Le GDPR

(General Data Protection Regulation)

Auteur : Jean-Michel Tyszka
https://www.linkedin.com/in/jeanmicheltyszka/

Date dernière mise à jour : 5 juin 2017

le cnam

Antoine Vigneron : Formateur en grandes écoles, Délégué Général AFAI / ISACA

TABLE DES MATIERES

1. INTRODUCTION

Nous vivons aujourd'hui dans un monde hyper connecté dans lequel les échanges de données sont omniprésents que ce soit au niveau des individus (échanges de mails, réseaux sociaux), entre sociétés et individus (consultation et téléchargement de contenu, achats de biens ou services en ligne, etc.), entre sociétés (échanges de services ou transactions de tous ordres) ou bien encore entre individus ou sociétés et administrations. L'intégration économique et sociale au niveau de l'Union Européenne (UE) n'a fait qu'amplifier le phénomène.

La "Donnée" est ainsi devenue un élément majeur du commerce mondial et constitue un terreau idéal pour le développement du cybercrime qui prend des formes aussi multiples qu'inventives pour subtiliser ce "trésor numérique". Cette nouvelle forme de banditisme ne met pas seulement en jeu l'intégrité des individus (vols d'identité, comptes en banque, etc.), elle peut également mettre en péril les entreprises qui auront laissé passer les intrus : tout un chacun a en tête les cas récents de la « Panama leak », du cas de la cyberattaque qui aurait pu sonner l'arrêt de TV5 Monde ou des vols d'identifiants à grande échelle chez LinkedIn, Google, Yahoo ou Hotmail.

S'il en va de la responsabilité des entreprises de protéger leurs biens propres, il était urgent de mettre en place un cadre réglementaire concernant la protection des informations qu'elles détiennent sur les individus (que ce soit leurs clients propres, des prospects, via des données collectées en ligne ou achetées à des partenaires ou encore leurs employés). Jusque-là, chaque pays à travers le monde portait la responsabilité de la mise en place d'une règlementation qui pouvait être plus ou moins stricte et plus ou moins contraignante (voir carte ci-dessous). C'était bien le cas en Europe où la situation était à peu près aussi diversifiée que l'union peut compter de pays. [1]

Figure 1-1 : Plus de 80 pays imposent des contraintes sur les données personnelles [1]

[1] Cours du CNAM du NFE210

Il était donc grand temps de définir des règles claires et cohérentes en matière de protection des données à caractère personnel au niveau de l'UE. Ainsi, en 2012, la Commission Européenne a lancé une réflexion sur le sujet et proposé la mise en place d'un règlement sur la protection des données. Un règlement européen (le "GDPR") qui en a découlé est finalement entrée vigueur le 24 mai 2016 et sera applicable dès le 25 mai 2018.

Peu d'entreprises ont encore porté attention à cette règlementation ; moins encore ont débuté les travaux de mise en conformité : selon un sondage Ipswitch réalisé fin 2014 sur 316 entreprises européennes, 52% des sondés ont répondu ne pas être prêts. Plus grave encore 56% ne savaient pas exactement à quoi correspond le sigle GDPR. Presque un an plus tard (Sept 2015), si plus des 2/3 (69%) des professionnels de l'IT ont pris consciences que le GDPR va impacter leur business, presque 1/5 (18%) n'ont toujours aucune idée quant à savoir s'ils seront impactés. En 2017, comme le montre l'article de Laurent Leloup paru sur finyear.com basé sur des résultats issus d'un rapport Véritas de 2017 (« GDPR Report »), voir « Annexe 1 : Non-conformité au GDPR : les entreprises craignent de mettre la clé sous la porte », le situation n'a guère évoluée : les entreprises sont certes maintenant plus au fait de ce qu'est le GDPR mais près de la moitié redoutent de ne pas être en mesure d'y répondre et près de 40% estiment ne simplement pas être en mesure d'identifier et localiser les données concernée par le règlement alors que moins d'un tiers des répondants pense être en conformité. Face aux enjeux d'une part et aux dépenses nécessaires pour se mettre en conformité (le rapport estime qu' « e*n moyenne, les entreprises prévoient de dépenser plus de 1,3 millions d'euros* ») d'autre part, bien des directions restent perplexes.

Si les travaux ne sont pas encore entamés, il y a maintenant urgence à agir !

Nous débuterons ce document de synthèse par un rappel des grandes lignes du projet GDPR, les principaux points à retenir sur le contenu du projet, avant d'aborder la méthodologie pour se mettre en conformité telle que suggérée par la CNIL. Viendront ensuite les difficultés et risques à attendre de l'entreprise : comme toute activité structurante, le GDPR n'est pas sans en comporter. Néanmoins, des opportunités d'envergure pourrait également s'offrir à qui saura les saisir : nous les aborderons également avant de conclure.

Bonne lecture à tous ; n'hésitez pas à me faire part de vos commentaires et remarques !

2. GRANDES LIGNES DU PROJET GDPR

En préambule de la page du Conseil Européen traitant du règlement général sur la protection des données, il est précisé que « cette règlementation met à jour et modernise les principes édictés dans la Directive de Protection des Données de 1995. Elle définit les droits des individus et établit les obligations de ceux qui traitent et de ceux qui sont responsables du traitement des données. Elle établit également les méthodes permettant d'assurer la conformité ainsi que la portée des sanctions qui pourraient être infligées aux personnes qui ne respectent pas les règles. »

Il est à noter que ce texte est à effet direct (c'est à dire qu'il n'y a pas besoin de loi nationale pour le transposer) et sera donc applicable de-facto dès le 25 mai 2018 dans l'ensemble des 28 pays membres de l'Union Européenne (UE) et pour chaque citoyen de l'UE.

