MASTER SIC
EM SORBONNE

UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE

UNIVERSITÉ PARIS 1
PANTHÉON SORBONNE
ÉCOLE DE MANAGEMENT
DE LA SORBONNE

Université Paris 1 Panthéon – Sorbonne

Mémoire de Master

SYSTÈMES D'INFORMATION ET DE CONNAISSANCE

Sous-parcours Big Data

Promotion 2019-2020

« NORMES ET REGLEMENTS COMME OPPORTUNITE DE MAITRISE ET DE PROTECTION DU PATRIMOINE INFORMATIONNEL D'UNE ORGANISATION

Mise en application du Règlement Général sur la Protection des Données au sein d'un service RH »

RÉDIGÉ ET SOUTENU PAR : Rébecca AVRANE

DIRECTEUR DE MÉMOIRE : Samuel PARFOURU

DATE DE SOUTENANCE : 8 octobre 2020

L'UNIVERSITE N'ENTEND DONNER AUCUNE APPROBATION
NI IMPROBATION AUX OPINIONS ÉMISES
DANS CE MÉMOIRE :
CES OPINIONS DOIVENT ETRE CONSIDÉRÉES
COMME PROPRES À LEUR AUTEUR

Identification du travail effectué

Dans le cadre de mon Master 2 Management des Systèmes d'Information et de Connaissance parcours Big Data à l'École de Management de l'Université Paris 1 - Sorbonne, j'ai réalisé mon alternance en tant que SIRH et Contrôle de gestion sociale au sein d'Atos Management France pour une durée de deux années – du 22 octobre 2018 au 31 octobre 2020, sous la responsabilité du responsable SIRH et Contrôle de gestion sociale et de la directrice du CSP-RH.

L'étude portée dans ce rapport traduit et clotûre une démarche engagé durant ses deux années passées au sein du CSP-RH en abordant le sujet des normes et règlements comme opportunité de maitrise et de protection du patrimoine informationnel d'une organisation.

Remerciements

L'écriture de ce mémoire représente un engagement personnel et professionnel long et intense. Ce document est le fruit d'un vaste travail de réflexions et de recherches qui n'aurait pu se faire sans les échanges, mais aussi quelquefois les phases de remise en question et de doutes. Ce travail a été réalisable grâce à la présence des personnes m'ayant accompagnées et soutenues tout du long de cette année d'écriture.

Ainsi, avant de débuter la lecture de ce mémoire, je souhaiterais remercier ici, celles et ceux qui ont contribué, à leur manière, à ce travail.

Je souhaite, en premier lieu, remercier Monsieur **Samuel PARFOURU,** mon directeur de mémoire, pour son suivi, sa bienveillance et ses conseils avisés. Il a su, dès notre première discussion, m'encourager et me faire confiance. Sa disponibilité et son accompagnement m'ont apporté une méthodogie de travail et une aide précieuse tout au long de cette année si particulière.

Je tiens aussi à remercier Madame **Manuele KIRSCH PINHEIRO** pour le regard extérieur qu'elle a su porter sur mon travail. Tout au long de nos échanges, elle a su m'apporter des conseils et réponses bienveillantes qui ont su me mettre en confiance.

Ce travail n'aurait été possible sans la présence et l'accompagnement de Madame **Selmin NURCAN,** directrice du master Management des Systèmes d'Information et de Connaissance, qui m'a permis d'intégrer cette formation en alternance et de Madame **Florence AUBERT,** chargée de missions au CFA AFIA.

Au sein de mon entreprise d'accueil, Atos, je souhaite remercier mon manager **Yoan** pour sa confiance et son accompagnement. L'ensemble des missions confiées a été déterminant dans le choix de ce sujet et m'a permis d'avoir un terrain de recherche sur lequel m'appuyer. Je le remercie pour ses conseils durant ces deux années passées à ses côtés. J'ai également une très grande pensée pour la directrice du CSP-RH **Catherine** qui a rendu possible mon expérience au sein de l'équipe et qui a également été d'un très grand soutien. Je n'oublie pas l'ensemble des personnes au sein d'Atos à qui j'ai pu parler de mon travail et qui ont été d'une aide particulière.

Enfin, je souhaite remercier ma famille et mes proches pour leur présence et leur aide. Ils ont su me donner motivation et encouragements afin d'obtenir une ouverture d'esprit plus grande et des questionnements aboutissant sur ce travail.

Résumé

L'espace informationnel est inhérent aux organisations qui doivent adopter des mesures nécessaires et adéquates afin d'assurer sa maitrise et sa protection. Les normes et règlements s'imposent aux organisations comme un changement prescrit, progressif et imposé. Un long travail s'impose alors aux organisations afin de parvenir à cette maitrise et cette protection.

Ce mémoire de recherche aborde le sujet des normes et règlements comme opportunité de maitrise et de protection du patrimoine informationnel d'une organisation. Il prend pour exemple la mise en application au Règlement Général sur la Protection des Données (RGPD) au sein d'un service RH. La question de recherche posée est : De quelles manières la mise en conformité peut contribuer à la maitrise du patrimoine informationnel et former un levier de performance opérationnelle interne ?

Ce travail de recerche a été initié il y a deux ans durant ma période d'apprentissage au sein du groupe Atos en tant qu'alternante SIRH et Contrôle de gestion sociale. Ces deux années ont permis d'aborder un terrain réel. Ce travail est le fruit de réflexions et d'analyses théoriques et pratiques sur les problématiques de mise en conformité ainsi que la maitrise et la protection de la notion de patrimoine informationel.

Ce document présente la mise en conformité aux normes et réglements comme opportunité et levier de performance opérationnelle interne pour une organisation, et en particulier au sein d'un service RH.
Il constitue un guide pratique permettant d'accompager les organisations en général ainsi que les personnels chargés de la mise en application des normes et règlements, dans la sensibilisation des acteurs et la mise en conformité.

Il confirme l'hyopthèse selon laquelle la mise en conformité aux normes et règlements, au-delà d'être une imposition, est une opportunité pour la maitrise de l'espace informationnel.

Mots Clés :
Patrimoine informationnel, Données, Informations, Connaissances, Données à caractère personnel, Traitement, Gouvernance des données, Organisation, Cadre légal, RGPD, Normes ISO, Mise en conformité, , Enjeux, Opportunités, Risques

SOMMAIRE

Table des illustrations

Introduction générale

« Je ne connais pas d'être vivant, de cellule, tissu, organe, individu et peut-être même espèce, dont on ne puisse pas dire qu'il stocke de l'information, qu'il traite de l'information, qu'il émet et qu'il reçoit de l'information. » - Michel Serres (Abiteboul, 2012)

Nous vivons dans un monde où la technologie et le numérique sont devenus omniprésents. La digitalisation et la numérisation des activités sont devenues deux sujets cruciaux pour les organisations. La diversité des technologies et l'émergence de nouvelles problématiques, telles que l'intelligence artificielle, la cybersécurité ou la protection des données, démontre que nous sommes au cœur d'une transition numérique considérée comme la quatrième révolution industrielle. On peut la définir par l'union des technologies et la suppression des frontières entre domaines physique, numérique et biologique.

L'essor des nouvelles technologies a des incidences fortes tant sur notre vie personnelle que sur notre vie professionnelle et accélère notre rapport au numérique. Qu'ils s'agissent de nos pratiques d'achat par la vente en ligne ou de nos pratiques de travail avec l'expansion du télétravail ces derniers mois et pour les mois à venir pour faire suite à la pandémie mondiale (COVID-19), nous avons dû nous adapter et veiller à notre identité numérique. (Rieffel, 2014)

Face à un monde qui s'accélère, notre rapport au temps est modifié. Nous vivons dans une société du numérique et devons faire face à une explosion des flux d'informations.
L'émergence de cette révolution numérique et l'évolution rapide de nos systèmes d'information bousculent notre rapport aux technologies. En effet, elles voient leur puissance de traitement et leur capacité de stockage évoluer de manière exponentielle.
L'accès aux informations et aux connaissances est également modifié face à ce tsunami informationnel.

Le Big Data désigne cette démultiplication du volume de données créées, collectées, stockées et manipulées par les hommes et les organisations. Chaque jour, un nombre exponentiel de données est créé tant par les géants du numérique – les GAFAM –, que par les organisations ou les individus. Une étude, menée par Statista Digital Economy Compass en 2019, montre que le volume annuel de données numériques créées dans le monde va passer de 47 zettaoctets en 2020 à 2142 zettaoctets d'ici 2035, comme le montre la figure ci-dessous. (Armstrong, 2019)

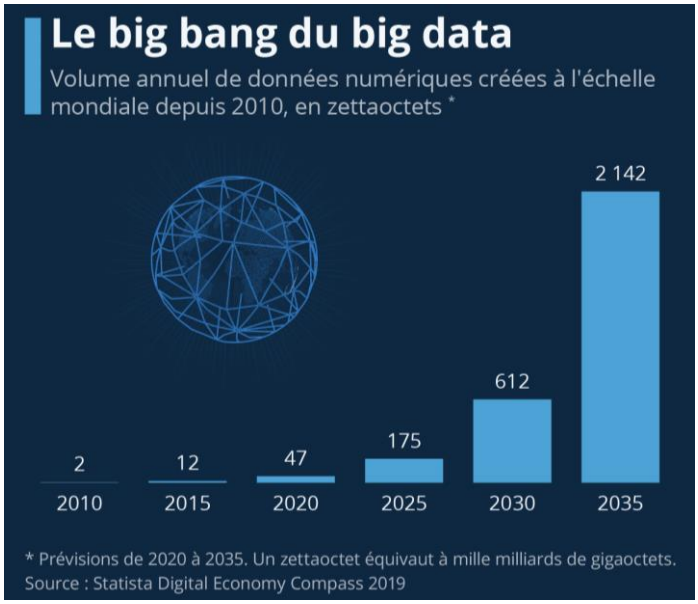

Figure 1 – Le Big bang du Big data (Gaudiaut, 2020)

Cette infobésité résulte de la multiplication des sources et d'une pluralité des supports de stockage tant personnels que professionnels. Au cœur de ce tsunami informationnel, on observe une multiplication des données non structurées (mail, texte, photo). Elles représentent aujourd'hui 80% des données de l'organisation avec une croissance d'environ 30% chaque année. Ces données font partie intégrante du patrimoine informationnel d'une organisation.

De nos jours, les données sont considérées comme une véritable ressource et matière première pour les organisations. Elles sont souvent nommées le nouvel or noir. La gestion et la maitrise des données sont ainsi devenues cruciales. Les données servent de point de départ pour comprendre les usages de nos organisations. Leur maitrise requiert une compréhension des flux d'informations, des traitements réalisés et nécessite la connaissance du rôle de chaque acteur. Néanmoins, la dispersion des données et l'évolution de nos systèmes d'information rendent leur compréhension toujours plus complexe. En effet, il est difficile d'acquérir une compréhension du patrimoine informationnel sans en avoir au préalable une cartographie référençant l'ensemble de celui-ci. Cette question de gestion des données est bien souvent occultée par des organisations qui sous-évalue le rôle des données ou pour lesquelles cette question n'est pas au cœur de leur préoccupation. (Régnier-Pécastaing, 2008)

Dans ce contexte, et face aux enjeux que représente le patrimoine informationnel, les organisations se doivent de transformer le management de ce patrimoine informationnel pour parvenir à sa gouvernance. Celle-ci vise à la maitrise et la protection du patrimoine informationnel.

Afin de parvenir à cette gouvernance des données, il est nécessaire de mobiliser l'ensemble des acteurs d'une organisation pour assurer la gestion et la protection des données en réponse aux nouveaux risques et menaces. Celles-ci se font plus nombreuses et plus fréquentes, avec, par exemple, les cyber-attaques ou les vols des données. Ces menaces bien réelles créent de nouveaux risques pour les organisations. Il est donc nécessaire de mettre en place un cadre légal et normatif afin d'assurer la protection du patrimoine informationnel.

Cette gouvernance du patrimoine informationnel provoque une normalisation des approches et requiert la mise en place de processus visant la gestion du cycle de vie du patrimoine informationnel. (Akoka & Comyn-Wattiau) Elle nécessite également le respect d'un cadre légal établi qui peut être interne ou externe à l'organisation. Ce besoin de gouvernance n'est pas nouveau mais devient une nécessité face à des défis plus complexes, comme celui de la protection du patrimoine informationnel, en particulier la protection des données personnelles. (Pagnamenta, 2014)

La problématique de ce travail de recherche est : De quelles manières la mise en conformité peut contribuer à la maitrise du patrimoine informationnel et former un levier de performance opérationnelle interne ?
Pour répondre à cette problématique, le document se présente en deux parties : une partie visant la revue de la littérature et une partie visant la présentation des pistes de résolutions et de la méthode de recherche.

Partie 1 – Contexte et Problématique

La société de l'information se définie par la progression du numérique qui a suscité des transformations en matière de partage de l'information suite à l'évolution des technologies. L'UNESCO précise que le partage du savoir et de l'information a la capacité de bouleverser les économies et les sociétés. (UNESCO)

Dans un contexte où les données se démultiplient et où les systèmes d'information évoluent à grande vitesse, l'environnement règlementaire est en constante évolution. Les données se trouvent au cœur des enjeux liés à la mise en conformité rencontrés par les organisations dans un monde marqué par de nouvelles attaques, notamment les cyber-attaques ou le vol de données. Ces attaques et menaces démontrent l'importance des données et nous évoquent le fait qu'elles font l'objet de convoitise.

Les normes et règlements se font plus nombreuses. On peut citer les normes d'organisation internationale, règles européennes et règles d'entreprise. Ce contexte règlementaire strict et renforcé permet d'aborder les problématiques de gouvernance du patrimoine informationnel, de gestion et maitrise des risques et de mise en conformité. Les normes et règlements, et en particulier le Règlement Général sur la Protection des Données, (RGPD) imposent un cadre juridique et opérationnel. Celui-ci amène une prise de conscience collective initiée par un besoin d'identification, de maitrise et de protection des données. Cette règlementation vient faire face à de nouvelles menaces et nécessite de réduire les risques pour les organisations. Elle crée de nouvelles attentes plus présentes et plus fortes aussi bien en interne, par les organisations et les salariés, qu'en externe par les autorités de régulation et de contrôle et plus largement par la société civile.

Ce contexte règlementaire constitue un cadre au service de la gouvernance d'entreprise et de sa mise en place appropriée pour la gestion du patrimoine informationnel. Il forme un cadre légal qui encadre les systèmes d'information d'une organisation. Une contradiction demeure entre volonté de sécuriser à un niveau optimal le patrimoine informationnel et simplifier l'usage des outils. Cette contradiction doit trouver un équilibre entre protection et expérience utilisateur.
Les organisations doivent réfléchir à leur approche des données c'est-à-dire à leur manière de les utiliser et de les traiter.
Le traitement des données amène à s'interroger sur leur protection et les moyens mis en œuvre pour assurer leur protection. Cette notion de protection des données est, depuis le projet SAFARI initié en 1973 et l'entrée en vigueur du Règlement Général sur la Protection des Données en 2018, un sujet d'actualité. Les organisations doivent trouver les moyens et solutions pour assurer cette protection des données, notamment celle des

données à caractère personnel. Selon une étude menée par Ponemon Institute en mars 2017, une grande partie des organisations s'interroge sur les potentielles amendes encourues en cas de non-conformité. Si 67% des personnes interrogées lors de l'étude connaissent le Règlement Général sur la Protection des Données, seule 50% des organisations représentées ont dédié un budget spécifique pour agir en réponse aux nouvelles règlementations. 74% des personnes interrogées déclarent que le respect du RGPD aura un impact important et négatif sur leurs organisations notamment à cause des amendes potentielles et de la portée du règlement. (Roemer, 2018)

Ce sujet de mise en conformité et les problématiques afférentes touchent l'ensemble des organisations. La conformité est un sujet qui n'est plus une option pour les organisations mais bien une obligation. Les résultats doivent exister et être justifiables par les acteurs et l'organisation en cas de demande. Les organisations doivent faire face à ce besoin de conformité, qui exige une gestion et maitrise du patrimoine informationnel, et de protection des données.
Si les normes sociales sont reflétées dans les normes et les règlements, elles le sont également lorsque ce cadre règlementaire est implémenté dans le système d'information d'une organisation.

En tant qu'entreprise de service du numérique, Atos, l'entreprise dans laquelle j'ai réalisé ma formation en alternance au cours des deux dernières années, mène un travail important en matière de mise en conformité afin de respecter ce contexte règlementaire omniprésent.
Au cours de mes deux années d'alternance, j'ai pu constater les manques et les difficultés auxquels une entreprise peut faire face et découvrir les moyens et les actions nécessaires à mettre en œuvre afin d'être en conformité. Ayant réalisé mon alternance dans un service RH, j'ai pu observer les conséquences et les impacts d'une mise en conformité sur les organisations et les services RH en particulier. Ces derniers sont au cœur du traitement des données et de l'usage qui en est fait. Ils sont au centre de cette nécessité de mise en œuvre d'une gouvernance appropriée pour la gestion et la protection du patrimoine informationnel par les organisations dans le respect du contexte règlementaire.

Ce travail de recherche vise à comprendre de quelles manières la mise en conformité peut contribuer à la maitrise du patrimoine informationnel et former un levier de performance opérationnelle interne. L'étude vise en particulier le cas de la mise en conformité au Règlement Général sur la Protection des Données dans un service RH.

Si le patrimoine informationnel est intrinsèquement lié à l'organisation et au traitement qui est réalisé, les données personnelles sont irrévocablement liées à l'individu et doit faire l'objet d'une protection spécifique.

Pour répondre à la question de recherche, il s'agira tout d'abord de définir la notion de patrimoine informationnel. À partir de ces définitions, on s'interrogera sur la valeur et le traitement des données.
Par la suite, une analyse du cadre légal existant et de son développement sera proposée. Il s'agira ici de spécifier son étendue et les nouvelles obligations amenées par le Règlement Général sur la Protection des Données aux organisations. Enfin, une étude des méthodologies pouvant être mises en œuvre et les risques associés à la protection des données personnelles sera menée.

Ce cadre légal, ces nouvelles obligations et la nécessité d'une mise en conformité amènent plusieurs questions : Quels sont les comportements à adopter par les organisations ? Quels sont les moyens à mettre en place ? Quels sont les enjeux et l'utilité d'une mise en conformité ? Quels sont les principaux acteurs touchés par le développement de ce cadre légal ? Quel est le rôle de ces acteurs ? Quels sont les risques auxquels les organisations doivent faire face ?
Apporter des éléments de réponses à ces questions doit contribuer à répondre à la question plus globale : **La mise en conformité est-elle une contrainte ou une opportunité pour les organisations** ?
Le travail porté dans ce travail de recherche vise à apporter des éléments de réponses pour l'ensemble de ces questions.

Pour donner suite à la revue de littérature, une approche de résolution sera proposée. Cette approche comportera, tout d'abord, une présentation de la démarche de recherche par une exposition de la méthodologie choisie et du terrain de recherche. Etablit sur les deux années d'alternance en tant que SIRH et Contrôle de gestion sociale au sein d'Atos, le terrain choisi permet d'établir mes propositions de solutions. L'ensemble de ces propositions sera, par la suite, discuté lors d'entretiens menés auprès de membres de cette organisation. La portée de ces entretiens vise à mettre en lumière les retours obtenus et de comprendre les avantages comme les inconvénients des solutions proposées. Les questions posées auront pour but de connaître leur opinion sur ce sujet d'actualité et d'obtenir leur retour d'expériences.

Étant au cœur de l'actualité et en constante évolution, le sujet traité est vaste et complexe. Ce mémoire vise à apporter une réponse la plus complète possible. Le lecteur peut choisir de faire une lecture de manière linéaire ou par bloc.
Une lecture linéaire, faite dans la totalité du document, donnera l'opportunité au lecteur d'avoir pleine compréhension des différents éléments afin d'acquérir une vision détaillée du sujet.
Au contraire, une lecture par bloc permettra au lecteur d'avoir une vision spécifique sur des aspects précis du sujet et des impacts des normes et règlements pour les organisations, et en particulier les services RH.

Partie 2 – Etat de l'art

I. Patrimoine informationnel

A. Définitions

1. Système d'information

Afin de comprendre plus précisément la notion de patrimoine informationnel et ce qui en découle, il est d'abord important d'apprécier et de comprendre la notion de système d'information pour une organisation. Le système d'information est « la partie du réel constituée d'informations organisées, d'événements ayant un effet sur ces informations et d'acteurs qui agissent sur ces informations ou à partir de ces informations, selon des processus visant une finalité de gestion et utilisant les technologies de l'information. » (Berthier, Morley, & Maurice-Demourioux, 2005)

Selon James A. O'Brien, un système d'information est l'ensemble des acteurs, des procédures, et des ressources permettant le recueil de l'information, afin de la transformer et la distribuer dans une organisation. (O'Brien, 1995)

Les auteurs Reix et Rowe définissent le système d'information comme un « système d'acteurs sociaux qui mémorise et transforme des représentations via des technologies de l'information et des modes opératoires ». (Reix, Fallery, Kalika, & Rowe, 2016)

Le système d'information s'appuie donc sur des ressources diverses : des ressources humaines, matérielles, liées au logiciel et procédures ainsi qu'aux données. L'ensemble de ses ressources associées simultanément permet d'acquérir de l'information, de la traiter, de la stocker et de communiquer. Le système d'information est ainsi un objet multidimensionnel comprenant quatre dimensions. La première reflète l'aspect organisationnel d'une structure puisque le système d'information intègre celle-ci. La seconde reflète la dimension informationnelle qui va nous intéresser principalement ici puisqu'il s'agit du fait de produire des informations. La troisième dimension est liée à la technologie et les outils techniques. Enfin la dernière dimension représente le fait que ce tout doit être géré et administré.

2. Patrimoine informationnel

Le terme de patrimoine d'entreprise traduit « l'ensemble des biens immobiliers, mobiliers, outils de production ainsi que les éléments de propriété intellectuelle appartenant à l'entreprise ». (L'internaute) Au-delà de sa richesse matérielle, tels que ses actifs comptables, la richesse d'une organisation se trouve dans son patrimoine informationnel ou capital immatériel (Direction générale des entreprises).

Le patrimoine informationnel est une notion aussi large que complexe à définir de manière précise et complète. Toute organisation possède son propre patrimoine informationnel qui est, de fait, différent d'une autre organisation. Il peut être définit comme « l'ensemble des données et des connaissances, protégées ou non, valorisables ou historiques d'une personne physique ou morale ». (Caprioli, De Kervasdoué, Pépin, & Rietsch, 2007) Acquis par une organisation au fil des années, il est constitué de plusieurs types d'informations sur l'organisation. Nous pouvons ainsi citer les informations commerciales, financières, industrielles, technologiques ainsi que les informations sur la clientèle et le personnel ou les savoir-faire de l'entreprise. (Delbecque)
Cette notion possède une nature juridique importante qui valorise « l'aspect immatériel et évolutif de ce dernier » (Asseman, Etude exploratoire des facteurs de risque du détournement en interne du patrimoine informationnel, 2011)

Jean Mourain, vice-président de la stratégie globale de la société RSD[1], spécialisée dans l'archivage d'entreprise, définit le patrimoine informationnel comme « une information reconnue comme ayant une valeur pour une organisation, quelle que soit sa forme physique ou électronique et la manière dont elle est stockée » (Solutions Numériques, 2013). Yves Granmontagne définit, quant à lui, la notion de patrimoine informationnel comme « l'ensemble des données et des connaissances » qui reposent aussi bien sur des propriétés intellectuelles qu'industrielles. (Grandmontagne, 2016) En 2009, Snyder & Crescenzi utilisaient le terme « capital intellectuel » afin de désigner l'ensemble des informations et données acquis par une organisation. Ils considèrent ce capital comme une « force majeure de la compétitivité ». (Asseman, Etude exploratoire des facteurs de risque du détournement en interne du patrimoine informationnel, 2011)
En 1997, Stewart assure que les ressources intellectuelles comme l'expérience, les connaissances et l'information forment des outils créant la richesse et caractérise le capital intellectuel comme la nouvelle richesse des organisations. (Escaffre, Bouabdellah, & Damak Ayadi, 2018) En 2010, Hassid estime que les actifs immatériels sont devenus les principaux actifs des organisations et constituent « une large partie de la valeur de l'entreprise ». Du fait de la place du patrimoine informationnel dans les organisations, les entreprises sont plus vulnérables aux attaques liées à l'information.

[1] Editeur suisse de logiciels

En se rapportant aux définitions précédentes, le patrimoine informationnel regroupe l'ensemble des actifs immatériels d'une organisation et forme un des éléments du patrimoine immatériel des entreprises. (Bensoussan, 2010)
Ainsi, le terme de patrimoine informationel regroupe sous un même concept les notions de données et d'informations que nous allons aborder dans la partie suivante.

3. Données, informations, connaissances

Selon le Larousse, une donnée peut être définie comme « ce qui est connu ou admis comme tel, sur lequel on peut fonder un raisonnement, qui sert de point de départ pour une recherche » ou « un renseignement qui sert de point d'appui ». En prenant l'étymologie du terme « donnée », nous apprenons qu'il est issu du latin *datum* révélant « ce qui est donné ». L'Académie Française, sous l'angle du domaine informatique, établit la donnée comme étant la « représentation d'une information sous une forme conventionnelle adaptée à son exploitation ». (Académie française, 2019)

En complément de cette définiton, nous pouvons citer celle proposée dans le livre blanc « Approches contemporaines en hébergement et gestion des données », (Cérin, 2017) dans lequel une donnée est spécifiée tel « un ensemble de valeurs faisant référence à la représentation et au codage d'une information ou un savoir sous une forme adaptée à un usage ». En tant que consultant en technologie de l'information et chroniqueur chez Information Today, Donald Hawkins caractérise les données comme « des faits et des statistiques qui peuvent être quantifiées, mesurées, comptées, et stockées ». (Guédri, Gomery , & Vuichard , Qualité des données, 2011)

L'information est une donnée qui s'accompagne d'une interprétation et d'une mise en contexte. Elle est immatérielle et s'inscrit dans une relation hiérarchique ou contractuelle au sein d'une organisation. (Chabin, Des documents d'archives aux traces numériques, 2018) L'information fournit des représentations sur un fait et apporte un message sensoriel transmis au cerveau. Elle possède une place centrale dans les organisations et la société en étant au cœur des décisions et des interactions. Elle peut concerner les clients, les salariés, les contrats, les innovations, les procédures techniques ou les documents de travail. (Asseman, Etude exploratoire des facteurs de risques du détournement en interne du patrimoine informationnel, 2011)

Dans les organisations, l'information se traduit par la connaissance d'un fait, d'une chose et par la capacité à réutiliser cette information dans un autre contexte. De ce fait, une donnée n'est pas une information puisqu'elle requiert une explication pour devenir une information. L'Académie Française détermine une information comme la combinaison de données et de connaissances associées à un même thème. De manière plus détaillée, l'Académie Française définie une information comme un ensemble de données

collectées dans un contexte précis et nécessaire pour une prise de décision. L'information dépend des données auxquelles s'ajoute un contexte et une analyse. (Académie française, 2019)

Une connaissance est le fait de comprendre et de connaitre les propriétés, les caractéristiques et traits spécifiques de quelque chose. Il s'agit ainsi d'informations permettant d'aboutir à une action. Les connaissances sont le savoir relatif des différentes composantes d'une organisation et de son environnement. Le patrimoine informationnel d'une entreprise repose sur cette connaissance qui est une source de valeur et représente une ressource vitale pour l'entreprise.

Comprendre le patrimoine informationnel d'une organisation, c'est gérer le cercle vertueux de la connaissance qu'elle possède en l'identifiant, la préservant, la valorisant, la partageant et enfin la maintenir à jour au fil du temps.

Les données, éléments brut et sans contexte, sont multiples et dépendent de « ce qui est donné » et réalisé. Elles sont le résultat d'une construction en cela qu'elles sont ce que l'on collecte, traite, modifie, conserve, échange, analyse et finalement archive. De cette façon, la donnée « brute » et « naturelle » n'existe pas. Une donnée existe pour être étudiée et discutée mais existera toujours en tant que donnée. L'historien Daniel Rosenberg explique en ce sens qu'une « donnée reste une donnée lorsqu'elle est contredite » (Rosenberg, 2013)

Ainsi, les données peuvent être de différentes natures, structurées, semi-structurées ou non-structurées. Une donnée peut également être définie en tant que données de références ou données opérationnelles.

4. Typologie d'une donnée

a) Données structurées, non-structurées ou semi-structurées

Il s'agit de la principale manière de répertorier les données dans notre nociété qui est une société de l'information, au sein de nos entreprises et leurs directions des systèmes d'information mais également, pour les responsables métiers. Notons que cette différenciation peut également être connu sous les termes d'informations structurées et d'informations non structurées. (Chabin, Données structurées et données non structurées, 2018)

Les données structurées sont des informations sous forme de valeurs numériques ou de chaines alphanumériques, comme par exemple, des mots, des signes ou des chiffres. Elles sont « contrôlées par des référentiels et présentées dans des champs d'une base de données qui permettent leur interprétation et leur traitement par des machines. » (Chabin, Données structurées et données non structurées, 2018) Autrement dit, elles

sont stockées dans des bases de données et renseignées dans un modèle de données clairement défini. (Régnier-Pécastaing, Gabassi, & Finet, 2008)

Bill Inmon caractérise les données non structurées comme « tout document, fichier, image, rapport, formulaire qui n'a pas de structure standard définie qui permettrait de le stocker facilement dans un dispositif de traitement automatisé ». (Guédri, Gomery, & Vuichard, Qualité des données, 2011) Les données non structurées sont, par exemple, issues des e-mails ou des feuilles de calcul qui sont en nombre croissant et important dans nos organisations. Leur volume est très important en entreprise et parfois difficilement mesurable.

Les données semi-structurées sont des données qui ne témoignent pas d'un schéma déterminé. Leur structure pouvant être irrégulière ou incomplète implique qu'elles ne puissent être stockées dans des bases de données relationnelles. (Coulondre) En effet, il s'agit de données n'ayant pas été organisées au sein d'un référentiel spécialisé, comme c'est par exemple le cas dans une base de données. Elles possèdent toutefois « des informations associées, des métadonnées par exemple, qui les rendent plus faciles à traiter que des données brutes ». (Rouse, 2016)

Une part croissante des données valorisées relève des données non ou semi-structurées. Ces deux types de données sont facilement compréhensibles en entreprise et sont sous forme de flux représentant les données produites lors de l'utilisation des réseaux sociaux ou d'une recherche Internet. Paul Zikopoulos, vice-président d'IBM, estime que ces données vont augmenter quinze fois plus rapidement que les données structurées. (Chignard & Benyayer, 2015)

b) Données opérationnelles et données référentielles

Nous pouvons distinguer des données dites opérationnelles et des données dites référentielles.

Les données opérationnelles, ou données de flux, sont liées à l'activité journalière d'une organisation. Etant utilisées quotidiennement, elles évoluent rapidement, sont volatiles et peuvent être en lien avec des événements ponctuels. Ces données créent de l'information utile à l'entreprise. (Trouchaud, Guédri, & Gomery)

Les données de référence, ou *master data*, sont des données dites stables, riches sur le plan sémantique. Elles ne changent pas ou peu dans le temps. (Trouchaud, Guédri, & Gomery) Pour Michel Herbert, les données de référence sont utilisées pour « classifier ou qualifier les autres données ». Elles peuvent être définies en interne, comme par exemple la catégorisation du crédit des clients, ou être issues de l'externe, pouvant être la liste des devises. (Hébert, 2016) Les données de référence sont nécessaires au bon

fonctionnement des processus des organisations. De multiples acteurs, internes ou externes à l'organisation, produisent, utilisent et partagent ces données. Elles sont spécifiées par leur sens, leur valeur, leur distribution et la réutilisation qui peut être réalisée par des acteurs de l'organisation ou des logiciels du système d'exploitation. En effet, la valeur de ces données est un critère essentiel de leur utilisation. Cette valeur a des conséquences sur l'efficacité des processus, et plus largement sur la gouvernance et le pilotage de l'organisation. Leur durée de vie est supérieure à celle des processus qui les exploitent. La simplicité d'accès de ces données conditionne l'efficacité globale des solutions utilisées pour exploiter ces données. (Direction interministérielle des systèmes d'information et de communication, 2013)

L'identification des données de références conditionne la performance des échanges et de leur usage. Elles peuvent prendre une forme semi-structurées ou structurées. Toutefois, elles peuvent posséder des informations incomplètes ou fausses, ou des doublons ce qui peut amener à une mauvaise gestion ou à une mauvaise prise de décision.

Parmi ces données de références, il est possible de distinguer trois types de données (Poussineau, 2013) :
- les données « maitres », au cœur du système d'information et des différentes applications ; (Direction interministérielle des systèmes d'information et de communication, 2013)
- les données « constitutives » composées d'attributs et qui caractérisent les données « maitres » ; (Régnier-Pécastaing, Gabassi, & Finet, 2008)
- les données « paramètres » se rapportant à des tables de valeurs ou catalogues de données comme par exemple les codes postaux. (Régnier-Pécastaing, Gabassi, & Finet, 2008)

L'ensemble de ces données de référence représentent les données les plus partagées au sein du système d'information d'une organisation. La différence faite entre ces trois types de données de référence s'inscrit dans le périmètre d'action des acteurs les utilisant ainsi que dans le périmètre d'analyse.

c) Métadonnées

Les différentes approches des données que nous avons observées nous amène à étudier la notion de métadonnée, « fréquemment définie comme étant une "donnée sur la donnée" ». (Zeenea, 2019)

Les métadonnées sont des « données au sujet des données et de leur contexte ». (Régnier-Pécastaing, Gabassi, & Finet, 2008) Autrement dit, il s'agit d'informations dites descriptives sur les données. Par exemple, lors de l'achat d'un produit, l'étiquette

apporte des informations sur ce produit tel que sa composition, sa provenance, la date de péremption s'il s'agit de nourriture, ou le mode d'emploi. De manière équivalente, les métadonnées sont une donnée caractérisant une donnée. Elles apportent des informations utiles pour le suivi, le traitement, l'historisation ou le stockage d'une donnée.

Les métadonnées sont utiles pour documenter les données dans une entreprise. Elles regroupent entre autres les dictionnaires et modèles de données. (Hébert, 2016) En effet, elles sont couramment déterminées par des registres que le système d'information utilise pour percevoir des données utilisées par différents logiciels. La réunion des données avec leurs métadonnées permet à un acteur de pouvoir utiliser ces données. (Cérin, 2017) Ainsi, les métadonnées visent à la description des données utilisées lors d'analyses et de prises de décisions. En cela, elles font références à l'exactitude des données dans leur sémantique, l'origine et la source des données, mais également à la méthode de calculs ou d'agrégation, aux règles métiers s'y référant. Enfin, elles font références au processus d'extraction et de transformation qui a été mis en place. Les métadonnées permettent ainsi d'acquérir un vocabulaire pour l'ensemble de l'organisation. (Régnier-Pécastaing, Gabassi, & Finet, 2008)

On différencie les métadonnées « métiers » des métadonnées « techniques ». (IBM, 2019)
Les métadonnées métiers exposent l'organisation et les correspondances entre les objets métier observés par un usager et les objets techniques correspondants. (IBM, 2019) Elles visent la compréhension de la nature et l'origine des données au niveau des rapports et des analyses pour les utilisateurs. De plus, elles permettent la compréhension des référentiels de données pour les développeurs dans le but de définir et parfaire la construction des rapports précédemment cités. (Régnier-Pécastaing, Gabassi, & Finet, 2008)
Les métadonnées techniques décrivent une construction permettant de documenter et maîtriser (en termes d'analyse d'impact, de sauvegarde) les structures utilisées dans les processus de chargement et de traitement des données (longueur d'un champ, définition d'un mapping...). (Direction interministérielle des systèmes d'information et de communication, 2013) Ces métadonnées techniques sont utiles lors de la spécification, la maitrise et le maintien des référentiels liés à la business intelligence. Elles servent également à diriger des outils dans un grand nombre de cas. En cas d'analyse d'impact, ces métadonnées sont également utilisées lors de changement ou d'évolution des systèmes BI. Enfin, les métadonnées techniques servent au traçage des données calculées et à la compréhension des données des systèmes sources. (Régnier-Pécastaing, Gabassi, & Finet, 2008)

Par nature, les métadonnées fournissent des informations sur le contenu des données, leur structure et leur environnement. Nous pouvons distinguer les métadonnées

descriptives qui s'appliquent au contenu des données structurelles, qui s'appliquent à la structure interne d'une donnée, et administratives, qui s'intéressent à la gestion des données. (Régnier-Pécastaing, Gabassi, & Finet, 2008) Ainsi, nous pouvons suivre les métadonnées selon trois niveaux de compréhension. Le dictionnaire présentant la définition ou la description de la donnée permet d'avoir un niveau de compréhension lié à l'aspect descriptif. Le second niveau de compréhension regroupe les informations utilisées pour la mise en œuvre d'une gouvernance des données ainsi que pour la nomination d'un responsable des données. Enfin, le dernier niveau détermine le degré de confidentialité des données et le niveau de protection des données.

L'administration de ces métadonnées est l'activité principale dans l'activité de gestion des données car elle participe à la valorisation des données et en facilite leur usage. De plus, les métadonnées constituent un vecteur de valorisation des données. (Régnier-Pécastaing, Gabassi, & Finet, 2008) Leurs apports se situent au niveau de la gouvernance par la garantie d'une définition spécifique des données ou des principes associés en vue de l'alignement métier. Ces apports se situent également par la connaissance de l'environnement des données pour permettre l'analyse d'impact lors de changement d'une règle. Ils se situent également dans l'administration de preuve en matière de sécurité ou de conformité. En effet, afin de répondre aux contraintes d'une mise en conformité, la gestion de « l'instance de donnée » et la maitrise de sa cohérence tout au long du cycle de vie des données utilise les métadonnées. Enfin, les apports des métadonnées se retrouvent lors de la gestion du patrimoine infomationnel en matière de sécurité et de la qualité. Cela dans une double dimension de protection en permettant l'alignement entre le cadre sécuritaire et la sensibilité des données et de valorisation qui prend en compte des indicateurs visant le pilotage des dimensions de valorisation des informations. (Régnier-Pécastaing, Gabassi, & Finet, 2008)

d) Données à caractère personnel

Une donnée est considérée comme étant à caractère personnel dès lors qu'elle permet d'identifier directement ou indirectement une personne. Cette dernière peut être identifiée selon différents élements : son nom, son prénom, mais également son adresse email ou son numéro de téléphone, une donnée démographique telle que la fonction professionnelle, le sexe, l'âge ou encore géographique par l'adresse personnelle ou le lieu de travail.

Les informations purement numériques d'un internaute, telle que l'adresse IP, ou encore les données comportementales, telles que les visites sur un site web par exemple, sont aussi considérées comme données à caractère personnel. Les données partagées par une personne comme la mise en ligne d'une photo ou un like, sont également à considérer dans cette catégorie. (Biriotti, 2018)

L'identification d'une personne physique peut se faire en utilisant une unique donnée mais aussi un croisement de plusieurs données. (CNIL, 2019)
Ainsi, dès 2001, Latanya Sweeney, doctorante au sein du MIT, démontre que protéger la confidentialité de données à caractère personnel n'est pas une démarche aisée. Dans son étude réalisée en mai 2002, Latanya Sweeney explique de manière très explicite que certaines catégories de données personnelles telles que la date de naissance et le sexe se retrouvent à la fois dans une liste électorale et dans une base de données médicales. (Sweeney, 2002) En croisant une liste électorale et une base de données médicales pseudonymisée, c'est-à-dire nettoyée de l'ensemble des éléments identifiants mais contenant des codes postaux, et dates de naissance, elle retrouve 90% des individus et parvient à prendre connaissance des données médicales du Gouverneur de l'Etat du Massachussetts de l'époque, William Weld. (Montjoye, 2016) La maitrise du patrimoine informationnel comportant des données à caractère personnel aurait pu permettre d'identifier les documents à protéger afin que ce croisement ne soit pas possible.

