usage (mobilité, cloud computing, réseaux sociaux, « bring your own device », etc.) rend-elle la gestion de la confidentialité des informations plus difficile ?



Une analyse par secteur d'activité apporte un éclairage différent avec des écarts significatifs pour le secteur Banques / Assurances. Une vision plus pessimiste que pour les autres secteurs...

	61 répondants	73 répondants	81 répondants
Oui, même impossible	16 %	7 %	7 %
Beaucoup plus difficile	61 %	71 %	71 %

On retiendra que :

• Si la somme des deux premiers choix se situe autour de 80%, les participants des Banques / Assurances apparaissent les plus pessimistes.

À titre d'exemple, le Cloud Computing bénéficie d'un battage marketing important. N'oublions pas qu'il n'est qu'un emballage de plusieurs types de pratiques d'externalisation (applications, infrastructures, services) bénéficiant d'une évolution des modèles économiques réduisant les investissement au profit de charges de fonctionnement « à la demande ».

Zoom « Cloud computing »
(Déclarations de confidentialité)

		SalesForce	Microsoft	Amazon	Google
Label TRUSTe Safe Harbor		x			
		x	x	x	
Types de données	Données personnelles	x	x	x	x
	Numéros de cartes bancaires	x		x	
	Emails			x	x
	Navigation Web	x	x	x	x
	Localisation				x
Usages des données	Services / transactions demandés	x	x	x	x
	Paiements	x		x	
	Suggestions de produits / services		x	x	
	Communication	x			
	Marketing	x			
	Publicité				
	Informatique sociale	x			
	Amélioration du Site	x	x	x	
Partages des données	Sociétés affiliées		x	x	x
	Partenaires	x		x	x
	Prestataires de services tiers		x	x	
	Fournisseurs	x	x		
	Sociétés externes pour paiements	x			
	Annonceurs			x	
	Si la loi l'oblige	x	x	x	x
	En cas d'activités frauduleuses, atteintes à la sécurité, ou problèmes techniques	x			x
Mesures de sécurité	Chiffrement des données (SSL)	x	x	x	x
	Environnement sécurisé	x	x	x	x
	Contrôle d'accès aux données	x	x	x	x
	Sécurisation des paiements			x	

Le tableau de la page précédente présente, à titre d'exemple, les déclarations de confidentialité de quatre acteurs clés du secteur. Cette vision publique et transparente doit bien sûr être complétée par des engagements contractuels et des actions de contrôle / audit.

4.6. Synthèse

L'enquête annuelle du Cercle Européen de la Sécurité et des Systèmes d'Information révèle des pratiques hétérogènes et finalement très variables en matière de secret et confidentialité dans le numérique.

Des écarts significatifs sont mis en évidence entre secteurs d'activité. Les Industries / Services, a priori plus matures dans le domaine, s'avèrent parfois en retrait. Privilégiant la continuité et les aspects matériels, la confidentialité des données numériques reste en jachère pour de nombreux acteurs. Nous devons cependant modérer ce propos car la taille de l'entreprise et son secteur d'activité précis, peuvent bien sûr affecter ce bilan.

À titre d'exemple, la libéralisation, très tardive en France, de l'usage du chiffrement, n'a pas facilité le développement du marché. Par ailleurs, les questions d'Intelligence Économique ont été abordées avec une approche très « défensive » et de repli sur nos patrimoines à défendre. À l'heure de la globalisation et de la coopétition (coopération avec ses compétiteurs) généralisée, tout cela n'est-il pas fini ?

Face à l'ampleur de la tâche, il semble fondamental pour de nombreux professionnels des SI et de la SSI de participer à la création d'un contexte favorable à une véritable réflexion d'ensemble, en synergie avec l'ensemble des acteurs concernés. Celle-ci s'appuiera sur une approche nouvelle de la classification (plus ciblée, plus pragmatique) associée à un véritable processus d'acculturation impliquant en premier lieu, les décideurs.

