Méthodologie de pérennisation des données sensibles en entreprise : Études de terrain sur le patrimoine immatériel dans son organisation

Carole Henry, Sahbi Sidhom, Imad Saleh

Méthodologie de pérennisation des données sensibles en entreprise : Etudes de terrain sur le patrimoine immatériel dans son organisation.

Carole HENRY [1], Sahbi SIDHOM [2] et Imad SALEH [3],
[1] : Université Paris 8, laboratoire Paragraphe, chenry05@etud.univ-paris8.fr.
[2] : Université de Lorraine, laboratoire Loria, sahbi.sidhom@loria.fr.
[3] : University Paris 8, laboratory Paragraphe, imad.saleh@univ-paris8.fr.

Résumé : *La pérennisation des données sensibles de l'entreprise est un point clef de sa réussite. Pour maintenir sa compétitivité et maintenir son avantage concurrentiel, elle doit prendre conscience des enjeux du management de ces données pour la poursuite de ses activités dans des conditions optimales. Au travers de l'observation des trois entreprises luxembourgeoises de tailles et d'activités très différentes, cette analyse proposera une méthodologie adaptable du traitement des données sensibles dans l'entreprise et plus globalement du patrimoine immatériel de l'organisation.*

Mots-clés : *données sensibles, méthodologie, système d'information, patrimoine immatériel, outil de gestion des données, sécurité, risque.*

1. Introduction

En 2014, selon des chiffres diffusés par IBM [1] , 800 millions de données ont été volées, avec un coût de 3,5 millions de dollars en moyenne principalement dû aux incidents sur les données et 42 % des RSSI (Responsables de la Sécurité et des Systèmes d'Information) considèrent que le risque de menaces externes sur les données a augmenté en 2014 par rapport à 2013. Quid de 2015 et des années à venir ? Le terrain d'étude de cet article couvre l'expérience de trois entreprises luxembourgeoises et de leur traitement des données sensibles. Chaque entité à des spécificités qui lui sont propres. Ainsi, nous allons observer si et comment les données sensibles sont identifiées et avec quels moyens ? Pour des raisons de confidentialité il est impossible de communiquer le nom de ces entreprises dans cette étude. C'est pourquoi nous les dénommerons respectivement **cabinet de conseil A, l'agence de publicité B et la compagnie d'assurance vie C.** Le premier terrain d'étude est celui du **cabinet de conseil A**. Société ayant un effectif d'une trentaine de consultants externalisés chez le client, la gestion des informations et des connaissances de cette société était très particulière. En effet, il s'agissait d'une société qui considérait ses employés comme des « entrepreneurs » à part entière. Pour la plupart d'entre eux, ils font des prestations directement chez le client avec leurs propres équipements informatiques. Elle avait principalement des clients grands comptes et des institutions françaises. Lors de sa faillite en 2011, le traitement des données a été malmené et nous reviendrions sur cette période de crise pour l'entreprise. Nous aborderons ensuite le cas d'une agence de publicité, **l'agence de publicité B**. Véritable partenaire des entreprises, elle est souvent amenée à manipuler un certain nombre de données qualifiées sensibles. Cela était notamment le cas lors de la réalisation de brochure de résultats annuels avant leur publication officielle ou bien lors de la mise en place d'un site web avec gestion de bases de données offline ou d'intranet offline et online. La stratégie et la confidentialité des données se sont également manifestés dans le choix des sous-traitants. Les effectifs étaient très variables puisque composée entre 5 à 15 salariés sur une période observée de deux années avec un turnover important ce qui multiplie les risques (mars 2013- février 2015). La troisième entreprise étudiée est **la compagnie d'assurance vie C** observée depuis mars 2015. Filiale d'un grand groupe bancaire français qui est présent dans 76 pays dans le monde et qui regroupe 148 300 collaborateurs au service de plus de 30 millions de clients, elle bénéficie d'un tout autre cadre pour le traitement des données sensibles. Nous reviendrons dans cet article sur les méthodes déployées par un groupe bancaire et financière pour protéger ses données : cela concerne par exemple par les mails, à la consultation de documents, en passant par la signature de clauses stricts de confidentialité et le déploiement de formation AML (lutte anti-blanchiment). Nous étudierons ici l'efficacité et les limites de ces systèmes. Cette étude a pour fil conducteur la réflexion croisée entre ces trois entreprises et le parcours des données sensibles en positionnant notre problématique comme suit: comment circulent les données sensibles et les garanties apportées dans ces entreprises si différentes alors que les moyens attribués aux questions de sécurité sont différents ? Notre analyse se décomposera en trois parties, à savoir : dans un premier temps, nous allons analyser comment les données sensibles sont générées et identifiées sur le terrain de l'entreprise; nous étudierons ensuite les moyens déployés par les entreprises pour pérenniser son patrimoine immatériel. Enfin dans un troisième temps, notre attention se portera sur les garanties apportées par les outils mis en place pour pérenniser les données sensibles.