Les informations médicales entrent dans une catégorie spécifique des données à caractère personnel. Il s'agit des données dites sensibles. Cette catégorie de données sensibles renvoit aux informations relevant des opinions politiques, des convictions religieuses ou philosophiques d'une personne mais aussi l'appartenance syndicale, l'orientation sexuelle, les données génétiques ou biométriques ayant pour finalité l'identification d'une personne physique. Le règlement européen de la protection des données, que l'on décrira dans la partie 51Cadre légal, interdit de récolter ou d'utiliser ce type de données excepté dans des cas spécificiques. (CNIL)

B. Valeur d'une donnée

Le système d'information d'une organisation, en tant que résultat d'une construction menée à la fois par et pour ses utilisateurs afin d'atteindre un objectif spécifique, permet la production de la valeur en fournissant l'information à des acteurs spécifiques. Ainsi, la donnée est une ressource, un actif d'une organisation de manière équivalente à un bien matériel. De ce fait, elle peut être valorisée et posséder un cycle de vie. (Régnier-Pécastaing, Gabassi, & Finet, 2008)

Le principe de valeur d'une donnée est large et se pose afin de connaître en quoi la donnée prend part aux directions stratégiques d'une organisation. Le schéma de création de valeur à partir d'une donnée brute peut être résumé par la Figure 2.

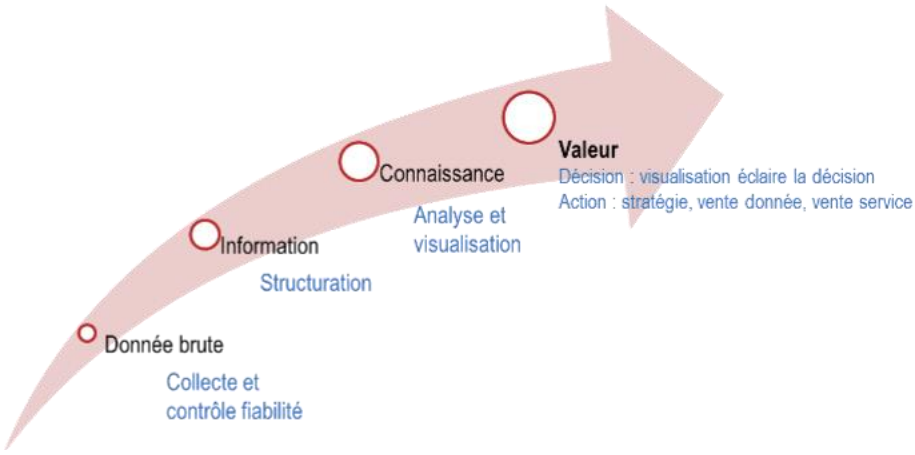

Figure 2 – Transformation de la donnée en valeur (Magniez, 2016)

Le point de départ de la valeur est la collecte de données brutes qui sont transformées en informations à la suite du traitement accompli et de la structuration. Par la suite, grâce aux analyses et à la visualisation des informations, celles-ci deviennent connaissances avant de permettre la production de valeur pour l'organisation au travers des décisions prises.

On peut désigner la valeur d'une donnée comme étant « la différence entre les bénéfices obtenus et les coûts engendrés (de stockage, d'administration, de maintenance). » (Régnier-Pécastaing, Gabassi, & Finet, 2008)
Selon Simon Chignard et Louis-David Benyayer, la donnée peut prendre trois types de valeur. (Chignard & Benyayer, 2015) Elle peut posséder une valeur marchande lorsqu'elle est perçue, avec un aspect marketing ou comme matière première. Pour le domaine de la distribution, elle peut prendre une valeur de levier de performance lorsqu'elle est collectée afin de réduire leur coût de fonctionnement. Enfin, la donnée peut prendre une valeur d'actif stratégique lorsqu'elle permet à son organisation de prendre une position stratégique ou supporter la décision.

Afin de fixer la valeur d'une donnée, il est important de définir et maitriser son cycle de vie et ses prérequis. Comme il sera décrit par la suite, la donnée obéit à une suite complexe de traitement durant laquelle elle est d'abord collectée, contrôlée, protégée, partagée puis analysée afin de faciliter la prise d'une meilleure décision ou pour encourager l'innovation. Seule une donnée qui est stockée, utilisée et transformée peut prendre une valeur. De ce fait, une donnée dite « brute », qui n'a ainsi pas reçu de traitement, ne peut prendre de valeur. La valeur d'une donnée demeure dans l'information qu'elle communique. Ainsi, une donnée a pour première valeur ce qu'elle vaut à produire et à acquérir. Elles obtiennent de la valeur selon les moyens mis en place tout au long de leur cycle de vie.
La valeur d'une donnée s'acquière dans son utilisation ou autrement dit, dans ce que l'on peut en faire. L'usage d'une donnée est ainsi considérable puisqu'il s'agit de l'origine

principal de l'économie de la donnée. Elle prend divers rôles et permet d'exécuter des actions pouvant être efficaces et efficientes et de supporter les décisions pour une organisation. Par exemple, dans la fonction RH, elle est le premier élément utilisé. D'abord stockée, elle est utilisée pour réaliser les reports mensuels produits par l'équipe reporting ou lors de l'étude d'un profil lors d'un recrutement.

Une donnée prend également sa valeur dans l'assemblage des données accessibles et utilisées relatives à un collaborateur, ce qui donne des informations sur son comportement. C'est d'ailleurs ce que le sociologue Bruno Marzloff indique lorsqu'il dit que « la valeur d'une donnée est proportionnelle au carré du nombre de données auxquelles elle est associée ». (Chignard & Benyayer, 2015) Autrement dit, la valeur d'une donnée est formée à partir d'autres données. Disponible de manière toujours plus croissante, elle est complexe à protéger et facilement reproductible comme on a pu le montrer précédemment avec l'étude de Latanya Sweeney dans la partie Données à caractère personnel. Une donnée utilisée ne peut disparaitre, au contraire, elle peut être utilisée plusieurs fois ce qui lui attribue comme valeur son potentiel de réutilisation. Cette valeur d'utilité diffère selon les acteurs qui les utilisent et les usages effectués. Une même donnée peut donc connaitre des usages distincts entre les différents services d'une organisation et posséder une valeur propre à l'usage. Ces différents usages entraînent la collaboration entre les acteurs afin d'obtenir un partage de la valeur et une connaissance plus précise du patrimoine informationnel dans sa globalité et en particulier dans son usage.

La troisième source de valeur d'une donnée est en lien avec son immédiateté soit le fait qu'elle est directement observable. En effet, elle peut saisir sa valeur en temps réel par l'utilisation par l'utilisateur. On peut observer que les données étudiées hier ont une valeur différente que celles qui le seront aujourd'hui ou bien demain. Cette observation est faite car chaque traitement d'une donnée permet d'acquérir plus d'informations et donc plus de valeur à celle-ci. Chaque utilisation enrichit notre connaissance de la donnée. Il ne faut toutefois pas négliger les données « d'hier » puisque celles-ci apportent de précieuses informations qui sont nécessaires lorsqu'elles sont associées à celles d'aujourd'hui pour les prises de décisions. L'immédiateté d'une donnée fait référence à sa valeur d'option, soit au fait qu'elle est amenée à être maniée dans un avenir proche. En effet, alors que les données se créent massivement et qu'on fait face à une explosion des données, celles-ci ne sont pas toutes immédiatement utilisées et nécessitent que des nouveaux usages surgissent. Dans l'attente de ces nouveaux usages, la valeur d'option augmente.
Finalement, la dernière source de valeur d'une donnée est sa rareté, ou a contrario son abondance. Les données sont aujourd'hui en croissance continue du fait de leur création par et pour tout le monde. Cette création continue amène à une abondance des données. Elles forment une représentation du monde qui nous entoure, qu'il s'agisse du monde de l'entreprise ou dans la vie quotidienne.

C. Traitement des données

1. Cycle de vie des données

Le système d'information possède quatre fonctions primaires : l'acquisition, le stockage, le traitement et la diffusion. Le stockage est lié à la conservation de l'information et sa protection que ce soit lorsqu'elle se situe dans les disques durs internes d'une organisation ou dans des entrepôts de données. Le traitement d'une donnée reflète la transformation et l'enrichissement de celle-ci en une information nouvelle. La diffusion est nécessaire lors de la mise à disposition de l'informaiton auprès des utilisateurs et dans le respect de leurs besoins.

Chacune de ces quatre fonctions apparait dans le cycle de vie des données. La gestion du cycle de vie des données, ou *Data Cyclelife Management*, est définie comme la réunion de processus ou actions de traitement nécessaires pour gouverner les données de l'entreprise et ce de leur collecte jusqu'à leur retrait par l'archivage ou la suppression. La gestion du cycle de vie des informations, ou *Information Lifecycle Management* (ILM), est le processus de « gestion des données et des métadonnées qui les décrivent depuis la conception de l'information jusqu'à sa destruction ». (rever data engineeers, 2019)

Comme évoqué précédemment, dans son état brut, la donnée ne possède pas ou très peu de valeur. Pour en acquérir, elle a besoin d'être validée, transformée, puis analysée afin de s'élever en tant que données, informations ou connaissances. Ce traitement permet de procurer de la valeur à l'organisation.

Une approche globale des données par les entreprises doit être prise en considération afin de permettre de garantir leur qualité, leur protection et leur accessibilité au plus grand nombre.

Le CIGREF (Cigref, 2014) décrit le cycle de vie des données selon les étapes décrites dans le schéma de la figure suivante :

Figure 3 - Schéma du cycle de vie des données (Cigref, 2014)

Pour exister, chaque donnée doit d'abord être créée et collectée comme défini par l'étape d'acquisition des données. La création d'une donnée exige préalablement la mise en œuvre de mécanismes techniques, l'utilisation de bases de données afin de permettre leur stockage et mise à disposition. La création d'une donnée étant issue de sa collecte, le travail nécessaire est réduit lors de cette première étape. Le coût de création d'une donnée est presque nul. Elle est de plus en plus réalisée de manière inconsciente et peu explicite pour les acteurs. Citons l'exemple des captchas qui sont les tests produits en informatique pour soutenir qu'une réponse est donnée par un homme et non de manière automatique par un robot. Lorsqu'un internaute demande un nouveau captcha, celui-ci est généré automatiquement de manière aléatoire et ne nécessite pas d'effort lors de sa création.

La seconde étape du cycle de vie est définit par le transport des données c'est-à-dire leur transfert d'un lieu de création à un endroit de stockage ou de conservation (deuxième étape de la Figure 3). Les données sont par la suite traitées et transportées afin de permettre leur utilisation ou leur visualisation. Afin d'être déplacées, les données s'appuient sur des infrastructures de télécommunications tel que des réseaux.

Par la suite, les données sont stockées et protégées pour être conservées dans des serveurs. Leur préparation et leur qualification représente l'étape suivante du cycle de vie, soit l'étape de transformation. Il s'agit d'une étape importante afin de nettoyer les données. Cette étape de transfomation permet notamment de localiser les données manquantes ou incomplètes et ainsi la correction d'erreurs. L'intégration des données est un processus qui peut être considéré comme faisant partie de cette étape de transformation de la donnée. En effet, ce processus combine des données issues de sources diverses en vue de l'unification des données. (Pearlman, 2020)

L'analyse des données lors de l'étape 4 constitue la production de résultat qui conduit à une prise de connaissance ou une prise de décision. L'analyse des données mobilise des compétences statistiques et analytiques nécessaires à la maitrise du patrimoine informationnel. Le fait de visualiser des données apporte une signification à des volumes de données parfois hétérogènes et permet de valoriser le patrimoine informationnel.

Pour finir, le cycle de vie aboutit sur l'archivage ou la destruction des données qui doivent être encadrées par des moyens techniques reflets de la réglementation ou la politique interne.

Notons que toute opération de traitement faite lors du cycle de vie des données peut constituer un danger pour l'entreprise du fait de l'existence des risques multiples comme la perte de données, le non-respect des règlementations en vigueur, ou une confusion des données.

2. Méthodes de traitements et exploitation des données par l'entreprise

D'après la CNIL ou Commission Nationale de l'Informatique et des Libertés, le traitement des données réside dans l'ensemble des actions réalisées sur les données lors du cycle de vie (collecte, stockage, changement, consultation, utilisation, suppression ou destruction). (Cnil)

En France, dans les organisations, il existe des méthodes de traitements définis. Par exemple, lors d'un recrutement, seules les données nécessaires dans le cadre de l'activité des acteurs traitants les données sont collectées. Ainsi, certaines données considérées comme sensibles tel que les opinions politique ne sont pas recueillies.

Le traitement des données par une entreprise est faite au cours de multiples activités : la sélection des collaborateurs lors du recrutement, la gestion administrative des collaborateurs, la gestion de la rémunération, des badges, des frais, celle de l'organisation du travail ou encore celle des carrières et de la mobilité.

D. Rôles et Enjeux pour l'organisation

Les systèmes d'information sont des supports de gestion et d'aide à la décision qui permettent le pilotage des processus, l'analyse des performances, l'anticipation des évolutions et la prise de décisions. Dans cet objectif, les informations se doivent d'être particulièrement actualisées et fiables. L'ensemble des technologies de l'information et de la communication, mieux connu sous le sigle TIC, est devenu particulièrement important pour les organisations du fait de l'économie mondiale. Celle-ci est une économie de l'information soit une économie dans laquelle la connaissance et la maitrise acquise des différentes informations stratégiques permettent d'acquérir et de maintenir le statut de leader. La maitrise du patrimoine informationnel requiert des ressources importantes pour l'organisation (Allal-Chérif & Dupouet, 2014)

Lors de la partie sur la Valeur d'une donnée, nous avons pu observer différentes facettes se révéler. Lors des premières phases de leur cycle de vie (collecte et traitement), la donnée forme une matière première pour l'entreprise qui après valorisation peut appuyer la décision. Lorsqu'elle devienne information et en étant convenablement partagée au sein des différents acteurs d'une entreprise, la donnée devient une connaissance et forme une source de savoir pour l'entreprise. Lorsque cette transmission est faite, on parle de gestion et de partage de connaissance. Ce partage est nécessaire afin de permettre la maitrise du patrimoine informationnel. Cette maitrise ne se limite pas au partage mais nécessite d'autres actions de la part de l'organisation.
Considérées comme actif numérique de l'entreprise, les données possèdent une capacité de création de valeur autorisant l'entreprise à se développer. En effet, ayant un rôle stratégique, elles forment un levier pour l'entreprise qui peut ainsi se positionner au niveau stratégique. En ce sens, elles ont le potentiel de créer de nouveaux services et

usages et servent l'attribution de ressources ou le développement de résultats. Les données ont ainsi un rôle décisif sur le pilotage des activités puisqu'elles permettens d'établir des décisions à partir des informations sur les systèmes d'information décisionnels. Au travers de leurs impacts sur les décisions prises dans les organisations, les données ont un rôle primordial dans la transformation d'une entreprise.

Chaque entreprise dispose ainsi d'un véritable enjeu dans la connaissance et la maitrise de la chaine de valeur des données autour desquelles se trouvent des obligations de protection et de sécurité. Les entreprises s'appuient sur le contexte attribué aux données afin de prendre des décisions, choix et orientations nécessaires à son évolution.

II. Développement d'un cadre légal pour le patrimoine informationnel

A. Définition de la gouvernance

En tant qu'unité de coordination, une organisation exige une même compréhension des informations pour l'ensemble des parties prenantes sans pour autant que celles-ci possèdent le même niveau de précision, sur la réalité de l'entreprise. Cette unité d'organisation doit posséder les outils nécessaires afin de connaitre les informations issues de son environnement. Cette connaissance des informations permettra à l'organisation et ses acteurs de respecter les différentes étapes du cycle de vie des données et ce aux moments nécessaires, auprès des acteurs impliqués, cela dans l'objectif final de construire une compréhension commune entre ses membres et l'aider à considérer l'avenir. (Nurcan & Rolland, 2006) Historiquement, les systèmes d'information ont été construits autour des domaines fonctionnels et des processus qui y sont associés. Les processus métiers et leurs données de références se placent au centre des systèmes d'information des organisations. Toutefois, cette logique de placer les processus au centre a eu pour effet de minimiser le rôle des données comme composant structurant des processus précités. (Régnier-Pécastaing, Gabassi, & Finet, 2008)

Présente depuis les années 90, l'idée de gouvernance requiert en amont l'implication et la prise de responsabilité des différents acteurs dans les aspects décisionnels, en particulier les prises de décisions.
La gouvernance des systèmes d'information a pour but d'aligner les dimensions technologiques, organisationnelles et managériales les unes avec les autres. Cet alignement permet d'acquérir une cohérence entre l'ensemble des ressources d'une organisation. De plus, il est essentiel que cette stratégie globale d'organisation soit cohérente avec la stratégie des systèmes d'information. (Allal-Chérif & Dupouet, 2014) Il s'agit de l'alignement stratégique.

La gouvernance de l'information dans une organisation se dissocie en deux axes. Le premier, l'axe « utilisateurs », vise à l'amélioration continue de l'accès à l'information pour les parties prenantes. Le second est l'axe « responsabilité d'entreprise » qui implique la protection et la conservation des actifs informationnels de l'entreprise, mais aussi la destruction des éléments inutiles ou périmés. (Chabin, Des documents d'archives aux traces numériques, 2018)

Pour le *Data Governance Institute*, la gouvernance des données est un « système de responsabilités et de droits de décision pour les processus en lien avec des données, exécuté selon des modèles définis. Ces modèles déterminent qui peut réaliser telle ou telle action avec quelles informations, à quel moment, dans quel contexte et à l'aide de quelles méthodes ». (Open Data Soft, 2018) Cette première approche de la gouvernance des données est complétée par celle de l'entreprise américaine de conseil et de recherche, *Gartner,* qui présente la gouvernance des données comme « une collection de bonnes pratiques qui considèrent l'information comme une ressource à part entière de l'entreprise ». (Régnier-Pécastaing, Gabassi, & Finet, 2008) ou encore comme « la spécification des droits de décision et le cadre de responsabilité permettant d'assurer un comportement approprié en matière d'évaluation, de création, de consommation et de contrôle des données et des analyses. » (Gartner)
Le cabinet de conseil, *Baseline Consulting*, complète ces approches en définissant la gouvernance des données comme un « processus de supervision et de décision qui permet de hiérarchiser les différents investissements, d'allouer les ressources adéquates et un pilotage par les résultats, tout ceci pour s'assurer que les données utilisées au sein des projets sont valorisées et répondent aux enjeux et aux objectifs de l'entreprise ». (ETS, 2011)
Autrement dit, cette gouvernance a pour caractéristique l'ensemble des pratiques, règles et des processus visant à soutenir l'exploitation des données et consent à une administration suffisante et appropriée de celle-ci grâce aux outils et logiciels utilisés. Elle couvre l'ensemble des facteurs techniques, humains, opérationnels et organisationnels dont une organisation a besoin pour disposer de données de grande qualité avec un niveau de protection adéquat.

La mise en place d'une gouvernance des données permet de reconnaître les responsables de traitements des données ainsi que la mise en place de démarches à adopter autour de celles-ci. Ces démarches permettent de répondre aux critères de qualité, de protection et de sécurité. L'organisation doit s'assurer de leur respect dans leur mise en application. En cela, et afin de réaliser une gouvernance des données, il est nécessaire d'avoir une instance spécifique pour avoir une politique globale liée au patrimoine informationnel et spécifique en matière de données personnelles. L'enjeu d'une gouvernance des données est l'identification des traitements effectués pour l'ensemble des métiers. (Delayat & Bouteiller, 2014)

Une gouvernance des données se veut anticipative, participative, recherchée, rétro-corrective, intelligible, exacte et valable : anticipative afin de prévenir tout risque et toute menace liée au patrimoine informationnel, participative puisqu'elle nécessite l'implication d'un large panel de parties prenantes.

L'un des objectifs de la gouvernance des données est l'exploration des données et la facilitation de l'innovation avec des initiatives de transformation digitale. Selon ETS, les objectifs d'une telle gouvernance se trouvent dans la qualité des données, les obligations réglementaires et la mise en place de projets spécifiques liés aux données. En effet, les initiatives d'une telle gouvernance sont déterminées par le besoin de se conformer aux règlementations en vigueur notamment le RGPD pour les organisations françaises et européennes, ou les normes internationales telles que les normes ISO dont la norme ISO / CEI 38500 liée à la gouvernance des technologies ou la norme ISO 9241-11 relative à l'ergonomie de l'interaction entre l'homme et le système. Nous reviendrons plus en détails sur ces règlements et normes dans la partie sur le Cadre légal.

Le fait de mettre en place une démarche de gouvernance des données dans une organisation révèle de nombreux défis pour celle-ci. En effet, l'organisation doit faire face à l'engagement des acteurs et doit prendre en considération les processus existants, même en cas de situation d'urgence d'un projet. L'organisation se doit de surmonter l'idée selon laquelle cette gouvernance des données alourdit les processus. La gouvernance des données permet, au contraire, à l'organisation de mieux connaitre ses processus et les données qui sont utilisées ainsi que le rôle de chaque acteur.
Ainsi, afin d'initier une telle démarche, le périmètre d'action des parties prenantes est souvent aggrandit et dépassé par les difficultées rencontrées. La nécessité d'avoir une gouvernance résulte donc de l'engagement des parties prenantes au niveau opérationnel mais également au niveau décisionnel et stratégique. Pour agir et avoir un impact, une gouvernance nécessite d'avoir un point de départ servant de motivation aux acteurs. La mutualisation des ressources et des connaissances pourrait être un exemple de motivation. (Campagne Infolab de la FING, 2017)
La protection des données dans le système d'information s'effectue au moyen d'accès sécurisé pour et par les acteurs afin qu'ils puissent les traiter en toute sécurité. Cette sécurité des données et la gestion des droits d'accès aux données permettent d'assurer la disponibilité des données. Celle-ci permet aux personnes concernées de pouvoir accéder à des données dans le strict cadre de leur activité et de leur fonction afin d'intervenir dessus.

L'intégrité des données est un aspect à mettre en relation avec la disponibilité. Pour être gouvernées, les responsables de traitement doivent savoir quand les données doivent être supprimées ou conservées. Elles se doivent d'être cohérentes, fiable et à jour. Enfin, pour assurer cette gouvernance, il faut mettre en place une politique permettant de sécuriser les données de l'entreprise. La CNIL préconise la mise en place de la

sécurisation des données lors du contrôle des accès, des déclarations de traitements liées à l'activité et la gestion des violations de données. La gouvernance des données est une « notion cruciale pour la cyber sécurité, le respect de la vie privée, de l'intégrité de l'activité, la qualité des services ou encore l'image d'une entreprise. (R, 2018)
La gouvernance des données est aujourd'hui présente dans toutes les entreprises bien qu'elle soit parfois réalisée inconsciament. Le fait de donner des droits ou des accès aux données à des collaborateurs en fonction de leur poste relève de la gouvernance des données.

La notion de MDM ou *Master Data Management* est une discipline des technologies de l'information qui traite de la gestion des données de référence. Elle apporte la garantie de la cohérence entre diverses architectures de systèmes et fonctions métier. Le module *Master Data Management* (MDM) se révèle être un accélérateur pour constituer les référentiels des données. En effet, il vise la gestion de la qualité et du cycle de vie des référentiels au travers de la consolidation, le suivi et l'auditabilité. Ce module utilise des fonctionnalités telles que la modélisation, la gestion de la qualité des données avec la définition de règles de gestion de la qualité, la gestion du cycle de vie, l'accès et la diffusion des référentiels. (Bentounsi M. , Cante, Coya, Darmon, de Chambourcy, & Gnokam, 2019)

La mise en place d'un cadre de gouvernance de données aide chaque organisation à l'identification de ses enjeux et besoins. Au niveau métier d'abord, la gouvernance des données vise à la valorisation des données tout en maintenant ces données à jour et fiables. Un tel cadre de gouvernance vise également la réduction des temps liés au cycle métier liés aux données de référence afin d'améliorer les processus grâce à ces données de références.

Ainsi, gouverner et piloter le patrimoine informationnel d'une organisation vise à améliorer les gains comme il serait possible de le faire en améliorant les processus. Une gouvernance des données de référence est essentielle pour assurer la gestion des données sur l'ensemble des applications et logiciels utilisé par les organisations.

B. Les acteurs majeurs

1. Acteurs internes à l'organisation

a) Direction des ressources humaines et direction juridique

La Direction des ressources humaines (DRH) occupe un rôle essentiel dans une organisation afin de maintenir « la coordination entre la stratégie générale formalisée par la direction générale de l'entreprise et les compétences des forces en présence de la structure ». (Reactive-Executive, 2020) Du fait de la diversité de ses activités et missions tel que la gestion de la paie, le recrutement, la formation professionnelle, la direction des affaires sociales, la Direction des ressources humaines a une responsabilité forte pour la réussite de l'organisation. Ces missions représentent un levier de dévelopemment pour l'organisation, en particulier car l'humain occupe un enjeu stratégique. (Reactive-Executive, 2020)
Chargée de tenir à jour un registre du personnel, elle occupe une place importante de l'utilisation des données qui sont elles-mêmes la ressource principale des missions des acteurs de la Direction des ressources humaines. La DRH est en effet un des consommateurs les plus importants de données au sein d'une organisation. Elle effectue divers traitements sur les données tout au long de leur cycle de vie et suivent la qualité des données. En ce sens, la Direction des ressources humaines participe grandement à leur gouvernance et s'associe à la mise en oeuvre de projets. Elle doit contribuer au respect de la conformité des traitements des données à caractère personnel en particulier en impliquant l'ensemble des responsables de traitement.

La direction juridique d'une entreprise dispose d'un rôle de conseil, de sensibilisation et d'accompagnement vis-à-vis des opérationnels ou métiers concernant l'ensemble des questions ayant un lien avec la règlementation sur la protection des données.
Cette direction est en charge de la rédaction de guides de bonnes pratiques relatives à la protection des données personnelles et notamment du code de conduite, s'il existe. Celui-ci est prévu à l'article 40 du RGPD et est destiné à participer au bon respect du règlement dans l'ensemble des secteurs de traitement et de leurs besoins spécifiques.
La direction juridique est notamment sollicitée pour la relecture des contrats et leur révision sur des points précis tels que l'existence de clauses dédiés à la protection des données personnelles et au transfert des données sensibles.

Le *compliance Officer* est le responsable opérationnel au quotidien du programme de conformité. Il a pour rôle de rapporter périodiquement au top management sur l'efficacité du programme de conformité. De plus, il travaille en collaboration avec les autorités.

Le *Data Protection Legal Expert* ou DPLE est le responsable de la partie légale du RGPD. Il travaille en collaboration avec le *Data Protection Officer*.

b) Direction des systèmes d'information

La direction des systèmes d'information est la direction en charge du système d'information d'une organisation. Elle s'occupe de « définir l'architecture du SI, concevoir, installer et déployer et exploiter le SI ». (mc2i, 2012) Elle fixe les évolutions des systèmes d'information selon des besoins opérationnels et la stratégie de l'organisation.

Elle est en charge de la supervision de la conception, de la mise en place et du maintien opérationnel des systèmes informatiques. Enfin, elle supervise et participe au pilotage des projets liés aux systèmes d'information. Elle analyse les besoins des utilisateurs, définit et contrôle l'application des procédures en matière de qualité et de sécurité des systèmes d'information. Elle s'occupe de la mise à jour des documentations techniques des systèmes d'information.

La direction des systèmes d'information a un rôle important en cela qu'elle porte l'activité de l'organisation et des politiques en matière de sécurité. Elle se trouve au cœur d'une politique de gouvernance des données.

c) Responsable de traitement

La CNIL décrit le responsable de traitement comme étant « la personne morale (entreprise, commune, etc.) ou physique qui détermine les finalités et les moyens d'un traitement, c'est-à-dire l'objectif et la façon de le réaliser. » (CNIL) Ainsi, le responsable de traitement est celui qui doit documenter ses traitements à travers des documents de conformité et des analyses d'impacts sur la vie privée et les risques. Le responsable de traitement peut aussi être appelé *Owner* d'un traitement. Son rôle est important dans la lutte pour la protection des données puisqu'il est chargé de la gestion générale de la mise en application du RGPD dans une entreprise. Il a plusieurs missions qui permettent de protéger efficacement les données et de fixer la stratégie dans laquelle entre l'organisation en matière de protection des données. Le responsable de traitement a de nombreuses obligations telles que l'obligation d'avoir un registre de traitement, d'appliquer les mesures techniques et organisationnelles en matière de protection des données, de coopérer avec les autorités en cas de contrôle, de respecter les droits des individus notamment en matière de droit d'accès et de droit à la modification de leurs données.

Si une entreprise s'associe à une ou plusieurs organisations, elle détermine conjointement « pourquoi » et « comment » les données à caractère personnel sont traitées. Dans ce cas, on parle alors de coresponsabilité puisqu'ils définissent ensemble les finalités et les moyens utilisés pour le traitement. Cette coresponsabilité implique une prise de décision commune qui se doit d'être en accord avec l'ensemble des personnes responsables. Afin d'écarter toute confusion, il est important que ces

responsables de traitement identifient de manière claire et explicite le rôle et les obligations de chacun.

Les responsables de traitement peuvent être accompagnés par des sous-traitants dans la définition des objectifs du traitement et sa réalisation. Les sous-traitants utilisent ainsi les données personnelles seulement pour le compte du responsable du traitement. Ils sont de manière générale extérieurs à l'organisation mais peuvent également être internes s'ils ne sont pas dans le même pays ou le même service. De ce fait, ils sont également encadrés par le Règlement Général sur la Protection des Données et doivent assurer un niveau de protection similaire avec une obligation d'alerte en cas d'incident de sécurité et d'assistance pour veiller à la protection des données à caractère personnel. Le responsable de traitement doit être le garant du respect des obligations du RGPD par les sous-traitants. (N.C., 2019) Les sous-traitants peuvent réaliser des missions diverses comme proposer des solutions informatiques. Toutefois, ils ne peuvent pas recruter ou nommer un autre sous-traitant pour réaliser une partie de leur mission sans avoir préalablement une autorisation écrite du responsable du traitement. (Commission européenne)

d) DPO, Délégué à la protection des données

Le Délégué à la Protection des Données (DPO), ou *Data Protection Officer,* est un acteur clé de la gouvernance des données, notamment des données à caractère personnel. Il remplit des missions d'information, d'accompagnement grâce à l'apport de conseils, de suivi et contrôle afin d'encourager, combiner les actions à mettre en place pour garantir la conformité de l'organisation. Il est ainsi l'interface entre l'organisation, les structures de contrôle comme la CNIL et les acteurs ou parties prenantes concernées.

Dans son rôle d'accompagnement, le DPO a pour mission de sensibiliser les parties prenantes aux différentes règlementations existantes concernant la protection des données à caractère personnel et d'une manière plus général du patrimoine informationnel. En cas de demande, il peut également fournir des instructions pouvant mener à une action précise comme, par exemple, lors de la réalisation de documents de conformité ou d'analyses d'impacts qui visent à vérifier et contrôler la conformité des outils. Dans cet objectif de pilotage de la conformité, il soutient et aide les parties prenantes à mettre en place et suivre les mesures techniques et organisationnelles visant au respect des règlementations en application, tel que le Règlement Général de la Protection des Données ou RGPD. Etant conseiller, il peut identifier les outils de paramétrages permettant d'assurer, dès leur conception, la protection des données (*privacy by design)* ou de participer à la mise en oeuvre de processus internes liées à la protection des données. Le DPO doit documenter l'ensemble des mesures prises en vue de respecter les obligations issues du RGPD (*accountability).*

Afin d'assurer le contrôle de la conformité, il participe à l'identification et au recensement des activités de traitement effectuées par l'organisation. Cela se traduit par la mise en place d'un registre de traitement. Pour chacune d'entres elles, il doit veiller au travers des documents de conformité rédigés par les o*wners* du traitement que seules les données nécessaires sont collectées. Ces dernières doivent aussi être traitées et utilisées conformément à des conditions confirmant l'intégrité et disponibilité des données. Enfin, elles doivent être détruites, archivées ou anonymisées dès lors qu'elles ne sont plus utilisées.

Enfin, le DPO intervient pour faciliter les relations entre l'organisation, les parties prenantes concernées et la CNIL. Il doit être en capacité de répondre aux demandes en cas de contrôle par la CNIL au sein de l'organisation. Il veille au traitement des demandes des droits tels que le droit d'accès, le droit d'opposition ou le droit de suppression pouvant être faits par les collaborateurs et s'assure que les réponses fournies soient transmises dans les délais accordés. Par exemple, le DPO dispose, avec l'aide des parties prenantes comme la DRH, d'un délai d'un mois pour répondre aux droits des personnes concernées.

Sa nomination au sein d'une organisation n'est pas obligatoire et est faite en fonction de sa taille. Une telle nomination est faite en ayant préalablement vérifié que le DPO est protégé de tous conflits d'intérêts pour s'assurer qu'il pourra agir de manière juste et objective. Enfin, le DPO doit avoir les moyens adéquats à l'exercice de ses fonctions tant au niveau financier que des équipements fonctionnels cela s'accompagnant d'une autonomie d'action.

e) CDO, Chef de la sécurité des données

Le *chief data officer* est le chef de la sécurité des données. Autrement dit, il est le « directeur des données de l'entreprise » (Data Analytics post, 2019) ou le représentant du patrimoine informationnel et de sa gouvernance.
Il crée le lien entre les métiers liés à l'informatique et les métiers opérationnels c'est-à-dire les clients, les partenaires ou fournisseurs. Son rôle est l'analyse et l'utilisation des données pour mettre en œuvre une stratégie pour répondre aux besoins de l'organisation. Ainsi, son rôle est lié à la vérification de la qualité et la cohérence des données afin de déterminer une stratégie appropriée aux données collectées. Il prend part à la mise en application d'une Politique Globale de Sécurité, ou PSSI, conforme aux obligations locales, conduit les réunions en matière de sécurité entre les différentes parties prenantes et assiste aux réunions globales de sécurité. Leader de la sécurité des données, il est en charge de l'implémentation des outils visant à faire progresser cette sécurité. Il est également en charge de contrôler la coopération des salariés dans les projets de sensibilisation en matière de sécurité. Enfin, il produit les reports nécessaires en cas d'incidents de sécurité, avant de les analyser et de gérer les crises.

2. Acteurs externes

a) CNIL

La Commission Nationale de l'Informatique et des Libertés ou CNIL est une autorité de contrôle créée pour veiller à la bonne application de la loi Informatique et Libertés du 6 janvier 1978. En tant qu'autorité administrative indépendante (AAI), la CNIL est une institution publique indépendante agissant au nom de l'Etat, sans pour autant être sous l'autorité du gouvernement ou d'un ministre. Elle est formée d'une Présidente, Marie-Laure Denis, et de « 18 membres élus ou nommés et s'appuie sur des services ». Elle a pour rôle d'alerter, de conseiller et d'informer l'ensemble des organisations. Elle possède également un pouvoir de contrôle et de sanction. (CNIL)

La première mission de la CNIL est une mission d'information et de protection des droits. En cela, elle répond aux demandes des personnes que ce soit des demandes individuelles ou des demandes d'une organisation. Elle conduits des actions de communication auprès du grand public et met en libre accès des outils éducatifs tel qu'un MOOC[2] sur le Règlement Général sur la Protection des Données. En tant que régulateur des données à caractère personnel, elle veille à ce que l'accès aux données personnelles pour les personnes le demandant soit le plus efficace possible. Elle a pour rôle de contrôler leur protection lorsqu'elles sont issues des fichiers et des processus papiers ou informatiques tant dans le domaine public que privé.

Sa deuxième mission est liée à l'accompagnement à la mise en conformité et au conseil. En cela, et à l'heure où la mise en conformité d'une entreprise relève d'une bonne gouvernance, elle aide les organisations, quel que soit leur taille, dans leur mise en conformité et aide les particuliers à maîtriser leurs données à caractère personnel et à faire valoir leurs droits. (CNIL) De plus, elle conseille et accompagne les organisations en les aidant à mettre en place les solutions permettant de remplir leurs objectifs tout en respectant les droits et libertés des individus.

Sa troisième mission est liée à l'anticipation et à l'innovation. En effet, la CNIL s'intéresse aux signaux faibles qui peuvent exister. Elle prend part à la réalisation de débat de société portant sur les sujets et objectifs éthiques des données. De plus, elle collabore au développement de solutions protectrices de la vie privée s'appuyant sur le *privacy by design.* Elle veille également à ce que l'informatique soit au service de l'individu et qu'il ne nuit pas « à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. » (CNIL) A titre d'exemple, et pour rester proche de l'actualité, la CNIL a pu se positionner lors de la mise en place de l'application mobile *StopCovid*.

[2] Massive Open Online Course – formation en ligne ouverte à tous

Enfin, la dernière mission qui n'est pas des moindres renvoie au contrôle et la sanction. La CNIL peut contrôler les organisations après avoir reçus des plaintes ou des signalements ou simplement parce qu'elle se saisit d'un cas précis. (CNIL) Ces contrôles peuvent s'exercer sur place, à distance ou via des auditions. La CNIL peut prévenir l'entreprise de son intention de contrôle afin qu'elle ait le temps de rassembler les pièces utiles au contrôle ou le réaliser de manière totalement imprévue. En tant qu'organisme de contrôle, la CNIL peut, en cas de manquements observés, mettre en demeure ou prononcer différentes mesures ou sanctions envers une organisation. Le fait de contrôler les organisations vise à avoir un moyen d'intervention « auprès des responsables de traitements sur la mise en œuvre concrète de la loi ». En dehors des sanctions financières, la CNIL peut également donner un avertissement à une organisation pour donner suite à l'entrée en vigueur du RGPD. Cet avertissement n'a pour objectif d'informer les organisations qu'un traitement déjà mis en place ou en cours de déploiement ne respecte pas les textes en vigueurs. Enfin, la CNIL peut mettre en demeure des organisations ne respectant pas certains aspects du RGPD de se mettre en conformité dans un délai limité. (CNIL)

Ainsi, la CNIL est chargée de veiller au respect de l'identité humaine, de la vie privée des individus et de leurs libertés dans un monde numérique de plus en plus présent.
En comparaison aux autres organisations de contrôle existantes dans les pays voisins de la France, la CNIL est considérée comme une autorité de contrôle mature avec un pouvoir de sanction. Certaines autorités de contrôle en Europe n'ont pas ce pouvoir de sanction. La maturité de la CNIL s'est construite sur le fait qu'elle dispose d'un système de blacklistage pour les processus considérés à risque pour les personnes concernées. Ce système de blacklistage n'implique pas l'abandon du processus pour autant mais requiert la réalisation d'une analyse d'impact dont on discutera en détail ultérieurement. Pour ne donner qu'un exemple, le traitement de détection et de gestion de « hauts potentiels » au sein d'une organisation fait partie des processus blacklisté. (CNIL)

3. Responsabiliser les métiers

La responsabilisation est une notion utilisée pour décrire l'état d'esprit qui permet d'être plus responsable et d'avoir de meilleures capacités et plus d'autonomie. (Wikihow)
La responsabilisation des parties prenantes et des métiers est une étape indispensable en matière de performance de l'organisation et afin de mettre en oeuvre une gouvernance des données. Le Règlement Général de Protection des Données intègre l'idée de responsabilité des parties prenantes au cœur de ses éléments. Il s'agit de la notion d'*accountability* qui place les organisations en tant qu'acteur et responsable de leur propre conformité. Autrement dit, ils doivent avoir une mise en conformité dynamique ce qui signifie que les organisations doivent s'interroger sur la conformité de

leurs traitements et sur les rôles des acteurs concernés par ces traitements. Elles doivent aussi être capable de justifier cette conformité en matière de protection des données. Cette responsabilisation des métiers et des parties prenantes passent par le fait de mettre en œuvre une documentation explicite sur les traitements et la protection des données en détaillant leur conformité. Le fait de responsabiliser certains acteurs vise à encourager tous les acteurs responsables des traitements d'être capable de motiver le respect de la minimisation et de la sécurité des données tout comme le respect de leur durée de conservation.
Cette responsabilisatiton des acteurs se veut dynamique puisqu'elle exige la mise en œuvre de mesures dans le respect de la réglementation ainsi qu'une valorisation ou revalorisation des mesures existantes de manière à les mettre à jour. Elle se veut également globale puisque pour être efficace elle nécessite l'implication de l'ensemble des acteurs de l'organisation et ce quelque soit leur position dans celle-ci.