5- CONCLUSION

Nous avions terminé le Livre Bleu 2010 sur une citation du philosophe Luc Ferry qui fait l'honneur de sa participation à l'édition 2011 des Assises. « Nous avons l'impression que les forces économiques, les marchés financiers, les nouvelles technologies transforment notre vie de tous les jours bien davantage que nos ministres ou nos parlementaires. »

Notre propos consacré au secret et à la confidentialité dans l'univers numérique semble en phase avec cette tendance. Les atteintes à la confidentialité des données et l'affaiblissement du secret sont davantage liés aux nouveaux usages du numérique dans la société qu'à l'exigence de transparence démocratique inscrite dans la loi. Initiée par les questions financières et de gouvernance des entreprises, la tendance se poursuit sur les questions de consommation, d'alimentation, d'écologie, d'énergie, de santé, de transport, etc. Partout, les données numériques sont au cœur de la problématique et tous les secteurs se doivent d'agir dans le domaine.

Par exemple, à la suite de l'enquête du crash du vol « Rio-Paris », une proposition d'enregistrement de toutes les conversations dans la cabine de pilotage des avions a été effectuée. Exagération émotionnelle liée au drame ou tendance de fond à tout enregistrer (« logger ») au cas où ?

Il semble aussi désormais que ce n'est pas seulement « qui fait quoi » ou « qui sait quoi » voire « qui dit quoi » qui est le plus sensible mais, de plus en plus, « qui est qui ? » et « qui est où ». La vidéo-protection et la géo-localisation associées à l'identité numérique s'inscrivent fondamentalement dans le champ du secret et de la confidentialité qui rejoignent ainsi très étroitement les questions de traçabilité.

5.1. À quoi sert la protection des données ?

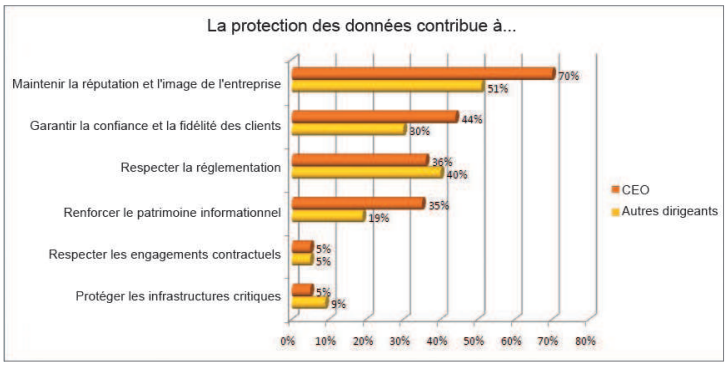
Concentrons-nous sur les points qui concernent plus précisément les acteurs de la Sécurité SI au sein des entreprises et des administrations et par voie de conséquence les offreurs de services et de solutions.

En quoi, la protection des informations – sous-entendu en termes de confidentialité – contribue-t-elle à l'atteinte des objectifs des entreprises et organisations. Une étude de l'Institut Ponemon[33] auprès de 140 dirigeants britanniques apporte un éclairage intéressant sur ce point (voir schéma ci-dessous).

Incontestablement, les implications externes comme l'atteinte à la réputation, la confiance des clients et le respect de la réglementation sont les plus importantes.

Nous proposons maintenant, en guise de conclusion, quelques axes de réflexion qui resteront à approfondir lors des travaux du Cercle. Pour cela, nous devrons sans doute nous ouvrir à d'autres acteurs de la gestion des risques et de la Sécurité / Sûreté.

[33] Business case for data protection (mars 2010)



5.2. Un pré-requis : « la transversalité »

Inutile d'imaginer régler les questions de confidentialité au sein d'une DSI avec des contrôles d'accès logiques par ci, un peu de chiffrement par là et du DLP au cas où. Toute Politique Sécurité des SI affirme répondre aux objectifs de Disponibilité, Intégrité, Confidentialité et Traçabilité. Le RSSI, qui est le garant de sa mise en œuvre, essaie autant qu'il le peut, de faire accepter les contraintes de ses méthodes et outils que de faire utiliser les solutions qu'il propose. Pourtant, ne faut-il pas sortir la confidentialité de la démarche « politique » de la SSI ? Certains, notamment dans l'Industrie le font déjà...