2.1. Quoi de neuf ?

Aujourd'hui, en France, les données personnelles sont déjà sujettes à protection par la loi « Informatique et Libertés » du 6 janvier 1978, réformée par la loi du 6 août 2004, qui transposait, de façon libre, la directive européenne du 24 octobre 1995. On est alors en droit de se demander ce qui change par rapport à la législation en rigueur.

Les principes posés restent les mêmes : les entreprises doivent collecter des données proportionnellement à la finalité du traitement, cette collecte doit être loyale (elle doit donc se faire en toute transparence), les personnes concernées ont un droit d'opposition et il existe une interdiction de principe de collecte de données sensibles.

En revanche, le devoir d'information des personnes concernées et les cas dans lesquels leurs consentements sont nécessaires avant la collecte de leurs données ont été renforcés : si une entreprise ou une organisation n'est pas dans une relation contractuelle ou une obligation légale, ne vise pas l'intérêt général ou les intérêts vitaux d'une personne, ou n'a pas de motif légitime pour détenir des données personnelles sur celle-ci, elle n'est pas en droit de les traiter (ce qui comprend la collecte, la conservation, le traitement, la revente, etc.), sauf si elle a obtenu pour ce faire un consentement explicite (dont elle devra être en mesure de faire la preuve sur demande des autorités de contrôle), non équivoque et non tacite, sous une forme simple et intelligible.

Quelques grands principes sont à retenir à ce sujet. Ils sont précisés dans les paragraphes suivants.

Surtout, cette mesure est enfin assortie d'une sanction à la hauteur de l'enjeu. Jusqu'à présent les entreprises en infraction risquaient une amende maximale de 300 000 € en cas de récidive ; et les sanctions étaient bien rares. Avec le GDPR, les sanctions pour l'entreprise reconnue coupable pourront monter jusqu'au maximum entre 4% du chiffre d'affaires annuel mondial de l'exercice précédent ou 20 millions d'euros. Il y a donc fort à parier que ces montants vont faire frémir, tant les dirigeants d'entreprises que les autorités en charge de faire appliquer ce nouveau règlement, bien que pour des raisons diamétralement opposées.

Au cœur de ce dispositif, la CNIL conserve d'importants pouvoirs d'enquête et de sanction. Elle ne sera en revanche plus destinataire des formalités préalables (déclaration, autorisation) : cela renforce en soit l'obligation de moyens des entreprises qui sont désormais supposées être en conformité et qui auront d'autant plus de mal à invoquer leur « bonne foi ». L'autorité de contrôle peut cependant être consultée préalablement au traitement lorsqu'une analyse d'impact indique que le traitement pourrait présenter un risque élevé.

Par ailleurs, des autorités de contrôle européennes pourront désormais renforcer les décisions ou prononcer des décisions conjointes.

2.2. Données à Caractère Personnel (DCP)

Avant d'examiner le GDPR plus en profondeur, il semble indispensable de définir ce que l'on entend par Données à Caractère Personnel (DCP) : il s'agit (selon l'article 2 de la loi informatique et liberté) de 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.

Cela couvre un large périmètre incluant par exemple :

- Des données évidentes d'**identité individuelle** comme :
  - Les noms, prénoms, lieu et date de naissance, numéro de sécurité sociale, adresses (physique et électronique), numéro de téléphone, plaque d'immatriculation d'un véhicule, photo ou vidéo, etc…
- Des **informations professionnelles** telles que statut professionnel, salaire, etc…
- Les **données bancaires** et **fiscales** comme les numéros de carte de paiement, IBAN, revenus ou situation fiscale, etc…
- Des informations sur la **vie personnelle** telles que centres d'intérêt, cookies et autres traces internet, etc…
- Des informations sur la **localisation** telles que géolocalisation (GPS ou GSM), adresse IP, etc…
- Ou encore des **données « sensibles »** nécessitant une attention particulière :
  - Des informations sur la vie personnelle telles qu'origines raciales ou ethniques, habitudes de vie, préférences religieuses, philosophiques, politiques, syndicales, orientation sexuelle
  - Des données médicales, génétiques, biométriques (empreintes digitales, ADN), etc…
  - Des données légales telles que les infractions, condamnations, etc…
  - Des données concernant des mineurs.

Le champ des DCP est donc extrêmement large et il faudra rester extrêmement vigilant à bien prendre en compte tous les domaines d'application et les possibilités de recoupement.

Il est à noter qu'actuellement la majorité des internautes n'ont pas connaissance des données récoltées ni ce pourquoi elles l'ont été.

2.3. Portée du règlement

Nous nommerons dans la suite de ce document « responsable du traitement » toute personne physique ou morale, autorité publique, service ou autre organisme qui, seul ou conjointement avec d'autres, traite des DCP (à savoir effectue toute opération ou tout ensemble d'opérations, à l'aide de procédés automatisés ou non, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction).

Sont concernés en premier lieu les responsables du traitement localisés au sein d'un pays membre de l'UE. Sont également concernées les responsables du traitement hors UE qui collectent, traitent ou stockent des données issues d'un citoyen de l'UE. Ces dernières devront dès lors désigner par écrit un représentant dans l'UE.

Cela couvre en outre le transfert de données personnelles vers des pays tiers ou des organisations internationales. Ces transferts devront avoir été autorisés au préalable par la Commission (si le territoire destinataire est considéré comme étant conforme à ses exigences). Dans le cas contraire, des clauses de sauvegarde contractuelles devront être établies.

Enfin, si un responsable du traitement fait appel à un sous-traitant, il doit s'assurer que ce dernier sera en mesure de respecter le GDPR et devra mettre en place un « contrat ou autre acte juridique au titre du droit de l'Union ou du droit d'un État membre, qui lie le sous-traitant à l'égard du responsable du traitement, définit l'objet et la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, et les obligations et les droits du responsable du traitement »[2] ! Le sous-traitant devra pouvoir apporter la preuve au responsable du traitement qu'il est bien en conformité avec le GDPR et devra l'autoriser à mener des audit et inspections sur les traitements, par lui-même ou un autre auditeur qu'il aura mandaté. Or, il est à noter que, le sondage Ipswitch réalisé fin 2014 a fait ressortir que 79% des sondés font appel à un fournisseur cloud, mais seulement 6% ont pensé à demander à leur prestataire s'il était en règle avec le règlement européen : il reste encore bien du chemin à parcourir ...