Ce vaste travail de responsabilisation des acteurs et de respect d'une gouvernance nécessite la mise en œuvre d'une conduite de changement afin de sensibiliser, informer et former les parties prenantes. Pour responsabiliser, la première démarche à mettre en œuvre est d'expliciter et de faire comprendre les attendus et leur importance afin de favoriser la motivation des parties prenantes en donnant du sens. De plus, il est nécessaire d'avoir des objectifs SMART c'est-à-dire simples, mesurables, accessibles, réalisables et délimités dans le temps. De ce fait, la responsabilisation des parties prenantes s'effectue avec le temps et ne peut être mesurable qu'à la suite d'actions impliquant leur participation et coopération.

C. Enjeux et utilité

1. Identification des usages de la donnée

Les données visent à donner une visibilité sur l'ensemble des aspects d'une organisation. Elles peuvent avoir un pouvoir d'ordre commercial ou stratégique sur les décisions de l'entreprise. Effectivement, ces dernières années, on observe que les données ont pu jouer un rôle clé dans certaines décisions importantes comme pour l'élection américaine suite à Cambridge Analytica. (Deniau, 2018) En cela, nous pouvons constater que les données que nous partageons sur les réseaux sociaux, comme Facebook pour le cas de Cambridge Analytica, sont susceptibles d'entrer en considération lors des recommandations qui nous sont proposées. Chacune des recherches sur Internet que nous faisons laisse une trace numérique qui peut être exploitée, parfois à notre insu. L'affaire Cambridge Analytica illustre cette idée. En effet, les données laissées par de millions d'américains ont été étudiées pour déterminer ce que pourraient être leurs intentions afin de les encourager à avoir un comportement particulier et prévisible.

Nous pouvons observer l'usage de ses techniques dans des cas totalement différents. Par exemple, lors de la réalisation d'une recherche sur internet, nous avons par la suite, le jour même ou les jours suivants, des annonces directement en lien avec ces recherches que nous avons effectués auparavant. Cette méthode peut être utilisée à des fins marketing afin de cibler de manière plus précise les futurs acheteurs.

Les données visent à acquérir une vision de la situation réelle. Elles donnent la possibilité de modéliser afin d'avoir une répresentation du réel en excluant les éléments pouvant être superflus. Cette modélisation du réel donne la possibilité d'avoir une représentation générale qui peut faciliter et aider la prise de décision et servir de support de gestion. A partir de l'analyse de la situation, les données permettent d'obtenir des projections dans le but de connaitre le résultat possible. Il s'agit du *forecast* c'est-à-dire d'une prévision. Les données possèdent un caractère prédictif puisqu'elles permettent, à partir d'une analyse du passé et des connaissances acquises, de faire des prédictions sur un état à venir. Le Big Data et l'intelligence prédictive sont des éléments qui permettent de réaliser ces prévisions et donnent la possibilité à une organisation de pouvoir prendre une décision en amont. L'association de l'analyse d'une situation actuelle donnée pour prédir une situation à venir n'est pas possible sans l'existence des données. Cette tendance à la prédiction liées aux données tend à s'amplifier tirant avantage des techniques liés au Big Data et aux technologies d'intelligence artificielle comme le *Machine Learning* et le *Deep Learning.*

2. Aspect business

Comme on a pu le voir précédemment, la donnée, et plus largement le patrimoine informationnel, est une matière essentielle pour une organisation. En effet, au travers de son cycle de vie, la donnée, d'abord information avant de devenir connaissance, constitue le savoir d'une entreprise. (Delayat & Bouteiller, 2014)
Elle ne peut être reconnue comme actif numérique que si elle a une capacité à pouvoir créer de la valeur pour l'organisation. L'information transportée par les données forme une réelle richesse pour l'organisation à condition d'être en capacité et d'avoir les moyens et ressources pour l'utiliser et la valoriser. Nous pouvons dire qu'au fil des années, la donnée a évolué pour devenir le nouvel or noir pour l'ensemble des entreprises. Afin d'acquérir davantage de valeur issue des données, le fait de maitriser son cycle de vie est primordial, tout comme le suivi de leur chaîne de valeur. En effet, il est essentiel de connaitre pleinement les processus mis en œuvre par les différents métiers de la collecte à la destruction ou l'archivage. Les notions de protection, sécurité, qualité et d'éthique sont aussi des éléments à considérer lorsque l'on étudie les données. En effet, le fait de ne pas protéger ses données ou de ne pas avoir des données de qualité peut engendrer un coût opérationnel. Les données sont des leviers pour l'organisation lorsqu'elles visent à maximiser la distribution des ressources ou lorsque le chiffre d'affaire augmente.

Dans le film *Le Stratège* (Miller, 2011), inspiré de faits réels, le manager d'une équipe de baseball dans la ville d'Oakland aux Etats-Unis se sert des données à sa disposition dans le but d'augmenter les compétences présentes dans son équipe. Pour valoriser davantage ses joueurs, il se sert des ressources limitées dont il dispose et recrute de nouveaux joueurs ayant un talent particulier. En se servant des données avec une vision statistique de son sport, grâce à la sabermétrie, il réussit à obtenir une conception exacte de la situation de son équipe. Il révolutionne ainsi l'entraînement de l'équipe des Athletics d'Oakland à travers une méthode pour le moins originale. A partir d'indicateurs de performance, il évalue le taux de succès pour chaque joueur dans la perspective de créer une équipe capable de remporter la Ligue majeure de baseball aux Etats-Unis. Suite à la formation de sa nouvelle équipe, ce manager et ses joueurs obtiennent vingt victoires consécutives malgré le fait d'être perçue comme incompétente. Par ces résultats, cette équipe démontre la force que peuvent avoir les statistiques et, d'une manière plus générale, les données. Ainsi, selon le manager de cette équipe « tout est affaire de qualités d'évaluation et de calcul de coûts associés ».

Par cet exemple filmatographique, on observe facilement que les données impactent les prises de décisions dans des domaines très variés. A partir de leur performance, les entreprises ont la possiblité de pouvoir mieux décider, plus rapidement et avec un taux d'erreurs faible. Les données, et les informations qu'elles fournissent, sont une réelle ressource qui donne la possibilité de réfléchir et de repenser notre manière de prendre des décisions.

3. Aspect sécuritaire

Pour assurer la gouvernance des données, il est essentiel de réfléchir à la sécurité des données ainsi qu'à leur protection.
Luc Germain, directeur Open Solutions chez Devoteam[3], explique que « la sécurisation des données peut être assurée par le cryptage des informations, par la mise en place de règles de segmentation et droits d'accès aux données ou par la segmentation des données dans différentes bases. Le renforcement de la sécurisation des données peut être fait par le système SSO et double authentification. Pour éviter le piratage de données en cas de perte ou de vol des codes d'accès, un système de fermeture de comptes et d'accès rapide doit être mis en place. » (Silicon)

La pseudonymisation est une technique visant à sécuriser de manière réversible les données. Cette méthode permet de diminuer les relations pouvant être faites entre les données d'identification d'une personne et toutes autres données ayant été collectées. Selon l'article 28 du Règlement Général de Protection des données, la pseudonymisation des données vise à « réduire les risques pour les personnes concernées ».

[3] Entreprise de services du numérique (ESN)

Le chiffrement des données est une autre méthode visant à protéger les données en particulier les données à caractère personnel. Il permet de rendre illisible les informations pour toute personne n'ayant pas les clés d'accès ou les autorisations nécessaires à la lecture des fichiers. Les méthodes de chiffrement sont décrites dans la norme ISO/CEI 27040.

Enfin, l'anonymisation est la méthode qui repose sur le fait de rendre les données inintelligibles à toute personne. Cette méthode rend la ré-identification des individus irréalisable même après toute forme d'opération et de traitement.

4. Aspect légal

La gouvernance des données fixe le cadre permettant la mise en œuvre de règles internes à l'organisation et des obligations juridiques ou réglementaires en vigueur. Certaines réglementations, comme les normes ISO, la loi Informatique et Libertés et le Règlement Général sur la Protection des Données, démontrent le besoin de gouvernance des données. Ces réglementations et normes permettent d'avoir un suivi de la démarche de maitrise du patrimoine informationnel.

La partie qui suit vise à faire une revue de la littérature des normes et règlements qui existent.

D. Cadre légal

1. Normes ISO

Une norme est un document officiel fourni par un organisme conventionné. Citons, parmi les plus connus, les normes Afnor et ISO.
L'AFNOR définit une norme comme étant « un cadre de référence qui vise à fournir des lignes directrices, des prescriptions techniques ou qualitatives pour des produits, services ou pratiques au service de l'intérêt général. Elle est le fruit d'une co-production consensuelle entre les professionnels et les utilisateurs qui se sont engagés dans son élaboration. » Toute organisation peut s'y référer ou non. En cela, la norme est dite volontaire. (AFNOR)
Selon l'International Organization for Standardization (ISO), organisation internationale non gouvernementale, la norme est un « document établi par consensus et approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques, pour des activités ou leurs résultats garantissant un niveau d'ordre optimal dans un contexte donné ». (Ooreka, 2019) L'ISO élabore des normes internationales, adoptées par les entreprises en tant que « référentiels de bonnes pratiques à usage volontaire, dans le cadre de certifications

imposées par des règlementations sectorielles ou par des exigences contractuelle ». (Foucault, Panhaleux, Renaud, & Begasse, 2018)

Les normes peuvent concerner plusieurs domaines : normes de produits, méthodes d'essai, code de bonne pratique ou encore normes de système de management.
Les normes ISO peuvent être différenciées selon quatre types de normes :

- « les normes fondamentales qui ont pour but de règlementer les sigles symboles et leur nomenclature ;
- les normes de spécifications ayant pour rôle d'informer sur les caractéristiques et les performances pouvant être réalisé par un service ;
- les normes d'analyses et d'essais qui apportent des indications sur les tests à faire avant la mise en place d'un service ou produit ;
- les normes d'organisation concernent le management de la qualité et le process qualité ». (Ooreka, 2019)

Parmi les normes ISO relatives à la sécurité de l'information, l'organisme a publié un ensemble de normes parmi lesquelles la norme ISO 27000, la norme ISO 27001, la norme ISO 27002, la norme ISO 27005 et la norme 27018-2014 qui sont les plus souvent rencontrées. Ces différentes normes relatives à la sécurité des systèmes d'information sont à mettre en lien avec le Règlement Général sur la Protection des Données et en particulier l'article 40 qui expose : (Foucault, Panhaleux, Renaud, & Begasse, 2018)

> *(RGPD, art 40)* « Les Etats membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite destinées à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises. » (le Parlement Européen et le Conseil de l'Union Européenne, 2016)

Selon les normes ISO, la sécurité du patrimoine informationnel a pour but de protéger et préserver les trois propriétés suivantes :

- Confidentialité : il s'agit de la protection des données contre les accès non autorisés, les divulgations et les processus ;
- Intégrité : cela fait référence à la protection de l'exactitude et de l'exhaustivité des données des modifications non autorisées ;
- Disponibilité soit l'assurance de l'accessibilité et de la convivialité des données sur demande d'une entité autorisée. (Loukil, Ghedira-Guegan, Benharkat, Boukadi, & Maamar, 2019)

La sécurité du patrimoine informationnel peut impliquer la protection de l'authenticité, l'autorisation en veillant à ce que les entités puissent être tenues responsables.

- Authentification qui vise à garantir qu'une caractéristique revendiquée est correcte ;
- Autorisation qui se rapporte à l'autorisation de fournir des informations ;
- Responsabilité qui se réfère à la responsabilité des parties prenantes pour leurs actions. (Loukil, Ghedira-Guegan, Benharkat, Boukadi, & Maamar, 2019)

Les normes ISO / CEI sont considérées comme l'une des références en matière de protection des données et de la vie privée. L'ISO définit cette problématique comme « la préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information ». (ISO, 2019)

Les normes ISO issue de la famille 27000 ont été publiées à partir de 2005 par l'Organisation Internationale de Normalisation et par la Commission Electrotechnique Internationale. Ces normes accompagnent les entreprises dans leur résolution d'assurer la protection de leurs informations et les soutient dans le management de la sécurité des informations. Les exigences relatives à ces normes de la famille 27000 aident les organisations à protéger leurs données et informations sensibles qui sont échangées au sein de leur service. (Skills4All) Ces normes s'appliquent en particulier lorsqu'il s'agit de données financières, de documents soumis à la propriété intellectuelle, ou d'informations liées au personnel ou pouvant être confiées par des tiers. (ISO, 2019)
Cette famille ISO 27000 est composée de 12 normes, dont les normes ISO 27001 et ISO 27002.

a) ISO / IEC 27001

La norme ISO 27001 vise à aider les entrepises à adopter, maintenir et améliorer leurs systèmes de gestion de la sécurité de l'information. Cette norme est considérée comme pionnière en matière de sécurité informatique. Elle assure que les risques liés à la sécurité d'une entreprise sont gouvernés de manière durable et vise à communiquer un message positif aux clients et aux collaborateurs : « cette entreprise fait les choses correctement ». (Sitbon, 2019)

Elle vise à la mise en œuvre de processus permettant l'identification et la gestion des risques pouvant exister dans un processus d'entreprise de traitement du patrimoine informationnel. En effet, la norme ISO 27001 permet d'identifier et de maitriser toute défaillance informatique, de répondre aux obligations légales et réglementaires associées à une norme internationnale, de prendre des décisions concernant la gestion des risques dans le respect des objectifs stratégiques d'une organisation et de maintenir un niveau de sécurité pour les informations de l'entreprise. De plus, la norme ISO 27001 vise à permettre aux entreprises de pouvoir concentrer leur attention sur les informations et données considérées comme sensibles et ce quelque soit leur forme.

Avoir la certification ISO 27001 permet à l'entreprise d'avoir une image améliorée et différenciée de celle de la concurrence. Enfin, la norme ISO 27001 assure aux clients d'une entreprise la solidité du système de management des systèmes d'information ou SMSI et assure de la fiabilité des systèmes d'information. (Bureau Veritas)

Cette norme ISO 27001 contraint les entreprises à apprécier les évolutions et l'efficacité en matière de sécurité de l'information à travers trois actions importantes. Tout d'abord, la surveillance de la sécurité de l'information et de l'efficacité du système de gestion de la sécurité de l'information par la mise en place d'évaluation des performances. La deuxième action est liée à la mise en œuvre d'audits internes à intervalles réguliers pour informer de la conformité de gestion de la sécurité de l'information en fonction de la situation. Enfin, la troisième action est l'examination du système d'information en réalisant une analyse par la direction du système de gestion de la sécurité de l'information de l'entreprise et ce, de façon régulière afin d'assurer de son efficacité. (Sitbon, 2019)

b) ISO / IEC 27002

La norme ISO 27002, publiée en 2005 et révisée en 2013, est un code de bonnes pratiques couvrant de multiples aspects aussi bien techniques, organisationnels, sociaux et juridiques pour la sécurité de l'informaion. Elle a pour objectif « d'aider à l'évaluation et au traitement des risques de sécurité des informations liés à la confidentialité, l'integrité et aux aspects de la disponibilité ». Elle applique le modèle de gestion de la qualité PDCA (*Plan Do Check Act*). (Takvorian, 2013)

La norme ISO 27002 : 2013 expose les lignes directrices en matière organisationnelle pour la sécurité de l'information et les bonnes pratiques de management de la sécurité de l'information, « incluant la sélection, la mise en œuvre et la gestion de mesures de sécurité prenant en compte le ou les environnement(s) de risques de sécurité de l'information de l'organisation ». (ISO) Cette norme est élaborée pour les organisations voulant choisir les mesures nécessaires dans le cadre du processus de mise en place d'un « système de management de la sécurité de l'information (SMSI) selon l'ISO/CEI 27001 » mais aussi pour celles voulant mettre en place des mesures de sécurité de l'information et « élaborer leurs propres lignes directrices de management de la sécurité de l'information ». (ISO)

c) ISO / IEC 27005

La norme ISO 27005 comporte les lignes directrices liées à la gestion des risques en sécurité de l'information. Elle confirme les concepts généraux présents dans l'ISO 27001. Cette norme est conçue pour aider à la mise en œuvre de la sécurité de l'information fondée sur une approche de gestion des risques. (ISO) Cette norme apporte une méthodologie de gestion des risques qui est utilisée dans le cadre

d'analyses de risques de la vie privée des personnes, telle que le *Privacy Impact Assesment* que nous détaillerons plus loin. (Foucault, Panhaleux, Renaud, & Begasse, 2018) Elle constitue un support des concepts décrits dans la norme ISO 27001 et permet de soutenir la mise en place de la sécurité de l'information tout en se basant sur une gestion des risques.

d) ISO / IEC 27040

La norme ISO/ IEC 27040 présente le sujet de la protection des données et du respect de la vie privée. La vie privée est « la revendication des individus, des groupes ou des institutions à décider eux-mêmes quand, comment et dans quelle mesure les informations les concernant sont communiquées aux autres. » (Loukil, Ghedira-Guegan, Benharkat, Boukadi, & Maamar, 2019)

La norme ISO / IEC 27040, intitulée « Sécurité de stockage » et publiée en 2015 par l'ISO, est un ensemble de « préconisations techniques détaillées concernant la manière dont les organismes peuvent définir un niveau approprié d'atténuation du risque grâce à l'emploi d'une approche reconnue et cohérente de la planification, la conception, la documentation et la mise en œuvre de la sécurité de stockage des données. » (ISO, 2019) Elle donne un descriptif général des concepts de sécurité du stockage et réunit des conseils sur les aspects relatifs aux menaces, à la conception et à la mise en place des caractères architecturaux de la sécurité des moyens de stockage. Cette norme aborde des principes tel que les méthodes de conservation des données (rétention à long terme et à court terme), les notions de confidentialité et d'intégrité des données ainsi que les méthodes de chiffrement et le nettoyage des données.

e) ISO / IEC 29100

La norme ISO/IEC 29100, appelée *Privacy Framework* ou Cadre Privé, a été publiée en 2011. Cette norme définit les principes liés à la protection de la vie privée et place les aspects tant organisationnels que techniques ou procéduraux au sein d'un cadre global dédié à la protection de la vie privée. Elle définit les acteurs et leurs rôles dans le traitement de données à caractère personnel et décrit les éléments à prendre en compte pour assurer cette protection. (ISO, 2011)

Les principes fondamentaux proposés par cette norme sont le consentement éclairé des personnes concernées, la légitimité et la communication de la finalité de traitements, la limitation des données qui sont collectées en étant adéquates et pertinentes au regard du traitement qui sera effectué. De plus, les autres principes sont la minimisation et le cloisonnement des données, la limitation dans la diffusion des données et la communication pour les personnes concernées du traitement effectué. Enfin, le droit d'accès et de rectification des données par les personnes concernées, *l'accountability,* la

sécurité des données et la gestion des risques sont les derniers principes proposés dans cette norme.
Ces principes fondamentaux, ainsi décrits, représentent une base de référence dans la gestion des mesures de protection des données personnelles au sein des systèmes d'information d'une entreprise pour d'autres normes. Elle fournit ainsi des renvois à d'autres principes de protection de la vie privée pour les technologies de l'information. Ils sont compatibles avec le Règlement Général sur la Protection des Données. (AFNOR, 2017)
Cette norme s'applique à l'ensemble des personnes physiques et organisations qui participent « à la spécification, à l'architecture, à la conception, au développement, à la maintenance, à l'administration et à l'exploitation des systèmes de technologies de l'information et de la communication dans lesquels des mesures de protection de la vie privée sont requises pour le traitement de données à caractère personnel ». (ISO, 2011)
Elle permet de favoriser des solutions innovantes pour mettre en œuvre la protection des données personnelles au sein des systèmes de technologies de l'information et de la communication. Enfin, elle vise à améliorer les programmes de protection de la vie privée des organismes grâce à l'utilisation de meilleures pratiques. (ISO, 2011)

Ce cadre peut être utilisé comme base à des initiatives supplémentaires de normalisation dans le domaine de la protection de la vie privée, tel qu'une architecture de référence technique, la mise en place et l'utilisation de technologies spécifiques pour la protection de la vie privée. Il peut aussi être utilisé pour le management global de la protection de la vie privée. De plus, il peut servir à la mise en place de mesures dédiées à la protection de la vie privée pour les processus de traitement de données sous-traités et l'étude des risques sur la vie privée. (ISO, 2011)

f) ISO / IEC 29134

La norme ISO / IEC 29134 décrit les lignes directrices afin de mettre en place un processus d'évaluation des impacts sur la vie privée et une structure pour la réalisation d'un rapport d'évaluation des impacts sur la vie privée (PIA). Elle s'applique aux organisations de toutes tailles et de tous secteurs. Une analyse des impacts est un outil qui vise l'évaluation des potentiels impacts sur la vie privée d'un processus, d'un système d'information, d'un programme ou de tout traitement utilisant des données à caractère personnel. En consultation avec les acteurs impliqués, cette analyse permet de prendre les mesures nécessaires afin de gérer les risques sur la vie privée. (ISO, 2017)

Ainsi, l'ensemble de ces normes ISO sont importantes pour la gouvernance des données dans les aspects de management de la qualité et de la protection des données. Ce dernier aspect sera appuyé dans les sous-parties suivantes présentant la loi Informatique et Liberté et le RGPD.

2. Loi Informatique et Liberté

La loi Informatique et Libertés est liée au projet SAFARI démarré en 1973. Ce projet est un projet d'interconnexion des documents administratifs, en partant du numéro de sécurité sociale au sein d'un « Système Automatisé pour les Fichiers Administratifs et le Répertoire des Individus ». (Senat)

Au moment de la mise en place de ce projet, l'informatique se développant, la population française découvre que la collecte et le transfert des données révèlent certains dangers pour leurs données, ce qui met en lumière l'absence de cadre défini. Le projet SAFARI aboutit le 6 janvier 1978 à la loi relative à l'informatique, aux fichiers et aux libertés. L'article 1er de cette loi précise que « l'informatique doit être au service de chaque citoyen […] » et que « toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant ». (CNIL, 2019) De plus, cette loi assure la protection du patrimoine informationnel ainsi que la sécurité des informations.
Par la mise en application de la loi Informatique et Libertés, la France apparait après l'Allemagne comme étant précurseur sur la protection des données personnelles.

a) Principes et champs d'application

Créée en 1978, puis modifiée en 2004, la loi Informatique et Libertés vise l'ensemble des traitements automatisés liés aux données à caractère personnel. Elle s'applique à l'ensemble des secteurs faisant appel à l'usage des données à caractère personnel dans le cadre de leurs activités.
Les éléments clés de cette loi sont spécifiés dans l'article 2 qui précise notamment que cette loi s'applique à tous les « traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers […] ». (CNIL, 2019) Pour compléter, l'article 2 précise la définition d'une donnée personnelle qui est décrite comme « toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres ».
Cette loi comporte de nombreuses dispositions, reprise par le RGPD telles que :

- L'interdiction de collecter des données à caractère sensible, soit les données pouvant être liées à la religion, la santé, la politique sauf exceptions (dispositions légales ou consentement de la personne concernée) ;
- « Le principe de collecte loyale de données ;
- L'obligation d'assurer la sécurité de l'ensemble des données collectées ;
- L'obligation d'informer les individus concernés de la collecte de leurs données ;
- Le droit à l'accès, la modification et la suppression des données en question » (donnees-rgpd).

b) Droits et obligations

La loi Informatique et Libertés reconnait de nombreux droits aux individus concernés par le traitement de leurs données.
Le premier d'entre eux est le droit d'accès aux données qui permet à toute personne concernée capable de prouver son identité de pouvoir demander l'accès à ses données à caractère personnel ayant été collectées et de demander le type de traitement qui est pratiqué sur ses données.
Le second est le droit de rectification. Il donne la possibilité à tout individu de demander au responsable de traitement une correction sur ses données à caractère personnel s'il juge que celles-ci sont « inexactes, incomplètes, équivoques ou obsolètes » afin de les mettre à jour. De plus, ce droit de rectification permet à un individu de demander le verrouillage ou la suppression de ses données s'il juge que « la collecte, l'utilisation, la communication ou la conservation est illégale ». L'entreprise est elle-même tenue de corriger des données si elle se rend compte d'inexactitude.
Le troisième droit est le droit d'opposition qui permet à tout individu de s'opposer à ce qu'elle apparaisse dans un fichier de traitement de données et ce, en amont de la collecte ou à la suite d'un traitement réalisé. Pour y avoir droit, l'individu doit donner des motifs légitimes. Ce droit à l'opposition ne concerne pas les traitements liés à une obligation légale et n'est ainsi pas absolu sauf lorsqu'il concerne la prospection. La demande est jugée par le responsable de traitement et le DPO qui l'évalue afin d'y donner suite ou non.

La loi Informatique et Libertés fixe des obligations pour les responsables de traitement. Tout d'abord, le principe de licéité concernant la collecte des données, soit le fait que les données doivent être collectées en s'assurant que les individus ont conscience et connaissance du traitement qui sera réalisé. Le traitement ainsi réalisé doit respecter l'objet social de l'organisation. Les données doivent être collectées de manière légale et chaque collecte doit être associée à un objectif précis et défini en amont de celle-ci. Le traitement des données collectées doit ainsi être justifiée et correspondre à l'objectif défini. La collecte de données personnelles doit reposer sur un fondement légal tel que défini par la CNIL à savoir notamment l'existence d'une loi, un contrat, le consentement, l'intérêt légitime de l'organisation, la sauvegarde des intérêts vitaux de la personne concernée.
Les personnes concernées doivent ainsi être informées du nom du responsable de traitement, de l'objet de la collecte et de conservation des données durant une durée fixée par le responsable de traitement ou par une obligation légale. (Rispoli, 2016)
De plus, la loi Informatique et Libertés exige une obligation de sécurité. Le responsable de traitement doit assurer la disponibilité, l'intégrité, l'authenticité et la confidentialité des données contre toute attaque qu'elle soit volontaire ou accidentelle. Le responsable de traitement doit ainsi s'assurer des mesures de protection mises en place afin de maintenir la protection et la sécurité du patrimoine informationnel.

3. RGPD

Avec l'essor du Big Data, la multiplication des données, et de leurs échanges à travers Internet, a placé le sujet de la protection des données personnelles comme un enjeu de société. En effet, du fait de l'augmentation du nombre de données collectées par les organisations, et en particulier des données personnelles, leur cycle de vie est devenu un véritable sujet de discussion pour les organisations, aussi bien en terme de maitrise de ce patrimoine informationnel que de sa protection.

a) Présentation générale

La création du Règlement Général sur la Protection des Données s'est faite à la suite de la prise en compte des évolutions technologiques précédent sa mise en application, comme l'apparition des réseaux sociaux, le développement du commerce en ligne.
Les GAFAM (Google, Amazon, Facebook, Apple et Microsoft) sont les géants du numérique. Facebook observe près de 2.7 milliards d'utilisateurs considérés comme actifs tous les mois ou 1.79 milliard d'utilisateurs actifs de façon journalière à travers le monde. (Jdn, 2020)
Le droit relatif à la protection des données personnelles a dû évoluer à la suite de la mise en application de cette nouvelle réglementation européenne qui permet notamment de renforcer la protection et les droits accordés aux individus.

Le RGPD est le Règlement Général sur la Protection des Données qui est la dénomination simplifiée de « Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE. » (Foucault, Panhaleux, Renaud, & Begasse, 2018)
Dans un besoin d'amélioration de la protection des droits des individus pour lesquels leurs données sont collectées et d'unification du droit au sein de l'Union Européenne, le Parlement européen a validé le Règlement Général sur la Protection des Données, initié par Viviane Reding, le 14 avril 2016 et entré en vigueur le 25 mai 2018. Il se veut en continuité de la loi Informatique et Libertés de 1978 en présentant certaines évolutions.
Le premier objectif du Règlement Général sur la Protection des Données est d'harmoniser et d'unifier le cadre juridique européen des différents pays membres en matière de protection des données à caractère personnel et de renforcer la participation des autorités de protection de l'Union Européenne. La règlementation anglo-saxonne était articulée autour de la notion de défaut d'opposition alors que celle en France était davantage axée sur le consentement préalable des individus.
La vocation de ce règlement est également de renforcer la position des acteurs européens dans un contexte où le monde est globalisé. Viviane Reding a décrit que l'objectif de ce règlement est de « susciter la confiance dans les services en ligne parce que les utilisateurs seront mieux informés de leurs droits et auront une plus grande maitrise des informations qui les concernent ». En partant de cet objectif, le règlement

vise l'augmentation de la maitrise des individus sur leurs données transmises aux organisations. Il donne d'avantage de contrôle aux individus en augmentant leurs droits liés à la maîtrise de leurs données à travers le droit d'accès, le droit de rectification des données personnelles lorsqu'elles sont inexactes ou si l'objectif de leur traitement n'est plus légal ou approprié, le droit d'opposition et le droit d'effacement. (CNIL, 2019) Le droit d'accès permet « de contrôler l'exactitude des données et si nécessaire de les faire rectifier ou effacer » (Article 15, RGPD)

b) *Principes fondamentaux*

Le RGPD s'applique à l'ensemble des pays membres de l'Union européenne, dont la France, et concerne ainsi toute personne qui traite des données à caractère personnel d'individus au sein de l'Union Européenne dans le cadre de son activité professionnelle. Il s'applique également au traitement des données personnelles des individus européens réalisés dans des pays hors de l'Union européenne si l'entreprise est basée dans un des pays européens.

Le Règlement Général sur la Protection des Données repose sur deux piliers illustrés dans la figure ci-dessous.

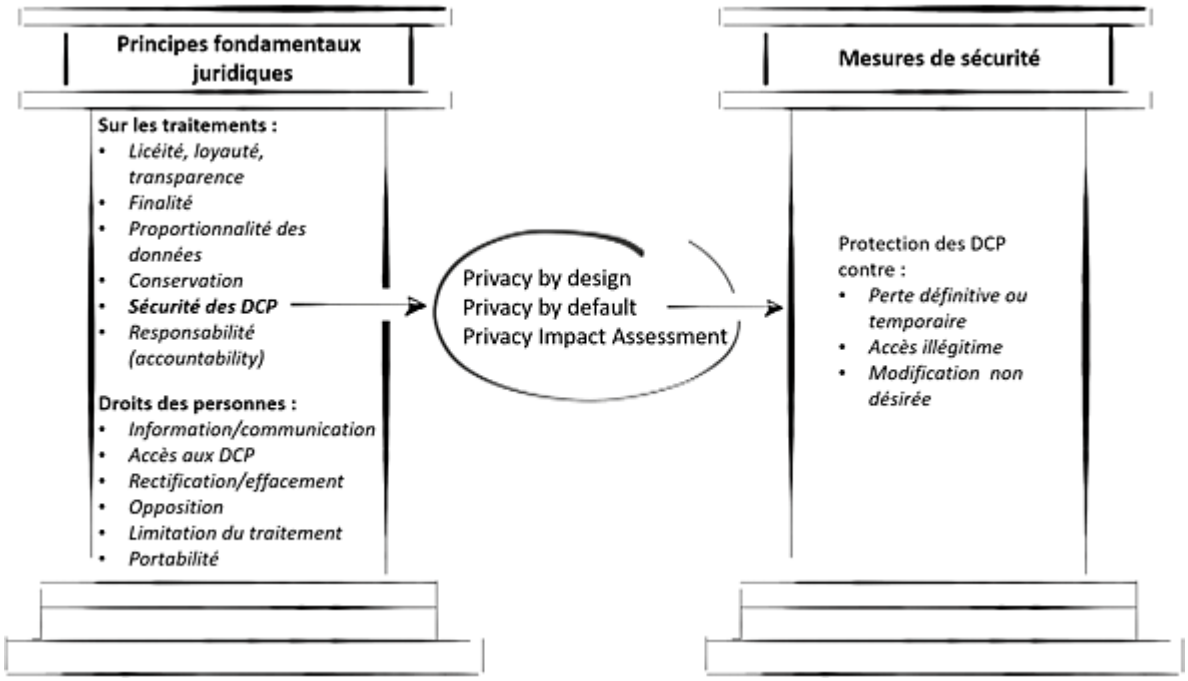

Figure 4 - Piliers du RGPD (Foucault, Panhaleux, Renaud, & Begasse, 2018)

Le premier est lié aux principes fondamentaux juridiques concernant les traitements de données personnelles comme la finalité de traitement et les principes liés aux droits des personnes concernées tel que le droit d'accès, le droit à l'oubli…

Le second porte sur la sécurité des données personnelles et traite des mesures de sécurité qui existent au niveau technique et organisationnel pour mettre en place une protection adaptée aux besoins. Il s'appuie sur des règles de base et les différents principes du RGPD tels que la transparence, la finalité de traitement, la conservation et protection des données mais également la responsabilité des acteurs. (Foucault, Panhaleux, Renaud, & Begasse, 2018)
Il apporte aux organisations des principes clés comme l'*accountability*, le *privacy by design*, le principe de durée de conservation des données, le droit à l'oubli et la portabilité des données.

Les points clés du RGPD sont :

- la minimisation de la collecte des données : seules les données nécessaires au but précis du traitement ne doivent être collectées ;
- la finalité du traitement doit être « déterminée, explicite et légitime ». Pour justifier que le traitement est licite, il existe des bases légales dont le consentement et l'intérêt légitime. Le consentement doit être « explicite ou éclairé » c'est-à-dire que la personne concernée doit connaitre l'identité du responsable de traitement et les finalités du traitement ; (Foucault, Panhaleux, Renaud, & Begasse, 2018)
- la transparence de l'objectif de la collecte et du traitement de données : les personnes concernées doivent avoir connaissance du traitement en amont de la collecte des données ;
- la mise en oeuvre d'une durée de stockage des données : elles ne peuvent être conservées sans limite par les organisations. Lorsque les objectifs des processus métiers sont atteints, elles doivent être archivées, supprimées ou anonymisées ;
- la sécurisation des données à caractère personnel et des équipements (matériel de stockage, de traitements) par le renforcement des moyens de contrôles et la mise en place de mesures de sécurité techniques et organisationnelles. En cas d'incident de sécurité et de violation des données à caractère personnel, toute entreprise a 72h à compter de la connaissance de l'incident pour le signaler à l'autorité de contrôle compétente, la CNIL pour la France.

Le RGPD donne une importance spéciale à la maitrise du partage des données, à l'identification des risques et à la capacité pour les organisations de démontrer leur conformité.
Il élève la sécurité comme principe fondateur lié aux traitements de données à caractère personnel. Il adapte et renforce ainsi les normes déjà existantes en matière de protection des données personnelles et impose aux organisations de traiter les informations dans le respect de certaines règles strictes. Le RGPD précise la notion de sécurité : « Les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction, ou les dégâts d'origine accidentelle, à l'aide de

mesures techniques et organisationnelles appropriées (intégrité et confidentialité) » (Foucault, Panhaleux, Renaud, & Begasse, 2018)

Le RGPD introduit les notions de « *privacy by design* » et de « *privacy by default* ».
Le « *privacy by design* » implique que les enjeux relatifs à la protection des données doivent être réfléchis et considérés à l'origine de tout projet impliquant un traitement de données personnelles et tout au long du projet. Le responsable de traitement doit intégrer la notion de protection des données, dès la conception et par défaut. Ainsi, ce principe de protection doit se faire dès la conception de l'outil de traitement.
Le « *privacy by default* », ou protection de la vie privée par défaut, décrit que les responsables de traitement doivent par défaut assurer du plus haut niveau de protection des personnes concernées. (Foucault, Panhaleux, Renaud, & Begasse, 2018)

Le principe d'« *accountability* » est le principe de responsabilité du responsable de traitements. Celui-ci doit recenser et vérifier les traitements tout en adaptant si besoin sa politique de protection des données. Il désigne l'obligation pour les organisations de mettre en place des mécanismes et des procédures en interne afin de prouver le respect des règles en vigueur en matière de protection des données.
Dans certains cas, et conformément à l'obligation légale, le responsable de traitement souhaitant mettre en oeuvre un nouveau traitement présentant des risques particuliers pour les droits et libertés des personnes cocernées, doit réaliser une autoévaluation des risques de son projet concernant la vie privée des individus. Cette analyse n'est obligatoire que dans des cas bien définis par la CNIL[4], notamment lorsque le projet présente des risques majeurs pour les droits des individus si aucunes mesures ne sont prises pour les diminuer.

Ce règlement introduit un nouveau rôle dans les organisations qui est celui de DPO (*Data Protection Officer*), comme décrit dans la partie *DPO, D*d). Cette désignation est obligatoire pour toutes les autorités ou organisations publiques traitant des données personnelles, si les activités de base de l'organisation entrainent un suivi régulier et systématique à grande échelle des personnes concernées ou si elles consistent en un traitement à grande échelle de données sensibles. Dans tous les cas, une personne dans l'entreprise se doit d'être identifiée comme s'assurer du respect du RGPD. Le règlement couvre aussi la possibilité que le DPO soit nommé en externe à l'organisation.
En cas de violation de sécurité des données, les organisations ont l'obligation de notifier à l'autorité de contrôle responsable dans un délai de 72h maximum à compter de la prise de connaissance de la violation, et dans certaines situations, d'en informer les personnes concernées. Ainsi, en cas de détection de violation sur un support physique, une application, un processus métier ou chez un partenaire, l'organisation doit être en

[4] La CNIL a défini 9 critères. Si deux de ces 9 critères sont remplis, la réalisation de l'analyse d'impacts est obligatoire.

mesure d'extraire les catégories de données concernées ainsi que d'identifier les personnes concernées par cette violation. Le respect de cette obligation passe par la sensibilisation de l'ensemble des acteurs qui peuvent tous être en situation de devoir informer en cas de violation de sécurité.