2. Création et identification des données sensibles dans l'entreprise

A. Identifier les données sensibles :

Les entreprises créent des données, de l'information et de la connaissance. [7] La protection des données sensibles, le maintient et la pérennisation des systèmes d'information et la sécurité sont les constituants du capital immatériel de l'entité. [8] C'est un enjeu fondamental pour la stabilité et la compétitivité de cette dernière. Cela peut, par exemples, concerner des domaines très variés de son activité comme ses créations techniques et ses brevets, ses savoir-faire et plus globalement les informations stratégiques. Toutefois, toutes les informations et toutes les données de l'entreprise ne sont pas sensibles. Il est nécessaire, dans un premier temps, de pouvoir identifier et différencier ce qui est sensible de ce qu'il ne l'est pas. Il est également important de savoir ce que l'on entend par données sensibles et de voir s'il existe des subtilités luxembourgeoises. Il existe comme la CNIL [6] en France un organisme qui veille à la protection des données [5]. Il s'agit de la Commission Nationale pour la Protection des Données (CNPD). La réglementation luxembourgeoise a une particularité qui est celle qu'il existe une responsabilité pénale du gérant et de l'entité morale en cas d'intrusion sur le système informatique d'une entreprise ayant causé des dommages et qu'a ce titre et dans le cas ou il s'avère que l'entreprise n'a pas pris les précautions nécessaires pouvant porter jusqu'à une amende de 125 000 € [2] pour la société. Tout comme en France, il existe au regard de la législation une confusion entre données à caractère personnel et données sensibles. Les données sensibles en entreprises sont souvent assimilées aux données stratégiques et de ce fait recouvre plus globalement l'ensemble des données reconnues par l'entité elle-même comme étant sensible en dehors de ce qui est caractérisé par données à caractère personnelle. Il n'existe pas au Luxembourg comme en France de définition juridique des données sensibles. Nous avons également constaté un amalgame fréquent dans le domaine opérationnel qui est celui de la confusion entre donnée et information. Au Luxembourg, la loi modifiée du 2 août 2002 modifiée par la loi du 27 juillet 2007 [3] relative à la protection des personnes à l'égard du traitement des données à caractère personnel, traite en partie de ces aspects avec notamment la possibilité dans certains cas définis par la loi de pouvoir mettre en place des traitements à des fins de surveillance des usages et des réseaux au sein des entreprise ainsi que la mise en place de chargé de la protection des données pour la déclaration des fichiers de données à caractère risqué (article 40). [4]

Le législateur a, dans le cadre de certaines activités, obligé à la mise en place de déclaration auprès de la CNPD [9]. Données biométriques, données relatives à la solvabilité pour les banques et les compagnies d'assurance, données de santé …

Toutefois, les données sensibles sont dans les faits et en pratique bien plus que cela. Il s'agit avant tout, selon le type d'entité, d'être en mesure des les identifier au sein même du système d'information.

B. Cartographier les données sensibles au sein de l'entreprise :

Il est nécessaire de réaliser un recensement avec les services concernés de l'ensemble des données de l'entreprise. Il peut s'agir par exemples d'informations techniques, commerciales, des informations économiques et financières ou bien encore organisationnelles ou hautement stratégiques.

Ces dernières sont confidentielles ou non. Une fois identifiées, il est nécessaire de voir si les informations détectées ont une importance particulière tant à l'interne qu'a l'externe. En fonction du type d'entreprise, les solutions à déployer pour garantir la sécurité des données sont différentes. Dans une PME (Petite et Moyenne entreprise) ou une TPE (Très Petite Entreprise), il est parfois difficile de reconnaître et de mettre en place des systèmes sécurisés de traitement de l'information. Les acteurs n'ont pas forcément conscience des risques encourus et des vulnérabilités de leur entreprise. [10] Il est important de souligner que les coûts liés à la protection des données sont souvent un frein psychologique à l'action. Le ratio est rapidement fait entre les coûts à engager et les bénéfices immédiats. Or, la protection des données sensibles peut avoir un bénéfice à plus ou moins longs termes. On ne peut prévoir les impacts sur la pérennité des entreprises. Il existe toutefois des solutions intermédiaires pour permettre de se protéger. Dans les grandes entreprises, les décisions sont différentes car les moyens et la prise de conscience sont plus importants. En fonction du type d'entreprise des missions spécifiques et des postes sont créés pour palier à la gestion des risques et les moyens attribués sont plus conséquents. Toutefois, nous pouvons observer que les accidents sont fréquents dans ce type d'entreprise. Comme annoncé en préambule de cet article, le risque est croissant. Le développement des nouvelles technologies a accentué ce phénomène. Mais cela concerne également les comportements des employés. L'information se diffuse beaucoup plus rapidement et la culture individuelle est également en mouvance vers une transparence totale. Nous sommes de plus en plus mobiles, et l'entreprise peut bénéficier d'outils formidables qui lui permettent par exemple de virtualiser et de délocaliser ses activités là où on ne l'imaginait pas il y a encore quelques années. [11] Certains collaborateurs luxembourgeois peuvent, par exemple, travailler de leur domicile et de ce fait ils disposent de certaines ressources des entreprises via leur réseau domestique. Dans ces conditions, il est normal de constater des exemples médiatisés de fuites d'informations sensibles alliées au jeu de la

désinformation comme ceux que nous allons évoquer [12] [13].