Dans les faits, on attend de voir comment seront traités les cas impliquant des responsables du traitement hors UE ou ceux des responsables du traitement (nombreux) qui font appel à des sous-traitants internationaux. Dans ce dernier cas, on pense notamment aux grandes sociétés (Salesforce, Microsoft et autres Amazon) offrant notamment des services de cloud privé. Il faudrait, en principe, que les responsables du traitement revoient l'ensemble de leurs contrats pour y inclure les contraintes et exigence du GDPR, mais auront-ils suffisamment de poids pour l'imposer face à des géants du net ?

2.4. Droit d'accès aux données & à leur portabilité

Une évolution importante apportée par le GDPR est le droit d'accès aux données : les individus auront maintenant le droit de demander à savoir si des données les concernant font l'objet de

[2] GDPR, Article 28

traitements et, le cas échéant, à quelle fin, quelle en est leur source et leur durée de rétention prévue.

Ils pourront, en outre, demander à ce qu'elles soient rectifiées et exiger de recevoir une copie de ces données sous un format « structuré, couramment utilisé et lisible par machine »[3], gratuitement afin de les transmettre, le cas échéant, à une entité tierce. Le texte va même plus loin en affirmant que la personne pourra demander à une entreprise de transférer directement ce fichier de données personnelles à une autre entreprise « lorsque cela est techniquement possible ».

Il faudra voir comment cette initiative de portabilité est reprise au niveau Européen ou Territorial. Certains accords de branches pourraient être mis en place pour la faciliter et la généraliser. En France, la portabilité est une réalité de longue date dans les télécoms (pour le numéro de téléphone) et le devient dans la banque et les assurances (encore qu'il faille généralement recréer son « dossier » chez les prestataire cible). Cela pourrait être amené à se généraliser et s'automatiser au profit des utilisateurs. On a vu, en revanche, que dans le domaine médical, il reste beaucoup de chemin à parcourir avant que le dossier médical universel ne devienne une réalité et même avant que les personnels soignants puissent récupérer et traiter les dossiers ou analyses effectuées par un confrère.

Enfin, afin de protéger les mineurs de moins de 16 ans, la collecte de données personnelles les concernant nécessitera un accord parental systématique.

2.5. Droit à l'oubli

Une autre évolution de taille permettra aux individus de demander au responsable du traitement, pour peu que leur demande soit légitime (voir 2.1 - Quoi de neuf ?), de supprimer leurs DCP définitivement de l'ensemble de ses systèmes, cesser de les disséminer et, le cas échéant, demander aux entreprises tierces à qui il les aura fournies, d'en cesser tout traitement, et ce, dans un délai de 30 jours.

Cette mesure concerne les données qui ne sont plus pertinentes dans le cadre initial de leur traitement ou celles pour lesquelles l'individu souhaite retirer son consentement concernant tout ou partie des traitements effectués sur ses DCP.

2.6. « Privacy by Design / Ethic by Design »

Il en découle assez naturellement pour les responsables du traitement qu'ils devront intégrer une nouvelle approche dite de "Privacy by Design" : il s'agit désormais de prendre en compte, dès la conception et tout au long du cycle de vie des produits et services, les aspects liés à la protection de la vie privée et des DCP. La protection des données doit devenir un standard, un incontournable de tout projet touchant de près ou de loin aux données personnelles. Elle devra ainsi être abordée dès les phases initiales des projets, faire l'objet d'ateliers dédiés, constituer un point clé dans les cahiers des charges et figurer dans les notes de cadrage et les spécifications. De même, les fournisseurs de services dans le Cloud se devront de respecter

[3] GDPR, Article 20

les normes de sécurité sur l'ensemble du cycle de vie de la donnée au même titre que le responsable du traitement.

Concernant la « Privacy by design », on peut citer par exemple les mesures suivantes :

- La minimisation des données qui consiste à ne collecter que des données adéquates, pertinentes et limitées à la finalité du traitement,
- La pseudonymisation, anonymisation ou cryptage qui permettent de ne plus pouvoir associer des données à une personne physique sans avoir recours à des informations supplémentaires,
- La limitation de finalité et des durées de conservation.

Plus encore, il faudra veiller à l'éthique des algorithmes mis en place : les traitements effectués sur les données personnelles ne devront en aucun cas porter atteinte à la vie privée d'un individu. Ainsi, par exemple, le responsable du traitement ne devra pas détenir par déduction plus d'informations sur l'individu qu'il n'en a lui-même ou, par recoupement à détourner l'anonymisation.

L'implémentation d'une telle approche constitue donc ainsi un gage supplémentaire de qualité et de confiance pour le responsable du traitement quant au traitement des DCP de ses clients mais également ses salariés, partenaires et prestataires.

Il est à noter que les DCP doivent être collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Ce point est important car, en pratique cette règle stricte pourrait rendre illicites de très nombreux projets (on pense notamment aux projets Big Data). Sans compter les traitements de données effectués dans les différents services de l'organisation, notamment dans le marketing, qui ne disposent souvent pas du consentement antérieur des personnes concernées. Une parade pourrait alors être de prévoir des clauses de consentement suffisamment larges et exhaustives pour couvrir une majorité de traitements … tout en veillant, rappelons-le, à ce que cette clause demeure explicite, non équivoque et non tacite, sous une forme simple et intelligible.