L'article 47 du RGPD (Parlement européen et du Conseil) met en lumière les règles d'entreprise contraignantes ou BCR[5]. Il s'agit d'une « convention intra-groupe » de l'organisation établie sur la « base de référentiels d'exigences ». Ces règles désignent une politique de protection des données au sein du groupe. Elles encadrent et assurent une continuité en matière de protection lors de transferts de données à caractère personnel hors de l'Union européenne. Couvrant l'ensemble des traitements réalisés par l'organisation, elles concernent majoritairement les entreprises privées multinationale, implantées dans plusieurs pays européens et non européens. (CNIL, 2020) Il existe deux types de BCR pour les responsables de traitement et pour les sous-traitants. Ces règles reposent sur le principe d'*accountability* et sont considérées comme « accélérateur de conformité et de démonstration de faisabilité ». En effet, elles permettent d'uniformiser les pratiques liées à la protection des données personnelles et de communiquer sur la politique d'organisation liée à la protection des données à caractère personnel auprès des partenaires, clients et salariés. Elles placent ainsi la protection des données comme préoccupation éthique de l'organisation. (CNIL, 2020)

Le RGPD met également l'accent sur les droits donnés aux personnes concernées en les renforçant et en leur consacrant de nouveaux droits. Il reprend et renforce les droits qui apparaissent dans la loi Informatique et Libertés comme :

- le droit d'accès aux données à caractère personnel pour les personnes concernées : La personne concernée peut demander d'obtenir l'ensemble de ses données personnelles le concernant, qu'elles soient traitées ou non ;
- le droit de suppression ou droit à l'oubli : il permet à la personne concernée par le traitement de ses données personnelles de demander l'oubli ou l'effacement de l'ensemble de ses données ;
- le droit de rectification : la personne concernée peut demander modification de ses données s'il juge celles-ci inexactes. Ce droit est en lien avec le principe d'exactitude des données ;
- le droit à l'opposition à tout traitement des données à caractère personnel : la personne concernée peut « s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement de données à caractère personnel ». (Foucault, Panhaleux, Renaud, & Begasse, 2018)

Il apporte de nouveaux droits :

[5] *Binding Corporate Rules* en anglais

- le droit à l'information : L'information sur les traitements réalisés doit être plus explicite et plus accessible aux personnes concernées. Parmi les informations diffusées, les coordonnées du DPO, la durée de conservation doivent être mentionnés ;
- Le droit à la portabilité des données qui est relatif au fait de transmettre les données à un autre responsable de traitement ou à récupérer l'ensemble de ses données à caractère personnel dans un format lisible et facile d'utilisation ;
- Le droit à la limitation de traitement qui autorise une personne concernée à demander une limitation dans le traitement de ses données. En cas de demande, les données seront alors uniquement conservées. Ce droit peut être exprimé lorsqu'un abonnement est arrivé à échéance par exemple ;
- Le droit post-mortem : une personne peut indiquer au responsable de traitement le nom de la personne qui pourra exercer ses droits et accéder à ses données personnelles après son décès.

Ainsi, toute personne physique peut faire valoir ses droits relatifs aux données à caractère personnel auprès de toute entreprise traitant ses données. Les entreprises disposent d'un délai légal de traitement d'une demande. En cas de demande d'exercice du droit d'accès par un individu, l'entreprise dispose d'un mois pour fournir les informations demandées.

Entreprises et individus sont concernés par la protection des données. Les risques pour les entreprises sont opérationnels (suspension ou suppression de l'autorisation du traitement des données) mais aussi financier puisqu'une amende pouvant aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaires annuel mondial peut être prononcée en cas de non respect ou de manquements de la règlementation européenne. Les manquements peuvent prendre plusieurs formes comme l'absence de consentement de traitement des données ou de base légale pour le faire, le non-respect des droits individuels ou la violation des règles sur le transfert des données.
Dans cette situation, comment mettre en œuvre la conformité et appliquer une règlementation en vigueur tel que le Règlement Général sur la Protection des Données ?

III. Mise en conformité : Application d'un cadre légal tel que le RGPD

Coordonner et maintenir la mise en conformité, en particulier la mise en conformité au RGPD, nécessite la mise en œuvre de méthodes et de moyens permettant d'assurer la maitrise et la protection de la vie privée et du patrimoine informationnel. Cette protection doit être réfléchie et mise en place dès la conception des processus métiers au sein des organisations, soit le *privacy by design*.

Par conséquent, il faut tenir compte des obligations relatives à l'utilisation des données à caractère personnel dans le plan d'urbanisme des systèmes d'informations. Le projet de plateforme de gouvernance des données personnelles, *ARIANE*, vise à industrialiser la protection de la vie privée en construisant un référentiel unique de personnes physiques. (Bentounsi M. , Cante, Coya, Darmon, de Chambourcy, & Gnokam, 2019)

La gouvernance et la protection des données étaient pris comme deux objectifs indépendants avant la mise en place du RGPD. Depuis son entrée en vigueur et sous la demande des personnes concernées, les entreprises doivent répondre aux besoins de protection de la vie privée tout en assurant la transparence sur le cycle de vie des données. Pour y parvenir, les entreprises doivent suivre des solutions pouvant mieux protéger les données et donner des rapports détaillés sur leur utilisation. (Bentounsi M. , Cante, Coya, Darmon, de Chambourcy, & Gnokam, 2019)

A. Les enjeux d'une mise en conformité

Le Règlement Général sur la Protection des Données encourage les organisations à réfléchir et revoir la gouvernance en matière de protection des données. Comme vu précédemment, la gouvernance permet d'identifier, de piloter et de contrôler les données grâce aux processus et acteurs. Mettre en place une gouvernance vise à développer un environnement pouvant utiliser les données tout en ayant un niveau adéquat de protection. (Rispoli, 2016)

La mise en conformité dispose d'un enjeu juridique. En effet, l'organisation doit respecter les normes et règlements en vigueur afin de satisfaire les autorités et éviter les sanctions administratives. Respecter les normes et règlements désigne le fait de mettre en place l'ensemble des mesures appropriées permettant d'être en capacité de prouver le respect des règles liées à la protection des données auprès des personnes concernées notamment ou des autorités de contrôle comme la CNIL. Le Règlement Général sur la Protection des Données impose la nomination d'un délégué à la protection des données (DPO), la cartographie des traitements et la mise à jour de leur base juridique tels que les contrats avec les sous-traitants.

Les données personnelles étant un actif stratégique à la fois précieux et vulnérable, les organisations ont pris conscience que les aspects juridiques et organisationnels ne suffisent plus pour être en conformité.

La mise en conformité présente également un enjeu technique afin d'assurer une protection suffisante et adéquate au patrimoine informationnel. L'organisation doit implémenter les mesures nécessaires pour éviter tout risque lié aux données. Le Règlement Général sur la Protection des Données laisse l'organisation libre de mettre en place les mesures qu'elle souhaite à condition qu'elles soient adaptées aux risques.
Un autre enjeu d'une mise en conformité est l'obtention de la confiance des salariés et des partenaires sociaux. La protection de la vie privée dès la conception d'un nouveau processus métier est considérée comme un gage de responsabilité. (Agostinelli, Marrella, Maggi, & Sapio, 2019) Cette protection permet d'assurer la sécurité des données tout au long de leur cycle de vie par l'utilisation de technologies de protection de la vie privée comme le chiffrement, l'anonymisation. Elle permet d'assurer l'exactitude et la traçabilité des données à travers la mise en place de règles de gouvernance. Cette confiance des salariés et des personnes concernées par la prise en compte de mécanismes proactifs visant à redonner le contrôle aux personnes concernées.

Enfin le dernier enjeu de la mise en conformité est le fait d'avoir une bonne image de marque à l'extérieur. Respecter les normes et règlements permet à l'organisation d'acquérir une bonne réputation vis-à-vis de ses salariés, des candidats mais également face à ses concurrents et ses partenaires.

B. Méthodologie de mise en œuvre

1. Documenter et outiller

Afin de gouverner le patrimoine informationnel, l'organisation doit constituer une documentation complète et adéquate afin d'être en capacité, grâce à un ensemble de justifications, de démontrer sa conformité en cas de contrôle.

Au préalable de la mise en place d'une documentation, il semble nécessaire en prérequis de mesurer et d'évaluer les systèmes afin de savoir quels sont ceux qui sont concernés. L'évaluation vise à porter un jugement sur ce qui est préalablement mesuré. Par la suite, il est nécessaire de contrôler et de piloter vers un objectif qui est la mise en conformité. Le contrôle vise à vérifier le respect des procédures afin de chercher la conformité et sa mise en place effective. Si des manques sont constatés, l'organisation et les responsables de traitement devront mener des actions correctives. (Foucault, Panhaleux, Renaud, & Begasse, 2018)

Disposer d'une représentation précise du patrimoine informationnel par la mise en place d'un inventaire des données et des logiciels existant vise à comprendre les relations en place. Connaître les relations entre les données et leur utilisation métier permet d'avoir une vision globale, partagée et commune entre les services. De plus, cette connaissancee vise également à replacer le contexte des utilisations des données et ainsi mieux connaitre la place et le rôle des parties prenantes impliquées. Une représentation des données implique également un travail sur le cycle de vie et la qualité des données. Le cycle de vie est primordial puisqu'il permet de s'assurer du respect des normes et règlements notamment en matière de collecte et de durée de conservation des données. L'ensemble de ces travaux d'analyse et de réflexion permet de mener au mieux cette gouvernance des données.

Par la mise en œuvre de plans d'action dédiés à la mise en conformité des traitements, l'organisation doit pouvoir être en maitrise de ce qu'elle traite et être en mesure d'apporter les preuves de sa conformité, et ainsi disposer des moyens nécessaires.
Ainsi, la mise en place d'une documentation vise à spécifier les usages des données et formalise les obligations et mesures décidées. Elle indique les conditions de traitement et de réutilisation des données, à travers par exemple un descriptif des durées de conservation des données personnelles.
Selon les auteurs M. Bentounsi, E. Cante, D. Coya, P . Darmon et al., l'intégration d'une solution comme Ariane s'effectue en deux phases. La première est liée à la construction de référentiels unifiés qui vise à centraliser l'ensemble des données métiers. La seconde est liée à la cartographie et mise en œuvre de règles de gouvernance des données pour l'ensemble des processus métiers d'une organisation qui utilise des données à caractère personnel. Ces cartographies visent à construire les liens entre les différentes couches du système d'information à travers les référentiels. (Bentounsi M. , Cante, Coya, Darmon, de Chambourcy, & Gnokam, 2019)

Cette documentation et sa mise en place nécessite d'impliquer les acteurs pour avoir une meilleure vision du réel et une maitrise des risques potentiels liés aux données et à leur cycle de vie. Impliquer les acteurs les encourage à réflechir sur leur traitement afin d'apporter des ajustements pour une meilleure maitrise ou une meilleure protection du patrimoine informationnel.

2. Cycle de Deming

Pour William Edwards Deming, l'amélioration dans une organisation s'effectue à travers un travail de réflexion nécessitant une prise de recul face aux pratiques et la transformation de son fonctionnement. Il traite des points qui convergent toujours vers une double réflexion d'analyse du management : sur l'organisation en tant que système et sur le personnel en tant qu'individus. Dès 1950, il « introduit la dynamique de l'amélioration continue, qu'il avait découverte dans le principe des études statistiques dans le cycle de Shewhart ». Ces derniers sont alors retenus par le Japon sous l'expression de cycle PDCA de Deming. (Chardonnet & Thibaudon, 2003)
Les systèmes de management se construisent à travers le temps selon un modèle cyclique nommée roue de Deming ou PDCA. (Foucault, Panhaleux, Renaud, & Begasse, 2018) Ce cycle, popularisé par William Edwards Deming, présente quatre phases à enchainer de manière successive afin de s'inscrire dans une méthode d'amélioration continue. (Fernandez, Qu'est-ce que la Roue de Deming ?, 2018) Les quatre phases sont la planification, le développement, le contrôle et l'amélioration, plus connu en anglais sous les termes Plan, Do, Check, Act. Elles sont représentées par le schéma ci-dessous.

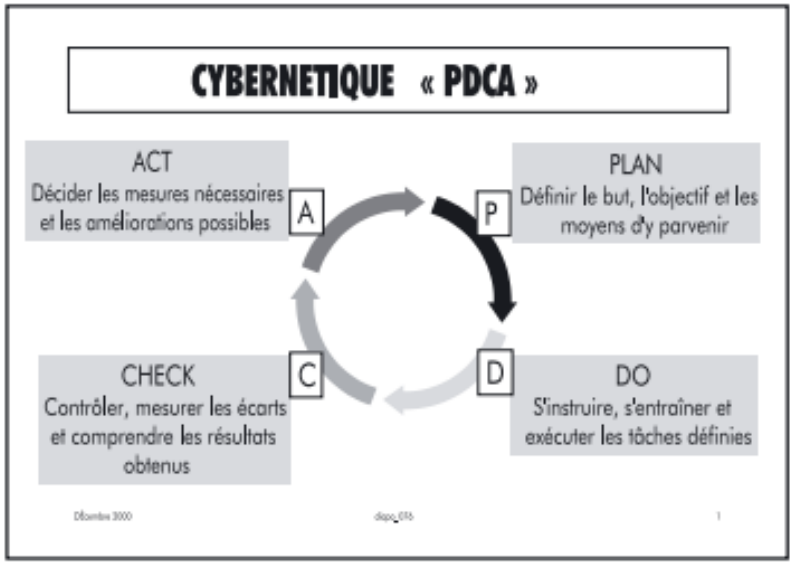

Figure 5 - La cybernétique PDCA (Chardonnet & Thibaudon, 2003)

La phase de planification (*Plan*) vise à définir l'objectif à atteindre, les actions mises en place pour y arriver ainsi que les ressources nécessaires.
La phase de développement (*Do*) vise à la réalisation des actions définies dans la phase précédente au moyen des ressources attribuées et disponible.
La phase de contrôle (*Check*) vise à la vérification de l'atteinte effective des objectifs tout en mesurant les écarts notamment si l'objectif n'est pas atteint.
Enfin, la phase d'amélioration (*Act*) vise à définir des actions permettant de réduire ses écarts et d'améliorer le système.

Cette roue d'amélioration continue s'adapte à la mise en conformité dans le cadre du Règlement Général sur la Protection des Données, comme le montre la figure ci-dessous.

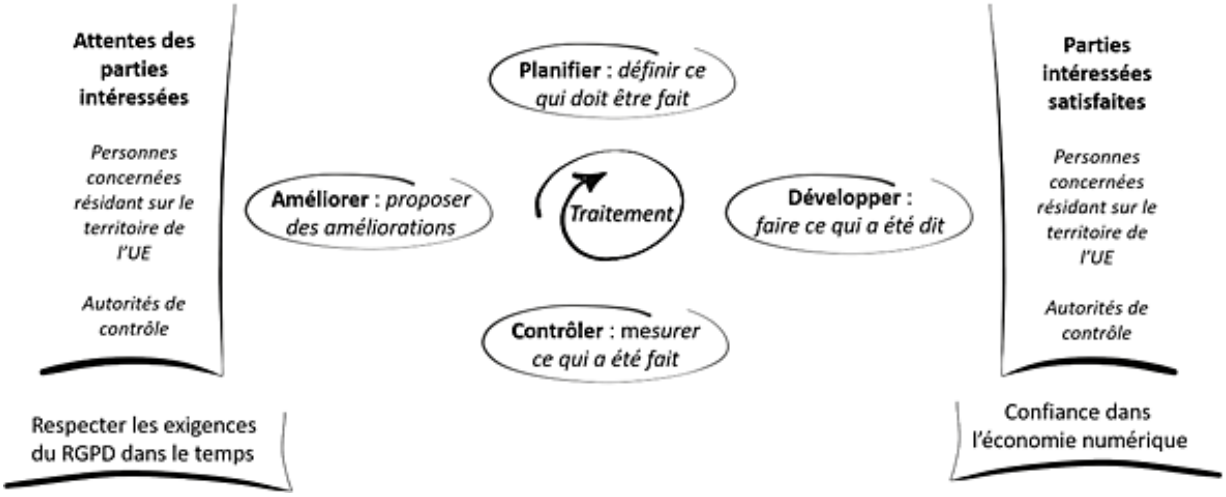

Figure 6 - Système de management des données à caractère personnel (Foucault, Panhaleux, Renaud, & Begasse, 2018)

En effet, chaque année, il est recommandé de faire une revue des processus et des politiques pour acter un nouveau plan de progrès. Cette revue représente l'étape de planification. Dans la phase de développement (*Do*), les conditions de réalisation restent les mêmes, il faut « s'assurer que les ressources et les compétences ont bien été allouées à l'exécution du plan de progrès ». (Foucault, Panhaleux, Renaud, & Begasse, 2018)
Les mesures sont « faites pour apprécier la réalisation des actions de progrès, mais aussi pour identifier des sources d'amélioration et de rationalisation des processus. » (Foucault, Panhaleux, Renaud, & Begasse, 2018)
Enfin, la phase d'amélioration s'effectue par la mise en place d'ajustements qui visent à proposer un nouveau plan de progrès et fait l'objet de la création d'un bilan annuel des activités du DPO. Il est requis de prendre en considération l'évolution du périmètre, les nouveaux traitements et les évolutions du règlement et des lois. (Foucault, Panhaleux, Renaud, & Begasse, 2018)

En complément de la roue de Deming, nous pouvons voir également la méthode DMAIC qui est la méthode du projet six sigma. Cette méthode est basée sur l'analyse des données dans le but d'optimiser et de stabiliser les processus de l'organisation. Les cinq phases de cette méthode sont : Définir (*Define)*, Mesurer (*Measure)*, Analyser (*Analyse)*, Améliorer (*Improve)* et Contrôler (*Control*).

Figure 7 - Méthode DMAIC (Fernandez, Comment utiliser la méthode DMAIC ? , 2018)

La première phase (*Define)* a pour but la définition des besoins métiers et la précision des objectifs et le cadrage du projet. Elle vise également la définition du périmètre, des ressources et des délais. Elle nécessite la cartographie du processus afin de mieux connaitre les problèmes et leur priorisation selon leur nature. Un problème d'un processus peut entrainer des dysfonctionnements sur d'autres processus. Le diagramme cause-effet peut être utiliser afin de suivre, mesurer, analyser et trouver des solutions.
La seconde étape (*Measure*) vise la collecte des données afin de mesurer la performance et d'acquérir une vision sur les progrès possibles.
La troisième phase (*Analyse)* est l'analyse soit l'utilisation d'outils dédiés à l'analyse pour repérer les causes de problèmes. Pour cette phase, il est nécessaire de connaitre les problèmes pour mettre en place les solutions adéquates afin de compléter l'écart entre la situation actuelle et les attendus.
La quatrième phase (*Improve)* est la phase d'amélioration. Il s'agit d'une phase de test pour les solutions retenues. Cette phase est précieuse pour l'identification et la mise en place de moyens correctifs.
Enfin, la dernière phase (*Control*) est la phase de contrôle. Il s'agit dans cette phase de suivre les actions mises en œuvre afin de prévenir tout retournement de situation. Cette phase peut nécessiter l'utilisation de documentation et de tableau de bord afin de permettre le pilotage dans la durée. Cette phase de contrôle nécessite un pilotage et une conduite du changement et le partage de connaissance. (Fernandez, Comment utiliser la méthode DMAIC ? , 2018)

C. Les risques attachés à la protection des données personnelles

La notion de risque occupe une place centrale dans la mise en place du Règlement Général sur la Protection des Données. Daniel Le Metayer, Directeur de recherche INRIA, a noté que les notions de risques et d'analyse d'impact sont présents plus de 100 fois dans le RGPD. La gestion des risques en interne et la responsabilisation des acteurs sont des enjeux réels lorsque l'on parle de protection des données personnelles. (Rispoli, 2016)

1. Identification des risques

La notion de risque se définit comme la « possibilité, probabilité d'un fait, d'un événement considéré comme un mal ou un dommage » (Larousse)
Cette notion a évolué lorsqu'elle est associée à la protection des données. Il existe un nombre important de vulnérabilités liées aux applications et aux serveurs. Ces risques ou vulnérabilités concernent désormais également directement les données et les processus s'ils sont mal maitrisés et protégés. Ainsi, si la sécurisation des systèmes d'information nécessitait l'installation de dispositifs tels que des pares feux, elle requiert aujourd'hui d'associer les parties prenantes. Le renforcement des processus nécessite un point de vue technique et humain par la mise en œuvre de sensibilisation. (Rispoli, 2016)
Les manquements conduisant aux risques sont de diverses natures. Ils peuvent être liés à l'absence de consentement de traitement des données ou de base légale pour le faire. Ces manquements peuvent également être associés au non-respect des droits individuels. Par exemple, on considère comme manquement si une entreprise n'est pas en capacité de répondre à une demande de droit d'accès dans la durée légale d'un mois pour le faire. Enfin, les manquements peuvent être associés à la violation des règles sur le transfert des données.
S'il permet de limiter les risques, une mise en œuvre mal gérée ou mal préparée du RGPD présente des risques aussi bien pour les acteurs que pour l'organisation en elle-même. Ces risques peuvent prendre différentes natures tant au niveau de l'image de l'organisation que d'un point de vue financier ou opérationnel.

a) Risque juridique

En cas de manquement ou de non-respect au Règlement Général sur la Protection des Données, l'organisation encourt un risque juridique. Celui-ci pèse essentiellement sur l'organisation en elle-même et sur son responsable de traitement mais peut également concerner les sous-traitants.

L'entreprise à travers son responsable de traitement est la première concernée par ce risque. En effet, en cas d'atteinte considérée comme grave, la CNIL comme autorité de contrôle peut dénoncer au Procureur de la République les manquements.
La CNIL a mis en place des sanctions graduées en fonction de la nature du manquement ou de violation du Règlement Général sur la Protection des Données, tout en s'appuyant sur les dispositions légales préexistantes notamment celles décrites par la Loi Informatique et Libertés. Le premier niveau de sanction est l'avertissement ou la mise en demeure de l'organisation reconnue comme fautive. Celle-ci reçoit également un rappel à l'ordre avec pour obligation la mise en conformité de ses traitements de données à caractère personnel. Le second niveau est l'injonction de cesser le manquement. Cette sanction peut conduire dans certains cas à l'injonction de limiter ou suspendre le traitement des données en cause, de manière temporaire. Le dernier niveau est la sanction administrative prononcée en cas de manquement aux principes et règles du RGPD. (Goldstein, 2019)

Les sanctions réellement prononcées sont généralement réduites à des sanctions administratives de la CNIL. Ces sanctions peuvent être la raison d'un certain désintérêt des entreprises au chiffre d'affaire conséquent. En 2014, la CNIL a condamné Google à 150 000 euros (maximum autorisé par la directive de 1995). Cette condamnation a permis de mettre en lumière le besoin de revoir les sanctions souvent inefficaces.
Récemment, la CNIL a sanctionné SPARTOO, la société de vente de chaussures en ligne, à une sanction de 250 000 euros accompagnée d'une astreinte pour divers manquements au RGPD parmi lesquels le « manquement à la sécurisation des données, au principe de minimisation des données, à l'obligation d'information des personnes ». (CNIL, 2020)

Depuis 2018, avec la mise en œuvre effective du Règlement Général sur la Protection des Données, les amendes administratives peuvent atteindre 20 millions d'euros ou jusqu'à 4% du chiffre d'affaire annuel mondial du groupe.

Le règlement renforce les obligations à l'égard du sous-traitant ce qui permet de répartir les relations entre le responsable de traitement et le sous-traitant. Ce dernier est soumis à des obligations telle que la tenue d'un registre ou l'obligation de sécurité. Le RGPD renforce également les obligations contractuelles du sous-traitant. Ainsi, le contrat liant le responsable de traitement et le sous-traitant doit être enrichi d'une clause relative à la protection des données précisant ainsi l'objet, la durée, la finalité du traitement ainsi que la liste des données traitées. L'absence de cette clause peut remettre en question la

légitimité du traitement concerné. Le sous-traitant doit être en capacité de montrer des garanties suffisantes permettant d'assurer l'existence de principes de sécurité et de confidentialité. Au même titre que les différentes mesures techniques et organisationnelles instaurées par le responsable de traitement, le sous-traitant doit également en mettre en œuvre afin de garantir la protection des données pour le compte du responsable de traitement. Le responsable du traitement dispose de l'obligation de surveiller leur respect.
Si le sous-traitant ne se conforme pas à ses obligations ou s'il agit hors des instructions du responsable de traitement, il sera alors responsable de « son » propre traitement. Il sera ainsi seul responsable en cas de manquement. En complément de la responsabilité qu'il a face au responsable de traitement, le sous-traitant pourra faire face à des sanctions pénales et administratives au même titre que le responsable de traitement.

b) Risque financier

Au-delà du risque juridique, le Règlement Général sur la Protection des Données instaure des sanctions financières très lourdes. Ce risque financier permet d'estimer l'étendue et la valeur des autres risques. Ainsi, une organisation qui ne serait pas en conformité avec le Règlement Général sur la Protection des Données encoure une sanction jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial de l'organisation.

Ce risque donne un aperçu de « l'état de santé de l'entreprise ». Ce sont en effet les conséquences de l'atteinte au risque juridique qui peuvent être graves pour l'entreprise et non le risque juridique en lui-même.

Citons à titre d'exemples quelques sanctions financières ayant été prononcées au cours de ces dernières années. En 2018, Optical Center (Les Echos, 2018) est sanctionné pour fuite importante de données sensibles à la suite d'une faille de sécurité ayant eu lieu en 2017. (CNIL, 2018)
En décembre 2018, Bouygues Telecom (Le monde, 2018) est condamné pour manquement à la sécurité des données pour les clients de la marque B&You. (CNIL, 2018)
En décembre 2018, Uber (BFM business, 2018) est condamné pour insuffisance de sécurité des données personnelles des utilisateurs. Ce manque de sécurité a entrainé le téléchargement d'informations de 57 millions d'utilisateurs dont 1.7 millions d'utilisateurs en France. (CNIL, 2018)
Google a également été condamné à hauteur de 50 millions d'euros pour manque de transparence, informations insatisfaisante et absence de consentement valable des utilisateurs pour le traitement de leurs données. La condamnation a aussi été prononcé pour personnalisation de la publicité.

c) *Risque d'image et risque business*

L'ensemble des sanctions précédemment décrites peut avoir un pouvoir dissuasif puisque les organisations ne veulent pas entacher leur image de marque pour manque de protection des données.
La gestion du risque d'image ou réputationnel est devenue un réel enjeu et une vraie préoccupation de management dans les années 1990. Pour mieux comprendre l'impact de la gestion de ce risque, nous pouvons citer à titre d'exemple les tribulations de Shell ayant eu lieu à la suite de sa décision de « couler la plateforme pétrolière Brent Spar en mer du Nord ». Malgré la prise en compte des potentiels impacts environnementaux, Shell n'avait pas anticipé les réactions de la population en réponse à cette action ni même la faculté des groupes de pression environnementaux à influer l'opinion publique. Cette pression a eu pour effet le boycott généralisé des produits et des stations Shell. Shell a surmonté la crise en effectuant une réorganisation interne. (Power, 2015)
Cet exemple démontre bien la force des groupes de pression et des médias à menacer la légitimité d'une organisation et à amplifier une situation. Il démontre également l'importance pour les organisations de prévoir toutes les mesures nécessaires permettant de maitriser une action.

La CNIL peut prendre la décision de rendre publique une sanction au regard de la gravité du manquement. Le risque d'image et de réputation est considéré comme un risque de second rang. Il touche la notoriété d'une organisation sur sa capacité à assurer et maintenir une protection des données à caractère personnel sur le long terme. Une défaillance dans la protection des données, une violation des données par un transfert inadéquat peut conduire à remettre en cause l'organisation.
De ce fait, ce risque peut conduire à une perte de légitimité vis-à-vis des clients de l'entreprise mais également des salariés de l'entreprise et du grand public. En effet, un manquement condamné peut conduire à la dégradation du climat social au sein de l'entreprise mais aussi dégrader les relations avec les partenaires sociaux. De plus, l'entreprise peut faire face à la perte de confiance ou à des plaintes de ses salariés en cas de manquements.

L'entreprise doit prendre en considération ce risque et disposer d'un budget utilisable pour améliorer son image. L'ampleur de ce risque est difficile à évaluer et résulte du niveau de conformité au RGPD.
Selon le sondage Opinion Way pour Havas paru en mai 2018, 8 Français sur 10 seraient prêts à « boycotter une entreprise » si celle-ci ne respecte pas les principes du RGPD. Dans ce même sondage, 55% d'entre eux sont prêts à démarrer une action en justice contre une entreprise si celle-ci porte atteinte à leur vie privée ou si elle ne respecte pas les obligations associées au Règlement Général sur la Protection des Données. (Salgues, 2018)

Afin de limiter les risques d'image, l'organisation se doit de communiquer, autant que possible et à tout niveau du traitement, sur les mesures qu'elle a prise afin de se mettre en conformité avec le RGPD. Cette communication peut se faire par la rédaction de mentions d'informations précisant les acteurs ayant accès aux données mais aussi des mentions expliquant de manière plus explicite le traitement des données réalisées. Ces mentions ou notices peuvent contenir les durées de conservation, rappeler les droits des personnes concernées mais aussi l'objet du traitement en lui-même ainsi que les destinataires et utilisateurs des données. L'ensemble de ces informations vise à prévenir les personnes concernées, à répondre à des interrogations potentielles mais également à être en conformité avec le Règlement Général sur la Protection des Données. En ayant ces notices ou mentions indiquées lors de la demande de collecte de données ou visible à tout instant du traitement, démontre la bonne volonté de l'organisation et son respect des données à caractère personnel de manière plus globale et donc son respect du règlement.

La CNIL pouvant décider de rendre public une décision de sanction, la presse représente un vecteur important afin de porter atteinte à l'image et la réputation d'une organisation. Celle-ci doit ainsi tout mettre en œuvre pour justifier sa mise en conformité et sa politique de gouvernance des données dans le respect du Règlement Général sur la Protection des Données.

Une organisation qui ne serait pas « *privacy-compliant* » accepte de prendre le risque d'avoir son image de marque dévalorisée. Ce risque d'image, précédemment décrit comme étant de second rang, a en fait toute son importance pour le business d'une organisation. En effet, ce risque ne peut être dissocié du risque business ou commercial d'une organisation qui est lui-même attaché au risque lié à la sécurité et la protection.
L'absence ou l'inefficacité de mesures de sécurité, qu'elles soient logiques ou physiques, peuvent conduire à une perte importante de données. Cette perte peut elle-même conduire à des sanctions, comme vu dans la partie précédente. En cela, en prenant le risque de ne pas disposer de mesures satisfaisantes de sécurité et de maitrise du patrimoine informationnel, l'organisation s'expose à un double risque, business et d'image, pouvant conduire à la perte de clients et à une baisse de son chiffre d'affaire.
Au contraire, prouver sa conformité et être en capacité de la justifier au travers de notices, mentions ou dans la presse peut représenter un réel avantage face à la concurrence. La mise en conformité peut ainsi représenter un sentiment de confiance et de sécurité qui peut se traduire par un levier de performance business et opérationnel non négligeable pour les organisations. Cet avantage concerne toute organisation et représente une opportunité pour l'ensemble des organisations.

d) Risque opérationnel, d'efficacité

Depuis le dispositif Bale II, le risque opérationnel est déterminé comme le « risque de perte résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'évènements extérieurs ». (Rispoli, 2016)
Le Règlement Général sur la Protection des Données apporte une analyse sur l'organisation des systèmes d'information. La mise en conformité ne peut se faire sans une prise en compte des risques opérationnels visant à acquérir une meilleure gouvernance des données. L'organisation se doit de définir les emplacements de stockage des données et de mettre en place des méthodes visant le respect des durées de conservation. Les exigences du RGPD nécessitent de repenser et de corriger les processus opérationnels informatiques et l'architecture des systèmes d'information.
Afin de diminuer le risque opérationnel, il est nécessaire de former les collaborateurs aux obligations du Règlement Général sur la Protection des Données. Développer de nouveaux outils est également nécessaire afin d'accroitre la collaboration entre le service informatique et les parties prenantes agissant sur la protection des données tel que le DPO.

Le risque d'efficacité ou de performance est lié à la performance de l'exercice des activités, tel que l'efficacité des processus et l'excellence opérationnelle. Ce risque est attaché à l'instabilité des procédures pouvant avoir des impacts sur la présence des ressources.

2. Evaluation des risques

Une gouvernance efficace exige l'identification des risques au sein d'une organisation, dans le but de les prioriser et de les traiter en listant les contrôles nécessaires. Une protection des données à caractère personnel efficace vise à surmonter chaque risque étudié dans la partie Identification des risques1 ci-dessus.

Le responsable de traitement a plus de responsabilités en cela qu'il doit disposer d'une documentation complète et à jour des traitements effectués. Celle-ci doit permettre de démontrer la conformité de l'organisation. La rédaction de documents de conformité est complétée par la réalisation d'analyses d'impact des risques. Ces analyses visent à obtenir une vision plus précise de l'analyse des risques pour certains traitements ayant été identifié comme sensibles ou à risque pour les personnes concernées.

a) *Présentation générale d'une analyse d'impacts*

À la suite de la mise en place du Règlement Général sur la Protection des Données, des formulaires de contrôle assurent la vérification de la conformité de traitement des données, l'identification et la minimisation des risques liés à la protection des données. La réalisation de cette analyse d'impacts est liée au principe d'« *accountability* » et l'obligation pour les organisations de suivre l'ensemble de leurs décisions, d'être en mesure de démontrer leur conformité et d'expliquer leurs actions.

Plusieurs termes existent pour désigner cette démarche d'analyse d'impact : DPIA ou *Data Protection Impact Analysis*, PIA ou *Privacy Impact Analysis*, EIVP pour Estimation des Impacts sur la Vie Privée ou encore AIPD pour Analyse d'Impact relative à la Protection des Données. (Foucault, Panhaleux, Renaud, & Begasse, 2018)

Cette démarche entre dans la mise en application des obligations du RGPD. Il s'agit d'un processus d'amélioration continue qui requiert parfois plusieurs itérations pour parvenir à un dispositif de protection de la vie privée acceptable. Ce processus s'impose dès lors que le traitement analysé implique des données sensibles, du profilage ou de la surveillance à grande échelle d'une zone accessible au public.

Cette démarche d'analyse des risques concerne en particulier neuf types de traitements.
Le type 1 est lié au « traitement de type « *scoring* » soit la cotation ou la notation, comprenant le profilage de personne, spécifiquement s'il s'agit de performances au travail, d'évaluations de situation économique ou de santé, de préférences personnelles ou d'habitudes, de déplacements… »
Le type 2 concerne les « traitements automatisés, à partir desquels sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire. »
Le type 3 concerne « la surveillance systématique à grande échelle d'une zone accessible au public. »
Le type 4 vise les traitements « de données sensibles (origine raciale, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données de santé) ou de données à caractère personnel relatives à des condamnations pénales et à des infections ». A noter qu'en France, la collecte de données sensibles liées à l'origine raciale, aux opinions politiques, aux conviction religieuses ou philosophiques est strictement interdite. Les données liées à la santé sont strictement réservées au domaine médical et au médecin du travail et ne peuvent être communiquées et transférées d'un service à un autre.
Le type 5 est relatif au « traitement à grande échelle de données à caractère personnel. Le terme « grande échelle pouvant se rapporter au nombre de personnes concernées, au volume de données à caractère personnel, à la durée de conservation, à la portabilité géographique du traitement. »
Le type 6 concerne « le croisement de fichiers. »

Le type 7 relève du « traitement concernant les personnes vulnérables, et notamment les enfants, les personnes âgées, les patients, les employés ».
Le type 8 traite du « traitement utilisant ce qu'on appelle encore « les nouvelles technologies » bien qu'elles soient courantes de nos jours (géolocalisation, objets connectés, réalité virtuelle, réalité augmentée, IA). »
Le type 9 vise le « traitement qui de lui-même empêche les personnes concernées d'exercer un droit, d'utiliser ou d'obtenir un service ». (Foucault, Panhaleux, Renaud, & Begasse, 2018)

Elle vise la conduite d'une analyse d'impact relative à la protection des données. Sa réalisation peut être demandée en complément de tout document de conformité de tout processus nécessitant le traitement de données à caractère personnel. En effet, conduire une analyse d'impacts est obligatoire si le traitement est susceptible de susciter des risques élevés sur les droits et libertés des personnes concernées (article 35 du RGPD).
Cet article 35 précise que « lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires» (Parlement européen, 2018)

Son objectif est la construction et la démonstration de la mise en place effective des principes de protection de la vie privée.

La démarche de conformité mise en œuvre en menant une DPIA repose sur deux piliers :

1. Les principes et droits fondamentaux, « non négociables », qui sont fixés par la loi et doivent être respectés, quels que soient la nature, la gravité et la vraisemblance des risques encourus ;
2. La gestion des risques sur la vie privée, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données. (CNIL, 2017)

La DPIA permet ainsi une évaluation poussée du système de traitement actuel basée sur une analyse des principes et des droits fondamentaux. Cette analyse est faite grâce à la description du traitement et du contexte. Plusieurs éléments sont nécessaires tels que l'identification des finalités, enjeux et durée de conservation des données, droits des personnes, identification des moyens de traitement des données.
Elle vise une étude des mesures mises en place initialement qui permettent d'assurer la protection des données personnelles.

Elle permet également une étude des risques sur la sécurité des données (abus, accès aux données personnelles, disparition des données) et sur le traitement (la divulgation, la détérioration, la corruption) avant de faire l'évaluation de la gravité des risques pour les droits et libertés des personnes physiques liées au traitement et de déterminer les mesures nécessaires pour y faire face,
Enfin, elle permet une prise de décision visant à prendre les mesures nécessaires à la minimisation des risques au niveau du traitement et la mise en place d'un plan d'action si mesures insuffisantes.

b) Démarche et principes de l'analyse d'impact

Cette méthode est conforme aux critères établis dans les lignes directrices du G29[6] et est aussi compatible avec les normes internationales de gestion des risques.
Les critères définis dans les lignes directrices du G29 sont « l'évaluation ou notation, la décision automatisée avec effet juridique ou effet similaire significatif, la surveillance systématique, les données sensibles ou données à caractère hautement personnel, les données personnelles traitées à grande échelle, le croisement d'ensembles de données, les données concernant des personnes vulnérables, l'usage innovant ou application de nouvelles solutions technologiques ou organisationnelles et l'exclusion du bénéfice d'un droit, d'un service ou contrat. » (CNIL, 2017) Ces neuf critères permettent de caractériser la notion de risque élevé.

L'analyse d'impact se réalise directement sur l'outil PIA mis à disposition par la CNIL en présence de quatre parties impliquées lors de sa réalisation, à savoir :

- Le rédacteur ou responsable de traitement qui répond aux différentes questions, valide l'analyse et s'engage à mettre en place le plan d'action défini durant le DPIA
- L'évaluateur qui émettre des commentaires sur les différentes réponses faites
- Le DPO qui émet un avis global sur le projet et élabore le plan d'action. Il se charge par la suite de vérifier sa bonne exécution
- Le validateur ou responsable de traitement

De manière générale, la DPIA doit se réaliser avant la mise en place du traitement. Il s'agit d'un processus itératif, en cela que les analyses effectuées doivent être revues et corrigées régulièrement notamment en cas de modifications notables sur les conditions de réalisation du traitement. Cette réalisation de DPIA est une pratique favorable visant la vérification que le traitement est bien conforme au RGPD et respecte la vie privée. Le traitement analysé peut être susceptible ou non de produire des risques importants sur la vie privée.

[6] Groupe de travail de l'article 29 qui réunit l'ensemble des CNIL européennes

L'analyse d'impact respecte le schéma de la norme ISO 27005 présenté dans le schéma ci-dessous.