C. *Exemples luxembourgeois de fuites de données sensibles :*

L'affaire Luxleaks est sans nul doute, l'actualité qui a le plus fait couler d'encre en 2014 et 2015 au Luxembourg et en Europe. [19] [20] Scandale financier relatif au « tax rulling » (rescrits fiscaux) mis à jour par les révélations de l'International Consortium of Investigative Journalist [14], au travers de la publication de centaines d'accords fiscaux confidentiels conclus entre de grandes entreprises comme Apple, Amazon, Heinz, Pepsi, ou bien encore Ikea et l'administration fiscale luxembourgeoise via des cabinets d'audit locaux comme PwC, EY, Deloitte et KPMG. Cette affaire est directement liée à la problématique de cet article. En effet, à l'origine les données qui ont été transmises aux médias sont des données confidentielles que des employés dont Antoine Deltour ont subtilisé et diffusé en dehors de l'entreprise illégalement. Dans ce cas précis, plusieurs anciens employés ont utilisé des fichiers mis à leur disposition dans le cadre de leur travail. Ici ce ne sont pas moins de 28 000 pages, de 548 accords fiscaux concernant 343 entreprises qui ont été subtilisés et diffusés. La confidentialité de ces documents était bien entendu à préserver.

En décembre dernier, Antoine Deltour s'est exprimé à ce sujet dans les médias [15]. Il reconnaît alors avoir copié chez son ancien employeur les documents ensuite diffusés dans le ICIJ, en avouant également ne pas avoir maitrisé la diffusion de ces documents. Il indique également que ces documents étaient en libre accès à l'ensemble des salariés. Enfin, il justifie son geste par ses valeurs personnelles via le mouvement des « lanceurs d'alerte » pour éclairer le débat sur la question de la justice fiscale et éviter le dumping social par des avantages disproportionnés octroyés par l'administration luxembourgeoise. Il est inculpé fin 2014 par la justice luxembourgeoise suite au dépôt de plainte du cabinet PwC à son encontre de vol domestique, violation du secret professionnel, violation du secret des affaires et blanchiment. [16] La plainte a fait suite à la diffusion en mai 2012 d'un numéro de télévision de Cash investigation dédié à l'évasion fiscale des entreprises. Cette diffusion relancera, les discussions au niveau européen quant à l'évasion fiscale et provoquera de nombreux débats. Le 3 juin 2015, Antoine Deltour se voit attribué le Prix du citoyen européen 2015 [17] par le Parlement européen au titre de sa contribution à la coopération européenne et à la promotion de valeurs communes. [18] Dans cette affaire révélée par les médias, on peut s'interroger à plusieurs titres. Sans entrer dans le domaine judiciaire ou du jugement des faits qui ne sont pas les objectifs de ce paragraphe, que doivent retirer les entreprises et les employés de cette affaire ? Au vue des éléments mis à disposition de l'employé, nous pouvons être amené à penser que PwC aurait fait preuve de négligence en termes de sécurisation de ses données sensibles. Toutefois, l'employé est engagé contractuellement et tenu légalement responsable de la diffusion des éléments. Le mal est fait et l'expérience démontre la nécessité d'une prise en compte du caractère confidentiel et du risque encouru en amont de la mise à disposition même interne de ces données sensibles. Dans le cas de Luxleaks, le cabinet d'audit, prestataire d'audit d'Apple, d'Amazon, de Heinz, de Pepsi, ou bien encore Ikea a manqué à ses engagements relatifs à la sécurisation des données confidentielles de ses clients. Sa responsabilité peut donc être engagée à ce titre. Dans tous les cas, le scandale a laissé des traces et l'image de la société est alterée.

3. Les moyens déployés pour pérenniser les données sensibles dans l'entreprise

Le constat est sans appel. Les entreprises doivent, une fois les données sensibles identifiées, mettre en place des processus de protection. Notre terrain d'étude porte sur trois entreprises de tailles et à vocations différentes. Le Luxembourg est pour la Grande région un pôle d'attractivité et de vie économique internationale. Ce pays est une zone géographique où la concentration d'entreprises est forte ce qui induit la gestion des données sensibles à l'échelle locale mais aussi parfois au niveau international, selon les cas. Il existe de nombreuses entreprises de tailles variées et dont les activités sont complémentaires ou non. Les conclusions de cette étude sont transposables dans les entreprises françaises présentant des caractéristiques similaires.