2.7. Notification de violation

Dernier point à relever en ce qui concerne les droits de l'usager : il devient obligatoire de mettre en place un mécanisme de notification de violation dans l'ensemble des pays membres de l'UE dès lors qu'une fuite de données risque de porter atteinte aux droits et libertés des individus. Ce mécanisme doit être déclenché dans un délai maximal de 72 heures suite à sa détection : les responsables devront informer les autorités compétentes pour leur indiquer les catégories de données, les enregistrements affectés et le nombre approximatif de personnes concernées.

Dans le cas où la violation est susceptible d'engendrer un risque élevé, la personne concernée devra en être informée dans les meilleurs délais.

Cette exigence est assortie d'une obligation de moyens en termes de mise ne place d'un niveau de sécurité adapté au risque, que ce soit pour le responsable du traitement comme pour ses sous-traitants.

2.8. Mais comment faire ?

L'ampleur de la réforme est conséquente. Sa mise en place le sera également. Pour aider les organisations dans cette transformation, la Commission Nationale de l'Informatique et des Libertés (la CNIL) a proposé une méthodologie dont nous allons voir les grandes lignes.

3. METHODOLOGIE

La mise en conformité au GDPR nécessite d'identifier l'ensemble des DCP se trouvant dans l'entreprise ainsi que les traitements qui leurs sont associés. Si on pense immédiatement aux outils de type SIRH, réseaux sociaux d'entreprise, messagerie, ERP (Enterprise Resource Planning), CRM (Customer Relationship Management), MDM (Master Data Management), DMP (Data Management Platform), Data Warehouse et autres Data Lakes, il faudra une grande application et beaucoup de rigueur pour s'assurer de l'exhaustivité de l'étude ; d'autant que certains utilisateurs pourront avoir pris l'habitude de faire des copies plus ou moins « privées » d'une partie de ces données en local ou, du moins, dans un environnement spécifique. La tâche risque d'être d'autant plus rude si l'entreprise est encore organisée en silos et qu'une partie de ces données est copiée, dupliquée ou ressaisie entre différents services, qu'elle est répartie dans plusieurs entités, elles-mêmes potentiellement situées dans différents pays et qu'une partie des données et de leurs traitements est sous la responsabilité d'un ou plusieurs niveaux de sous-traitants.

Avant de s'attaquer à la tâche, il va donc falloir définir une méthodologie claire.

Deux approches sont envisageables :

- Respecter à la lettre le GDPR (la question à se poser alors est de savoir si c'est possible), ou
- Parer aux urgences par niveaux de risque (approche pragmatique).

Nous allons essayer de définir ici une approche aussi complète que possible, en se basant notamment sur la méthodologie proposée par la CNIL. Il sera certainement nécessaire de définir une stratégie par paliers, fonction des priorités, des risques mais aussi des opportunités qui auront pu émerger de l'étude, une approche « Big Bang » étant illusoire dans ce type de projets, ne serait-ce que pour l'implémentation du principe de « Privacy by Design » qui nécessiterait une remodélisation complète de l'ensemble du système d'information.

A tout un chacun ensuite de voir jusqu'où l'appliquer la méthodologie et les actions à prendre pour y répondre.

La méthodologie proposée par la CNIL se décompose en 6 étapes :

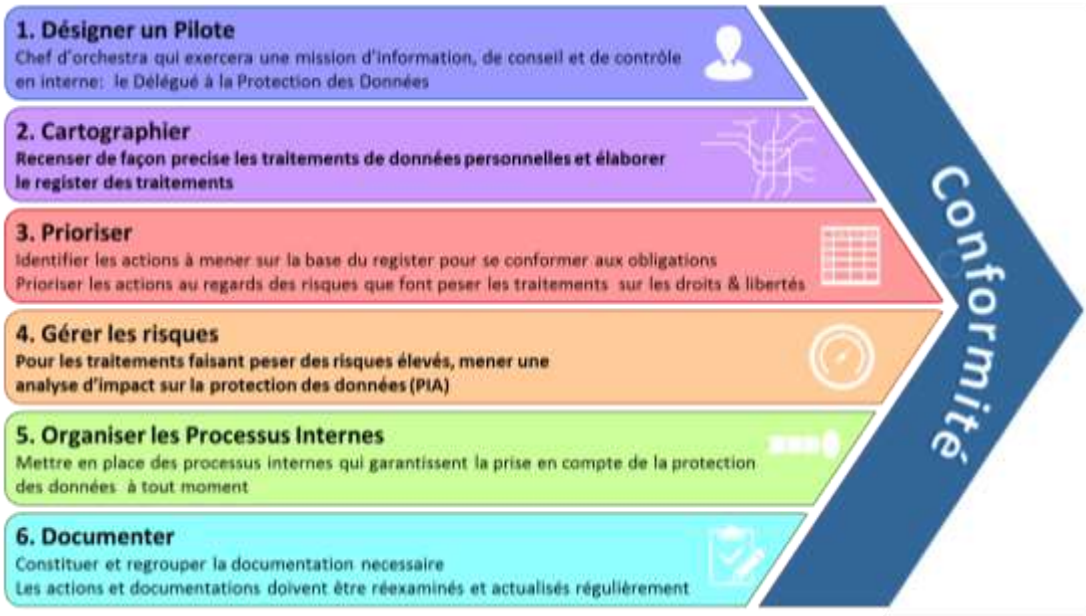


Figure 3-1 : La mise en conformité au GDPR en 6 étapes

3.1. Etape 1 : Désigner un Pilote

Partir sur un projet tel que celui-ci sans désigner de pilote reviendrait à vouloir faire un tour du monde à la voile sans capitaine.

Commençons par le commencement : il est avant tout indispensable que les directions de l'organisation et celle du SI incluent le GDPR comme une priorité stratégique et soutiennent le projet de bout en bout.