Être transversal consisterait donc :

• À établir une Politique de confidentialité qui cible mieux les enjeux, les objectifs et les moyens (notamment via une norme de classification avec des seuils d'impacts validés par les dirigeants)
• À définir les rôles et responsabilités en la matière notamment entre Sécurité et Sûreté, entre sécurité physique et informatique, entre conformité et juridique, entre gestion des risques et contrôle / audit
• À identifier, responsabiliser et impliquer les « propriétaires », « dépositaires », « destinataires », « gardiens », « hébergeurs », etc. en contrôlant mieux leurs pratiques[34]
• À consolider les atteintes à la confidentialité qui ne sont pas toutes de nature informatique mais dont les origines comme les conséquences peuvent concerner les usages des SI (ex : ingénierie sociale).

C'est justement parce que le champ du secret se réduit qu'il faut le traiter au bon niveau et de manière efficace, plus pertinente aussi, en tenant mieux compte du facteur humain.

5.3. Une exigence : « la contextualisation »

Une fois une véritable Politique de confidentialité établie au niveau de l'entreprise / organisme, il convient de la « contextualiser ». Quel rapport y a-t-il entre la protection des données des clients ou des collaborateurs avec le plan stratégique et les négociations commerciales ? Comment prendre en compte au bon niveau et de manière très spécifique les exigences réglementaires liées au secret et à la transparence entre la finance, les RH, la stratégie et le marketing, les systèmes d'information eux-mêmes, etc. ?

[34] Fin 2010, la CNIL a mis en évidence que des hébergeurs de données de santé ne respectaient pas leurs obligations voire n'étaient pas agréés au titre du décret paru en 2006

Contextualiser consisterait donc :

• À définir une responsabilité formelle au sein des Directions en termes de mise en œuvre de la politique, de son contrôle et du reporting.
• À mener une réflexion « locale » par Direction ou Service (ou dans le cadre d'un projet) sur l'importance accordée à la confidentialité. L'enjeu n'est pas de faire un audit interne mais un diagnostic « terrain » par ceux qui sont les plus concernés, le cas échéant avec une assistance.
• À s'intégrer dans tout projet structurant comme l'externalisation, la géo-localisation, la traçabilité, la cyber-surveillance, etc.
• À communiquer au Comité de Direction, ou au Comité des Risques s'il existe, le bilan de cette réflexion associé à une proposition d'actions, si nécessaire.

5.4. Une obligation : « le pragmatisme et la simplicité »

En relation avec l'élaboration d'une Politique de confidentialité mieux ciblée qu'une PSSI vaste et complexe, voire lourde et souvent très partiellement appliquée, il semble plus que jamais nécessaire de revenir à une approche « *bottom up* » et non « *top down* » beaucoup plus pragmatique. Ainsi, la démarche consisterait à :

• Poser à chaque membre de comité de direction une seule et unique question : « *Quelle est l'information dont la divulgation à un acteur ou un tiers non autorisé vous empêcherait de dormir pendant une semaine ?* » voire « *... menacerait votre fonction ?* ».
• Effectuer des contrôles voire des tests sur les conditions de gestion de cette information, sous toutes ses formes et définir les possibles scénarios d'atteinte à sa confidentialité.
• Définir (ou redéfinir) la classification de cette information et revoir ou mettre en œuvre les mesures et outils de sécurité appropriés notamment en termes de stockage, d'accès, d'échange comme de destruction.
• Marquer les documents, supports, sites voire pages web, fichiers contenant des données selon leur degré de classification.
• Cadrer juridiquement les relations et échanges avec les tiers.
• Mener des actions de sensibilisation voire de formation ciblées auprès des personnels détenteurs ou destinataires de cette information, dès l'embauche et jusqu'au départ de l'entreprise / organisme. Le cas échéant, faire signer un engagement de responsabilité individuel.
• Et ne pas omettre de la réflexion la durée de classification !

5.5. Une vigilance : « l'externalisation des services »

Le mode de gouvernance des entreprises est progressivement passé de la verticalité à l'horizontalité et au réseau. Facilitant la communication, développant la transparence et renforçant la transversalité, cette évolution a aussi été associée à la multiplication des projets et à un management par processus. L'ensemble a ainsi généré une plus grande complexité où chacun peut parfois avoir du mal à se retrouver. Et les Systèmes d'Information ont joué un rôle clé dans ces évolutions.

La tendance lourde concerne aujourd'hui l'externalisation des activités et processus qui ne sont pas au cœur de la stratégie de l'entreprise / organisation. Le cloud computing devient une réalité et au-delà de l'effet marketing, il repose sur une double préoccupation : économies et transfert de risques.