A. *Cabinet de conseil A (observation de 2009 à 2011) :*

Société d'une quarantaine de collaborateurs, le cabinet de conseil S exerçait dans des domaines variés comme l'informatique (IT), les Ressources Humaines ou bien encore dans les domaines industriels et de la formation. 80 % des collaborateurs étaient des consultants externalisés directement chez les clients dans toute l'Europe. Seulement 20 % des effectifs étaient basés quotidiennement au Luxembourg. De ce fait, chaque collaborateur disposait d'outils informatiques de type ordinateurs portables et mobiles qu'il utilisait chez le client ou il utilisait directement les infrastructures et outil de client. Aucun système de centralisation des données n'existait et chacun gérait son activité quasiment comme un indépendant leur ferait s'il travaillait pour son propre compte. Le respect d'une charte graphique uniformisée et la récupération des données issues du travail de ces consultants et par exemple des formateurs étaient très compliqués car

le monde du consulting est frileux à l'idée de diffuser ses données. En fonction des missions, les données traitées étaient plus ou moins sensibles. Toutefois la clientèle était composée de clients grands compte, d'institutions principalement françaises, de fiduciaires luxembourgeoises, d'industrie et de petites et moyennes entreprises. Un seul type de données sensibles étaient identifiées par la direction : il s'agissait des données comptables, financière et plus spécifiquement salariales. La méthode utilisée de sauvegarde était mensuellement de faire une copie des données dites « sensibles » sur un disque dur externe et de faire des copies papier des documents stockés au domicile du gérant. Une partie de l'activité des consultants informatique était dédiée au déploiement de soft (logiciel) et d'ERP (d'outils virtualisé de gestion de données y compris sensibles). Avec ce développement, l'entreprise a loué des espaces de stockage externalisés auprès de prestataire sous traitant qui garantissait la pérennisation des données. En 2011, cette société suite à un désaccord avec un des associés qui venait d'obtenir une autorisation d'exploitation sur un brevet pétrolier (autre versant de l'activité de la société), a été mise en faillite. La procédure a duré plusieurs mois et les clients, notamment des solutions informatiques, ont eu beaucoup de difficultés à faire basculer leurs données les plus sensibles vers de nouveaux fournisseurs.
Une procédure particulière de préservation des données sensibles et du capital informationnel en cas de faillite y compris de petites entreprises serait à étudier et à développer [22].

B. L'agence de publicité B (observation de janvier 2013 à mars 2015) :

L'agence de publicité B est composée d'une dizaine de collaborateurs au plus sur la période observée de 2013 à 2015 et a été créée en 2001. Son activité repose sur la mise en place et l'accompagnement dans le domaine de la communication et de la publicité pour des clients grands compte en France, au Luxembourg et en Allemagne ainsi que pour des clients de type PME dans des domaines variés come le BTP et la construction, 'importation de fruits et légumes et de la grande distribution, les banques, le « facility management » …Tous les salariés travaillent sur site et la société est équipée d'un réseau informatique dédié à ses activités qui a été mis en place par l'un des salariés. Ce dernier a géré, jusqu'à son départ fin 2014, la gestion quotidienne, la maintenance du réseau, la création et la gestion des comptes utilisateurs. Il était aidé parfois par une entreprise informatique pour des cas de pannes plus importantes. Suite à son départ, l'entreprise confie ponctuellement les missions aux deux salariés en charge du développement de sites web. Le parc informatique se compose d'ordinateurs fixes et plusieurs ordinateurs portables que les salariés et la direction utilisent à domicile ou lors de présentation de travaux à des clients. Environ une fois tous les deux mois une sauvegarde manuelle est réalisée sur des disques durs externes. Un serveur est localisé au sein de l'agence pour maintenir les données créées quotidiennement. Le volume de données traitées est une problématique importante pour une agence de publicité de petite taille. En effet, le poids des fichiers photos et de création graphique est très lourd et posaient régulièrement des problèmes de ralentissement du réseau. Les employés, pendant la période observée, n'avaient pas de mot de passe sur leur poste ni d'identifiant et les mots de passe et identifiant des différentes applications étaient sauvegardés manuellement par l'un des membre de l'équipe. Un turnover important a été constaté pendant les deux années d'observation ce qui amplifie les risques de diffusion ou de perte externe de données sensibles. Toutes les données de l'agence ne sont pas confidentielles. Toutefois, elles proviennent de deux sources principales : interne pour les données de compatibilité et de facturation et externe en ce qui concerne les données des clients. Lors de la mise en place d'une relation contractuelle, le processus consiste en la prise du brief et la mise à disposition de données, la réalisation de la mission puis de a livraison.