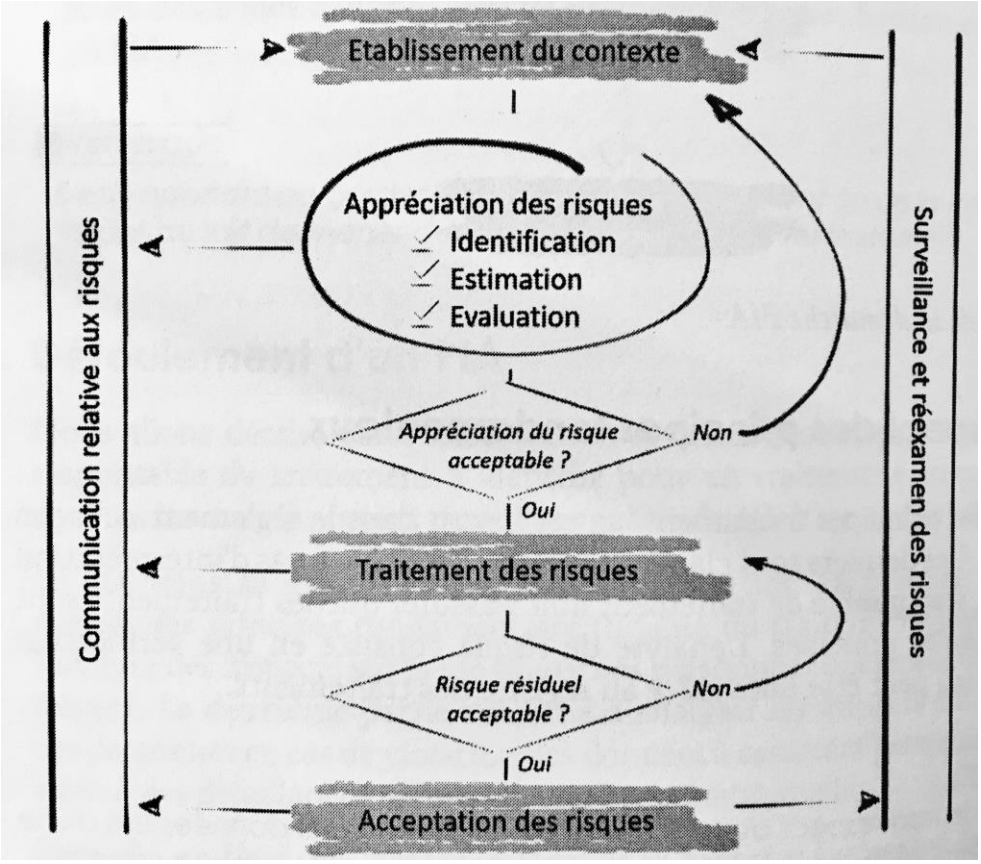

Figure 8 - Schéma norme ISO 27005 (Foucault, Panhaleux, Renaud, & Begasse, 2018)

La Figure 8 - Schéma norme ISO 27005 nous montre la démarche itérative que représente une analyse des risques proposée par la norme ISO 27005. Cette démarche s'aligne sur les phases de la roue de Deming *(Plan-Do-Check-Act).* La tâche principale de cette démarche est la phase de mise en place initiale qui permet l'estimation du risque. La partie évaluation dans l'appréciation des risques représente la phase d'analyse des risques. La démarche s'applique à la démarche d'analyse des risques décrite dans le Règlement Général sur la Protection des Données.
Une analyse d'impact est divisée en quatre étapes qui sont les quatre étapes classiques en matière de gestion et d'analyse des risques.
La première étape est la description du contexte du processus étudié. Cette étape permet d'interroger sur les traitements et leurs finalités. Cette étape vise également à connaitre les données concernées par ce traitement soit les données qui sont collectées et traitées. Enfin cette étape vise à comprendre les supports de données utilisés.

La deuxième étape nécessite les observations et commentaires sur les risques. Elle pose des questions sur les mesures existantes ou prévues dans le traitement qu'elles soient juridiques, liées à la protection et la sécurité ou liées à l'organisation.
La troisième étape permet de considérer les risques pour les droits et libertés des personnes concernées. Cette considération des risques vise à s'interroger sur les sources des risques, qu'ils soient redoutés ou qu'ils aient déjà eu lieu. Cela vise par la suite à évaluer leur vraisemblance et leur gravité. Cette étude permet de prendre les mesures adéquates afin d'agir sur les risques. De plus, cette étape aboutit sur une prise de décision avec la mise en place d'un plan d'action déterminé en accord avec l'ensemble des parties pour réduire les risques. Enfin, la quatrième et dernière étape est l'étape de validation.

Ainsi, comme évoqué, il existe de nombreux moyens permettant la mise en conformité et l'application d'un cadre légal tel que le Règlement Général sur la Protection des Données. Ces moyens permettent une revue des traitements et une identification des risques attachés à la protection des données personnelles. Une question persiste : le RGPD est-il une contrainte pour l'organisation ou, au contraire, une opportunité ?

D. Contrainte ou opportunité ?

Les organisations ont l'obligation de se mettre en conformité avec les exigences imposées par les normes et des règlements en vigueur sous peine de faire face à des risques importants ou des sanctions. Pour cela, comme nous avons pu le voir, les organisations ont une nécessité de prise de recul sur leurs traitements afin de les analyser pour connaitre leurs risques, identifier les manquements et ainsi éviter les sanctions. Une mise en conformité peut parfois imposer une refonte des processus.

Le Règlement Général sur la Protection des Données change la façon dont les organisations vont traiter les données des personnes. Il permet aux organisations d'être vigilantes sur les traitements qu'elles effectuent et sur le stockage des données dans l'optique de ne pas s'exposer à une violation de leur usage.

A première vue, une mise en conformité, en particulier au Règlement Général sur la Protection des Données ressemble à une contrainte supplémentaire pour les organisations. Il s'agit d'une contrainte externe qui impose un changement prescrit, progressif et imposé. Elle représente, en effet, une charge de travail importante pour les acteurs d'une organisation. Cette charge de travail se retrouve en particulier au sein de la direction des ressources humaines qui est responsable d'un nombre important de traitements de données au sein d'une organisation : la gestion de la paie, le recrutement, l'administration du personnel...

Le Règlement Général sur la Protection des Données impose aux organisations un certain nombre d'obligations comme des obligations organisationnelles et la nomination d'un délégué à la protection des données personnelles. Les organisations doivent aussi faire face aux obligations liées à la nature de leur traitement par la revue de conformité, la réalisation de documents de conformité et la cartographie des traitements des données. Elles doivent également mettre en œuvre des moyens humains et techniques afin d'être en capacité de respecter et d'appliquer les droits des personnes concernées. De plus, la mise en conformité implique une revue des moyens de collecte de données afin que la collecte des données personnelles réponde au principe de minimisation des données et qu'elle soit adéquate et pertinente. Le Règlement Général sur la Protection des Données peut conduire à la création de nouveaux processus afin d'être en conformité. Les organisations doivent disposer d'une base légale pour s'assurer d'être en conformité.
La mise en conformité est un travail long et complexe pouvant prendre des mois voire des années pour que celle-ci soit la plus complète possible. Elle doit être intégrée dans la mise en place de projets.

Toutefois, la mise en conformité n'est pas que contrainte. Il est important de voir cette mise en conformité comme richesse pour les organisations.
La mise en conformité permet aux organisations d'être plus transparentes et plus claires sur les traitements de données réalisées et ce, dès la collecte avec l'ajout de mentions dédiées qui exposent les finalités du traitement, les destinataires et la durée de conservation. Ce règlement permet aux organisations de repenser la manière d'utiliser les données, de renforcer et d'améliorer le contrôle des traitements tout en simplifiant la transmission des données.
Chaque mise en conformité permet la responsabilisation des acteurs afin qu'ils développent une certaine agilité à manipuler les données tout en adoptant une gouvernance des données adéquate.

Le Règlement Général sur la Protection des Données constitue un meilleur encadrement sur les questions de protection des données et de droits des personnes concernées. Il représente une opportunité d'adoption d'une réelle organisation autour des données visant à améliorer et sécuriser le traitement, à gagner en efficacité et finalement en productivité. (Foucault, Panhaleux, Renaud, & Begasse, 2018)
Grâce à la réalisation des documents de conformité et des cartographies des données, l'organisation dispose d'un avantage réel et peut choisir d'améliorer la qualité des données et la fluidité du processus. Cela permet aux organisations de repenser la manière d'utiliser les données, de renforcer et d'améliorer le contrôle des traitements tout en simplifiant la transmission des données. Ce travail de mise en conformité permet de réfléchir aux traitements qui pourraient être améliorés et vise à mieux connaitre le rôle de chacune des parties impliquées. L'organisation peut, à travers cette meilleure connaissance d'un processus, optimiser une partie ou la totalité de ce dernier.

Travailler sur les traitements et les processus offre à l'organisation une occasion d'améliorer sa communication auprès des personnes concernées afin de les informer au mieux sur les méthodes d'utilisation des données. Réfléchir sur les traitements et penser leur amélioration vise également à une meilleure connaissance des partenaires. Le Règlement Général sur la Protection des Données permet de placer les sous-traitants comme responsables à part entière des données qu'ils traitent.
Se mettre en conformité permet aux organisations de s'interroger sur les risques potentiels et vise ainsi à prendre les mesures adéquates en matière de sécurité des données. Cela peut conduire l'organisation à mettre en place des actions de sensibilisations des acteurs et d'adopter des solutions visant une meilleure sécurité. Ces questions de sécurité encouragent également les organisations à repenser leur politique de gestion des accès et habilitations et leur traçabilité. En incitant les organisations à protéger davantage leurs données, le RGPD favorise la préservation du patrimoine informationnel.

La mise en conformité est une démarche continue qui vise l'amélioration des processus de collecte et l'exploitation des données. Cette démarche continue permet la mise en place d'un climat de confiance aussi bien à l'interne, auprès des salariés, qu'à l'externe, auprès des clients ou des partenaires.
Il s'agit d'un levier de performance opérationnelle interne puisqu'il permet l'adoption de nouvelles pratiques impliquant une meilleure connaissance du patrimoine informationnel et une meilleure compréhension des principes de protection. La mise en conformité permet ainsi à l'organisation de suivre une stratégie unique.

Partie 3 – Approche de résolution

I. Démarche de recherche

A. Méthodologie

1. Rappel de la problématique

La gouvernance du patrimoine informationnel doit permettre d'acquérir une meilleure compréhension de l'information tout en ayant un langage commun, accessible à toutes les parties prenantes.
L'objectif de ce travail de recherche est d'engager une réflexion et discussion autour des normes et règlements comme opportunité de maitrise et de protection du patrimoine informationnel d'une organisation. Ce travail vise ainsi à distinguer les manières avec lesquelles la mise en conformité contribue à la maitrise du patrimoine informationnel. Il vise également à montrer de quelles manières la mise en conformité peut former un levier de performance opérationnelle interne pour les organisations. L'étude portée dans ce mémoire s'intéresse aux moyens mis en œuvre par les organisations afin de garantir cette mise en conformité ainsi qu'aux avantages et des inconvénients issus de cette mise en conformité.

Plus particulièrement, ce travail met en lumière la mise en application du Règlement Général sur la Protection des Données au sein d'un service RH.
Au cœur du flux et du traitement du patrimoine informationnel, ce dernier est amené à traiter des données à caractère personnel d'une organisation. La mise en conformité au RGPD est donc devenue un sujet clé pour les organisations dans leur ensemble et notamment pour les services RH. Les directions des ressources humaines doivent s'interroger sur ce sujet.

Comme discuté, dans un contexte où la technologie et le numérique nous entourent et où nous faisons face à la croissance accrue du volume des données, le contexte règlementaire est le reflet des normes sociales. Il cadre les systèmes d'information au sein d'une organisation. La mise en conformité peut être un moyen de compréhension du système d'information. Elle permet d'établir et d'adopter une méthodologie de mise en œuvre ayant pour objectif la gestion et la protection du patrimoine informationnel.
Le Règlement Général sur la Protection des Données apporte une évolution sur la maitrise et la protection du patrimoine informationnel et c'est en cela qu'il encourage les organisations à s'interroger sur les supports de stockage des données et leur typologie. Il les encourage aussi à mettre en place des moyens contribuant à la maitrise et la protection du patrimoine informationnel.

Quels sont ces moyens dans la pratique ? Quelles actions doivent être mises en place par les organisations ? Quels sont les impacts pour les organisations ? De quelles manières la mise en conformité peut contribuer à la maitrise du patrimoine informationnel et former un levier de performance opérationnelle interne ?

Lors de la revue de littérature, des éléments de réponses ont pu être apportés à une partie de ces questions. Il existe un cadre légal très vaste qui implique de nombreuses obligations pour les organisations. De nombreuses mesures doivent être prises par les organisations afin de s'y conformer. Les enjeux d'une mise en conformité et les méthodologies de sa mise en œuvre ont également été décrits. Celles-ci peuvent se traduire par la mise en place d'une documentation et l'existence d'outils adéquats répondant aux enjeux de mise en conformité et à l'application d'un cadre légal comme le RGPD. Par la compréhension de ce cadre légal et des enjeux d'une mise en conformité, certains grands principes liés à l'évaluation des risques attachés à la protection des données personnelles ont pu être avancés.

Cette seconde partie vise à adapter cette théorie à la pratique et ainsi discuter de quelles manières la théorie peut être adoptée dans les organisations, notamment dans un service RH, au quotidien. A travers le partage d'éléments réels, elle vise ainsi à mieux comprendre les moyens qu'une organisation peut mettre en place.

2. Présentation des hypothèses

La revue de la littérature et l'approche pratique du sujet ont permis de déterminer plusieurs hypothèses que ce travail de recherche permet de vérifier ou d'infirmer.

La première hypothèse est le fait que la méconnaissance des faits pratiques des règlements est due à une présentation trop théorique ou générale. Cette présentation manquerait d'exemples pratiques à adapter au quotidien. Cette présentation trop théorique ne donnerait pas les moyens pratiques pour une mise en application effective du cadre légal.

La seconde hypothèse est le fait que cette méconnaissance des faits pratiques influe sur la mise en conformité réalisée par les parties prenantes des organisations, en particulier les responsables de traitement. Tout comme l'approche trop théorique et généraliste des formations serait un frein à la mise en application du cadre règlementaire, la méconnaissance des faits pratiques serait également un obstacle pour cette mise en conformité.

Ces deux premières hypothèses montrent que les manques de connaissances humaines peuvent être considérées comme étant au cœur du problème.

La troisième hypothèse est celle selon laquelle la sensibilisation des acteurs est le préalable nécessaire à toute mise en conformité. Si les acteurs font face à une information trop généraliste et une méconnaissance des faits, l'un des moyens permettant de combler ces manques serait de les sensibiliser et former aux enjeux et aux bonnes pratiques. Cela pourrait conduire à la mise en place d'une conduite de changement permettant à terme la mise en place de nouvelles pratiques.

La quatrième hypothèse est celle selon laquelle la mise en conformité est vue comme contrainte. Elle serait appréhendée comme une activité longue et complexe à mettre en œuvre. De plus, cette mise en conformité serait perçue comme un frein aux activités de l'organisation. Considérée comme peu productive, les parties prenantes délaisseraient le sujet et ne verraient pas les bénéfices cachés et visibles d'une mise en conformité.

Chacune de ses hypothèses a permis de guider la réflexion tant au niveau de l'approche théorique que de l'approche de résolution qui est présentée ci-dessous.

3. Présentation de la méthode choisie

L'utilisation d'une méthode lors d'un travail de recherche est essentielle car elle expose le procédé choisi pour atteindre un but. Cette méthode ne présente pas la solution mais la manière pour l'atteindre en associant les connaissances théoriques à la pratique. Dans le cas de ce travail de recherche, le but à atteindre est de présenter le cadre règlementaire existant, constitué des normes et règlements, comme une opportunité de maitrise et de protection du patrimoine informationnel pour les organisations. Plus précisément, l'objectif est de montrer les moyens à mettre en œuvre par les organisations pour assurer une mise en conformité efficace.
Plusieurs méthodes de recherche existent. Elles sont classées selon deux types : quantitatives ou qualitatives. La méthode quantitative se traduit par la recherche des faits pour analyser des résultats chiffrés tandis que la méthode qualitative repose sur des interprétations et des expériences pratiques afin de répondre à une question de recherche.

Dans le cadre de ce travail, il a semblé opportun de choisir la méthode qualitative pour traiter la question de recherche. En effet, cette méthode descriptive s'appuie une recherche documentaire ainsi que sur des expériences pratiques de terrain avec leurs interprétations et significations. Les observations tout comme les entretiens sont par ailleurs les fondements de cette méthode de recherche. Les résultats ne sont alors pas chiffrés mais décrit de manière explicative avec des mots.
Les hypothèses exprimées précédemment comme les solutions, qui seront présentées par la suite, sont extraites d'une approche pratique du sujet. L'utilisation de cette

méthode de recherche pour traiter la question a pour objectif la compréhension des comportements observés et les pratiques en place. Ainsi, les données qui seront utilisées proviennent de constats, d'observations et d'entretiens.

La conceptualisation est utilisée afin de compléter cette méthode de recherche. Il s'agit de regrouper différents exemples pour constituer une idée globale sur un sujet. L'objectif de la conceptualisation est de générer une idée globale ancrée sur la connaissance du monde et de la société. Ici, il s'agira d'apporter une conceptualisation à partir de ce qui a été observé sur le terrain ainsi que des ressentis sur le sujet de certains acteurs La problématique de ce travail de recherche constitue un fil conducteur à suivre pour la recherche d'un concept.

B. Présentation du terrain de recherche

1. Contexte général des activités

Atos est une « entreprise de services du numérique (ESN) française » créée à partir d'une fusion en 1997. Elle fait partie des 10 plus grandes ESN au niveau mondial grâce à un chiffre d'affaire de 13 milliards d'euros en 2017. (Wikipédia)
« Leader international de la transformation digitale », le groupe est, en effet, leader européen dans les domaines du Cloud et de la cybersécurité. Disposant d'une base mondiale de clients, il apporte « des services d'infrastructure et de gestion de données ». Ainsi, le groupe offre des services transactionnels, des solutions de conseil, d'intégration de système et d'infogérance ». Enfin, il aide ses clients à accomplir leur vision de l'entreprise de demain et délivre les technologies visant l'accélération de leur développement. (Atos, 2020)

La raison d'être d'Atos est de participer à la construction de l'espace informationnel. Ancien président-directeur général, Thierry Breton a déclaré que « les données personnelles et professionnelles des résidents européens font partie d'un espace informationnel qui se doit d'être règlementé, encadré et surveillé… par l'Europe. » (Feugey, 2013) En particulier, il a expliqué que « les données, c'est l'or numérique, l'or noir de demain. » Il considère comme nécessaire que l'espace informationnel soit règlementé et organisé comme l'ont été les espaces terrestres, maritimes et aériens. (Labialle, 2019)

La responsabilité de l'organisation est de contribuer à structurer, rendre sûr et accessible tout l'espace informationnel. Pour y parvenir, sa raison d'être repose sur trois piliers parmi lesquels la garantie de la « sûreté, la sécurité et la confiance dans l'espace informationnel » (Atos, 2020) Elle est inscrite comme suit dans les statuts de l'entreprise : « Avec nos compétences et nos services, nous supportons le développement de la connaissance, de l'éducation et de la recherche dans une approche pluriculturelle et contribuons au développement de l'excellence scientifique et

technologique. Partout dans le monde, nous permettons à nos clients et à nos collaborateurs, et plus généralement au plus grand nombre, de vivre, travailler et progresser durablement et en toute confiance dans l'espace informationnel. » (Atos, 2020)

Le sujet de la protection des données est un sujet d'actualité pour l'ensemble des entreprises. Il s'agit d'une préoccupation de premier plan pour Atos qui considère les données comme un actif précieux et stratégique. Ainsi, l'organisation propose un programme complet afin d'aider à la préparation au RGPD et à assurer la conformité en continue après sa mise en œuvre.

Le terrain de recherche choisi se situe au sein de la direction des ressources humaines France d'Atos. Cette direction rassemble plusieurs services composés de « fonctions support » telles que la direction des affaires sociale, le département lié au développement des carrières et à la formation, le *Workforce management*, le département lié aux rémunérations et avantages sociaux et le CSP-RH, qui est le cœur du terrain de recherche.

Le CSP-RH est le centre d'expertise paie du groupe Atos pour la France. Il rassemble plusieurs pôles : le pôle Paie & Administration du Personnel, le pôle Santé, le pôle SIRH & Contrôle de gestion sociale, les postes centrés sur les *Process* et le *Knowledge Management* , la gestion de projets RH et les outils paie administration.
Le pôle « SIRH & Contrôle de Gestion Sociale » se découpe en deux axes clés: « SIRH » et « Contrôle de Gestion Sociale ». Au niveau « SIRH », il réalise une expertise du fonctionnement des systèmes d'information utilisés. Il participe à la transformation des systèmes d'information actuels et à la mise en place de nouveaux projets d'optimisation et de digitalisation des processus RH. Il agit également lors de la correction de bugs et l'exécution de tests. Au niveau « Contrôle de Gestion Sociale », il procède au traitement des données des collaborateurs et à la gestion des contrôles sur les reports.
De plus, ce pôle est un acteur clé au sein de la direction des ressources humaines pour la coordination et la mise en place d'actions liées à la mise en conformité au Règlement Général sur la Protection des Données pour les différents logiciels ou progiciels utilisés dans les fonctions RH.
Au cours de mon alternance, j'ai pu avoir différentes missions liées à la mise en application du RGPD telles que le suivi et la coordination de la rédaction de documents de conformité et des analyses d'impacts pour les outils RH utilisant des données personnelles des collaborateurs ou la mise en place de sensibilisation au RGPD de la population RH.

2. Constats

La recherche de conformité prend une place importante dans l'ensemble des projets de l'équipe « SIRH et Contrôle de gestion sociale » afin d'assurer l'encadrement des traitements d'informations.
Entre discussions avec l'équipe DPO, rencontres avec les responsables de traitements, et échanges avec les sous-traitants, la mise en conformité est devenue un réel enjeu et responsabilité pour ce service. En effet, deux personnes sont en charge de la revue et la coordination de la mise en conformité pour les processus RH.

Il y a deux ans et à la suite de l'entrée en vigueur au Règlement Général sur la Protection des Données, aucune action n'avait été amorcée pour la mise en conformité au niveau local France pour les processus RH. Aucun dispositif n'existait afin de répondre à l'exercice des nouveaux droits des personnes concernées. L'entrée en vigueur du Règlement Général sur la Protection des Données a accéléré ce travail en accordant une place plus importante pour les sujets liés à la maitrise et la protection du patrimoine informationnel.
De nouvelles responsabilités ont ainsi été attribuées au CSP-RH et en particulier à l'équipe « SIRH et Contrôle de gestion sociale » afin d'assurer le respect du règlement. Pour y répondre, une nouvelle organisation du travail et de nouvelles réflexions ont dû être menées. Ainsi, des étapes préalables ont été nécessaires. Tout d'abord, un travail de compréhension, de réflexion et d'analyse de l'existant a été mené. Il a également fallu se renseigner plus en détail sur les attendus réels du Règlement Général sur la Protection des Données.

Comme énoncé dans les hypothèses, un long travail s'amorçait pour le CSP-RH d'Atos comme pour une grande partie des entreprises en France qui devait démarrer ce travail de mise en conformité. Les premières actions ont été mises en place au début de l'année 2019.

A l'heure actuelle, de multiples actions ont été menées. Quelles soient achevées, en cours ou à venir, ces actions requièrent un réel investissement de la part de l'ensemble des acteurs internes de l'organisation Atos. Ces derniers ont connaissance de l'existence du Règlement Général sur la Protection des Données et des problématiques en matière de maitrise et de protection du patrimoine informationnel. Toutefois, il existe des écarts entre le niveau de connaissances entre les acteurs. Une partie d'entre eux sont pleinement sensibilisés au sujet alors qu'une autre partie dispose d'une connaissance approximative du sujet.

Si des actions ont été menées, des écarts sont à noter entre celles menées au niveau groupe et celles menées au niveau local, à l'échelle de la direction des ressources humaines.

II. Propositions

« L'intelligence économique peut être définie comme l'ensemble des actions de recherche, de traitement, de diffusion et de protection de l'information utile aux différents acteurs économiques. Ces acteurs sont conçus comme un système global destiné à inspirer la stratégie de la direction générale de l'entreprise, tout comme à informer en continu et à innerver ses différents niveaux d'exécution, afin de créer une gestion offensive et collective de l'information, qui devient une richesse principale. » (Rouach, 2016)

Comme évoqué dans la partie État de l'art, les normes et règlements font émerger de nouveaux modes de fonctionnement en matière de gestion et protection du patrimoine informationnel, en particulier au niveau des données personnelles. Toutes les entreprises, quelque soit leur taille et leur domaine, sont concernées par ce devoir de mise en conformité, qu'elles soient propriétaires, utilisatrices ou hébergeurs de données. L'ampleur du travail, l'apparente complexité et les échéances du Règlement Général sur la Protection des Données peuvent le rendre intimidant. Cependant, les pénalités prévues par la CNIL incitent à l'approcher avec une volonté sans faille.
Projet d'organisation incontestable, le Règlement Général sur la Protection des Données va au-delà de l'unique dimension réglementaire et doit nourrir la transformation numérique. Véritable bouleversement pour les entreprises, il impose de disposer d'une approche dynamique associée à la mise en œuvre de processus organisationnels et de contrôles de sécurité. L'enjeu de cette mise en conformité se place sur la durée et sur le fait d'être en capacité de le démontrer.

Dans un environnement en perpétuel changement et où la donnée joue désormais un rôle central, il s'agit pour l'entreprise d'un défi majeur qui s'inscrit au cœur même de sa transformation digitale. Bien plus qu'un projet, se conformer au RGPD relève d'une démarche globale, structurée et dans la durée.
Cette démarche débute par la nécessité de réaliser un état des lieux de l'existant associé à un besoin de sensibilisation des parties prenantes. Elle n'est possible que par la mise en place d'une gouvernance capable de fédérer l'ensemble des métiers et des parties prenantes au sein de l'organisation. Il est important que l'ensemble des métiers soit impliqué afin que les mesures de mise en conformité soient correctement intégrées dans l'ensemble des processus de l'organisation. Cela nécessite d'établir un cadre organisationnel, décisionnel et de suivi.
Cette démarche vise la mise en place d'une conduite de changement par la mise à jour des processus métiers. En outre, si la dimension métier est importante, la dimension technique l'est tout autant par la mise en place de mesures de sécurité.
Si une transposition de cette démarche devait être faite à l'architecture des systèmes d'information, les couches métier, fonctionnelle, applicative et technique seraient impliquées. En effet, le métier est celui qui a la connaissance des processus et des différentes fonctionnalités (couche fonctionnelle). De plus, le métier doit connaître les

flux de données (couche applicative), et l'emplacement des données (couche technique). Chacune de ces couches permet de répondre aux questions « Pourquoi ? », « Qui ? », « Quoi ? », « Comment ?» et « Avec quoi ?».

En s'appuyant sur la revue de littérature et sur l'approche pratique sur le terrain, il a paru essentiel de diviser cette démarche en trois axes :

- la sensibilisation des acteurs
- l'organisation de la conformité par l'inventaire et la documentation
- l'implémentation de nouveaux processus

A. Sensibiliser les acteurs

« Knowledge is that you can put into. »[7] *- William James*

Le premier problème rencontré est inhérent aux lacunes humaines et à la méconnaissance des faits pratiques.
La formation est un enjeu crucial au cœur de la stratégie de maitrise et de protection des données et de la mise en œuvre d'une démarche dédiée.
Sensibiliser permet en premier lieu d'informer les parties prenantes sur la définition réelle du Règlement Général sur la Protection des Données. Au-delà d'informer, sensibiliser permet de rappeler le cadre légal avec ses enjeux et les nouvelles obligations en matière de réponse aux demandes d'exercice de droits par les personnes concernées. La sensibilisation vise à rappeler les devoirs et les risques encourus tant d'un point de vue financier avec les sanctions prévues par la CNIL pour l'organisation que les risques potentiels au niveau d'un service. Sensibiliser les acteurs comporte aussi un rappel des moyens à disposition et des outils existants en matière de sécurisation des données personnelles. Enfin, à l'issue de la sensibilisation un rappel des contacts des acteurs principaux peut être fait.

Le fait d'organiser des sensibilisations permet de cibler les acteurs et de répondre à des besoins spécifiques. De plus, sensibiliser les acteurs permet de responsabiliser les acteurs sur leur rôle et sur l'impact au niveau d'un service et au niveau de l'organisation. Responsabiliser les parties prenantes permet de les rendre acteurs de cette mise en conformité. Des acteurs capables d'informer à leur tour et de répondre aux obligations légales. La notion de responsabilité, *« accountability »,* est un des principes juridiques fondamentaux du Règlement Général sur la Protection des Données.

[7] « Le savoir est ce que vous pouvez mettre en action. »

La **première étape** est liée à la préparation, la compréhension et l'assimilation. En effet, cette première étape a pour but de définir les objectifs de la mise en place d'une sensibilisation.

Que cherche-t-on à développer comme compétences ou connaissances par ce biais ?

Dans le cas d'étude présent, l'objectif était d'apporter des clés pratiques pour la compréhension et la mise en œuvre de la mise en conformité au RGPD.

Le texte n'est pas simplement lié à la conformité mais a pour objectif de transformer les exigences en levier de performance opérationnelle. Il vise l'accompagnement de l'entreprise dans sa transformation digitale. Cette transformation ne relève pas uniquement des changements apportés au digital mais relève de la gouvernance des données afin d'avoir une vue globale sur les actions à réaliser.

Cette première étape s'effectue en réalisant d'une part une analyse d'écart entre les sensibilisations existantes et le besoin sur le terrain, et d'autre part une analyse entre compétences réelles et celles souhaitées.

Dans le cas présent, il existait une formation interne obligatoire prodiguée à tous les nouveaux salariés disponible en ligne qui présentait de manière globale et théorique le règlement. Une absence de présentation de cas pratiques avec une présentation des moyens existants et pouvant être mis en œuvre a été soulevé à de nombreuses reprises comme manquant à la formation existante.

Cette étape de compréhension et d'assimilation a permis la constitution d'un support de formation prenant la forme d'un support PowerPoint.

Seconde étape pour parvenir à sensibiliser les acteurs, l'organisation nécessite le pilotage et l'identification des parties prenantes à sensibiliser.

La sensibilisation est-elle à destination d'un service composé de quelques personnes ou est-elle à destination d'une direction dans sa globalité et qui regroupe ainsi plusieurs corps de métiers ?

L'origine de la cible et sa taille permet d'adapter aussi bien le discours et le contenu qui sera présenté lors de la sensibilisation que le format choisi.

Cherche-t-on à être général et à présenter simplement les enjeux ou cherche-t-on à être spécifique en axant sur des besoins particuliers ?

Ci-dessous une cartographie simplifiée des acteurs ayant eu un rôle essentiel dans la mise en place de sensibilisation.

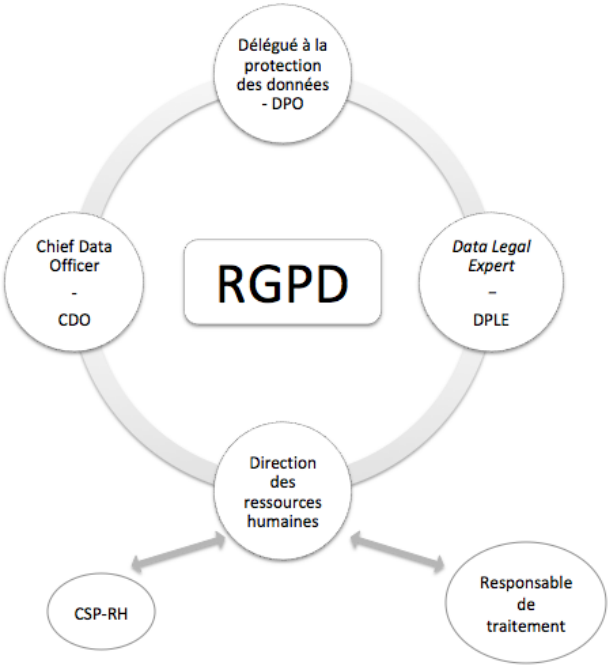

Figure 9 - Cartographie des acteurs

Chaque acteur présent sur la carte ci-dessus dispose d'un rôle à jouer dans la sensibilisation des parties prenantes et se doit d'être impliqué lors de sa constitution. Dans le cas étudié, le CSP-RH est l'initiateur et le porteur de cette sensibilisation pour la population RH qui regroupe des responsables de traitement des données. La direction des ressources humaines agit comme sponsor de cette démarche. Elle valide l'action de mener une sensibilisation, aide à définir les meilleures dates et enfin communique auprès des acteurs les informations relatives à la sensibilisation. Enfin, les équipes DPO et DPLE agissent comme soutient et ont pu confirmer et valider les informations renseignées dans le support de formation.

Dans le cadre de la sensibilisation au Règlement Général sur la Protection des Données, la cible était dans un premier temps un service rattaché à la direction des ressources humaines avant de globaliser la sensibilisation à l'ensemble de la population RH au niveau local France.
Le fait d'avoir eu une première cible pouvant être considérée comme un échantillon représentatif a permis d'améliorer la sensibilisation en apportant de nouveaux éléments aussi bien au niveau théorique que pratique.

La **troisième étape** est la réalisation et l'exécution de la sensibilisation. Il s'agit d'assurer les sessions de sensibilisation et de retenir l'attention de la cible choisie sur un thème défini et communiqué à l'avance. Cette étape est cruciale afin de conseiller les « apprenants » et transmettre les bons messages. Ces derniers encourageront le démarrage d'un nouveau travail autour de l'organisation de la conformité et de la mise en œuvre d'actions. Enfin, ils permettront, à travers la diffusion d'un guide de bonnes

pratiques, de déclencher une conduite de changement au quotidien avec l'adoption de nouveaux comportements afin d'être plus en maitrise du patrimoine informationnel et d'en assurer une plus grande protection.
Cette troisième étape permet de se confronter aux interrogations des acteurs et à son impact sur le fonctionnement interne. Lors d'une sensibilisation, plusieurs profils peuvent être rencontrés :

- des acteurs inconsciemment incompétents c'est-à-dire qui ont conscience de ne pas savoir ce qu'ils ne connaissent pas et qui n'ont ainsi pas de recul sur le sujet puisqu'il leur est totalement inconnu. Lors de la sensibilisation sur le terrain, aucune personne n'avait ce profil ;
- Des acteurs consciemment incompétents c'est-à-dire des acteurs conscients de ne pas tout savoir. Ils sont conscients de ne pas disposer de tous les éléments sur le sujet ;
- Des acteurs consciemment compétents qui sont dans une vision où ils connaissent ce qu'ils ont acquis comme connaissances. Ils sont capables d'appliquer au quotidien ce qui est transmis lors de la sensibilisation mais cherchent à s'améliorer en continue afin d'avoir plus de maitrise ;
- Des acteurs inconsciemment compétents qui n'ont pas conscience de leurs connaissances. Ces acteurs sont capables d'agir grâce à son inconscient, de manière automatique. Ils peuvent expliquer à d'autres acteurs leurs connaissances.

Ces quatre profils nécessitent d'adapter le discours afin de répondre aux attentes de chacun.
Un suivi des impacts pourra être fait afin de réaliser une vérification et un contrôle.

Une sensibilisation permet d'apporter des réponses. Pour effectuer un suivi des questions et des réponses apportées, un document de foire aux questions (FAQ) peut être initié afin d'annoter les questions, le contexte qui a amené cette question ainsi que la réponse associée. À l'issue de la sensibilisation, une nouvelle réflexion destinée à l'amélioration du support peut être initiée. De même, des besoins de sensibilisation spécifique peuvent être identifiés grâce à une sensibilisation générale apportant des cas pratiques. Ainsi, une sensibilisation est amenée à être complétée, modifiée et adaptée en continu.

La mise en place d'une sensibilisation est un travail dans la durée qui nécessite de discuter avec les bons acteurs au sein de l'organisation mais doit également s'appuyer sur une bonne documentation qui pourra être facilement transmise.

B. Organiser la conformité : Entre inventaire et documentation

« Organiser la collecte du renseignement, optimiser les processus de valorisation de la juste information, rendre l'entreprise et ses décideurs plus intelligents et orientés vers l'action devient un outil de souveraineté qui garantit la pérennité de l'entreprise » (Rouach, 2016)

« Gouverner, c'est prévoir » - Emile de Girardin

Si la sensibilisation des acteurs est une étape essentielle et obligatoire à la mise en conformité, elle ne constitue qu'une première étape permettant d'aligner le niveau de connaissances et de montrer la nécessité de l'implication des acteurs. En effet, chaque acteur est une clé indispensable pour la mise en conformité. La sensibilisation constitue un fondement nécessaire afin d'organiser la conformité.
Organiser la conformité nécessite une méthodologie rigoureuse avec analyse de l'existant et ajustement afin d'être apte à gérer et prévoir les risques.

La **première étape** est celle de la planification qui vise à identifier les besoins et définir un cadre et périmètre d'étude pour cibler les processus à étudier. Ce cadrage est nécessaire comme pour tout programme de transformation. Le délégué à la protection des données personnelles ou DPO travaille en étroite collaboration avec le chef de projet identifié pour accompagner et effectuer un suivi tout en s'assurant de la mise en conformité. Le cadrage définit la feuille de route à suivre pour l'identification des principaux acteurs à contacter et rencontrer. Le périmètre défini vise l'analyse de l'existant afin de réaliser un inventaire des processus et des données personnelles traitées par l'organisation. Les informations collectées permettent la connaissance du fonctionnement interne de l'organisation et la compréhension de la responsabilité de chaque acteur.
Dans l'étude en présence, il s'agit de l'inventaire des processus RH traités au niveau de la direction des ressources humaines ou confiés à ses prestataires ou sous-traitants.
La réalisation de cet inventaire est un travail long et continu qui nécessite la connaissance des acteurs, de leur rôle dans l'organisation et des processus métiers. Ce travail vise à lister les processus, son responsable de traitement et son domaine d'application. Il est une base pour l'élaboration du registre des traitements des données personnelles qui est indispensable à la mise en conformité au Règlement Général sur la Protection des Données.

Une fois l'inventaire réalisé, un plan d'actions est identifié pour l'évaluation des processus, la réalisation des documents de conformité, l'identification des risques liés à la gestion des données personnelles réalisée dans un traitement, la réalisation d'analyse d'impact des risques et la mise en place d'actions visant l'amélioration des processus étudiés.

Le Règlement Général sur la Protection des Données requiert l'évaluation et la réévaluation continue de l'ensemble des processus et des risques associés.

La **seconde étape** vise donc cette évaluation des processus. Pour y parvenir, il est essentiel que l'implication et la responsabilité des parties prenantes soient réelles et actives. L'évaluation des processus nécessite la réalisation de documents de conformité qui se présentent sous la forme de formulaire de conformité et de contrôle. Cette évaluation s'intègre en amont de la mise en place d'outils ou sur le *legacy* soit l'existant. Elle permet le renseignement de toutes les informations relatives au traitement des données. Ce formulaire vise le respect de l'obligation légale, imposée par le RGPD, de disposer d'un registre des traitements. Il vise la vérification de l'adoption de l'ensemble des principes de protection des données associée à l'identification et la minimisation des risques liés à la protection des données. Il apporte la réponse à différentes questions telles que : *Qui est le responsable de traitement ? Quel est l'objectif du traitement ? Quelles sont les données personnelles et sensibles concernées par le traitement ? Quels sont les supports de données utilisés ? Quelles sont les durées de conservation ? Le processus fait-il appel à des sous-traitants ? Le traitement permet-il d'assurer la modification, suppression ou l'extraction des données en cas d'exercice de droits de la part des personnes concernées ?*
La liste complète des questions peut être consultée en annexes.

Cette évaluation de contrôle et de conformité est à remplir pour l'ensemble des logiciels ou de progiciels impliquant le traitement de données personnelles au sein d'une organisation.
Dans le cas d'étude, une cinquantaine de traitements a été répertorié dans la phase 1 de planification et d'inventaire. Ces traitements ne concernent que la direction des ressources humaines et sont liés aux différents services. Le délégué à la protection personnel (DPO) est le propriétaire du formulaire utilisé et le communique aux responsables de traitement ou au chef de projet afin de permettre sa complétion.
Afin de compléter ce formulaire, l'organisation de réunions d'étude et de suivi avec les responsables de traitement est nécessaire pour comprendre la logique de fonctionnement du processus, les flux d'informations et les interactions existantes entre les acteurs intervenant lors du processus. Il s'agit aussi d'amener les organisations à s'interroger sur l'emplacement des données et d'évaluer pour chacun des progiciels leur intégration et traitement.