Cette quête d'économies et ce transfert de risques vers des prestataires spécialisés dans la mise en œuvre de SI et d'infrastructures complexes, doivent renforcer le degré de vigilance des professionnels de la sécurité, essentiellement en termes de protection des données. En effet, on n'élimine évidemment pas le risque et les questions de confidentialité sont au cœur de la problématique.

5.6. L'équilibre des forces : « des opportunités et des menaces »

Nous terminerons sur un double constat en appelant à la vigilance de la profession. Opportunités et menaces se combinent dans une conjonction de forces antagonistes (voir schéma ci-dessous).

D'une part, l'entrée dans l'ère numérique associée aux exigences sécuritaires[35] des individus et au poids des règlementations renforcent l'importance de la fonction SSI au sein des entreprises et des administrations. Le marché est en croissance, de plus en plus de secteurs se préoccupent du sujet et embauchent des experts en SSI. Si les questions de continuité sont globalement prises en charge et alors que le champ du secret se réduit, la gestion de la confidentialité devient alors sans doute plus stratégique, plus cruciale dans le cadre d'une sécurité numérique globale.

D'autre part, les acteurs ne doivent pas être ignorants de forces centripètes qui menacent ce constat quelque peu idyllique. La sécurité numérique s'inscrit aussi dans un conflit à 3 dimensions où la Sécurité des SI pourrait se diluer : d'une part avec la conformité (ex : protection des données personnelles, PCI DSS, etc.), et d'autre part avec les questions de Défense (ex : intelligence économique et protection du patrimoine, veille et cyber-surveillance), enfin avec la gestion du risque au sens large (ex : gestion d'incidents, aspects économiques, etc.).

[35] Voir le Livre Bleu des Assises 2009 : « Développement de la culture des risques informatiques / informationnels »

5.7. L'information, le numérique et le pouvoir

Osons pour conclure, une ouverture. C'est un lieu commun de rappeler que la possession de l'information a longtemps conféré un pouvoir d'influence ou de décision. À l'heure de la globalisation et du numérique, est-ce que ce paradigme va s'effondrer ou perdurer ? Dans quel format de gouvernance ?

Les principes démocratiques tels que nous les connaissons en Occident, qui donnent le pouvoir à l'individu, développent la transparence et la liberté de communiquer, perdureront-ils à l'ère du numérique ? La question se pose au niveau planétaire, à l'échelle d'un continent ou d'une nation, pour une entreprise, une équipe, un projet, une association, et pourquoi pas au sein d'une famille, d'un réseau ou d'une communauté…

Que restera-t-il du secret et de la confidentialité dans 15 ans, quand les générations X et Y seront associées à la suivante (qui commence à préparer son BAC) ? Où s'exerceront les pouvoirs, alors que l'empire News Corp chancelle, que Steve Jobs quitte Apple (plus grosse capitalisation boursière), que la solvabilité des banques est plus que chancelante, que des États occidentaux sont en situation de faillite et que les peuples arabes s'émancipent de leurs dictateurs ?

« La vérité sera un jour la force.
« Savoir, c'est pouvoir[36] » est le plus beau mot qu'on ait dit. »

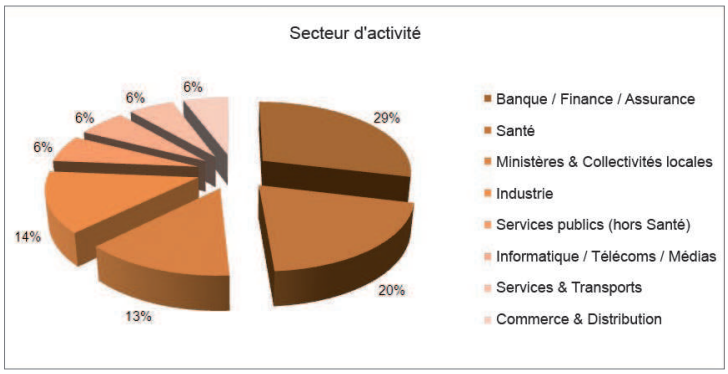
Ernest Renan
Extrait de Dialogues et fragments philosophiques