Brief ->	**Réalisation ->**	**Livraison**
Mise à disposition par le client de données de l'entreprise	Utilisation des données	Conservation des données localement

Tab. 1 : processus de création de données y compris sensibles.

Dans ce type de structure, il existe un risque majeur de défaillance du système d'information tant sur le plan technique que humain pour l'entreprise comme pour ses clients. La sécurité et l'attention portée aux données ne sont pas suffisantes face aux enjeux économiques et judiciaires. Certains clients, principalement des grandes entreprises, concluent avec leur agence un accord de confidentialité (ou NDA –Non Disclosure Agreement) qui engage la responsabilité de l'agence dans le cas de perte ou de la diffusion de données ou d'information à caractère confidentiel ou stratégique. Au regard des enjeux, cela n'est pas suffisant.
Dans le cadre du choix de partenaires pour externaliser tout ou partie de ses missions et de fait de ses données y compris sensibles l'entreprise se doit de disposer de garanties qui doivent aller au delà des aspects contractuels.

C. la compagnie d'assurance vie C (observation mars 2015 à septembre 2015) :

Filiale d'un groupe français bancaire, la compagnie d'assurance vie C se compose d'environ 90

employés au Luxembourg pour cette activité. Ses clients sont des clients fortunés issus principalement de la banque privée. Les données sensibles occupent deux dimensions de l'entreprise. Dans un premier temps, la compagnie est particulièrement attentive au traitement des données de ses clients. Le contexte bancaire et financier nécessite la mise en place de solutions hyper-sécurisées pour garantir l'intégrité et la sécurité des informations. La gestion de ces données est très encadrée et l'entreprise fait appel tant en interne (entité ou groupe) qu'à l'externe à des personnes hautement qualifiées et des outils à la hauteur de leurs besoins. Chaque collaborateur dispose d'un ordinateur fixe (physique) et d'un accès sécurisé de type bureau virtuel. Chacun bénéficie d'un accès spécifique qui lui permet d'accéder aux données auxquelles il est autorisé d'accéder uniquement. L'accès aux sites internets est limité aux seuls sites autorisés et exclu de fait les réseaux sociaux et les webmails. Un service dédié au helpdesk a en charge l'assistance et le dépannage de premier niveau. L'accès aux locaux est restreint et sécurisé par des badges et un système de vidéo surveillance et de gardiennage 24h/24. Les échanges par mails sont sécurisés et il est possible de classifier les échanges par une indication qui indique aux destinataires le niveau de confidentialité du message : C1 pour les messages les moins confidentiels à C5 pour les informations les plus sensibles. Chaque salarié, lors de son intégration, prend connaissance et signe une charte de bonne conduit et d'engagement tant par rapport à la diffusion d'informations sensibles qu'à l'usage des systèmes d'information et des outils mis à sa disposition. Depuis peu, le déploiement de tablette tactile auprès de l'ensemble des collaborateurs du groupe, pose de nouvelles interrogations. Il n'est par exemple pas admis par la législation luxembourgeoise de faire signer un document via cet outil et d'en faire reconnaitre la valeur, alors que la technologie le permet. De plus, le collaborateur disposant de cet outil sera amené à utiliser des connexions internet externes à l'entreprise (réseaux privés ou publics). Cela nécessite l'augmentation du niveau de sécurité des outils déployés. Enfin, de nouvelles applications sont en cours de déploiement notamment à destination d'apporteurs extérieurs. Dans ce cadre, plusieurs entreprises spécialisées dans le déploiement de solutions informatiques sont consultées. Les critères de choix ont été élaborés de manière classique en interne lors de réunions de brain storming, d'échanges techniques et des premières rencontres avec les prestataires. La limite posée à ce type de mise en place de critère est que la ou les personnes en charge du projet n'ont pas nécessairement la connaissance métier technique nécessaire à la prise en compte de l'ensemble des facteurs de risques pour la gestion des données sensibles.

D. Synthèse et comparaison des systèmes :

L'observation de ces trois entreprises luxembourgeoises permet de mettre en avant la comparaison suivante :

Cabinet de conseil A	Agence de publicité B	Compagnie d'assurance C
Prestataire et sous-traitant	Prestataire et sous-traitant	Entreprise qui externalise vers des prestataire
Présence de données sensibles dans le système d'information	Présence de données sensibles dans le système d'information	Présence de données sensibles dans le système d'information
Risque non géré	Risque compris et traité partiellement	Risque compris, intégré dans les démarches de gestion des données
Sécurisation faible	Sécurisation moyenne	Sécurisation forte à l'interne

Tab. 2. Comparaison de la prise en compte des données sensibles dans les trois entreprises.