Il faut également qu'elles s'assurent que l'ensemble des directions y sont sensibilisées très tôt et offrent leur entière coopération. On peut ici citer à titre d'exemple le programme développé par Orange pour accompagner sa transformation digitale qui a mis en place un « Passeport Digital » et un « Visa Big Data » (examen accessible en ligne à destination de l'ensemble des collaborateurs) ainsi qu'une « Journée de sensibilisation » pour les managers afin que la culture du Big Data s'enracine durablement. S'il n'est pas obligatoire dans le cadre de la mise en place du GDPR, un programme similaire est cependant recommandable.

Un « Pilote » devra alors être identifié pour mener le projet à bien : il doit être le point de contact désigné au sein de l'organisation.

Le règlement prévoit d'ailleurs la nomination d'un délégué à la protection des données (DPO ou Data Protection Officer en anglais). En pratique, beaucoup d'organisations choisiront sans doute de nommer leur Correspondant Informatique et Libertés (CIL) actuel au poste de DPO.

Attention, la désignation d'un DPO est obligatoire pour :

- Les autorités ou les organismes publics,
- Les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle,
- Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et des infractions.

En dehors des cas de désignation obligatoire, la désignation d'un délégué à la protection des données est fortement encouragée par les membres du « Groupe 29 » (ou G29)[4].

3.1.1. Rôles et responsabilités du DPO

Les évolutions requises par le GDPR mêlent de façon étroite des aspects juridiques, métiers et IT ; il faudra donc de préférence quelqu'un qui connaisse le métier de l'entreprise, soit sensibilisé aux questions de cyber-sécurité et aux processus informatiques mais qui ait aussi une approche juridique du sujet.

Il rapportera directement au niveau le plus élevé de la direction et devra bénéficier des ressources nécessaires (y compris l'accès aux données et traitements) pour effectuer sa mission, ainsi que de formations lui permettant d'acquérir et maintenir ses connaissances en la matière.

Il aura notamment comme prérogatives :

- D'informer l'organisation et le personnel de leurs obligations en matière de traitement des DCP,
- De superviser la mise en œuvre et le suivi des initiatives de mise en conformité au GDPR et d'en contrôler le respect sur le long terme, notamment par la mise en place d'un registre des traitements et en s'assurant que ce registre et la documentation interne sont à jour,
- De coopérer avec l'autorité de contrôle,
- D'être le point de contact et de centralisation de toutes les demandes d'application des droits des personnes (droit à l'oubli, droit d'accès, droit à la portabilité, demande de modification, etc.),
- Par la suite, de participer à l'élaboration des études d'impacts sur la vie privée (PIA – Privacy Impact Assessment), obligatoires pour certains types de traitements (profiling, données sensibles, etc.).

Le DPO n'est cependant pas personnellement responsable de la conformité du GDPR. Il devra cependant prendre garde de documenter le processus de décision en cas d'absence de prise en compte de ses avis ou opinions. Son indépendance doit donc être garantie.

3.1.2. Les objectifs de l'entreprise en matière de GDPR

En pratique, les organismes, sous l'impulsion du DPO, devront :

[4] Le G29 ou Groupe de travail Article 29 sur la protection des données est un organe consultatif européen indépendant sur la protection des données et de la vie privée.

- Réaliser l'inventaire des traitements de DCP mis en œuvre,
- Évaluer leurs pratiques et mettre en place des procédures (notification des violations de données, gestion des réclamations et des plaintes, etc.),
- Identifier les risques associés aux opérations de traitement et prendre les mesures nécessaires à leur prévention,
- Maintenir une documentation assurant la traçabilité des mesures.

Nous verrons tout cela plus en détails dans les paragraphes suivants.

3.2. Etape 2 : Cartographier les traitements de données personnelles

Nous rentrons dans le vif du sujet : il s'agit ici de faire un état des lieux exhaustif de toutes les DCP traitées par l'organisation. Il va falloir pour cela désigner des correspondants dans chaque service ou direction pour prendre en charge l'étude de ses données.

Pour cette étape, il va falloir mettre en place une méthodologie de type industrielle.

La cible de cette phase sera d'initier le « Registre des traitements » qui devra par la suite être complété et maintenu à jour à chaque nouveau traitement ou chaque modification de traitement existant.

3.2.1. Cartographie des traitements

Pour chaque DCP traitée, il s'agira de se poser les questions :

- **Qui** :
  - Nom & coordonnées du responsable légal & du responsable opérationnel du traitement au sein de l'organisme,
  - Le cas échéant, les sous-traitants impliqués (avec à nouveau les coordonnées d'un point de contact),
- **Quoi** : Catégories de données traitées & niveau de risque (en fonction de leur sensibilité particulière ; par exemple, les données relatives à la santé ou les infractions),
- **Pourquoi** : précise la/les finalité(s) du traitement (exemple : gestion de la relation commerciale, gestion RH…),
- **Où** : lieu où les données sont hébergées (pays vers lesquelles elles sont éventuellement transférées),
- **Combien de temps** : quelle sera la durée de rétention ?

> **Comment** : mesures de sécurité qui sont mises en œuvre pour minimiser les risques d'accès non autorisés aux données et donc d'impact sur la vie privée des personnes concernées. Cette question amènera à effectuer une étude d'évaluation approfondie pour les zones à risques et potentiellement à revoir certains pans de la sécurité du SI.