Cette évaluation permet de s'interroger sur les accès des utilisateurs ayant une lisibilité sur les données personnelles en lecture mais également ceux qui effectuent un traitement sur ces mêmes données. Le responsable de traitement doit ainsi s'interroger sur les rôles et privilèges d'accès et s'assurer qu'une mise à jour régulière de ces accès est effectuée. Cette revue des accès peut être réalisée dans le cadre d'une politique spécifique propre au traitement étudié. La finalité de cette revue est de s'assurer que seule les parties prenantes concernées ont accès aux données afin d'éviter tout risque de

fuite ou suppression par exemple ou simplement d'accès illégitime aux données. Par exemple, une personne ayant changé de poste et de service au sein de la même entreprise ne doit plus avoir les accès liés à son ancien poste.

La réalisation de ces documents de conformité est assimilable au fonctionnement de la roue de Deming. En effet, elle se divise en quatre phases :

- Une phase *PLAN*, ou initiale de recherche d'informations, lecture de documentations existantes en interne, utilisation de l'outil, rencontre avec les responsables de traitement ;
- Une phase *DO,* ou de réalisation visant à remplir le formulaire ;
- Une phase *CHECK,* ou de contrôle par la vérification du formulaire par le responsable « *Owner* » de l'outil et l'équipe DPO et la validation finale par le délégué à la protection des données. A l'issue de cette phase, une phase de correction peut être déclenchée afin d'apporter des précisions sur le premier formulaire transmis. Cette modification du formulaire initial est associée à un retour vers la phase *DO* ;
- Une phase *ACT* avec la mise en application du plan d'action défini à l'issue de la complétion des documents de conformité.

De plus, cette évaluation permet de s'interroger sur la sécurité établie par la réalisation d'un audit sécurité. Celui-ci intervient en complément de la réalisation du document de conformité. Il vise la connaissance du niveau global de sécurité pour un système d'information. Il permet l'identification et l'optimisation des mesures de sécurité établies afin de s'aligner sur l'application des bonnes pratiques. Afin de le réaliser, il est nécessaire de s'intéresser au mécanisme de sauvegarde, d'archivage ou de suppression des données, mais aussi au schéma d'architecture. Il s'appuie ainsi sur l'ensemble des données nécessaires à la revue de sécurité tel que la documentation existante sur le traitement ou les informations de développement. L'objectif de sa réalisation est l'identification des risques, internes ou externes, et des vulnérabilités aussi bien techniques qu'organisationnelles.

La réalisation de cette seconde étape entraine nécessairement la **troisième étape.** Il s'agit de la revue et l'analyse des mentions légales des documents transmis aux personnes concernées ainsi que la revue des clauses contractuelles en matière de protection des données personnelles liant l'organisation aux sous-traitants choisis.
Cette étape est liée aux deux étapes précédentes et met en lumière les manques. Les mentions et clauses sont obligatoires à la mise en conformité et visent à informer les personnes concernées et rendre un traitement valide. Leur existence permet de favoriser la création et le maintien d'un climat de confiance entre l'organisation et les personnes concernées. De plus, elles permettent d'assurer une certaine transparence sur les traitements en informant sur les durées de conservation, les destinataires des données et l'objet du traitement.

Dans le domaine RH, ces mentions apparaissent dans les formulaires de collecte de données personnelles qu'ils s'agissent de formulaires à l'embauche ou de formulaire pour des traitements spécifiques comme la gestion des notes de frais ou la collecte d'informations dans le cadre d'un recrutement.

A l'issue de la réalisation de l'évaluation par le formulaire de conformité et de la revue des clauses contractuelle, une analyse complémentaire peut être demandée et réalisée. Il s'agit de la **quatrième étape**. Elle se concentre sur les risques encourus sur le traitement et leur impact au regard de la protection des données et la vie privée. Cette analyse se déroule en phase comme le formulaire de conformité :

- une phase liée à la délimitation du contexte et la définition du processus étudié ;
- une phase liée à l'étude des mesures garantissant les principes fondamentaux. Cette phase permet de s'intéresser aux aspects techniques de sécurisation du patrimoine informationnel. Différents dispositifs peuvent être mis en œuvre tels que l'anonymisation, la pseudonymisation des données, le chiffrement des flux, l'archivage des données et la gestion des accès logiques ;
- une phase liée aux risques, leur nature et les moyens utilisés pour les traiter et les réduire ;
- une phase de validation pour donner suite à l'élaboration d'un plan d'actions dédié à améliorer le processus et réduire les risques. Ce plan d'actions doit être défini et validé par le responsable de traitement et le délégué à la protection des données.

Cette analyse d'impacts reposant sur les principes et droits fondamentaux ainsi que sur la gestion des risques de violation de la vie privée est une démarche de long terme. Lorsqu'elle doit être effectuée, elle doit être anticipée autant que possible et employée dès la conception d'un nouveau processus de traitement des données personnelles. Il s'agit d'un processus d'amélioration continue qui requiert parfois plusieurs revues et itérations avant d'aboutir à un dispositif complet de protection des données personnelles et de la vie privée. De plus, une veille est nécessaire afin de surveiller les évolutions dans la durée du traitement et anticiper les menaces potentielles. Par cette analyse, au-delà de gérer les risques, la manière avec laquelle ils seront appréhendés et évalués est formalisée. Cette vigilance continue et la rigueur requise pour réaliser ces analyses conduisent à la gestion du changement et à une meilleure maitrise du patrimoine informationnel.

Cette phase se traduit également par la constitution d'un guide dédié à la réalisation d'analyse d'impacts. Ce guide rappelle les raisons et le déroulé d'une telle évaluation. Il permet d'informer les parties prenantes et de préparer les acteurs.

La **cinquième étape** de l'organisation de la conformité est la mise en place d'un tableau de bord. Cette étape se réalise en parallèle de toutes les étapes précédentes afin d'assurer un meilleur suivi. Le tableau de bord peut comporter la liste des entités et

traitements, le nom du responsable de traitement associé, un rappel des actions menées et leur état d'avancement. Disposer d'un plan d'action clair est indispensable afin d'organiser et de planifier en toute confiance la mise en conformité au RGPD. Véritable outil de travail, disposer d'un tableau de bord permet d'accéder à l'ensemble des informations nécessaires pour avoir une vision précise des tâches à accomplir. De plus, il permet d'avoir à disposition des métriques de suivi de l'état d'avancement afin d'adapter si nécessaire les actions. En effet, ils comportent les traitements pour lesquels l'évaluation de la conformité est terminée et ceux pour lesquels l'évaluation est en cours ou à accomplir.
Les graphiques associés aux métriques simplifient la lecture du tableau de bord et assurent une communication efficace entre les acteurs pour mener la prise de décisions. Véritable outil de gouvernance pour assurer la mise en conformité et la maitrise du patrimoine informationnel, le tableau de bord permet d'entretenir la dynamique de progrès et d'être en capacité de répondre en cas d'audit. Il constitue un élément de preuve que des actions sont menées pour la rédaction des documents de conformité et des analyses de risques.

Maitriser le fonctionnement des processus, être en capacité de maitriser les risques et définir des plans d'actions visant l'amélioration des processus sont autant de moyens nécessaires et utiles à la maitrise du patrimoine informationnel et à la performance opérationnelle interne. Les documents présentés sont autant d'éléments à suivre quotidiennement afin de les mettre à jour. Bien plus que sa mise en conformité, l'entreprise disposera avec ces outils d'une méthodologie de travail responsable et rigoureuse qui est un élément pour établir la confiance et ainsi une performance opérationnelle interne par la maitrise de ses processus et de son patrimoine informationnel.

C. Organiser la conformité : Implémentation de nouveaux processus

De bien des manières, le RGPD ne constitue pas une règlementation ordinaire. Entré en vigueur pour permettre une protection accrue des droits des personnes concernées sur le territoire européen, il montre aux organisations les axes et les moyens utiles pour obtenir et conserver la confiance des personnes.

Dans un contexte où les personnes concernées disposent de la possibilité de faire une demande pour l'exercice de leurs droits, il est essentiel de disposer d'outils permettant d'y répondre rapidement.

Dans le cas étudié, le CSP-RH est actuellement responsable de la mise en œuvre de moyens pour assurer la collecte des données et le suivi des demandes. Pour répondre à ce nouveau besoin, il est nécessaire d'implémenter de nouveaux processus internes.

Cela requiert au préalable une analyse de l'existant et un recueil spécifique des besoins. Ce travail d'analyse a permis d'identifier les requêtes existantes pour extraire les données personnelles d'un collaborateur et ainsi répondre à la demande de droit d'accès. Accessibles depuis l'ERP utilisé pour la gestion des données de chaque salarié d'un point de vue administratif, il était plus simple d'avoir des requêtes dédiées pour ce nouveau besoin d'extractions de données.

La **seconde étape** de cette implémentation de nouveaux processus est la mise en place d'une démarche spécifique de récupération des données afin de mieux cibler les données utiles lors d'une demande de droit d'accès d'un collaborateur.
La création de ces requêtes nécessite plusieurs phases :

- Une phase de réflexion afin de déterminer la liste des données personnelles d'un collaborateur ;
- Une étape de centralisation afin de regrouper les types de données par domaine : Données personnelles (Nom / prénom / adresse…), Données professionnelles (poste / identifiant / matricule / manager / HRBP…), Informations complémentaires (numéro de téléphone professionnel / adresse email / numéro de bureau), Informations liées à la famille (liste enfants / situation maritale / personnes à contacter en cas d'urgence), Informations bancaires, Informations liées à la formation ;
- Une étape de recherche pour trouver l'emplacement des données au sein des logiciels ;
- Une étape de création de requêtes afin de remonter les données personnelles identifiées.

Cette démarche manuelle a nécessité la création d'une documentation et d'une procédure spécifique pour présenter les étapes à suivre lors de la constitution d'une réponse en cas d'exercice de droit d'accès d'un salarié. La mise en place d'un tel processus constitue une valeur ajoutée importante au CSP-RH mais reste cependant très manuel. L'aspect manuel rend cette démarche contraignante pour l'utilisateur qui la met en œuvre du fait du temps nécessaire à son exécution et mise en forme. Afin de la rendre plus accessible et plus efficace, elle est amenée à évoluer et à connaître des ajustements.

Tout comme les documents de conformité, l'organisation de la conformité par l'implémentation de nouveaux processus nécessite la mise en place d'un tableau de bord. Ce dernier vise uniquement à suivre le nombre de demandes dans le temps. Véritable outil de travail, il permet de visualiser les pics de demandes. Les graphiques assurent une lecture simple et rapide pour une communication efficace. Outil de gouvernance, il permet d'entretenir la dynamique de progrès.

Alors que les demandes se font de plus en plus nombreuses, le besoin a évolué. Si la démarche manuelle était très efficace pour les premières demandes, il est devenu

nécessaire de repenser la démarche en réfléchissant aux moyens pouvant être utilisés pour son automatisation. Elle vise à diminuer le temps utilisé pour réaliser la demande et extraire les données. Ce nouveau projet requiert une phase de préparation avec l'identification des exigences et des éléments d'entrée et de sortie. Il nécessite également une phase de recherche et développement afin de reconnaître la faisabilité du processus d'accès et d'extraction des données personnelles dans le format attendu. À l'issue de cette phase, il sera possible d'aboutir à un nouveau processus. La réflexion est aujourd'hui encore à mener. La solution à court terme serait le développement d'un outil qui remonterait automatiquement les données personnelles d'une personne concernée à partir de son adresse mail par exemple.
Sur le long terme, serait-il possible de disposer d'un outil global pouvant agir comme satellite et portail unique pour accéder aux données de tous les outils ? Par exemple, à partir des portails *self-service* auxquels a accès un salarié, serait-il possible d'ajouter un « bouton » permettant à un salarié de télécharger en une seule fois une copie de l'ensemble ou une partie de ses informations à tout moment ? À l'image de ce qui peut exister dans certaines entreprises, le salarié pourrait choisir la période souhaitée, la catégorie des données, le format de visualisation de ses données et demander le téléchargement à partir d'un processus protégé.

Ce travail nécessite une évaluation technique pour statuer sur la possibilité de mener un tel projet d'automatisation.

D. Synthèse - Concept global

La gouvernance de confidentialité des données repose sur des fondements qui font le lien entre politiques, cadre légal, stratégie de sécurité, processus de cycle de vie des données à caractère personnel, gestion des accès et administration des processus de gestion de la sécurité et les technologies.

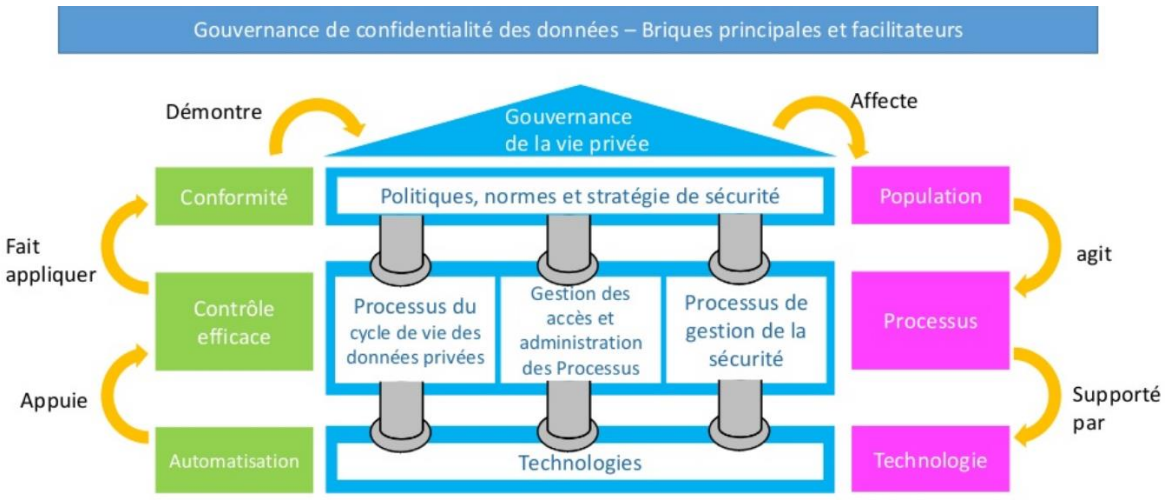

Figure 10 – Gouvernance de confidentialité des données (VALCIN, 2017)

La gouvernance de la vie privée et des données personnelles affecte la société et soutient les changements et l'application des politiques ce qui contribue à accélérer l'adoption de contrôles spécifiques. Pour permettre une conformité durable, la gestion des accès doit se concentrer sur la population, les processus et les technologies.

Nous l'avons vu, mener un travail de mise en conformité ne s'improvise pas. Ce travail requiert une organisation de la conformité par la mise en place de sensibilisation, la réalisation d'inventaire et de documents de conformité ainsi que la mise en place de nouveaux processus. Cet éventail de missions requiert la présence d'un personnel dédié à part entière à ce travail afin d'être l'interlocuteur privilégié de l'équipe DPO et des différents services métiers.

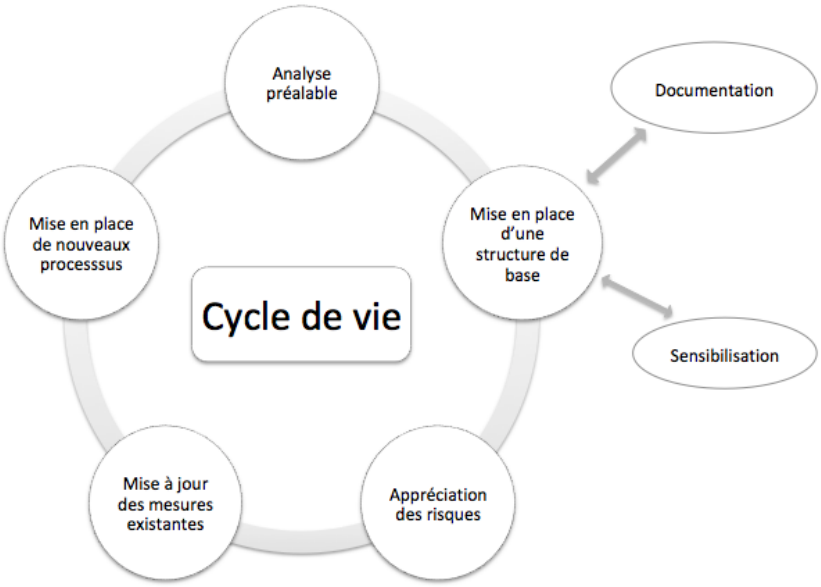

Figure 11 - Cycle de vie de la mise en conformité

Ce long travail n'est possible qu'au prix de la mise en place d'une organisation responsable traitant de la gouvernance consacrée à la protection des données personnelles. Cette gouvernance nécessite l'investissement et l'implication de l'ensemble des parties prenantes. Elle a pour moyens la cartographie des données personnelles, l'inventaire des traitements et la mise à jour des processus opérationnels. De plus, la mise en conformité permet la maitrise du patrimoine informationnel car elle vise la gestion du cycle de vie des données en considérant la définition des durées de conservation et la mettre en place de méthodes pour sécuriser les données.

La démarche de mise en conformité est ainsi un processus composé de différentes étapes :

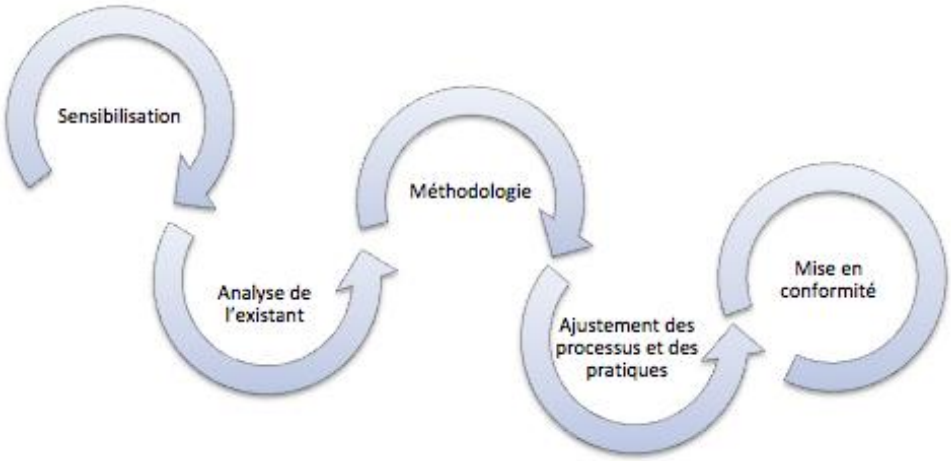

Figure 12 - Démarche de mise en conformité

Nous l'avons vu, la sensibilisation est le point de départ pour une implication des acteurs qui doit se faire de manière continue et diffuse tout au long de la démarche. L'organisation de la mise en conformité nécessite l'analyse de l'existant afin de parvenir à une méthodologie ou plan d'actions permettant d'organiser le travail. Cette organisation du travail est découpée par la réalisation des documents de conformité et ou analyses d'impacts et la revue de mentions d'informations et des contrats. Une fois cette étape passée, des ajustements sur les processus et des pratiques sont souvent nécessaires afin de parvenir à une mise en conformité.

Ce processus vise l'amélioration continue qui permet la mise en place de plan d'action spécifique à chaque traitement pour réduire les risques et les fuites de données personnelles.

III. Discussions et perspectives

A. Discussions

Contrainte ou opportunité : la discussion sur le Règlement Général sur la Protection des Données est au cœur de l'actualité encore deux ans après son entrée en vigueur.
L'objectif de ce travail de recherche est de répondre à la question :
De quelles manières la mise en conformité peut contribuer à la maitrise du patrimoine informationnel et former un levier de performance opérationnelle interne ?

Comme décrit, le Règlement Général sur la Protection des Données amène son lot de nouvelles règles à respecter et de nouvelles actions à mettre en œuvre. Documents de conformité, analyses d'impacts permettent à l'organisation de pouvoir avoir une plus grande connaissance des processus réalisés et d'acquérir une maitrise du patrimoine informationnel. Par l'explication et l'extériorisation de cette connaissance à la fois générale et détaillée, l'organisation pourra avoir une meilleure maitrise du patrimoine informationnel. Ces moyens permettent la mise en conformité d'une organisation.

Afin de compléter ce travail de recherche, des entretiens avec des parties prenantes impliquées dans la mise en conformité ont été réalisés. Les entretiens se sont faits exclusivement en interne de la société Atos. Les personnes interrogées ont été soigneusement choisies au regard de la question de recherche et du terrain d'étude. En effet, les répondants ont tous un rôle clé dans le travail initié pour la mise en conformité au Règlement Général sur la Protection des Données. Ces discussions, réalisées sous forme de court entretien d'une durée entre 30 minutes et une heure, avaient pour objectif d'obtenir un retour sur les solutions proposées et de répondre à la question en suspens.
Ces entretiens semi-directifs ont permis d'aborder des points précis du sujet mais également de garder l'opportunité de laisser libre court à la discussion et ainsi suivre d'autres trajectoires s'éloignant du fil principal lorsqu'elles étaient appropriées. Si aucun guide d'entretien n'a été formalisé au préalable, le fil conducteur était clairement identifié. Le but était d'avoir un retour sur chacune des trois solutions ainsi qu'un avis sur la question « Contrainte ou opportunité ? ».
Finalement, le but de ses entretiens était d'autoriser les acteurs à s'exprimer en toute confiance afin de les faire partager leur point de vue et de pouvoir par la suite les comparer. Ces entretiens sont consultables en annexes du document.

Sur la première solution relative à la sensibilisation des acteurs, plusieurs aspects ont été mis en avant par les personnes concernées. Tout d'abord, le fait que la sensibilisation revêt un caractère obligatoire afin d'être en conformité et d'être capable de le démontrer : « *toute entreprise doit s'assurer que ces employés ont un niveau de connaissance minimale. C'est quelque chose qui doit être démontré*. »

En dehors du caractère obligatoire de la formation, il y a un besoin que le support de formation intègre des cas pratiques et soit proche du terrain. En effet, d'après une personne interrogée « s*i je m'aperçois que ce support de formation ne convient pas à la réalité concrète du problème auquel je suis confronté, je vais avoir tendance à le mettre de côté, à l'abandonner et à ne jamais le rouvrir* ». Cette remarque caractérise parfaitement une des hypothèses formulées au début de ce travail : la méconnaissance des faits pratiques des règlements est due à une présentation trop théorique ou générale. Cette même personne confirme le fait qu'un support doit être « *pratico-pratique* ». En ses termes, la personne explique que « *si je m'aperçois que je m'en sers, c'est pratico-pratique. Je vais pouvoir l'ouvrir et être guidé au fur et à mesure de mon problème. À chaque étape, ce support de formation va être pratique, il va répondre à comment je dois faire ci, comment je dois faire ça.* » L'apport de ces formations est « *d'attirer l'attention* », « *de rester proche du terrain* » et « *d'être en contact avec les équipes* ». Avoir un support de formation est une obligation légale qui se doit d'être « *vraiment ancré sur le pratique et avoir un relationnel établit avec les équipes, régulier* ».

Mettre en place cette solution de sensibilisation n'est pas une action pour se « *débarrasser* » du sujet et de la problématique. Il est nécessaire que celle-ci soit régulière en organisant des rappels aussi fréquemment que possible. Comme l'a formulé une des personnes interrogées « *il faut saisir les occasions* ». De plus, la mise en place de sensibilisation unique n'est pas suffisante. Il est nécessaire d'être dans une démarche d'accompagnement qui vise une remise en cause. Proposer comme solution à la méconnaissance des acteurs une sensibilisation n'est pas le simple fait de la proposer et la mettre en œuvre. Il s'agit d'accompagner les acteurs, d'être en capacité de revenir sur la sensibilisation pour l'améliorer. L'accompagnement est le fait de créer une zone et un temps d'échanges, une zone de confiance afin d'entrer dans une démarche de suivi et d'adaptation.
L'écoute est également primordiale. Celle-ci permet de s'intéresser à des besoins spécifiques et ainsi donner des solutions adaptées à chacun pour s'assurer d'une mise en pratique effective. C'est cette mise en pratique qui permettra de déclencher des réflexes et une prise de conscience. L'écoute et le support déterminent l'impact de la sensibilisation sur les acteurs. L'apport d'une sensibilisation ne se limite pas à un bénéfice individuel. Il faut voir l'aspect général d'une sensibilisation notamment si celle-ci touche aussi bien les personnes directement impactées et devant agir que la hiérarchie de ces personnes.
Ces sensibilisations globales ont permis d'avoir un soutien de la part de la hiérarchie ce qui l'appui et l'officialise. Cela confirme l'importance du management dans la mise en conformité. Une sensibilisation globale peut être complétée par des sensibilisations transverses par petit groupe ayant pour but de développer la sensibilisation sur le long terme, comme l'a soumis une des personnes interrogées. L'apport d'une sensibilisation transverse est de créer une zone d'échanges pouvant créer une émulation entre des acteurs ayant des problématiques diverses mais également des interrogations proches

sur ce besoin commun de mise en conformité. La mise en place de ces sensibilisations transverses par petits groupes permettra aux personnes impliquées de pouvoir s'entraider et monter en compétences. Selon une des personnes interrogées, réaliser des sensibilisations croisées donne l'opportunité de *« faire en sorte que le RGPD fasse partie de notre quotidien, de nos gènes ».* Ce bénéfice vise à supprimer les réactions réticentes de certains acteurs tel que « *le RGPD je n'aime pas ça, je ne sais pas faire* ».
De plus, elles peuvent participer à supprimer la difficulté de toucher l'intégralité des acteurs.
Finalement, l'important à garder à l'esprit sur ces sensibilisations, qu'elles soient globales, individuelles ou par petits groupes, est le suivi dans la durée.

Sur la deuxième solution comme pour la première, le caractère obligatoire de la réalisation des documents de conformité est le premier point qui apparait, « *c'est une obligation légale et il faut qu'ils s'y conforment* ». De plus, le caractère contraignant est également mis en avant, ainsi qu'une certaine méconnaissance de la part des acteurs, « *je ne sais pas faire* », « *Le travail est contraignant et nécessite des mises à jour. Le travail est titanesque.* ». L'absence de document de conformité rend le traitement non déclaré. L'étape de la revue des clauses contractuelles et des mentions d'information est primordiale et n'est pas à négliger, même si elle peut-être souvent oubliée par les acteurs. En effet, l'une des personnes interrogées a mis en avant le fait qu'en l'absence de clauses, le contrat est invalide ou « *non causé* ».
Malgré le caractère obligatoire, la réalisation des documents de conformité a une réelle opportunité pour les parties prenantes. Elle vise une meilleure connaissances des flux d'informations et des traitements effectués, et ainsi « *une meilleure vision du process* ». Cette obligation a « *permis de nous poser, de poser les bonnes questions aux personnes qui savaient* ». De plus, cela a permis d'acquérir une « *grande base de connaissance* » sur l'ensemble des traitements étudiés. Ces documents de conformité comme l'analyse d'impact sont le « *reflet de la façon dont on travaille* ». Ils « *contribuent à améliorer la connaissance du patrimoine et de manière indéniable* ».
Pour parvenir à ce bénéfice, une réelle démarche de mise en conformité est nécessaire. Cette dernière commence par la sensibilisation et la responsabilisation des acteurs qui se fait de manière continue afin de créer « *une mécanique »* par des mécanismes et automatismes. Ces derniers donnent l'opportunité aux acteurs d'avoir le RGPD « *dans nos gênes pour y penser directement* ».

Concernant la dernière solution, il est important d'avoir des processus « *bien clairs »* établis avec diffusion auprès des services. Il ne s'agit pas d'un nouveau droit. Il faut que l'ensemble des acteurs ait conscience de leurs rôles et du fait que ce n'est pas de la responsabilité du DPO.

D'un aspect général, pour l'ensemble des personnes interrogées, le RGPD constitue d'abord une contrainte. Il s'agit d'une loi imposée concernant l'ensemble de l'entreprise

et qu' « *on est obligés de suivre* ». De plus, effectuer une mise en conformité implique du « *temps à investir* » et du « *travail supplémentaire* » qui a un coût direct pour l'entreprise. La mise en place du RGPD « *nécessite une nouvelle organisation, un recrutement spécifique pour des nouvelles missions, la mise en place de sensibilisations supplémentaires* ».
Bien qu'il s'agisse indéniablement d'un travail et processus continu contraignant pour lequel *« il n'est jamais possible d'être totalement conforme* », la mise en conformité au RGPD constitue une opportunité. Tout d'abord, comme expliqué, le RGPD a permis de constituer et d'augmenter la connaissance du patrimoine informationnel et des traitements. Cette connaissance permet d'acquérir une maîtrise et un aperçu global. Ce travail a « *permis de mettre en relief les mécanismes de traitements des données* ».
De plus, la réalisation de la documentation « *oblige à travailler propre* » et à s'interroger sur « *la sécurité, sur la qualité des livrables »* et sur les traitements allant être implémentés. Tout ceci constitue une amélioration puisqu'« *on améliore indirectement la qualité des produits* » livrés aux clients. Enfin, « *il permet le développement de solutions pour transformer ce règlement et cadre légal en opportunité ».*
Finalement, ce travail de mise en conformité entraine une mobilisation des acteurs à tous les niveaux, le changement de certaines pratiques et la mise en place d'actions permettant d'arriver sur une situation où la personne concernée est « à l'aise ».

B. Perspectives

Les normes et règlements, par leur vaste champ d'application, constituent une transposition des normes sociales nécessaire sur les systèmes d'information afin d'apporter maitrise et protection. Cette transposition permet d'avoir un cadre établit clair qui encourage les acteurs à s'interroger sur la notion de protection et de sécurisation des données, et plus largement du patrimoine informationnel.
En particulier, le Règlement Général sur la Protection des Données a permis une évolution importante en matière de gestion des données à caractère personnel. Celui-ci vise à la mise en place d'actions spécifiques ayant pour objectif d'établir un référentiel des données personnelles et une documentation des traitements.

Ce règlement impose aux organisations une mise en œuvre d'actions et de mesures efficaces pour assurer la sécurité des données à caractère personnel. Plus globalement, la démarche de mise en conformité permet de s'interroger sur la mise en place d'opérations dédiées à la sécurité des données. Ces questions de sécurité concernent notamment les aspects de chiffrement, pseudonymisation et d'anonymisation des données. De plus, la gestion des accès avec une revue régulière et spécifique de chaque traitement est également nécessaire pour assurer la protection des données. Elle vise à réduire les risques d'accès illégitimes aux données et d'intrusion. Cette gestion peut être encadrée par la mise en place de mesures spécifiques plus importantes avec l'utilisation d'une authentification à doubles facteurs ou l'usage de carte à puce par exemple.

Effectuer une revue des traitements vise, au travers des documents de conformité, à la revue des mesures existantes pour la mise en place de mesures d'accès aux données en cas d'incident. L'analyse des risques effectuée pour certains traitements permet de s'interroger sur les mesures existantes ou prévues afin de pallier les risques et contribuent à la sécurité des données. Cela permet également de s'interroger sur les risques, menaces et vulnérabilités des traitements effectués dans une organisation. Au-delà du caractère règlementaires des mesures de mise en conformité, les outils mis en place afin d'établir les documents de conformité sont proches de la gestion des risques.

De ces éléments, une question peut se poser : les normes et règlements, et en particulier, le Règlement Général sur la Protection des Données, servent-ils le domaine de la cyber sécurité ?
Le Règlement Général sur la Protection des Données permet de se questionner sur des problématiques existantes dans le domaine de la cyber sécurité. Il oblige les organisations à s'assurer de l'existence de mesures et de dispositifs appropriés contre le vol ou les fuites de données à caractère personnel. La cybercriminalité est un sujet d'actualité, accentué par la numérisation progressive des documents. Le risque d'utilisation frauduleuse des données de personnes concernées ne cesse d'augmenter avec des pratiques de plus en plus difficiles à identifier telles que l'hameçonnage («*phishing*»). Le fait d'identifier les risques et d'avoir connaissance des menaces peut permettre d'être en capacité de déceler les possibles intrusions.
L'humain, et non la technique, constitue une des plus grandes menaces. Ainsi, il est nécessaire que l'organisation mette en place une sécurité à plusieurs niveaux. Cette sécurité passe par des mesures organisationnelles, avec des sensibilisations et formations régulières, associées à des mesures techniques comme des pares feux ou des mises à jour régulières.

La cybersécurité, comme les normes et règlements, permet de s'interroger sur les bonnes pratiques et les standards en matière de management des risques ainsi que sur la notion de conformité et les politiques existantes telles que la politique de sécurité des systèmes d'information. Ces domaines nécessitent une démarche continue qui n'est pas implémentable en une seule fois pour être oubliée par la suite. Du fait de l'évolution constante tant des processus que des règlements, la gestion de la sécurité est un travail qui nécessite une amélioration, une revue des notices et politiques en place.

Conclusion

« Les données, c'est l'or numérique, l'or noir de demain. » - T. Breton

L'espace informationnel d'une organisation renvoie à l'ensemble des données, informations et connaissances. Cet espace, qui doit être géré et façonné, nécessite un cadre légal et normatif. Thierry Breton considère comme essentiel que l'espace informationnel soit règlementé et organisé comme l'ont été les espaces terrestres, maritimes et aériens. (Labialle, 2019) Il insiste sur le fait que les données personnelles et professionnelles « des résidents européens font partie d'un espace informationnel qui se doit d'être règlementé, encadré et surveillé… par l'Europe. » (Feugey, 2013) L'organisation doit mettre en place des moyens pour gérer, maitriser et protéger ce patrimoine informationnel afin d'améliorer l'existant et préparer l'avenir.

Le sujet traité porte sur les normes et règlements comme opportunité de maitrise et de protection du patrimoine informationnel d'une organisation avec une mise en application au RGPD au sein d'un service RH. Le sujet de cette étude est au cœur des préoccupations actuelles des organisations. Le choix de ce vaste sujet s'est fait en considérant les changements continus issus des environnements légaux et techniques, qui tend à s'accélérer ces dernières années. Ces changements sont influencés par une transformation numérique et digitale qui impose un rythme toujours plus rapide, nécessite une perpétuelle adaptation, d'où résulte des changements permanents.

Ce travail de recherche a proposé une description de la notion de patrimoine informationnel. Dans un monde où la technologie et le numérique sont omniprésents, les données, informations et connaissances sont au cœur du fonctionnement de nos organisations. Fondement nécessaire à tout traitement, leur compréhension est primordiale. Le cadre légal gravitant autour de ce patrimoine informationnel et les manières existantes visent à mieux le maitriser et mieux le protéger. Les organisations, face à une augmentation du volume des données et à un cadre normatif et légal qui ne laisse pas la place à la négligence, pâtissent souvent d'une insuffisance de connaissances et d'efforts appliqués à la gestion du patrimoine informationnel.

En complément de clarifier la notion de patrimoine informationnel, cette étude contribue à la compréhension des normes et règlements et, en particulier, leurs impacts sur les systèmes d'information. Cet objectif nécessite la connaissance de leur étendue et des obligations légales imposées aux organisations. Aussi, ce travail a explicité les impacts et démontrer les apports de la mise en conformité sur la maitrise et la protection du patrimoine informationnel. Le travail réalisé s'est tout particulièrement

intéressé au Règlement Général sur la Protection des Données (RGPD) et à son application dans le contexte d'un service RH qui a constitué le terrain d'étude.

Ce document de recherche a présenté la mise en conformité, et, au-delà de sa perception contraignante pour l'organisation, la révèle comme source d'opportunités et élément déterminant au service de la performance opérationnelle interne.
Ce travail a montré que le patrimoine informationnel est un véritable levier pour les organisations du fait qu'il représente une réelle source de connaissances. En cela, il requiert une attention particulière. Les organisations doivent définir une gouvernance spécifique visant la maitrise et la protection de ce patrimoine informationnel.

Cette gouvernance des données repose sur un environnement légal cadrant le patrimoine informationnel. Elle n'est pas aisée à organiser et nécessite une préparation suffisante afin de mettre en œuvre l'ensemble des mesures nécessaires. Lors de cette préparation et l'application de cette gouvernance des données, les différents acteurs des organisations jouent un rôle déterminant. Chacun doit avoir conscience que cette gouvernance fait partie de son travail. Elle est l'affaire de tous et doit entrer dans le quotidien de chacun. Dès lors, elle sera partie intégrante de la culture d'entreprise. Elle doit être transmise dès l'arrivée d'un salarié, et plus encore est un préalable, un prérequis au sein d'un service RH.

Le chantier de mise en conformité au cadre légal, et en particulier au RGPD, est un travail continu nécessitant une analyse et une certaine prise de recul afin de sensibiliser les acteurs et d'organiser la conformité. Cette organisation vise l'identification des données et des traitements pour la réalisation d'une documentation précise ainsi que l'implémentation de nouveaux processus. Les documents de conformité sont des mines d'informations car ils conduisent à comprendre et formaliser de manière explicite les traitements portés par l'organisation. Ils donnent l'opportunité aux acteurs de s'interroger de manière spécifique et globale sur leurs traitements afin d'en évaluer le bien fondé, de les améliorer et de mettre en œuvre un plan d'actions ainsi que des ajustements pour mieux protéger le patrimoine informationnel.

Malgré son caractère obligatoire ineffaçable et indéniable, la mise en conformité est une opportunité pour le développement des activités de l'organisation. En effet, elle permet de travailler « propre » et livrer des produits conformes et sécurisés aux clients. Investissement d'avenir et argument d'une confiance digitale, cette mise en conformité est un engagement pour l'organisation du fait de ses coûts directs et immédiats. En dépit du temps investi sur ce chantier, la mise en conformité permet la sensibilisation et responsabilisation des acteurs, le partage de bonnes pratiques et conduit à une connaissance accrue du patrimoine informationnel et des traitements de l'organisation. Les bénéfices d'image liés à cette conformité et l'amélioration de la qualité du travail fourni sont autant de bénéfices mais également d'opportunités.

En résumé, la mise en conformité, et plus encore le Règlement Général sur la Protection des Données, se révèle être davantage une opportunité qu'une contrainte car elle oblige à s'interroger, ordonner et gérer le nouvel or noir des organisations, la donnée. Ne se limitant pas uniquement à une cartographie des gisements, c'est tout le processus de raffinage de la donnée qui est explicité, capitalisé.

Cette mise en conformité, parfois difficile à mettre en œuvre et à appréhender, exige l'intervention combinée de plusieurs compétences dans une démarche d'amélioration continue. Cette démarche permet de s'adapter à l'évolution des traitements ainsi que celle des risques et des menaces pour l'organisation.

Cette gestion du patrimoine informationnel ainsi que l'organisation de la conformité doivent être considérées dans une perspective plus large telle que la gestion des accès, la gestion des risques et de la sécurité.
Le risque est considéré par toute l'organisation. Mettre en œuvre une gestion des risques au plus tôt dans un traitement donne l'opportunité à l'organisation de relever des défis et d'opérer des changements sur ses procédures et son fonctionnement. Disposer d'outils de gestion de risques requiert leur identification, l'appréciation de leur probabilité d'occurrence et une évaluation de leurs impacts pour l'organisation. L'analyse des risques nécessite également l'identification des mesures de sécurité existantes et la définition de parades tels que des plans d'actions spécifiques visant l'anticipation et la réduction des risques.

Une connaissance accrue et maitrisée des risques permet à l'organisation de pouvoir adopter ses mesures pour maintenir la protection du patrimoine informationnel.
Cette démarche d'amélioration continue liée à la mise en conformité amène ainsi les organisations à optimiser leur niveau de sécurité, en s'appuyant sur des audits, et ainsi répondre aux incidents et contraintes légales.
Cette gouvernance, par la maitrise des risques et la mise en oeuvre de mesures organisationnelles et techniques, vise à protéger les organisations face aux menaces de plus en plus nombreuses. La culture de la gestion des risques, tout comme la mise en conformité, et la cybersécurité sont l'affaire de tous. Elles doivent faire partie intégrante de la culture d'entreprise, être infusées, cultivées dans le temps.