Il existe un réel décalage entre les attentes des entreprises de type C par rapport à l'exemple des entités A et B qui ne proposent pas de garanties suffisantes. Des incidents (non communiqués aux clients) ont été constaté dans les entités A et B. On peut citer par exemples, une intrusion par des hackers sur le serveur ou bien encore un problème machine lors d'un violent orage. La notion de risque est de plus en plus prise en compte en interne. Elle est toutefois mise en péril lors de l'externalisation comme lors de l'impression de données sensibles de types bancaires [23].

Il en est de même avec les services. Les certifications, les installations, la mise en place et l'analyse par des gestionnaires de risques, ou bien encore l'analyse de l'expérience peut permettre de « rassurer ». Mais quelle méthodologie analytique tangible peut être déployée pour une prise en compte globale et réelle du risque de perte ou de détérioration de ses données sensibles ?

4. Les garanties apportées par les outils

Protéger ses informations stratégiques et donc ses données sensibles est un point très important que l'entreprise dit intégrer à ses processus décisionnels [24].

Nous avons pu observer, au travers de l'étude comparative menée que ces entreprises n'abordent pas de la même manière la préservation de leurs données sensibles. **Protéger ses données sensibles c'est protéger son entreprise.** Les menaces peuvent être internes ou externes, actives ou passives (avec ou non lune volonté de nuire). Les typologies de menaces sont variées. Certaines de ses

actions sont licites (analyse des sources ouvertes et publiques, exploitation de maladresses), ou illicites (exploitation de failles des politiques de sécurité). Une bonne protection nécessite la mise en œuvre d'une politique d'identification des menaces qui doivent faire l'objet du déploiement de dispositions permanentes ou occasionnelles de sécurisation. Le choix des outils de traitement des données sensibles est en ce sens primordial [25]. Innover est une des préoccupations permanentes de l'entreprise, trouver de nouvelles idées et maintenir ainsi son avantage concurrentiel. Le maintien et la sécurisation de ces données sensibles sont également des éléments qui permettent de maintenir un avantage important face à la concurrence et pourtant comme nous avons pu le constater, ils sont souvent ignorés ou sous estimés. Les outils déployés au sein de l'entreprise, doivent permettre de garantir la disponibilité, l'intégrité et la sécurité des données sensibles. C'est pourquoi il est important de s'appuyer, en fonction de son budget, sur des solutions fiables qui doivent garantir le respect de ces trois conditions [27]. Il est important de s'appuyer sur la connaissance d'experts du domaine et d'être en veille de nouvelles solutions techniques proposées. Avant tout déploiement de solutions, il est nécessaire d'identifier les données sensibles et de les cartographier. L'entreprise doit procéder à un audit de son système d'information [28]. Dans un second temps, la mise en place en interne d'un groupe d'individus en charge de la surveillance des outils et de ce fait de gestion du risque opérationnel (« *risk management* »[1]) peut permettre de mettre en évidence les failles du système d'information de l'entreprise et de mettre en place des plans d'actions appropriés pour les résoudre. Des tests ponctuels peuvent être également réalisés. Dans le cas de l'externalisation de tout ou partie de ses données sensibles, l'entreprise peut se référer aux labels et demander des garanties à son sous-traitants ou partenaire. Six règles clefs peuvent être déployées dans l'entreprise pour une bonne protection des données sensibles [29], comme une méthodologie préalable à appliquer :

i. Identifier les données importantes et signaler les données sensibles.
ii. Impliquer le personnel et sécuriser les systèmes d'information.
iii. Protéger les données sensibles, informations stratégiques par un accord de confidentialité [31].
iv. Assurer la confidentialité interne et externe [32] par des outils adaptés.
v. Sanctionner les manquements.
vi. Protéger ses innovations par les brevets [30].

[1] Gestion des risques

5. Conclusion

Prendre conscience de la valeur économique et stratégique des données sensibles de son entreprise est un facteur clef du développement de son activité et du maintien de sa compétitivité [33]. Toutes les entreprises ne traitent pas les données sensibles de la même manière et la maturité du sujet est différente. Les spécificités métiers et les budgets alloués sont différents d'une entité à l'autre. Toutefois, aujourd'hui dans un contexte économique difficile l'entreprise doit être capable d'identifier ces données sensibles dans son organisation. Elle doit procéder à une cartographie de son système d'information et ce quelque soit sa taille et son activité (i). Elle a la possibilité de s'appuyer également sur la mobilisation de son personnel car le facteur humain est également une source de risque pour les données sensibles comme nous avons pu le voir dans cet article avec Luxleaks (Cf. 2-c.) (ii et v). Protéger son entreprise, c'est protéger ses clients mais pas seulement. L'entreprise veille à sa réputation et la qualité de ses biens et services. Même dans le cas d'une faillite comme pour le cabinet de conseil A, la fin doit être autant que possible sereine pour les clients. Cela comprend également la sécurité de ses employés et des dirigeants et ce quelque soit la taille de l'entreprise. La mise en péril par une faille ou une indisponibilité technique peuvent avoir des conséquences économiques sur l'entreprise. Pendant la période d'observation de l'agence de publicité B, plusieurs accidents sont survenus dus aux choix techniques hasardeux de préservation des données sensibles. Ces derniers ont engendrés des coûts importants de remise en marche et de disponibilité du personnel pour y parvenir. Le choix des outils de gestion de l'activité de l'entreprise est un facteur clef de la réussite du management des données sensibles. Ils doivent en permettre de garantir, et ce sans concession la disponibilité, l'intégrité et la sécurité (iv). En 2015, le hasard n'est plus permis dans le management des données sensibles. Une attention particulière et souvent ignorée des entreprises, repose sur le fait que l'entreprise est dynamique.