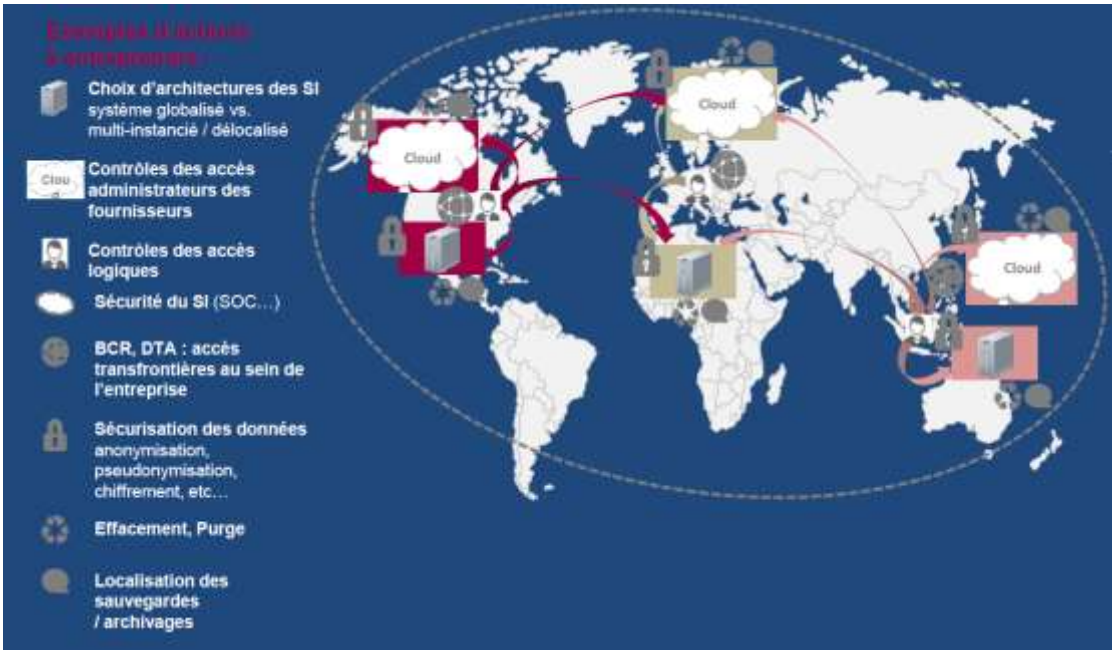


Figure 3-2 : Exemples de mesures de protection des données à mettre en place

3.2.2. Gestion des sous-traitants

En parallèle de cette action de cartographie des DCP, on pourra initier une « cartographie » des sous-traitants : il s'agira de s'assurer que les sous-traitants sont bien au fait de ce nouveau règlement et de préparer la signature d'avenants dans lesquels ils s'engagent à respecter le GDPR.

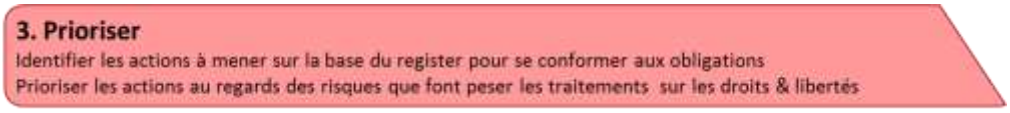
Il faudra en particulier :

> S'assurer qu'ils connaissent leurs nouvelles obligations et responsabilités,

> Ajouter le cas échéant des clauses contractuelles rappelant leurs obligations en matière de sécurité, de confidentialité et de protection des DCP traitées.

On peut s'attendre à ce que ces révisions contractuelles soient à la fois chronophages et laborieuses : il n'est donc jamais trop tôt pour lancer ce chantier !

3.3. Etape 3 : Prioriser les actions à mener



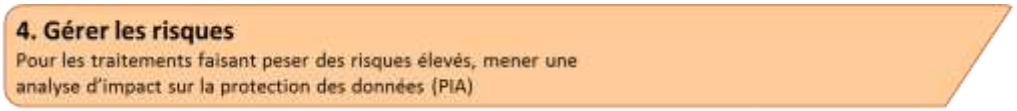
Quels que soient les traitements il faudra veiller à :

- La **minimisation des données** collectées,
- **L'identification de la base juridique** sur laquelle se fonde le traitement (par exemple : contrat, obligation légale, intérêt légitime, consentement de la personne),
- S'assurer que la **transparence** et le **droit à l'information** sont bien respectées,
- Prévoir les **modalités d'exercice des droits des personne**s concernées (droit d'accès, de rectification, droit d'oubli, droit à la portabilité, retrait du consentement...),
- Revoir les **mesures de sécurité** en place.

Certains traitements « à risques » nécessiteront des mesures particulières (par exemple : étude d'impact sur la protection des données (PIA), information renforcée, recueil du consentement, autorisation préalable, clauses contractuelles, etc.). Il s'agit en particulier des :

- Données sensibles (voir § 2.2 - Données à Caractère Personnel (DCP)),
- Traitements ayant pour effet ou pour objet :
  - La surveillance systématique à grande échelle d'une zone accessible au public,
  - Ou « l'évaluation systématique et approfondie d'aspects personnels […], y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative.[5] »
- Données transférées hors UE !

3.4. Etape 4 : Gestion des risques



Certains traitements sont susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées ? Il faudra alors mener pour chacun de ces traitements, une étude d'impact sur la protection des données (PIA ou Privacy Impact Assessment en anglais).

Pour traiter un risque identifié et le réduire à un niveau acceptable, il s'agira de mettre en place une ou plusieurs mesures d'atténuation des risques, fonction du type de risque à prendre en compte :

- Sur les données elles-mêmes : minimisation des DCP, chiffrement, pseudonymisation, anonymisation, mesures permettant l'exercice des droits, etc…
- Sur les impacts potentiels : sauvegarde des DCP, traçabilité, gestion des violations de données, etc.
- Sur les sources de risques : contrôle des accès, gestion des tiers, lutte contre les codes malveillants, etc.

[5] GDPR, Article 35

> Sur l'infrastructure : réduction des vulnérabilités matérielles, logicielles, réseaux, etc.