La mise en œuvre de bonnes pratiques, la gestion des connaissances, des politiques et des procédures, la gestion de projets de sécurité et la gestion des risques sont autant d'éléments qui permettent de transposer la mise en conformité à la cybersécurité.
La cybersécurité, tout comme les normes et règlements, s'impose à l'organisation comme un processus d'amélioration continue. Ainsi, la responsabilité de chacun est essentielle, la prise de conscience des enjeux et risques est un prérequis, la conformité

est une obligation. L'efficacité et la transparence des traitements devant être évidentes, le suivi nécessaire.

Les normes et règlements, à travers la mise en application au Règlement Général sur la Protection des Données, et la cybersécurité sont deux sujets devant répondre à un même défi, celui de la maitrise et surtout la protection et sécurité du patrimoine informationnel.

Bibliographie

Abiteboul, S. (2012). Sciences des données: de la logique du premier ordre à la toile. Collège de France.

Académie française. (2019). Dictionnaire de l'académie Française, 9ème. Consulté le 02 15, 2019, sur Dictionnaire de l'académie Française: https://www.dictionnaire-academie.fr/article/A9I1218

AFNOR. (2017, 01). AFNOR Guide protection des données personnelles. Récupéré sur Afnor: https://normalisation.afnor.org/wp-content/uploads/2017/02/AFNOR_Guide_Protection_des_donnees_perso_HD.pdf

AFNOR. (s.d.). Les normes en une définition. Récupéré sur AFNOR: https://normalisation.afnor.org/normes-definition/

Agostinelli, S., Marrella, A., Maggi, F. M., & Sapio, F. (2019, 06). Achieving GDPR Compliance of BPMN Process Models. Récupéré sur iris.uniroma1.it: https://iris.uniroma1.it/retrieve/handle/11573/1290908/1184104/Agostinelli_Postprint_Achieving-GDPR_2019.pdf

Akoka, J., & Comyn-Wattiau, I. Evaluation de la gouvernance de l'information.

Allal-Chérif, O., & Dupouet, O. (2014, 07). Optimisez votre système d'information ! Vers la PME numérique en réseau. Consulté le 2020, sur Boutique Afnor: https://www.boutique.afnor.org/resources/cf2326b4-e0a6-42c3-83ec-2bf7cc0965ef.pdf

Armstrong, M. (2019, 04 16). Global Data Creation is About to Explode . Consulté le 08 31, 2020, sur Statista: https://www.statista.com/chart/17727/global-data-creation-forecasts/

Asseman, A. (2011, Août). Etude exploratoire des facteurs de risque du détournement en interne du patrimoine informationnel. Récupéré sur https://papyrus.bib.umontreal.ca/xmlui/bitstream/handle/1866/6116/Asseman_Audrey_2011_memoire.pdf

Atos. (2020, 03). Atos document d'enregistrement universel 2019. Consulté le 2020, sur Atos: https://atos.net/content/investors-documents/2019/atos-document-enregistrement-universel-2019.pdf

Bensoussan, A. (2010, 03 09). La protection du patrimoine informationnel de l'entreprise. Récupéré sur Alain Bensoussan: https://www.alain-bensoussan.com/avocats/la-protection-du-patrimoine-informationnel-de-l%E2%80%99entreprise/2010/03/09/

Bentounsi, M., Cante, E., Coya, D., Darmon, P., de Chambourcy, A., & Gnokam, G. (2019, 07 12). ARIANE : la Gouvernance des Données comme accélérateur de conformité au règlement général sur la potection des données. Récupéré sur HAL archives ouvertes: https://hal.archives-ouvertes.fr/hal-02182579/document

Berthier, D., Morley, C., & Maurice-Demourioux, M. (2005). Systèmes d'information et management (Vol. Vol 10).

BFM business. (2018, 12 20). Uber : amende record pour protection insuffisante des données personnelles. Récupéré sur bfmbusiness.bfmtv.com: https://bfmbusiness.bfmtv.com/entreprise/uber-amende-record-pour-protection-insuffisante-des-donnees-personnelles-1592455.html

Biriotti, E. (2018, 04 18). RGPD et WordPress : Le guide ultime (et concret) pour se mettre en conformité. Récupéré sur WP marmite: https://wpmarmite.com/rgpd-wordpress/

Bureau Veritas. (s.d.). Certification ISO 27001. Récupéré sur Bureau Veritas France: https://www.bureauveritas.fr/besoin/certification-iso-27001

Campagne Infolab de la FING. (2017, 01). Nouvelles efficacités et création de valeur : les projets de gouvernance des données . Consulté le 03 16, 2019, sur Infolabs: https://infolabs.io/gouv16

Caprioli, E., De Kervasdoué, P., Pépin, J.-F., & Rietsch, J.-M. (2007, 10). Protection du patrimoine informationnel. Récupéré sur https://www.cigref.fr/cigref_publications/RapportsContainer/Parus2007/Protection_patrimoine_informationnel_CIGREF_FEDISA_2007_web.pdf

Cérin, C. (2017, 12 18). Approches contemporaines en hébergement et gestion des données. Consulté le 03 19, 2019, sur http://lipn.univ-paris13.fr/~cerin/Livre_blanc_data_hosting.pdf

Chabin, M.-A. (2018). Des documents d'archives aux traces numériques. Klog.

Chabin, M.-A. (2018, 09 06). Données structurées et données non structurées. Récupéré sur Arcateg: https://www.arcateg.fr/2018/09/06/donnees-structurees-et-donnees-non-structurees/

Chardonnet, A., & Thibaudon, D. (2003). Le guide du PDCA de Deming. Consulté le 2020, sur Acifr.org: https://www.acifr.org/ressources/livres_production_qualite/guide_du_pdca_extraits.pdf

Chignard, S., & Benyayer, L.-D. (2015). Datanomics, les nouveaux business models des données. FYP éditions.

Cigref. (2014, 10). Enjeux business des données : Comment gérer les données de l'entreprise pour créer de la valeur? Récupéré sur cigref.fr: https://www.cigref.fr/wp/wp-content/uploads/2014/10/CIGREF-Enjeux-business-donnees-2014.pdf

CNIL. (2019). Accountability. Consulté le 03 30, 2019, sur CNIL: https://www.cnil.fr/fr/definition/accountability

CNIL. (2018, 12 27). BOUYGUES TELECOM : sanction pécuniaire pour manquement à la sécurité des données clients. Consulté le 03 15, 2019, sur CNIL: https://www.cnil.fr/fr/bouygues-telecom-sanction-pecuniaire-pour-manquement-la-securite-des-donnees-clients

CNIL. (2020, 02 07). Ce qu'il faut savoir sur les règles d'entreprise contraignantes (BCR). Récupéré sur Cnil: https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-les-regles-dentreprise-contraignantes-bcr

CNIL. (s.d.). Donnée sensible. Récupéré sur CNIL: https://www.cnil.fr/fr/definition/donnee-sensible

CNIL. (2019). Données personnelles. Consulté le 03 10, 2019, sur CNIL: https://www.cnil.fr/fr/definition/donnee-personnelle

CNIL. (2017, 03 02). Gérer les risques. Récupéré sur CNIL: https://www.cnil.fr/fr/gerer-les-risques

CNIL. (s.d.). La CNIL, c'est quoi? Récupéré sur CNIL: https://www.cnil.fr/fr/cnil-direct/question/la-cnil-cest-quoi

CNIL. (2019, 06 17). La loi Informatique et Libertés. Récupéré sur CNIL: https://www.cnil.fr/fr/la-loi-informatique-et-libertes#article1

CNIL. (2019). L'Atelier RGPD. Consulté le 03 10, 2019, sur CNIL: https://atelier-rgpd.cnil.fr/apprenant/

CNIL. (s.d.). Le contrôle de la CNIL. Récupéré sur CNIL: https://www.cnil.fr/fr/le-controle-de-la-cnil

CNIL. (s.d.). Les missions de la CNIL. Récupéré sur CNIL: https://www.cnil.fr/fr/les-missions-de-la-cnil

CNIL. (s.d.). Liste des types d'opérations de traitements pour lesquelles une analyse d'impact relative à la protection des données est requise. Récupéré sur CNIL: https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-requise.pdf

CNIL. (s.d.). Mission (4) : Contrôler et sanctionner. Récupéré sur CNIL: https://www.cnil.fr/fr/mission-4-controler-et-sanctionner

CNIL. (2018, 06 07). OPTICAL CENTER : sanction de 250.000€ pour une atteinte à la sécurité des données des clients du site internet www.optical-center.fr. Consulté le 03 15, 2019, sur CNIL: https://www.cnil.fr/fr/optical-center-sanction-de-250000eu-pour-une-atteinte-la-securite-des-donnees-des-clients-du-site

CNIL. (2020, 02 07). Pourquoi mettre en place des BCR ? Récupéré sur CNIL: https://www.cnil.fr/fr/pourquoi-mettre-en-place-des-bcr

CNIL. (s.d.). Responsable de traitement. Récupéré sur CNIL: https://www.cnil.fr/fr/definition/responsable-de-traitement#:~:text=Le%20responsable%20de%20traitement%20est,incarn%C3%A9e%20par%20son%20repr%C3%A9sentant%20l%C3%A9gal.

CNIL. (2020, 08 05). SPARTOO : sanction de 250 000 euros et injonction sous astreinte de se conformer au RGPD. Récupéré sur CNIL: https://www.cnil.fr/fr/spartoo-sanction-de-250-000-euros-et-injonction-sous-astreinte-de-se-conformer-au-rgpd

Cnil. (s.d.). Traitement de données personnelles. Récupéré sur cnil.fr: https://www.cnil.fr/fr/definition/traitement-de-donnees-personnelles

CNIL. (2018, 12 20). UBER : sanction de 400.000€ pour une atteinte à la sécurité des données des utilisateurs. Consulté le 03 15, 2019, sur CNIL: https://www.cnil.fr/fr/uber-sanction-de-400000eu-pour-une-atteinte-la-securite-des-donnees-des-utilisateurs

Commission européenne. (s.d.). Qu'est-ce qu'un responsable du traitement des données ou un sous-traitant des données? Récupéré sur ec.europa:

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_fr

Coulondre, S. (s.d.). Semi-Structuré + Structure = Structuré ? . Récupéré sur CNRS: https://projet.liris.cnrs.fr/inforsid/sites/default/files/article170c1.pdf

Data Analytics post. (2019). Chief Data Officer : une fonction de pilotage stratégique - Data Analytics post. Consulté le 04 10, 2019, sur Data Analytics post: https://dataanalyticspost.com/fiche-metier/chief-data-officer/

Delayat, R., & Bouteiller, S. (2014). Enjeux business des données : Comment gérer les données de l'entreprise pour créer de la valeur? Paris: CIGREF.

Delbecque, E. (s.d.). Protection et défense du patrimoine. Récupéré sur http://www.helios-detective.com/Articles/Protection-du-patrimoine-informationnel.pdf

Deniau, K. (2018, 03 23). Cambridge Analytica : tout comprendre sur la plus grande crise de l'histoire de Facebook. Récupéré sur Siecle Digital: https://siecledigital.fr/2018/03/23/cambridge-analytica-tout-comprendre-sur-la-plus-grande-crise-de-lhistoire-de-facebook/

Direction générale des entreprises. (s.d.). Présentation des actifs immatériels. Récupéré sur Direction générale des entreprises: https://www.entreprises.gouv.fr/services/presentation-des-actifs-immateriels

Direction interministérielle des systèmes d'information et de communication. (2013, 12 18). Cadre Commun d'Architecture des Référentiels de données. Consulté le 03 20, 2019, sur https://references.modernisation.gouv.fr/sites/default/files/Cadre%20Commun%20d'Architecture%20des%20R%C3%A9f%C3%A9rentiel%20de%20donn%C3%A9es%20v1.0_0.pdf

Données RGPD. (2019, 05 7). Qu'est-ce que le Privacy by Design. Consulté le 05 10, 2019, sur Données RGPD: https://donnees-rgpd.fr/definitions/privacy-by-design/

donnees-rgpd. (s.d.). Qu'est-ce que la Loi Informatique et Libertés ? . Récupéré sur donnees-rgpd.fr: https://donnees-rgpd.fr/loi-informatique-libertes/

Escaffre, L., Bouabdellah, N., & Damak Ayadi, S. (2018, 10 29). L'impact du capital intellectuel sur la performance des entreprises : Le cas des pays BRICS. Récupéré sur hal.archives-ouvertes.fr: https://hal.archives-ouvertes.fr/hal-01907587/document

ETS. (2011). Gouvernance des données et gestion des données de référence. Récupéré sur https://cours.etsmtl.ca/mti820/public_docs/acetates/MTI820-Acetates-GouvernanceDesDonneesEtMDM_1pp.pdf

Fernandez, A. (2018, 09 26). Comment utiliser la méthode DMAIC ? . Récupéré sur piloter.org: https://www.piloter.org/six-sigma/methode-six-sigma.htm

Fernandez, A. (2018, 07 23). Qu'est-ce que la Roue de Deming ? Récupéré sur Piloter.org: https://www.piloter.org/qualite/roue-de-deming-PDCA.htm

Feugey, D. (2013, 08 27). Thierry Breton (ATOS) veut un espace Schengen de la donnée. Récupéré sur Silicon.fr: https://www.silicon.fr/thierry-breton-atos-donnees-personnelles-europeens-88802.html

Foucault, J., Panhaleux, L., Renaud, D., & Begasse, P. (2018). RGPD : Le comprendre et le mettre en oeuvre. ENI.

Gartner. (s.d.). Data Governance. Récupéré sur Gartner: https://www.gartner.com/en/information-technology/glossary/data-governance

Gaudiaut, T. (2020, 07 30). Graphique | Le big band du big data. Consulté le 08 15, 2020, sur Statista: https://fr.statista.com/infographie/17800/big-data-evolution-quantite-donnees-numeriques-creees-dans-le-monde/

Goldstein, S. (2019, 10 29). Sanctions en cas de non-respect du RGPD : guide complet. Récupéré sur LegalPlace: https://www.legalplace.fr/guides/rgpd-sanction/#:~:text=L'imprudence%20et%20la%20n%C3%A9gligence,caract%C3%A8re%20personnel)%20de%20nombreuses%20obligations.

Grandmontagne, Y. (2016, mars 02). DSI – Comment gérer le patrimoine informationnel de l'entreprise ? Récupéré sur CESIN: https://www.cesin.fr/article-dsi-comment-gerer-le-patrimoine-informationnel-de-l-entreprise.html

Guédri, Z., Gomery , R., & Vuichard , L. (2011, 07). Qualité des données. Consulté le 04 17, 2019, sur Micropole: http://www.micropole.fr/micropole/fr/fr-fr/file.cfm?contentid=1092&fbclid=IwAR2iSbCbVPrfyeXLzXRvShDLU9iuy2bp8G9ZIgd8X9TErnmFPYk35uvwOdg

Hébert, M. (2016, mai). Comparaison de deux approches de conception pour un système de gestion des données de référence. Récupéré sur Usherbrooke.ca: https://www.usherbrooke.ca/cefti/fileadmin/sites/cefti/documents/Essais/Essai_hebert_michel_vFInale2.pdf

IBM. (2019). Gestion des métadonnées. Consulté le 04 03, 2019, sur IBM: https://www.ibm.com/support/knowledgecenter/fr/SSZJPZ_11.3.0/com.ibm.swg.im.iis.productization.iisinfsv.overview.doc/topics/cisomsintro.html

ISO. (2019). ISO 9000 : Management de la qualité. Consulté le 06 10, 2019, sur ISO: https://www.iso.org/fr/iso-9001-quality-management.html

ISO. (2019). ISO/IEC 27001 Management de la sécurité informatique. Consulté le 06 02, 2019, sur ISO: https://www.iso.org/fr/isoiec-27001-information-security.html

ISO. (s.d.). ISO/IEC 27002:2013 - Technologies de l'information. Récupéré sur iso.org: https://www.iso.org/fr/standard/54533.html

ISO. (s.d.). ISO/IEC 27005:2018 Technologies de l'information — Techniques de sécurité — Gestion des risques liés à la sécurité de l'information. Récupéré sur iso.org: https://www.iso.org/fr/standard/75281.html

ISO. (2019). ISO/IEC 27040:2015 - Technologies de l'information -- Techniques de sécurité -- Sécurité de stockage. Consulté le 05 20, 2019, sur ISO: https://www.iso.org/fr/standard/44404.html

ISO. (2011). ISO/IEC 29100:2011. Récupéré sur ISO: https://www.iso.org/obp/ui/#iso:std:iso-iec:29100:ed-1:v1:fr

ISO. (2017, 06). ISO/IEC 29134:2017. Récupéré sur ISO: https://www.iso.org/obp/ui/#iso:std:iso-iec:29134:ed-1:v1:fr

Jdn. (2020, 07 31). Nombre d'utilisateurs de Facebook dans le monde. Récupéré sur journaldunet.com: https://www.journaldunet.com/ebusiness/le-net/1125265-nombre-d-utilisateurs-de-facebook-dans-le-monde/

Labialle, J.-C. (2019, 05 28). Thierry Breton auditionné sur la souveraineté numérique. Récupéré sur Sénat: https://www.senat.fr/presse/cp20190528a.html

Larousse. (s.d.). Définition - Risque. Récupéré sur Larousse: https://www.larousse.fr/dictionnaires/francais/risque/69557

Le monde. (2018, 12 27). Une amende de 250000 euros à Bouygues Telecom pour ne pas avoir "protégé les données" de ses clients. Récupéré sur lemonde.fr: https://www.lemonde.fr/pixels/article/2018/12/27/protection-des-donnees-la-cnil-inflige-une-amende-de-250-000-euros-a-bouygues-telecom_5402633_4408996.html

le Parlement Européen et le Conseil de l'Union Européenne. (2016, 04 27). RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL. Récupéré sur https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679

Les Echos. (2018, 06 07). Données personnelles : une amende record pour Optical Center. Récupéré sur lesechos.fr: https://www.lesechos.fr/2018/06/donnees-personnelles-une-amende-record-pour-optical-center-992089

L'internaute. (s.d.). Patrimoine de l'entreprise. Récupéré sur L'internaute: https://www.linternaute.fr/dictionnaire/fr/definition/patrimoine-de-l-entreprise/

Loukil, F., Ghedira-Guegan, C., Benharkat, A., Boukadi, K., & Maamar, Z. (2019, 06 03). Privacy-Aware in the IoT Applications: A Systematic Literature Review. Récupéré sur HAL: https://hal.archives-ouvertes.fr/hal-01630125/document

Magniez, A. (2016, 12 26). Gouvernance des données : Etes-vous « Data Centric » ? Consulté le 03 10, 2019, sur IT-expert magazine: https://www.it-expertise.com/gouvernance-des-donnees-etes-vous-data-centric/

mc2i. (2012, 01 11). Qu'est-ce qu'une DSI ? Récupéré sur mc2i: http://www.mc2i.fr/Qu-est-ce-qu-une-DSI#:~:text=La%20direction%20des%20syst%C3%A8mes%20d,d%C3%A9ployer%20et%20exploiter%20le%20SI.

Miller, B. (Réalisateur). (2011). Le Stratège [Film].

Montjoye, Y.-A. d. (2016, 10 07). Métadonnées et vie privée, l'équation insoluble? Récupéré sur Variances: http://variances.eu/?p=1416

N.C. (2019, avril 21). Quel rôle pour le responsable de traitement? Récupéré sur données-rgpd.fr: https://donnees-rgpd.fr/traitement-donnees/role-responsable-traitement/

Nurcan, S., & Rolland, C. (2006). 50 ans de Système d'Information. Récupéré sur Panthéon Sorbonne: https://www.pantheonsorbonne.fr/fileadmin/diplome_mastersic/chapitreSI_anniversaire.pdf

O'Brien, J. (1995). Les systèmes d'information de gestion. De Boeck Université.

Ooreka. (2019). Normes ISO : tout savoir sur les normes ISO. Consulté le 05 30, 2019, sur Ooreka: https://qualite.ooreka.fr/comprendre/norme-iso

Open Data Soft. (2018, 07 04). Qu'est-ce que la gouvernance des données? Récupéré sur Open Data Soft: opendatasoft.com/fr/blog/2018/07/04/definition-de-la-gouvernance-des-donnees

Pagnamenta, R. (2014, 08 29). Gouvernance de l'information : définition, enjeux et perspectives en ville de Genève. Consulté le 08 31, 2020, sur doc.rero.ch: http://doc.rero.ch/record/232841/files/M12_TM_PAGNAMENTA.pdf

Parlement européen. (2018, 05). Article 35 EU RGPD "Analayse d'impact relative à la protection des données". Récupéré sur privacy-regulation.eu: https://www.privacy-regulation.eu/fr/35.htm

Parlement européen et du Conseil. (s.d.). Art. 47 GDPR - Binding corporate rules | General Data Protection Regulation (GDPR). Récupéré sur gdpr-info.eu: https://gdpr-info.eu/art-47-gdpr/

Pearlman, S. (2020, 06 23). Intégration des données - Présentation générale. Récupéré sur Talend: https://fr.talend.com/resources/what-is-data-integration/

Perrin, J. (2016, 03 15). Chiffrement : fonctionnement et enjeux. Consulté le 06 10, 2019, sur le-vpn.com: https://www.le-vpn.com/fr/chiffrement-fonctionnement-et-enjeux/

Poussineau, J. (2013, 05 23). Les différents modèles de gestion des données de référence (MDM). Consulté le 04 4, 2019, sur AXOPEN: https://blog.axopen.com/2013/05/les-differents-modeles-de-gestion-des-donnees-de-reference-mdm/

Power, M. (2015, 06 01). Un nom, c'est quoi ? Le risque image et la transformation de la notion de responsabilité sociale. Récupéré sur Cairn.info: https://www.cairn.info/revue-securite-et-strategie-2011-2-page-5.htm

R, G. (2018, 02 07). Data Governance ou gouvernance des données : Qu'est-ce que c'est? Consulté le 05 20, 2019, sur Le Big Data: https://www.lebigdata.fr/data-governance

Reactive-Executive. (2020, 02 12). Les différents métiers et rôles du service des ressources humaines. Récupéré sur Reactive-Executive: https://www.reactive-executive.com/metier-ressources-humaines/

Régnier-Pécastaing, F., Gabassi, M., & Finet, J. (2008). MDM : Enjeux et méthodes de la gestion des données. Malakoff: Dunod.

Reix, R., Fallery, B., Kalika, M., & Rowe, F. (2016). Systèmes d'information et management. Vuibert gestion.

Rever data engineers. (2019, 10 21). La gestion du cycle de vie des données, c'est quoi ? . Récupéré sur dataengineers.eu: https://www.dataengineers.eu/fr/la-gestion-du-cycle-de-vie-des-donnees-quesaco/

Rieffel, R. (2014). Révolution numérique, révolution culturelle ? . (Gallimard, Éd.) Consulté le 08 31, 2020, sur Excerpts.numilog: http://excerpts.numilog.com/books/9782070451722.pdf

Rispoli, N. (2016). L’audit de la protection des données personnelles dans l'entreprise. Récupéré sur ifaci.com: https://www.ifaci.com/wp-content/uploads/RISPOLI-Nadege.pdf

Roemer, K. (2018, 04 24). GDPR Compliance : Redefining the price of privacy. Consulté le 08 31, 2020, sur CItrix blogs: https://www.citrix.com/blogs/2017/04/04/gdpr-compliance-redefining-the-price-of-privacy/

Rosenberg, D. (2013). Data is before the Fact.

Rouach, D. (2016). La veille technologique et l'intelligence économique. Paris: Puf.

Rouse, M. (2016, 04). Données semi-structurées. Récupéré sur Whatis.com: https://whatis.techtarget.com/fr/definition/Donnees-semi-structurees#:~:text=Les%20donn%C3%A9es%20semi%2Dstructur%C3%A9es%20sont,traiter%20que%20des%20donn%C3%A9es%20brutes.

Salgues, F. (2018, 05 14). 8 Français sur 10 prêts à boycotter les marques non-conformes au RGPD. Récupéré sur emarketing.fr: https://www.e-marketing.fr/Thematique/data-1091/Breves/Fran-ais-prets-boycotter-marques-non-conformes-RGPD-330714.htm

Senat. (s.d.). dossiers d'histoire - Le Sénat invente les autorités administratives indépendantes. Récupéré sur senat.fr: https://www.senat.fr/evenement/archives/D45/context.html

Silicon. (s.d.). Garantir la disponibilité des données. Récupéré sur Silicon: https://www.silicon.fr/hub/hpe-intel-hub/garantir-la-disponibilite-des-donnees

Sitbon, D. (2019, 01 7). Norme ISO 27001: qu'est-ce que c'est ? Décryptage. Consulté le 06 5, 2019, sur Le blog AEC: https://www.blog-logiciel-btp.com/2019/01/07/quest-ce-que-la-norme-internationale-iso-27001/

Skills4All. (s.d.). Certification ISO 27000 : Pourquoi se former ? Comment ? Récupéré sur Skills4All: https://www.skills4all.com/certification-iso-27000-pourquoi-se-former-comment/

Solutions Numériques. (2013, mai 1). L'actif informationnel, valeur sûre de l'entreprise. Récupéré sur Solutions Numériques: https://www.solutions-numeriques.com/articles/lactif-informationnel-valeur-sure-de-lentreprise/

Sweeney, L. (2002, 05). k-anonymity : a model for protecting privacy. Récupéré sur https://epic.org/privacy/reidentification/Sweeney_Article.pdf

Takvorian, J.-F. (2013, 05 22). Présentation de la norme ISO 27002 – code de bonnes pratiques pour le management de la sécurité de l'information. Récupéré sur InfoQualité: https://www.infoqualite.fr/presentation-de-la-norme-iso-27002-code-de-bonnes-pratiques-pour-le-management-de-la-securite-de-linformation/

Technopedia. (2019). What is data security? . Consulté le 06 10, 2019, sur technopedia: https://www.techopedia.com/definition/26464/data-security

Trouchaud, P., Guédri, Z., & Gomery, R. Qualité des données : Quelle(s) vérité(s) dans les entreprises. Livre blanc.

UNESCO. (s.d.). Construire des sociétés du savoir. Récupéré sur Unesco: https://fr.unesco.org/themes/construire-soci%C3%A9t%C3%A9s-du-savoir

VALCIN, G. (2017, 12 04). Livre Blanc RGPD. Consulté le 08 2020, sur slideshare: https://www.slideshare.net/GuillaumeValcin/guillaume-valcin-livre-blanc-rgpd-gdpr-white-paper-2

Wikihow. (s.d.). Comment responsabiliser ses employés. Récupéré sur Wikihow: https://fr.wikihow.com/responsabiliser-ses-employ%C3%A9s

Wikipédia. (s.d.). Atos. Consulté le 2020, sur Wikipédia: https://fr.wikipedia.org/wiki/Atos

Zeenea. (2019, 09 09). Les définitions : données et métadonnées. Récupéré sur Zeenea: https://zeenea.com/fr/quelle-est-la-difference-entre-les-donnees-et-les-metadonnees/

Annexes

Annexe 1 – Document de conformité

Cette annexe présente les questions inclues dans le document de conformité à remplir pour chaque traitement.

- Qui est le responsable de traitement ?
- Quel est le nom de la division en charge du traitement ? (nom du chef de service, nom du service)
- Quel est nom du traitement ?
- Quel est la nature et type de plate-forme (par exemple, application mobile, SaaS, licence,...)
- Quel est le calendrier du projet pour la mise en œuvre du traitement ? Quelle est la périodicité du projet ? S'agit d'un nouveau projet ou d'un projet déjà en cours ?
- Quel est le champ d'application du traitement ? S'agit-il d'un traitement local ou global ?
- Quel est le support sur lequel les données sont conservées (serveurs, logiciels, réseaux, papier) ?
- Quelle est la finalité du traitement ?
- Pourquoi le traitement est-il légitime ?
- Le traitement permet-il d'évaluer … ?
- Le résultat du traitement est-il utilisé pour prendre une décision sur la situation ou l'évolution de la personne concernée ?
- Le traitement comporte-t-il une prise de décision automatisée qui peut avoir une conséquence sur la situation ou l'évolution de la personne concernée ?
- Existe-t-il un seul responsable de traitement des données ou une autre entité est-elle un co-contrôleur ?
- Le traitement exige-t-il que le respect d'une réglementation ou un code de conduite spécifique ?
- Quelle est la localisation des personnes concernées ?
- Quelles sont les catégories de personnes dont les données sont traitées ? (employés, sous-traitants, visiteurs)
- Le traitement concerne-t-il des personnes "vulnérables" ? (enfant…)
- Quelles sont les catégories standard de données à caractère personnel traitées ?
- Quelles sont les catégories de données à caractère personnel "sensibles" traitées ? (données bancaires, données de santé…)
- Les ensembles de données sont-ils mis en correspondance ou combinés avec d'autres ensembles de données collectées autrement ?
- Le traitement implique-t-il une utilisation innovante de solutions technologiques ou organisationnelles ?
- Une durée de conservation a-t-elle été définie pour le traitement des données à caractère personnel ?
- Toutes les catégories de données à caractère personnel ont-elles la même durée de conservation ?
- Quelle est la durée définie de conservation des données à caractère personnel ?
- Veillez-vous à ce que les données restent exactes et à jour ?

- Comment les données personnelles sont-elles supprimées (afin de respecter la période de conservation des données définie) ?
- Quelle est l'origine des données ?
- Qui, au sein du groupe, a accès aux données à caractère personnel traitées ?
- Les données personnelles sont-elles partagées avec un tiers ?
- Le traitement implique-t-il la fourniture de tout ou partie des services par une société qui n'est pas la société initiale identifiée ci-dessus comme étant la société qui met en œuvre l'application (ci-après un "sous-traitant") ?
- Combien de sous-traitants sont-ils utilisés et où sont-ils situés ?
- Combien de sous-traitants externes sont utilisés ?
- Assurez-vous que des informations claires et complètes ont été fournies aux personnes concernées ?
- Comment les personnes concernées sont-elles informées du traitement de leurs données personnelles ?
- Êtes-vous en mesure de fournir des copies de données à caractère personnel si les personnes concernées en font la demande ?
- Avez-vous la possibilité de supprimer des données à caractère personnel si les personnes concernées le demandent ?
- Êtes-vous en mesure de modifier/corriger/mettre à jour des données si les personnes concernées le demandent ?
- Quelles sont les mesures de sécurité mises en œuvre ?

Onglet sous-traitant

- Quel est le nom de l'entité signataire de l'accord ?
- Quel est le service fourni ?
- Le fournisseur fournit-il des services d'hébergement, d'administration, de soutien, de maintenance ou d'autres services lui permettant d'avoir accès aux données ?
- Quelles sont les principales catégories d'activités de traitement des données à caractère personnel qui sont menées par le fournisseur ?
- Avant la sélection, le fournisseur (=processeur) a-t-il fourni des éléments démontrant qu'il offre des garanties suffisantes concernant le traitement des données à caractère personnel ?
- Un accord a-t-il été signé avec le sous-traitant ?
- Où se situent les activités de traitement du fournisseur A (y compris les serveurs, les bases de données et/ou les personnes qui ont accès aux données à caractère personnel à des fins d'assistance et de maintenance sur une base régulière ou occasionnelle, etc.) ?
- Si les données proviennent de l'Union européenne, veuillez préciser quelles garanties sont mises en œuvre si le fournisseur A (ou l'un de ses services) est/sont situé(s) en dehors de l'UE ou si des données personnelles sont disponibles en dehors de l'UE.
- Veuillez donner la liste du personnel du fournisseur A (catégories de personnes) ayant accès aux données à caractère personnel contenues dans ou générées par l'application ?
- Le fournisseur fait-il appel à un ou plusieurs sous-traitants (y compris des sociétés du même groupe)
- Les données à caractère personnel sont-elles destinées à être partagées avec une tierce partie à la convention avec le sous-traitant (autre qu'un sous-traitant du fournisseur) ?

Annexe 2 – Analyse d'impact des risques

Cette annexe présente la description de la réalisation d'une analyse d'impacts des risques.

La première étape permet la description du process étudié.

Contexte

Cette section permet d'obtenir une vision claire du(des) traitement(s) de données à caractère personnel considéré(s).

Vue d'ensemble

→ *Identifier et présenter l'objet de l'étude*

- Quel est le traitement qui fait l'objet de l'étude ?
- Quelles sont les responsabilités liées au traitement ?
- Quels sont les référentiels applicables ?

Données, processus et supports

→ *Délimiter et décrire le traitement considéré de manière détaillée*

- Quelles sont les données traitées ?
- Comment le cycle de vie des données se déroule -t-il (description fonctionnelle) ?
- Quels sont les supports des données ?

Principes fondamentaux

Cette section permet de bâtir le dispositif de conformité aux principes de protection de la vie privée.

Proportionnalité et nécessité

→ *Démontrer que vous mettez en œuvre les moyens nécessaires pour permettre aux personnes concernées d'exercer leurs droits.*

- Les finalités du traitement sont-elles déterminées, explicites et légitime ?
- Quel(s) est (sont) le(s) fondement(s) qui rend(ent) votre traitement licite ?
- Les données collectées sont-elles adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données ?
- Les données sont-elles exactes et tenues à jour ?
- Quelle est la durée de conservation des données ?

Mesures protectrices des droits

→ *Démontrer que vous mettez en œuvre les moyens nécessaires pour permettre aux personnes concernées d'exercer leurs droits.*

- Comment les personnes concernées sont-elles informées à propos du traitement ?
- Si applicable, comment le consentement des personnes est-il obtenu ?
- Comment les personnes concernées peuvent-elles exercer leur droit d'accès et droit à la portabilité ?

- Comment les personnes concernées peuvent-elles exercer leurs droits de rectification et droit à l'effacement (droit à l'oubli) ?
- Comment les personnes concernées peuvent-elles exercer leurs droits de limitation et droit d'opposition ?
- Les obligations des sous-traitants sont-elles clairement définies et contractualisées ?
- En cas de transfert de données en dehors de l'Union européenne, les données sont-elles protégées de manière équivalente ?

Annexe 3 – Retranscription des entretiens

Entretien 1

Cet entretien a été réalisé avec un membre de la Direction des Ressources Humaines.

RA : Bonjour, merci d'avoir accepté ce petit moment. Je t'en ai déjà un peu parlé, mon sujet de mémoire de M2 porte sur les normes et règlements comme opportunité de maitrise et de protection du patrimoine informationnel dans une organisation. J'étends ce sujet à une mise en pratique sur la mise en application du RGPD au sein d'un service RH. Mon but est de montrer qu'il s'agit d'une opportunité et non d'une contrainte et qu'il s'agit d'un levier de performance opérationnelle interne.

M : En fait, pour moi, il y a des contraintes. Il y a des contraintes. Parce que dès lors que tu parles de changement, c'est juste du travail supplémentaire. Il faut s'adapter au changement. Il y a des gens qui sont foncièrement opposés à tout changement parce que ça leur met du stress. Mais, à partir du moment où tu comprends que les avantages que tu vas en retirer sont beaucoup plus importants que de rester dans la situation actuelle... Tu as cinq étapes lors des changements : tu as la surprise, le rejet, l'hésitation, l'acceptation, et puis finalement, tu as aussi le cinquième qui est de dire, enfin tu ne passes pas forcément par tout ça mais aussi tu es à fond dans le truc. Ça arrive moins souvent mais tu peux porter et incarner le changement sur le thème qu'on t'a fixé au départ. En général, tu n'es pas en opposition. Tu passes par la surprise ou la joie c'est-à-dire ça fait longtemps que tu attends le changement. La plupart des gens s'arrête à la deuxième étape, c'est-à-dire ne sont pas content, ou freine des quatre pieds. C'est de toute façon une contrainte, mais le poids de cette contrainte si tu prends du recul et si tu regardes en projetant dans la nouvelle situation, potentiellement c'est une situation qui est… Moi c'est comme ça que je fais dans mon job. En fait, tu es dans une situation qui ne te convient pas sur un sujet, en général c'est sur un sujet bien précis. Tu veux faire évoluer le sujet pour que ça convienne une situation où tu es à l'aise. Ça peut être une opportunité.

RA : Ma problématique générale c'est ça. Après j'avais des sous-problématiques qui étaient : quels sont les comportements à adopter et quels sont les moyens à mettre en place ? À l'issue de ma partie théorique où j'ai défini le patrimoine informationnel, la différence entre donnée et information. J'ai aussi parlé de tout le cadre légal en passant par les normes ISO, les BCR, et finalement, le RGPD. La troisième partie de mon état de l'art porte sur les moyens et comment mettre en place la conformité. J'ai, pour ma partie résolution, trois solutions : la première sur la sensibilisation des acteurs avec une phase de préparation et de constitution du support et une phase de test pour savoir vraiment comment l'adapter et sensibiliser les acteurs.

M : Comment tu sensibilises tes acteurs ? C'est quoi ton axe principal ?

RA : Des réunions, créer un support de formation, le présenter aux les acteurs avec des cas pratiques pour éviter la présentation purement théorique et durant laquelle ils vont s'ennuyer et ne pas savoir l'appliquer.

M : Savoir comment s'en servir. J'ai un support de formation, c'est très très bien. On m'a tout expliqué. Si je m'aperçois que ce support de formation il ne convient pas à la réalité concrète du problème auquel je suis confronté, je vais avoir tendance à le mettre de côté, à l'abandonner et à ne jamais le rouvrir. Par contre, si je m'aperçois que je m'en sers c'est pratico-pratique. Je vais pouvoir l'ouvrir et être guidé au fur et à mesure de mon problème. À chaque étape, ce support de formation va être pratique, il va répondre à comment je dois faire ci, comment je dois faire ça. Plus tu te rapproches de l'utilisateur final en termes de support, plus le support de formation est chiant à faire mais il servira dans le temps. Tu vas te retirer du travail parce que tu en as consacré beaucoup au départ. C'est comme si je te disais tu dois former 10 services à un truc, tu passes 1 heure à faire le support de formation et puis les 10 services vont s'en servir une première fois quand tu vas leur présenter, et puis vont très vite l'abandonner car ne correspond pas à la réalité de leur terrain. Ce qu'ils vont faire c'est qu'ils ne vont pas se servir de ton support, mais par contre, dans chacun des services, tu as une personne qui va te contacter une fois par semaine, et ça va durer une heure, et donc globalement tu vas perdre 20 heures au téléphone avec chacun d'eux alors que tu aurais pu passer une seule fois 10 heures sur ton support de formation. C'est en ça que je me suis battu, j'ai arrêté parce que je n'ai plus le temps, mais lorsque j'étais au reporting, je disais « de faire très bien une documentation, parce que le mois prochain c'est une autre personne qui fait, il n'y a aucune question et la personne va se débrouiller toute seule. Vous ne faites pas très bien et la personne va venir te voir pour te demander « comment tu as fait ça ? Comment tu as fait ça ? » » Et globalement, le temps que tu pensais avoir gagné en ayant fait ton support de formation, la personne va se débrouiller par elle-même, tu ne l'auras pas du tout gagné. C'est super important. Rester proche du terrain. Je pense que nos élites perdent cette notion de rester proche du terrain lorsqu'ils prennent une décision. Ils ne se demandent pas concrètement « comment ça va être mis en œuvre ? Et qu'est-ce que ça va impacter ? » C'est normal, sinon aucune décision ne serait prise. On donne une décision, on donne un cap, voici ce qu'on veut mettre en place, maintenant la déclinaison pratique, ça les regarde quasiment plus. Ce sont les petites mains.
C'est une bonne idée le support de formation. Il faut rester en contact avec le terrain et en contact avec les équipes. Avoir un support qui est vraiment ancré sur le pratique et avoir un relationnel établit avec les équipes, régulier. Il ne s'agit pas de faire une formation au mois de septembre et de dire qu'on se revoit dans trois mois quand tout sera fera fait pour risquer de dire « je ne comprends pas rien est fait ».