C'est pourquoi, il est primordial au delà de l'interne d'identifier les menaces et de mettre en place des plans d'actions cohérents pour garantir aux entreprises un développement serein des activités. Qu'à ce titre, la proposition méthodologique issue des observations sur l'étude comparative s'avère plus que demandée.

6. Biographie

[1] RUNISO, table ronde mis en ligne 22/05/2015 «Données sensibles, sécurité critique ? » URL Visited 27/09/2015, http://www.runiso.com/donnees-sensibles-securite-critique/

[2] Commission Nationale pour la Protection des Données - Grand-Duché de Luxembourg, « Le

dirigeant d'entreprise face à la criminalité informatique » 01/04/2010, URL Visited 27/09/2015,
http://www.cnpd.public.lu/fr/actualites/articles-interviews/2010/04/dirigeant-entreprise-criminalite-informatique/index.html?print
[3] Legilux, Loi du 27 juillet 2007, protection des personnes a l'égard du traitement des données a caractère personnel, URL Visited 27/09/2015,
http://www.legilux.public.lu/leg/a/archives/2007/0131/a131.pdf
[4] Commission Nationale pour la Protection des Données - Grand-Duché de Luxembourg, Principaux changements de la loi du 27 juillet 2007, URL Visited 27/09/2015,
http://www.cnpd.public.lu/fr/legislation/droit-lux/principaux-changements/index.html
[5] CNIL, « Recommandations pour les entreprises qui envisagent de
souscrire à des services de Cloud computing », URL Visited 27/09/2015,
http://www.cnil.fr/fileadmin/images/la_cnil/actualite/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf
[6]- Loi informatique et liberté de 1978, URL visited 27/09/2015.
http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000006068624&dateTexte=20080609
[7] Carole Henry Optimisation de processus de collecte et d'exploitation d'informations sensibles: cadre d'étude du renseignement intérieur, ISKO Maghreb 2013
[8] De Courcy R., Les systèmes d'information en réadaptation, Québec, Réseau international CIDIH et facteurs environnementaux, 1992, no 5 vol. 1-2 P. 7-10
[9] Commission Nationale pour la Protection des Données - Grand-Duché de Luxembourg, « Déclarer» , URL Visited 27/09/2015,
http://www.cnpd.public.lu/fr/declarer/index.html
[10] ISO/IEC 27005:2011- Technologie de l'information- techniques de sécurité- gestion des risques liés à la sécurité de l'information, URL Visited 27/09/2015,
http://www.iso.org/iso/fr/catalogue_detail?csnumber=56742
[11] Relgerchot et Becker, Becker, F. 1990. The Total Workplace: Facilities Management and the Elastic Organiazation. Van Nostrand Reinhold, New York, USA
[12] Silicon, « Orange tente de minimiser l'impact du piratage des données de ses abonnés » 03/02/2014, URL Visited 27/09/2015,
http://www.silicon.fr/orange-tente-de-minimiser-limpact-du-piratage-des-donnees-de-ses-abonnes-92459.html
[13] Silicon, « Vol de données : 2014, année de tous les records (infographie)» 10/12/2014, URL Visited 27/09/2015, http://www.silicon.fr/vol-de-donnees-en-2014-le-milliard-depasse-infographie-103820.html
[14] l'International Consortium of Investigative Journalist, 09/12/2014, URL Visited 27/09/2015,
http://www.icij.org/project/luxembourg-leaks/explore-documents-luxembourg-leaks-database
[15] Libération, « LuxLeaks : «J'ai agi par conviction, la cohérence était d'assumer», 14/12/2014, URL Visited 27/09/2015,
http://www.liberation.fr/economie/2014/12/14/luxleaks-j-ai-agi-par-conviction-la-coherence-etait-d-assumer_1163578
[16] Le Monde, « Mise en examen d'Edouard Perrin, le journaliste qui a révélé le « LuxLeaks » », 23/04/2015, URL Visited 27/09/2015,
http://www.lemonde.fr/economie/article/2015/04/23/mise-en-examen-au-luxembourg-du-journaliste-qui-a-revele-le-luxleaks_4621546_3234.html
[17] Parlement européen – Actualités, « Le Prix du citoyen européen 2015 salue l'engagement de 47 Européens », 04/06/2015, URL Visited 27/09/2015,
http://www.europarl.europa.eu/news/fr/news-room/content/20150604STO62606/html/Le-Prix-du-citoyen-europ%C3%A9en-2015-salue-l'engagement-de-47-Europ%C3%A9ens
[18] Le Quotidien, indépendant luxembourgeois, « Antoine Deltour reçoit le Prix du citoyen européen », 04/06/2015,
URL Visited 27/09/2015,
http://www.lequotidien.lu/politique-et-societe/antoine-deltour-recoit-le-prix-du-citoyen-europeen/
[19] Le Quotidien, indépendant luxembourgeois, Dossier Luxleaks, URL Visited 27/09/2015,
http://www.lequotidien.lu/affaire-luxleaks/
[20] Le Monde, « LuxLeaks : l'auteur présumé des fuites inculpé de vol au Luxembourg», 13/12/2014, URL Visited 27/09/2015,
http://www.lemonde.fr/economie/article/2014/12/13/luxleaks-l-auteur-presume-des-fuites-sur-l-evasion-fiscale-inculpe-pour-vol_4539970_3234.html#
[21] Wort, « Steuerdumping im Großherzogtum» (Fr : Dumping fiscale dans le Grand duché), URL Visited 27/09/2015,
https://www.wort.lu/de/politik/luxleaks-steuerdumping-im-grossherzogtum-545b8016b9b398870808837e4
[22] Yosra Bejar. La Valeur Informationnelle du Capital Immat´eriel : Application aux Entreprises Technologiques Nouvellement Introduites En Bourse (1997 – 2004). Business administration. Université Paris Dauphine - Paris IX, 2006. French.
[23] Carole Henry, Sahbi Sidhom, Imad Saleh. Fondements de dématérialisation et traitement
des données sensibles: cadre d'étude sur l'impression bancaire.. SIDHOM Sahbi, GHENIMA