3.5. Etape 5 : Organiser les processus internes

A plus long terme, le GDPR nécessitera sans doute un certain nombre d'évolutions des procédures internes pour garantir un haut niveau de protection de la vie privée. Cela impliquera notamment :

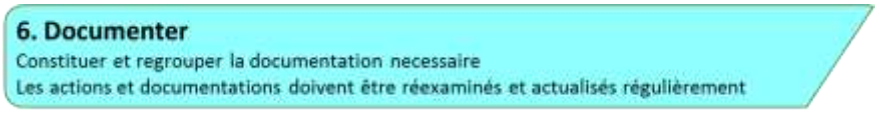
> De mettre en place la « Privacy by design » : cette notion doit désormais être prise en compte dès la conception d'une application, d'un traitement,

> De sensibiliser l'ensemble des collaborateurs et d'organiser des formations continues ainsi que la remontée d'informations,

> De mettre en place les processus nécessaires au traitement des réclamations et demandes concernant les droits d'accès, de rectification, d'oubli, d'opposition, droit à la portabilité, retrait du consentement en fonction des typologies de données,

> D'anticiper les violations de données en définissant le processus de notification à l'autorité de protection des données dans les 72 heures et aux personnes concernées dans les meilleurs délais.

3.6. Etape 6 : Documenter la conformité



En cas de contrôle ou de litige, il incombera au DPO d'apporter la preuve que les mesures de mise en conformité ont bien été prises. Il est donc primordial de constituer, bien organiser et tenir à jour la documentation nécessaire. L'ensemble des acteurs de l'entreprise doivent garder à l'esprit que tout changement de traitement ou de sous-traitant doit faire l'objet d'un contrôle de la part du DPO et d'une mise à jour de cette documentation.

Un tel dossier comportera :

> Une documentation sur les traitements des DCP :
  > Le registre des traitements,
  > Les analyses d'impact sur la protection des données (PIA) concernant les DCP susceptibles d'engendrer des risques élevés,
  > Le cas échéant, le cadre dans lequel s'effectuent les transferts de données hors de l'UE.

> Une information des individus :

  - Les mentions d'informations,
  - Les modèles de recueil du consentement des personnes concernées,
  - Les procédures mises en place pour l'exercice des droits.
- Les contrats avec les sous-traitants,
- Les procédures internes prévues en cas de violations de données,
- Les preuves de consentement lorsque le traitement repose sur cette base.

3.7. De la théorie à la pratique

Maintenant qu'on sait à quoi s'attendre, il ne reste qu'à mettre la théorie en pratique. Mais avant de se lancer, il est préférable de prendre un peu de recul pour tenter d'appréhender les risques et difficultés que l'on risque de rencontrer pour en anticiper, le cas échéant les mesures d'atténuation. Une liste est proposée dans le chapitre suivant. Espérons qu'elle ne s'allonge pas avec l'expérience.

4. DIFFICULTES / RISQUES :

Comme toute activité structurante, le GDPR n'est pas sans comporter des risques, que ce soit des risques inhérents à la mise en place même de la règlementation ou des risques liés à l'environnement de l'entreprise. Quoi qu'il en soit, il faut s'attendre à ce que l'implémentation du GDPR, en entreprise comme dans le secteur public, soit longue et difficile. Pas seulement parce que l'on découvre un grand nombre de traitements passés inaperçus sous le régime de la directive précédente ou que les ressources internes manquent cruellement pour respecter le délai de mai 2018, mais aussi parce que certaines dispositions du GDPR restent floues et posent pas mal de questions d'interprétation. Le G29 a commencé un travail d'analyse et de clarification de certains aspects du texte. Sa prochaine révision, prévue 4 ans après sa mise en application (en 2022 donc), permettra sans doute d'apporter les ajustements nécessaires à propos des sujets portant le plus à controverse. Il n'en demeure pas moins urgent de lancer les travaux pour adresser les DCP susceptible d'engendrer les risques les plus élevés.

4.1. Risques inhérents à la mise en place du GDPR

Il faut s'attendre à ce que la mise en place du GDPR ait des impacts importants à différents niveaux de l'organisation, que ce soit en termes d'efforts, de processus projets mais aussi pour des aspects légaux, juridiques et contractuels. Nous allons ici évoquer les principaux risques et difficultés à commencer par l'essence même du règlement qu'est l'harmonisation au niveau Européen.

4.1.1. Harmonisation Européenne de la gestion des DCP, vraiment ?

L'harmonisation Européenne de la gestion des DCP qui est à l'origine du DGPR est une belle et noble cause, mais serait-elle illusoire ? Sans doute portés par un climat de défiance vis-à-vis de Bruxelles, dans une Europe de nations de plus en plus tentées par le repli sur soi et le nationalisme, les Etats ont souhaité garder une certaine souveraineté sur la protection de la vie privée. Le GDPR leur laisse en effet la possibilité d'adapter (dans des mesures variées) certains chapitres fondamentaux de la règlementation, via la promulgation de lois nationales.

Nous citerons pour exemple les points suivants :

- La **licéité du traitement** (article 6 du GDPR),
- Le **consentement des enfants** (16 ou 13 ans selon les états),
- La définition du **caractère « particulier » de certaines DCP** : les Etats conservent une marge de manœuvre dans leur définition et ont la possibilité de déterminer des exceptions,
- La désignation d'**autorités de contrôle nationales** (La CNIL en France), les moyens dont elles disposeront et les pouvoirs qu'elles auront de faire appliquer le GDPR,
- Les **sanctions** mêmes qui pourront être appliquées pourront être variables d'un Etat à un autre.

Aussi compréhensible que soit cette possibilité de continuer à réglementer certains aspects de la règlementation sur une base spécifique et nationale, cela va à l'encontre de l'objectif du GDPR d'unifier les règles au niveau européen et met à mal l'objectif recherché du règlement. On risque alors d'assister à un véritable concours au « moins disant » : certains Etats membres pouvant être tentés d'être plus accommodants pour attirer les responsables du traitement sur leur territoire. D'autres, plus intransigeants, prendront le risque de voir leurs entreprises perdre en compétitivité face à une concurrence européenne et extra-européenne moins regardante et/ou moins contrainte vis-à-vis du respect de la vie privée.