RA : Oui. Quand j'ai conclu sur cette solution, j'ai précisé que c'était une amélioration continue puisqu'avec le retour des acteurs, on peut constituer une foire aux questions où

on peut avoir les questions, les situations qui ont amenées les questions et ça permet d'avoir un support complémentaire à la formation.

M : Il faut que tu prévoies aussi c'est qu'on a tendance à croire que le changement c'est « je viens, j'analyse une situation, j'apporte des solutions et j'accompagne les solutions ». A mon avis, ce qu'on oublie souvent c'est quand tu accompagnes les gens dans leurs solutions, c'est aussi de se remettre en cause. Ce n'est pas seulement la solution que je t'apporte, mais c'est la solution que je t'apporte et que je suis capable de revoir pour l'adapter pour avoir une meilleure solution. C'est ce que tu es en train de dire en partie. C'est une partie qu'on oublie. Ce n'est pas j'analyse, j'apporte une solution et je la décline et j'accompagne. C'est quand je dis j'accompagne ça veut dire que je suis capable de revenir sur ma solution et de la faire évoluer. C'est super important. Ce sont des points, comme tu dis j'accompagne, je décline, j'analyse, pour moi c'est un des points principaux de l'accompagnement.

RA : De pouvoir décliner la solution, de pouvoir accompagner…

M : Tu as l'analyse, l'accompagnement au sens je crée une documentation, je crée une formation, je crée un lieu d'échange, je les informe, je les accompagne… et je revois ma solution. C'est-à-dire si tu n'as pas le retour de la base, parce qu'ils vont être confrontés aux difficultés et que tu vas leur apporter ta solution. Et ils vont l'appliquer dans la mesure du possible, mais parfois, ta solution elle n'aura pas pensé à tout et potentiellement l'environnement aura aussi pu évoluer. Ta solution ne pourra plus s'appliquer, parfois sur un aspect particulier mais elle ne pourra plus s'appliquer. Revoir ta solution régulièrement avec eux, c'est l'avantage de cette remontée d'informations.
On pense souvent que j'ai la solution – on me demande de faire un truc, j'analyse, j'apporte une solution, un mécanisme, je mets en place, j'accompagne et je suis là pour répondre aux questions, et après je mets de côté. Ce que je vois souvent, ce qui manque souvent, c'est j'accompagne mais je me rends compte que « ça n'y avais pas pensé, je reviens sur mon support et je l'adapte ». L'adaptation ce n'est pas seulement les autres à qui on demande de procéder au changement, c'est aussi nous dans l'accompagnement de se dire, de se remettre en cause et de dire « je vais changer moi aussi ma façon de voir les choses ». Parce que je pensais que ça va être A, B, C, D et en fait, je m'aperçois que D n'existe plus.

RA : Selon toi, l'impact que ça peut avoir sur les acteurs d'avoir justement une sensibilisation et un suivi ?

M : Le suivi et l'écoute. L'écoute c'est super important. L'écoute c'est ce qu'on vient de dire. Il ne faut pas oublier ce point-là. L'impact peut être bien, après il ne faut pas oublier que la dimension terrain est très importante. Je suis super content d'avoir ce support, d'avoir des directives précises, je suis super content parce que dans ce projet-là, je sais

où je vais, je sais ce qu'il va m'apporter. Après concrètement, je n'ai pas le temps. Ce n'est pas que je ne veux pas, au contraire, je me dis, par rapport à ce sujet ou par rapport à un autre, quand on m'apporte une solution, très clairement je sais que ça va me faire gagner un jour de travail par mois. Je suis à fond pour cette solution. Je la décline auprès de mes équipes, j'essaie de faire en sorte que si moi je ne peux pas y aller directement au moins mes équipes puissent y aller. Peut-être que je n'ai pas le temps. La difficulté elle est là : quel est l'apport de la solution sur les équipes ? Je dirais que du positif. Mais l'environnement et la contrainte dans laquelle je me trouve à ce moment-là, je ne peux pas dire qu'il n'y a que du positif. C'est que je suis obligé d'adapter ce qu'on me demande à la réalité de mon environnement et de mon terrain. C'est comme si tu disais, tu as un stade de foot, tu as un terrain de foot, tu as mec qui vient te dire à un moment « on a changé les règlements, et dorénavant, on va faire plutôt un terrain trapézoïdal. Il ne va plus être rectangulaire. Il va changer ton environnement et il va te dire, par contre j'ai trouvé une solution au lieu d'être trapézoïdal comme ça – parce que ça c'est la contrainte qu'on me demande de faire – on va le faire trapézoïdal comme ça. Il ne sera plus rectangulaire vu du haut, je t'apporte la solution, on va tout décaler d'une telle manière, je vais t'apprendre à travailler sur ce nouveau terrain. Je t'apporte la solution et je vais te guider pour qu'on la réalise ensemble. Sauf qu'il y a 22 joueurs sur le terrain plus l'arbitre, il ne faut pas les déranger, ça joue encore. C'est ça la difficulté. Soit on arrête le match soit on trouve les moyens pour que la solution s'adapte à la situation pour être réalisée. Si on part du GDPR, ça ne date pas d'hier.

RA : Ça fait deux ans.

M : Voilà, donc ça devrait déjà être en train de jouer sur les bonnes règles. Je me dis, potentiellement jouer sur un terrain trapézoïdal adapté pourquoi pas. Il y a des nouvelles règles. L'accompagnement, le support tout est là. J'ai en face de moi quelqu'un de plutôt sympathique, agréable, avec qui je peux échanger, qui m'écoute. Mais je n'ai pas le temps.
L'apport, je ne sais pas comment te dire… On ne peut pas résumer à l'apport sur un utilisateur. C'est comme si tu avais des profils d'utilisateurs – pour lui, ça va impacter franchement son quotidien mais globalement le bénéfice il ne va pas le voir, ou alors nul pour lui. Par contre, pour son responsable ou le service qui travaille à côté, lui il ne va pas avoir beaucoup d'effort à faire, c'est l'autre qui va les faire, mais par contre les bénéfices il va les voir. Je pense on ne peut pas parler d'un apport en général. C'est un apport collectif et non individuel. Tu peux avoir un apport collectif pour la boite, pour tes process, mais il faut bien définir ce dont on parle.

RA : Si on revient sur la sensibilisation de janvier sur le RGPD.

M : La formation qu'on avait eue ? Oui c'était très bien. C'était très bien. Moi ce que j'ai aimé dans cette sensibilisation c'est qu'au-delà des acteurs on a sensibilisé également

nos clients. On n'a pas sensibilisé uniquement les gens qui jouaient sur le terrain, on a sensibilisé également les spectateurs autour, les publicitaires, les fédérations, les clubs de foot autour. On n'a pas sensibilisé seulement ceux qui devaient agir. On a sensibilisé tout le monde et donc ça veut dire que moi, si tu as sensibilisé mon chef, même si mon chef n'a aucune action à faire là-dedans, tu as sensibilisé mon chef. J'ai trouvé ça bien parce que ça touchait un public plus large que simplement ceux qui devaient pratiquer et qui pouvaient être contactés dans ce cadre. Les autres, nos clients, nos responsables, notre hiérarchie, nos environnements ont aussi été sensibilisé au fait. Donc, du coup, tu peux leur dire « tu comprends si je te demande ça c'est aussi parce qu'il y a ça derrière ». Ils comprennent mieux. Mon ressenti sur cette formation c'était très bien. Après, dans une moindre mesure et pas du tout dans le même sujet et pas du tout encore poussé au bout. Tu te souviens du projet qu'on a fait l'an dernier ?

RA : Oui, très bien.

M : Il y a eu une réunion de lancement, où il y a eu beaucoup de monde aussi. La sensibilisation qu'on a eue sur le RGPD avec l'ensemble de la communauté RH. Sauf que là, ce n'était pas sur l'ensemble de la communauté RH, c'était seulement sur quelques groupes de travail, mais simplement quelques groupes réunis en même temps en session plénière. Et souvent ça se passe comme ça les formations. Ça commence par je vous délivre. Ce qui m'a manqué c'est que… tu as accompagné les personnes des différents services, moi je le vois très bien, j'ai identifié la pro, l'experte du RGPD même si je sais que je dois le faire, je sais que si j'ai la moindre question sur comment remplir le document de conformité, c'est toi. Tu n'es pas seulement la référante, tu es la personne qui le fait. Tu as accompagné, tu as déployé cette solution à l'ensemble. Mais du coup, ton accompagnement il est individuel. Tu n'as pas, et tu aurais pu, je pense, développer cet accompagnement parfois par petit groupe et collectif. L'avantage que ça aurait amener comme solution, selon les groupes, on l'a vu sur le projet ça ne fonctionnait pas mais parce que le lien ne s'est pas fait. Si tu mets 2-3 groupes ensemble, et qui sont relativement proches au quotidien ses petits groupes. Si tu mets des petits groupes qui ont l'habitude de travailler ensemble et que tu les formes, les accompagne sur de nouvelles données peut-être qu'ils ne vont pas te solliciter toi mais s'entraider. Du coup, ils vont monter en compétences entre eux. Entre deux points réguliers, ce n'est peut-être pas toi qu'ils vont contacter mais ils vont s'auto-émulsionner. Il ne faut pas que ça aille trop loin parce qu'ils peuvent t'inventer de nouvelles règles, de nouveaux *templates*… mais peut-être que ça… C'est ce que je recherche de plus en plus quand on me donne un sujet parce que 1) je n'aime pas travailler tout seul et 2) j'adore travailler avec les autres.
Quand tu prends quelqu'un de la DAS, du CSP et du C&B et que tu les mets ensemble dans une salle en disant votre sujet c'est ça et vous devez avancer, ils vont se parler entre eux. Il y a une émulsion qui va se faire. Quand tu fais quelque chose d'un peu

transverse, ça peut partir un peu dans tous les sens aussi. En fonction des interlocuteurs tu ne les abordes pas de la même façon.
J'ai adoré avoir cette sensibilisation et j'ai trouvé ça très très bien parce qu'elle a été aussi officialisante. Ce n'est pas ta demande ou celle de ton service ou de l'extérieur. C'est une demande du groupe, de la hiérarchie. Cet accompagnement-là c'est aussi de l'accompagnement. Le fait que le DRH soit là, j'ai trouvé ça top, parce que j'ai trouvé aussi « j'appuie ce qui va être présenté et ça fait partie de votre job ». Ça officialise et j'ai trouvé ça très bien. Un panel d'invités plus grand ce sont les faits et l'avantage est que tu peux dire à ton client « tu as été convié comme moi à cette réunion-là ». Il sait que le RGPD existe, il sait pourquoi les questions sont posées, il sait que ça prend du temps. Il y a cet aspect-là : l'officialisation des choses et encore une fois, le fait d'avoir un panel plus large, agrandi, derrière tu rassembles les personnalités et tu fais des petits groupes et tu continues à accompagner en collectif transverse mais petit. Ça m'a manqué un petit peu, enfin ça ne m'a pas manqué parce que tu étais là et que ça s'est fait en individuel. Si tu partages une problématique avec d'autres acteurs sans que tu sois là, ça permet de se dire qu'on n'est pas seuls, de se dire qu'il n'y a pas que ma thématique, que d'autres services sont également concernés et de comprendre comment ils abordent le sujet, comment ils ont solutionné leurs problématiques. Après, très clairement sur mes sujets ce n'est pas eux qui vont faire le document de conformité pour moi, ils ont leurs problématiques et j'ai les miennes.

RA : Comme ils ont tous individuellement le même besoin et le même travail à réaliser.

M : Ils ont peut-être dégagé des éléments qui si je les avais appliqués, ça nous aurait permis nous deux d'aller plus vite. Peut-être. Peut-être pas. Peut-être que ça ne s'applique pas partout, peut-être que ça ne peut pas s'appliquer au RGPD. L'accompagnement et le support de formation et la sensibilisation, pour moi, ça a ouvert les portes du truc. Sans ouvrir les portes, les gens n'y vont pas.

RA : Il y a un projet, qui n'est pas encore mis à jour de faire une sensibilisation spécifique pour un service à partir de cas pratiques spécifiques à leurs problématiques.

M : Faire une sensibilisation globale, c'est très bien, faire une sensibilisation par service parce qu'il y a des spécificités c'est très bien. Faire une sensibilisation croisée en mêlant différents services, tu peux ne pas inviter tout le monde en une seule fois, d'ailleurs je pense que tu en as fait 2 ou 3 parce que tout le monde ne peut pas venir à la même, ne possède pas les mêmes disponibilités. Au-delà de ça, la sensibilisation croisée par petit groupe de continuer ce lien et ce façonnement. Tu me dis « la sensibilisation qu'est-ce que tu en as pensé ? » je te réponds que si elle n'avait pas eu lieu… Tu construis un projet en donnant un cap, en donnant une feuille de route, en identifiant les acteurs, en identifiant ce qu'ils vont faire mais en les intégrant au projet. Tu peux les intégrer de manière individuelle et les marquer individuellement mais tu peux aussi faire en sorte

que le RGPD fasse partie de notre quotidien, de nos gènes. Tu fais une piqure de temps en temps, et cette piqure t'injecte le RGPD. Que tu arrives dans un service RH, tu sais ce qu'est le RGPD. Aujourd'hui, j'ai parlé d'un sujet à une collègue qui va le gérer au quotidien en lui disant qu'il y aura aussi le RGPD pour ce sujet à s'occuper. Elle m'a répondu «le RGPD je n'aime pas ça, je ne sais pas faire. » Je lui ai répondu qu'elle ne sache pas faire c'est une chose mais qu'elle n'aime pas ça ce n'est pas possible. Le jour où dans les services et en particulier les services RH, on n'aura plus ce type de réaction, cette gêne, cette peur, cette crainte, ce recul systématique à chaque fois qu'on parle de RGPD, les choses seront gagnées. Il faut injecter dans nos gènes du RGPD. À tous les niveaux, et tout de suite. Je pense que la solution, le fait de faire par petit groupe permet de développer une sensibilisation sur le long terme et qui s'inscrit dans les gênes de la RH. Faire des sensibilisations, désigner un référent par service c'est un début. Ce qui peut me faire peur c'est que ce n'est pas du tout dans les gênes. Si je devais travailler avec une autre personne que toi, qui travaille différemment, j'avais l'habitude de travailler d'une certaine façon, si la personne change totalement sa manière de travailler et dis qu'elle va faire d'une telle manière, je ne le ferais pas. Ce n'est pas dans mes gênes. Il y avait un début avec toi. Tu avais une méthode, ça s'inscrivait dans une certaine façon de faire Il y avait une méthode de travail qui avait été initiée avec toi, une façon de faire qu'on a accepté. Si la méthode change, les gênes n'y sont pas. Je rentre chez Atos, je rentre en RH, je change de service, j'ai une formation RGPD, pas une formation informatique. J'ai un entretien avec la responsable. Pour moi, le RGPD c'est super important, surtout en RH. Je devrais avoir au sein de la RH une personne qui ne fait que ça. Ce n'est pas lui qui va faire, mais ça va être un peu comme le DPO, ça va être le point de contact. J'ai une question, je sais que cette personne est là, un groupe de travail peut se faire autour de cette personne. C'est tellement lourd le RGPD qu'au début on ne savait pas par quel bout le prendre. Quand je vois que les salariés ont accès librement à certaines de leurs données mais peuvent faire une demande pour avoir l'extraction de leurs données. Je pense que c'est quand même très lourd.

RA : Oui… Justement c'est ma troisième solution d'organiser la conformité en implémentant de nouveaux processus, une nouvelle procédure, une nouvelle démarche qui permet justement d'adapter l'existant avec la demande et le besoin.

M : Les solutions ne sont pas incompatibles. Ces trois côtés d'une seule politique. Je pense que c'est ça qu'il faut mettre en place. À mon avis, la sensibilisation à la qualité des données, la sensibilisation au traitement des données ça devrait s'inscrire dans le même cadre. Vous arrivez chez Atos, vous arrivez en RH, voilà ce qu'il faut savoir au début. Tout le reste sera important, mais déjà ça, c'est la première pierre. Il y a quelques cas comme ça : je fais appel à un nouveau prestataire, quelles sont les premières actions ?, un prestataire s'occupe d'une nouvelle société au sein du groupe, un document de conformité est déjà fait pour ce traitement, il est toujours valable…

RA : Oui, mais il faudra ajouter le nom de la nouvelle société dans le document de conformité du traitement concerné

M : Voilà donc il y a une action à faire : « rajouter le nom de la nouvelle société ». C'est quand même un mécanisme, une mécanique qu'il faut avoir dans nos gênes pour y penser directement. Ce n'est pas un frein, ce n'est pas une contrainte. Et ça je peux le faire seulement s'il y a quelqu'un qui me le dit, qui me dit les actions à faire. Dans tel cas, les actions sont les suivantes. Peut-être qu'il existe un guide de bonnes pratiques qui existe… C'est un travail à part entière, ce n'est pas évident.
A mon avis, le changement il est là quand on fait d'une contrainte une opportunité.

RA : Ma deuxième solution est l'organisation de la conformité à travers l'identification des processus et des traitements et des données et la documentation avec les documents de conformité, les mentions à ajouter…

M : Cette deuxième étape, phase de solution, comment tu la déclines concrètement ? Quel impact pour moi utilisateur ?

RA : Une meilleure connaissance du flux qui est fait pour les données, du flux de transmission. On l'a vu sur les derniers sujets qu'on a traité ensemble dans ce cadre, il nous manquait des petites briques

M : C'est exactement ça, il nous manquait des petites briques parce que je n'avais pas la connaissance. Ces documents de conformité nous ont permis de nous poser, de nous poser les bonnes questions aux personnes qui savaient « comment ça se passe ça et ça ? »

RA : Oui exactement. Ça nous a permis d'avoir une meilleure maitrise et de pouvoir mieux décrire.

M : Oui, on a pu avoir une meilleure vision du process pour mieux le documenter pour satisfaire les obligations légales. De moi-même, je n'ai pas le temps de me dire qu'il faut que je fasse ça. Le process c'est super important. En remplissant les documents de conformité, on s'est posé les questions sur les rôles de chacun, qui fait quoi ? à quel moment ? Et aussi le cheminement des données. C'est super important. Peut-être que le RGPD ça permet ça si la cellule RGPD accompagne le service, sinon moi je n'aurais pas le temps de le faire. C'est complètement dramatique, j'aurais préféré te dire « je n'ai pas besoin du RGPD pour connaître les procédures, les flux ». Je le fais parfois mais sinon je n'ai pas le temps de le faire. Le RGPD permet de le faire, à la marge. Quand je dis à la marge, ça dépend des services, il y a peut-être des services qui connaissent leur process, leur relation avec leur prestataire et le traitement des données. Mais, il y a des services qui n'ont pas le temps de le faire. Le RGPD a permis ça, a permis cette connaissance. A

permis de mettre en relief les mécanismes de traitements des données fait par le service ou le prestataire externe et de faire en sorte que le service en question comme le prestataire s'alignent sur une connaissance réelle du traitement des données.

Entretien 2

Cet entretien a été réalisé avec une personne de l'équipe DPO.

RA : Bonjour, je réalise mon mémoire sur les normes et les règlements comme opportunité de maitrise et de protection du patrimoine informationnel avec une problématique qui est de savoir de quelles manières la mise en conformité peut être une opportunité de maitrise et former un levier de performance opérationnelle interne. J'ai réalisé une partie théorique dans laquelle j'ai présenté ce qu'était le patrimoine informationnel, l'usage et la valeur des données. Une seconde partie où j'ai présenté le cadre légal avec les différentes normes et règlements et le RGPD et une troisième partie où je parle un peu plus des méthodes de mise en conformité. La seconde partie de mon mémoire est la partie pratique où là je présente trois solutions dans le cadre de mon sujet. Le but est de comprendre quels sont les comportements à adapter, quels sont les moyens à mettre en œuvre et les enjeux et l'utilité qu'il peut y avoir dans cette mise en conformité. Pour cela, j'ai mis en avant trois solutions. La première c'est la sensibilisation des acteurs et je souhaiterais savoir, selon toi, l'intérêt d'une sensibilisation et dans quel cadre le mettre en place et former un plus ou non.

T : Pour le RGPD ?

RA : Oui.

T : Déjà c'est une obligation légale, en fait de mettre en œuvre des programmes de sensibilisation. C'est-à-dire que toute entreprise doit s'assurer que ces employés ont un niveau de connaissance minimal. C'est quelque chose qui doit être démontré. C'est-à-dire si un jour on a un contrôle d'une autorité, ou le contrôle d'un client, ça peut aussi arriver, il faut qu'on soit capable de démontrer qu'on a bien fait les sensibilisations de nos personnels. La réponse qu'on a choisie c'est de faire des *trainings* obligatoires. Toute personne arrivant chez Atos est obligée de les réaliser. C'est suivi, c'est monitoré. On sait qui a fait le training et a réussi. A réussi c'est a passé le petit examen final. On sait qui a tenté et qui a réussi. On a la possibilité de faire des relances auprès des personnes qui n'ont pas réussi. Mais la difficulté qu'on rencontre par rapport à cette sensibilisation institutionnelle c'est que la notion de formation obligatoire en droit français ça ne peut pas exister en fait. Elle reste basée sur une notion de volontariat et là on rencontre des formes de réticence volontaire ou involontaire. Involontaire ce sont les personnes qui disent « je n'ai pas le temps » ou demander à avoir un code pour justifier ce qu'ils font.

Même si ces trainings durent une heure, enfin parfois un peu plus, parfois un peu moins, ça dépend de ta capacité. Une heure reste une heure, et tu as des personnes qui demandent à justifier le fait que la personne n'ait pas travaillé sur son projet exclusivement. On a des difficultés qui sont comme ça. Légalement, on ne peut pas imposer à quelqu'un de suivre une formation. Par rapport à cette difficulté là que l'on a, qui est réelle, et qui surtout visible en France, chez nos collègues on ne retrouve pas cette réticence. On est un peu à la traine par rapport à nos collègues. On est en dessous du seuil qu'il faudrait. Par rapport à ça, il y a eu des corrections efficaces qui ont été faites. La première est de dire que tout nouvel embauché passe les training obligatoires mais il y a toujours des difficultés. Par exemple, les directs qui sont directement envoyés chez leur client. On a une partie significative de personnes qui n'a pas les moyens matériels de faire ces trainings obligatoires. Des campagnes sont faites. Les managers ont cette responsabilité avec les équipes en charge de la formation de relancer.
Ce qu'on fait ensuite, côté DPO, c'est que j'organise des sessions, une à deux par mois, les personnes peuvent venir plus ou moins spontanément à ces sensibilisations où je fais la présentation, similaire au training informatique, à quelque chose prêt que c'est plus vivant, je suis là pour répondre aux questions, tout le monde peut poser sa questions. On a un certain succès. Les personnes apprennent des choses que ce soit pour leur vie pro que perso. Le RGPD ce n'est pas Atos pour Atos, c'est la vie du citoyen. Après, on a des trainings où les équipes doivent faire un document de conformité et on a fait, par le passé, des trainings sur l'art et la manière de les remplir. Ce sont les moyens de training et d'information qu'on fait. On fait aussi, au moins une fois par an, le jour du Data protection Day, une animation en passant par les équipes de formations. On a régulièrement avec le support de hiérarchie des communications sur ce qui se passe sur le RGPD.

RA : Comment sont communiquées les sensibilisations que tu réalises côté DPO ?

T : C'est fait sur un ciblage de personnes qui n'ont jamais suivi les trainings. Ils reçoivent un mail personnalisé qui est co-signé par la hiérarchie et le DPO et envoyé par la direction de communication.

RA : D'accord. Quel est l'impact selon toi de faire ses sensibilisations en dehors du caractère obligatoire ?

T : Ça nous a permis de remonter nos statistiques pour se rapprocher de nos objectifs. On a mis ça en place il y a à peu près un an. Le bénéfice c'est vu tout de suite, on a les moyens de savoir qui a suivi. On n'a pas atteint l'objectif du groupe mais on en est très proche.

RA : D'accord. J'ai présenté ma solution en décrivant qu'il y a quatre phases pour réaliser une sensibilisation : d'abord une phase de cadrage du périmètre, des acteurs qui

pouvaient être impactés, puis la création des support et la sensibilisation d'un périmètre restreint pour après l'élargir à la population RH dans mon cas.

T : Il y a, en effet des populations qu'on cible plus. Avec le RGPD, on cible plus les RH qui sont amenés à manipuler des données personnelles des employés. Il y a toute une série de training institutionnel ou informel qui existent. On a mis en place plusieurs actions pour que cette population ait un niveau correct de sensibilisation au RGPD. On l'a aussi pour les BID managers qui sont aussi des personnes importantes. Ils réalisent les registres de traitement pour les clients. On accompagne la personne pour la réalisation du premier document de conformité afin de répondre à ses questions. Par la suite, on ne l'aide plus pour entrer dans ce qui doit être fait c'est-à-dire une personne qui renseigne le document de conformité et une personne qui contrôle. Pour toi, comme pour certains BID manager, on a rempli l'objectif de l'autonomie pour réaliser le document de conformité. Ils sont capables de deviner les réticences qu'on [l'équipe DPO] peut avoir lors de la revue. Il est important d'avoir un regard critique lors de la réalisation de ces documents de conformité.

RA : D'accord. On a glissé vers le second point dont je voulais te parler, vers ma seconde solution. Il s'agit de l'organisation de la conformité à travers la réalisation d'un inventaire et d'une documentation.

T : Il y a un site institutionnel qui existe au sein d'Atos. On voit toutes les composantes avec des explications. Lorsqu'on a des audits qualité ou sécurité, ils disent que ces composantes sont très bien. On voit les principales policies du RGPD. Le reproche qu'on a c'est qu'il est en anglais.

RA : Il n'y a pas possibilité de le basculer en français ?

T : On devrait le faire mais il faut trouver un traducteur pour le faire et il y a vraiment de la matière derrière.

RA : Je vais juste revenir sur la partie précédente de la sensibilisation. Est-ce qu'il y a selon toi des moyens à mettre en place pour que les acteurs, par exemple pour le remplissage des documents de conformité, soient on va dire moins réticents à le faire ? Même si c'est obligatoire et qu'il y a un besoin. Qu'ils aient conscience d'avoir un vrai rôle et qu'ils sont acteurs réellement de cette action.

T : Il y a que le management vraiment qui peut avoir de la pression sur eux. C'est-à-dire les traitements, l'équipe DPO ne peut pas les deviner et si tu veux autrefois avant le règlement européen c'était le DPO qui était responsable de la tenue du registre. Le nouveau règlement dit « non ce n'est pas le DPO. Le DPO est juste là en soutien, en support. Le responsable de traitement porte la responsabilité de la tenue du registre. S'il

y a un contrôle, c'est lui qui sera interrogé. Bien-sûr je serais là, je viendrais qu'en qualité de soutien et non en qualité de responsable de traitement. Les personnes n'en ont pas forcément conscience. Ils se disent « il y a le DPO », mais ça ne fonctionne pas comme ça. Les auditeurs interrogeront les responsables de traitement et ça sera à eux de répondre, c'est une obligation légale et il faut qu'ils s'y conforment. Pour le moment, les contrôles ont été évité, mais un jour je vais partir, c'est bientôt et je ne sais pas comment ça va être gérer derrière.

RA : Est-ce que tu sais comment les encourager justement si on peut dire encourager ? pour que justement ce management porte le fait que ces documents de conformité soient faits ou qu'il y ait une sensibilisation de faite. Ça serait quoi les clés selon toi pour qu'ils soient réellement acteurs réels ?

T : Ça serait leur casser un bras si jamais ils ne répondent pas. Franchement là, on ne peut pas. Il n'y a que le patron qu'y puisse dire « faites les documents de conformité pour vos traitements ». Si un jour telle personne fait sa tête de mule et décide de ne pas les faire, d'abord je ne serais pas au courant, et puis il y aura des traitements qui vont échapper. Et puis, il y aura une plainte d'un collaborateur et qui partira à la CNIL. Par rapport à ça, on a des gens qui se sont plaints auprès de la CNIL pour des traitements qui n'ont pas de documents de conformité. Les personnes peuvent dire que le traitement n'a pas été déclaré. Il n'y a jamais eu de regard critique sur le document de conformité. S'il n'y a pas de clause RGPD dans le contrat, il devient dit « non causé » et donc est nul. On peut avoir une bonne solution technique, il n'est pas causé. Un jour, on aura un problème technique qui arrivera, dans toute technique il peut y avoir une anomalie, qu'est-ce qui va se passer ? La CNIL quand elle est venue il y a deux ans, elle a demandé les contrats, c'est la première chose qu'elle regarde et la première chose qu'ils verront c'est l'absence de clause RGPD. On pourra leur dire tout ce qu'on veut, on aura tort de base. Et là, ils verront ce que ça fait.

RA : Effectivement. C'est critique et important. Dans ma solution, que ce soit pour la sensibilisation ou pour la deuxième solution de réalisation des documents de conformité, j'ai dit que c'était un travail continu, d'amélioration continue.

T : Oui c'est un travail d'amélioration continue.

RA : Une fois qu'on a fait une sensibilisation et qu'on a les retours, les questions, on peut améliorer, apporter plus de contenu, avoir une fiche à côté avec des questions réponses avec la question et surtout le contexte de la question. C'est pareil pour les documents de conformité, à chaque fois qu'on a un retour, on voit bien qu'on améliore un petit peu. Même avec les DPIA, on voit bien avec les plans d'actions qu'on met en œuvre à la fin.

Ma troisième solution est l'organisation de la conformité sous l'angle de l'implémentation de nouveaux processus, par exemple de nouveaux processus dans le cadre des demandes de droit d'accès des collaborateurs.

T : Les demandes de droits d'accès ce n'est pas quelque chose de neuf et ce n'est pas quelque chose introduit pas le RGPD. Ça existait déjà sur la loi informatique et ça existe sous cette forme là depuis 1989. Les RH le savent. Autrefois, elles avaient des demandes d'accès, ça s'appelait « pouvez-vous me communiquer mon dossier » et donc elles le faisaient. Maintenant qu'elles ont appris qu'elles ont un DPO, elles se disent « on s'en débarrasse et on file ça au DPO ». Pareil, un jour ça ne marchera pas bien. Le RGPD est venu un peu pervertir en appuyant sur le fait qu'il y a un DPO. Sauf que le DPO n'a pas accès au dossier des personnes et il n'est pas question que les DPO aient accès au dossier des personnes. Ça impliquerait trop de responsabilités. On deviendrait co-responsables de traitement, et on n'y tient pas.

RA : Même si ce n'est pas nouveau c'est le RGPD qui l'a ramené sur le devant …

T : Ce qui se passe en fait, c'est que les gens avec le RGPD, c'est qu'il y a eu tellement de communications dessus, à la fois en interne puis à la fois dans les médias globaux que les personnes se disent « tient faut que j'aille regarder ça ». Il y a eu quelques magnifiques scandales qui sont paru dans les médias et que les gens se méfient du traitement de leurs données personnelles et ont appris qu'il y avait des dispositifs. Ils ont découvert ce droit-là, mais il existait depuis très longtemps. De même que les droits de rectification, suppression. Ça existe depuis une trentaine d'années.

RA : Même si ce n'est pas un nouveau traitement ça impliquerait de nouvelles démarches…

T : Non. Normalement les gens devraient directement demander à leur HRBP ou leur manager. Le passage par le DPO n'est pas du tout nécessaire. Après les personnes font ça parce qu'ils ont vu qu'il y avait un délégué à la protection des données personnelles qui lui devait tout mettre en œuvre pour récupérer les données. Ce sont plus les gens qui se sont dit « ça marchera mieux si je passe par le DPO qu'en passant par le manager». Le RGPD ne concerne pas que le numérique. Il concerne aussi les documents papiers.

RA : Oui, je comprends. J'ai une dernière question avant de conclure. Ma question générale est de savoir de quelles manières la mise en conformité peut contribuer à la maitrise du patrimoine informationnel et former un levier de performance opérationnelle.

T : Là très clairement, le fait d'avoir un registre de traitement pour le compte de nos clients constitue… contribue à former un catalogue des activités qu'on fait pour le

compte de nos clients. Tu ne vois pas parce que ce n'est pas dans le domaine, mais souvent les gens m'appellent pour demander si on fait ce genre de choses ailleurs. Comme on fait les documents de conformité pour toute la France, on devient une grande base de connaissance, avec notre registre on contribue fortement à améliorer la connaissance de notre patrimoine. Ce n'est pas nous qui le constituons mais il contribue à améliorer la connaissance du patrimoine et de manière indéniable.

RA : Dernière question – opportunité ou contrainte ?

T : Les opportunités c'est que ça oblige à travailler propre. Donc il faut bien segmenter, bien détailler les travaux qu'on est en train de faire et d'effectuer.
La contrainte, déjà pour une société comme nous, comme il y a une chasse aux indirects, il n'y a pas beaucoup de DPO, on a très peu de moyens à notre disposition. C'est une loi qui est imposée et donc on est obligé de suivre la loi, et là je parle au sens de l'entreprise. Ça se fait au détriment de la qualité de nos revenus. Tout ce qu'on fait au titre de la loi, on ne peut pas le refacturer au client. Donc le temps qu'on passe à faire sur un document de conformité, les allers retours qu'il peut y avoir dessus, ça c'est infacturable. Peut-être qu'un jour les commerciaux arriveront à trouver une astuce mais pour l'instant c'est un coût pour l'entreprise. C'est directement un coût. Je trouve que l'avantage, ce qui est bien c'est que ça oblige les projets à faire propre donc maintenant ils se posent des questions sur la sécurité, sur la qualité des livrables qu'ils font, sur les traitements qu'ils vont implémenter. Tout ça fait qu'on a une amélioration. On améliore indirectement la qualité des produits qu'on livre à nos clients. Ça augmente de manière considérable la connaissance, le catalogue du patrimoine informatique qu'on peut avoir. La contrepartie c'est un coût.

RA : Merci pour cette réponse complète et pour ta disponibilité.

Entretien 3

Cet entretien a été réalisé avec une personne de l'équipe DPLE.

RA : Bonjour. Merci pour ta disponibilité. Je te contacte aujourd'hui dans le cadre de mon mémoire réalisé pour mon master 2. Mon sujet porte sur les normes et règlements comme opportunité de maitrise et de protection du patrimoine informationnel d'une organisation. Ma problématique est de savoir de quelles manières la mise en conformité peut contribuer à la maitrise du patrimoine informationnel et former un levier de performance opérationnelle interne. Pour faire suite à la revue de littérature que j'ai été amené à faire, et dans le cadre de ma partie de résolution, j'ai mis en avant trois solutions. La première est la sensibilisation des acteurs. J'aimerais savoir ton opinion quant à la mise en place d'une telle action.

C : Tout d'abord, il faut savoir que d'un point de vue règlementaire, nous avons une obligation de formation. Nous avons deux occasions chaque année de pouvoir réaliser des actions de sensibilisation. Tout d'abord, le jour de l'anniversaire du RGPD (25 mai) et lors de la journée de protection des données (28 janvier). Un reporting de suivi est établi pour documenter les sensibilisations et actions qui peuvent être réalisées.

RA : Comme par exemple la sensibilisation au RGPD qui a pu être mise en place au début d'année pour la population RH… Quel est selon toi l'intérêt de faire une sensibilisation particulière pour cette population ?

C : La formation ou sensibilisation est la clé de voute pour Atos. Avoir des sensibilisations permet de respecter les obligations et de respecter des règles. Dans le cadre des demandes de droit d'accès, cela permet aux personnes qui vont mettre en place les actions d'avoir les informations nécessaires pour mettre en pratique. Il y a un intérêt particulier à sensibiliser sur des problématiques spécifiques. Par exemple, des sensibilisations sont faites pour les commerciaux qui vont voir les clients. Nous avons réfléchi à l'idée de mettre en place un jeu afin de rendre la sensibilisation plus vivante.

RA : Quel est selon toi l'impact de réaliser des sensibilisations ?

C : Cela permet d'abord de donner des bons réflexes mais aussi d'attirer l'attention sur ce sujet. En attirant l'attention et en donnant les bons réflexes, ça permet aussi de donner des réflexes supplémentaires comme le fait d'aller voir un juriste dans le cadre de la signature d'un nouveau contrat, ou aller voir le DPO. Cela vise aussi à permettre une prise de conscience des actions à réaliser en particulier pour les contrats. Enfin, l'impact des sensibilisations pour les acteurs est de savoir que ce règlement existe, qu'ils sont concernés et qu'il existe des risques, financier ou réputationnel pour l'entreprise en cas de non-conformité.

RA : Quelle est selon toi la fréquence à mettre en place pour réaliser ses sensibilisations ?

C : Je pense qu'il faut mettre des rappels tous les ans comme par exemple lors de l'anniversaire du RGPD ou de la journée de la protection des données. Il est important de faire des rappels réguliers auprès des acteurs. Il faut saisir les opportunités pour les réaliser. C'est la mise en pratique lors des sensibilisations qui va permettre de déclencher des réflexes. Il y a une prise de conscience du sujet lorsqu'on y est confrontés au quotidien. La sensibilisation a des limites puisqu'on ne peut pas prévoir tous les cas de figure.

RA : Merci pour cette réponse, je comprends bien le lien entre création de réflexes et sensibilisation régulière. Ma seconde solution est l'organisation de la conformité à travers l'inventaire des processus et la mise en place d'une documentation.

C : Dans une organisation telle que la nôtre, il faudrait avoir des outils plus automatisés étendus aux responsables de traitement et sous-traitant qui permettraient la réalisation de cette documentation. Une organisation est à mettre en œuvre et à maintenir avec le DPO et des personnes dans chaque organisation. Les documents de conformité sous format Excel qu'on a sont bien mais des outils plus lisibles et plus faciles d'accès seraient mieux afin d'avoir un meilleur suivi. Le travail est contraignant et nécessite des mises à jour. Le travail est titanesque. Il est plus difficile de mettre à jour les documents de conformité que de les créer.

RA : Quel est selon toi le rôle des acteurs ?

C : Selon moi, il faut des rôles définis avec des SPOC. Une personne responsable de tout ce travail ne suffit pas. Il est important de responsabiliser et sensibiliser chaque acteur pour que les personnes sur le terrain aient conscience des choses à faire et des choses déjà réalisées.

RA : D'accord merci. Pour ma troisième solution, c'est également sur l'organisation de la mise en conformité mais cette fois-ci sur l'implémentation de nouveaux processus en particulier par exemple pour l'exercice des demandes de droit d'accès.

C : C'est important selon moi d'avoir des processus bien clair. Il y a une réelle nécessité d'avoir une démarche identifiée pour une diffusion auprès des services concernés et une implication des acteurs.

RA : Oui et aussi des processus qu'on puisse mettre à jour régulièrement si besoin pour adapter au besoin. Une dernière question pour conclure : selon toi, le RGPD, plus contrainte ou opportunité ?

C : Il s'agit d'abord d'une contrainte. Sa mise en place nécessite une nouvelle organisation, un recrutement spécifique pour des nouvelles missions, la mise en place de sensibilisation supplémentaire. Une contrainte également car le RGPD nécessite du temps pour investir dessus et réaliser les actions nécessaires.
Le RGPD est également une opportunité car il permet le développement de solutions pour transformer ce règlement et cadre légal en opportunité. Il permet d'avoir une maitrise et un aperçu global ce qui est une bonne chose.
Peut-être sa mise en place permet d'empêcher les fuites ?
Il s'agit d'un processus continu puisqu'il n'est jamais possible d'être totalement conforme. Il y a toujours une mise en conformité nécessaire. Notamment car il y a une

mise à jour continue des outils qui évoluent parfois plus vite que notre capacité à se mettre en conformité. Finalement, l'important est de montrer qu'on est dans une démarche de conformité et d'avoir une vue globale de ce qui est fait. Il faut une mobilisation à tous les niveaux hiérarchiques. La mise en conformité au RGPD fait partie de leur métier, c'est une composante de leur métier. Il faut des process sur ce qui est fait au quotidien.

RA : Merci pour cette réponse complète.