Malek, BA¨INA Karim, BADACHE Nadjib, MEZIANE Abdelkrim (Eds.). 4th. International Symposium ISKO-Maghreb : Concepts and Tools for Knowledge Management (KM), Nov 2014, Alger, Algeria. 1 (1-2014), pp.7, 2014, Actes du Colloque International ISKO Maghreb 2014.<www.isko-maghreb.org & http://isko-maghreb.loria.fr & www.cerist.dz/isko-maghreb2014/>.<hal-01109154>

[24] Vincent Lalanne, Manuel Munier, Alban Gabillon. Gestion des Risques dans les Systèmes d'Information Orientés Services. 8ème Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information (SARSSI'2013), Sep 2013, Mont de Marsan, France. <hal-01082073>

[25] Kheira Dari Bekara. Protection des données personnelles côté utilisateur dans le e-commerce. Economies and finances. Institut National des Télécommunications, 2012. French. <NNT :2012TELE0045>.

[26] CNIL, Enjeux 2015 (2) : la protection des données, clé de voûte de l'innovation, 16/04/2015, URL Visited 27/09/2015, http://www.cnil.fr/nc/linstitution/actualite/article/article/enjeux-2015-2-la-protection-des-donnees-cle-de-voute-de-linnovation/

[27] B. Boutherin. Les étapes de la mise en sécurité. L'Informatique Professionnelle, Gartner EXPBLG, 2004, 220, pp.26-29. <in2p3-00020239>

[28] Louise Blas. L'audit d'un système d'information au sein d'une petite structure. Le cas de laFondation René Seydoux.. domain shs.info.gest. 2009. <mem 00486268>

[29] Guide pratique du MEDEF, La protection des données sensibles, URL Visited 27/09/2015, http://www.n2s.fr/IMG/pdf/MEDEF_GUIDE_DE_LA_PROTECTION_DES_INFORMATIONS_SENSIBLES.pdf

[30] BREESE, P. Stratégies de propriété industrielle - Guide des entreprises innovantes en action, Dunod, 2002.

[31] CORDIER G. Un point-clé des accords de confidentialité : le contrôle par le communicant des informations communiquées, Revue LexisNexis Jurisclasseur Communication–Commerce électronique, Avril 2008.

[32] LEMAIRE, C. La protection du secret des affaires devant le Conseil de la concurrence : une évolution bienvenue, JCP, éd. E, no 1161, 2006.

[33] Relgerchot et Becker, Becker, F. 1990. The Total Workplace: Facilities Management and the Elastic Organiazation. Van Nostrand Reinhold, New York, USA.[URL visited 23/02/14].http://www.journal.au.edu/au_techno/2002/jul2002/article4.pdf