[36] Citation de Francis Bacon (1561-1626), philosophe anglais

6- ANNEXE : L'ÉCHANTILLON

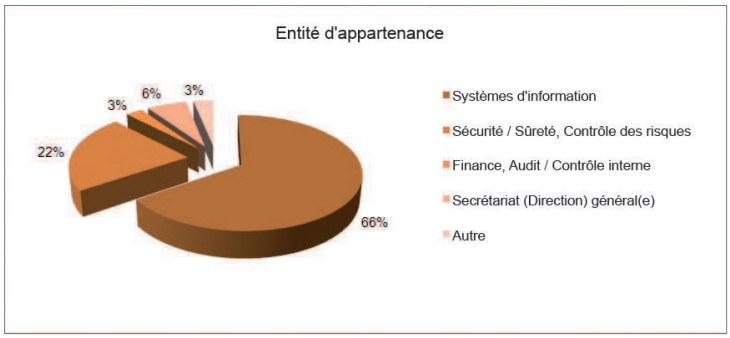
L'échantillon de l'enquête de 2011 est constitué de 223 professionnels. Leurs principales caractéristiques sont présentées ci-dessous.

6.1. Secteur d'activité



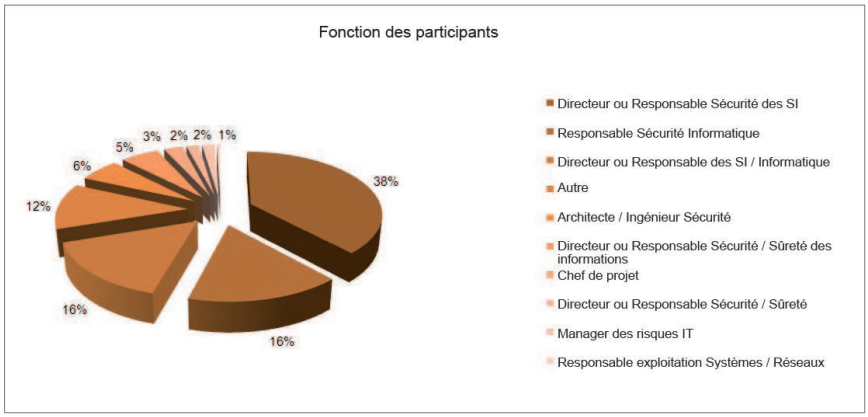
Une représentation stable d'année en année avec cependant une forte progression du secteur de la santé qui passe de 8% à 20%.

6.2. Entité d'appartenance



Une proportion importante de professionnels des SI (64% en 2010).

6.3. Titre et fonction



Une répartition qui est sensiblement identique à l'année dernière, avec une importante proportion de Directeurs / Responsables Sécurité des SI (38% en 2010).

NOTES

hapsis

LA PROTECTION DE VOS INFORMATIONS DANS UN ENVIRONNEMENT COMPLEXE

Sécurité des SI et complexité
une approche en 3 axes

Humain

Sensibilisation :

- Les Sensipacks

Ingénierie Sociale :

- SE Camp
- SE Response Team

s.e. Force

Maîtrise des coûts

- Externalisation
- Service +
- Do it better
- Cloud & sécurité
- DLP, oui mais
- Signature par mobile
- Mobilité

Pilotage

- Gouvernance
- Tableaux de bord
- Classification
- Analyse et cartographie des risques

www.hapsis.fr

12e édition

L'événement de l'année, ce n'est pas le Grand Prix. Rendez-vous à Monaco du 3 au 6 octobre 2012.

Pour la 12e édition, les Assises de la Sécurité et des Systèmes d'Information vous proposent de **vous immerger** au cœur des problématiques sécuritaires, **débattre** sur des thèmes à fort enjeu, **rencontrer** les meilleurs experts et **développer** votre networking.

Ne ratez pas l'événement le plus prisé des Responsables de la Sécurité des Systèmes d'Information qui rassemble, en un lieu unique, les décisionnaires des grands comptes stratégiques des secteurs public et privé.

Pour plus d'informations : 01 41 93 07 07
www.lesassisesdelasecurite.com

www.infoflash.fr

un événement comexposium

un événement

lesassises de la sécurité et des systèmes d'information

prix de l'innovation

lecercle