4.1.2. Mise en place/refonte des processus métiers

4.1.2.1. Licéité du traitement

Tout traitement portant sur une donnée personnelle doit être licite et conforme à la ou aux finalité(s) pour la/les-quelle(s) la donnée a été collectée. Celle-ci est donc en quelque sorte « figée » par sa finalité réelle de départ, sauf consentement de la personne ou autorisation légale. Pris à la lettre, cette disposition risque de mettre un frein aux projets type « Big Data » et d'une manière générale à tout projet décisionnel ou marketing qui reposent bien souvent sur des données personnelles existantes et qui n'ont pas nécessairement fait l'objet d'un consentement. Il faudra suivre de près la mise en application de ce dispositif qui, en l'état, risque de peser sur les entreprises Européennes face à une concurrence plus libre.

4.1.2.2. Consentement

Ce sera au responsable du traitement d'apporter la preuve du consentement de l'individu et donc, prévoir un archivage dans son processus de traitement.

Lors de la mise en place du GDPR, il s'agira également d'identifier les traitements nécessitant un consentement « vie privée » et de mettre en place la collecte de celui-ci !

En outre, il va falloir intégrer cette notion dans l'ensemble des traitements afin, le cas échéant, de pouvoir effectuer des traitements différenciés selon que l'individu aura donné ou retiré son consentement, partiellement ou totalement. Cela va non seulement compliquer la tâche des informaticiens mais aussi potentiellement biaiser certains résultats statistiques, décisionnels ou marketing, une partie de la population sur laquelle se base ces traitements, étant alors exclue.

4.1.2.3. Droit à l'oubli

Une fois la cartographie effectuée, l'organisation est sensée savoir (si ce n'était déjà le cas) où se trouvent les DCP. Il faudra encore automatiser (1) le processus de prise en compte de ce droit à l'oubli et (2) celui de mise en application : il faudra mettre en place des processus parfois complexes pour assurer l'exhaustivité de la manœuvre en prenant garde de bien dissocier les exceptions ainsi que les données nécessaires notamment à l'application du contrat.

On voit aisément comment la conception d'un tel service pourrait s'avérer complexe dans des systèmes d'information silotés, où les DCP - parfois de piètre qualité et faisant l'objet de multiples doublons - sont souvent répliquées dans une multitude d'applications consommatrices.

Cela va en outre nécessité de difficiles arbitrages d'intérêts, dont la responsabilité reposera d'abord sur le responsable du traitement.

Enfin, à charge du responsable du traitement d'informer les autres responsables (sous-traitants) qui traitent les données faisant l'objet de la demande d'effacement.

4.1.2.4. Droit de portabilité

On voit bien à nouveau les difficultés que pourrait soulever ce type de transfert entre des systèmes d'informations complètement hétérogènes. Si les modalités d'application de ce droit sont encore floues, il y a fort à parier que son application constituera un défi technique majeur, obligeant les concurrents d'un même secteur d'activité à se concerter et à travailler de concert.

Le texte ne dit rien sur l'utilisation ultérieure des données par le premier responsable auprès duquel ce droit est exercé. On en conclut que les principes généraux de protection continuent à s'appliquer et qu'il ne pourra les conserver que dans la mesure strictement nécessaire aux finalités annoncées ou pour des problématiques de réquisitions légales.

Il ne dit rien non plus sur le sort des données « générées » par l'utilisation d'un produit ou service et qui ne sont pas à proprement parlé « communiquées » par la personne : données de facturation, de trafic, de localisation, celles produites par les objets connectés, etc. Sont-elles visées par ce nouveau droit ?

4.1.2.5. Privacy by design

La Privacy by Design impose, pour être correctement mise en œuvre, une étroite collaboration entre différents métiers au sein de l'organisation du responsable du traitement et une sensibilisation, voire un véritable enseignement à chacun des principes en cause : les métiers techniques des data (programmeurs, analystes, statisticiens, etc.), les métiers du juridique et de la compliance et, le cas échéant, d'autres métiers opérationnels (marketing, etc.).

Une nouvelle gouvernance projet sera donc nécessaire à son application qu'il faudra intégrer au plus tôt.

4.1.2.6. Impacts sur l'organisation

Outre la mise en place d'une nouvelle gouvernance au sein de l'organisation, on peut s'attendre à de nombreux impacts dans le cadre de cette règlementation, tels que :

- La nécessité d'arbitrer entre différents postes existants pour redéfinir l'organigramme des fonctions des acteurs aujourd'hui impliqués. En effet, les missions du DPO risquent de déborder sur ceux des services juridique et de compliance et plus encore sur celui du délégué à la protection des données déjà en poste,
- De nouvelles compétences seront en outre nécessaires pour appliquer et faire appliquer cette règlementation. Il y a fort à parier que les places seront difficiles à pourvoir,
- La redéfinition du schéma directeur actuel pour prendre en compte les efforts nécessaires à la mise en place du GDPR qui risque fort d'engendrer des délais sur les projets programmés,
- A plus long terme, la prise en compte des nouveaux processus qui va engendrer des lourdeurs au niveau des projets et donc des coûts et des délais supplémentaires qu'il

faudra intégrer, rendant potentiellement les entreprises Européennes moins compétitives à l'international,

- Au vu des enjeux nouveaux du GDPR et des sanctions encourues, il est probable que les responsables du traitement mettent un frein, voire mettent en veilleuse les projets de type « Big Data », du moins le temps de bien appréhender comment le règlement sera réellement mis en application.

4.1.3. Aspects Légaux

Nous l'avons vu au chapitre précédent, le GDPR n'est pas sans poser de nombreux problèmes quant à sa mise en application. Les juristes auront eux aussi beaucoup à faire pour l'intégrer.

4.1.3.1. Champ d'application territorial

L'application extraterritoriale du Règlement était inévitable au vu de l'évolution des technologies et de la toute-puissance de certaines entreprises établies hors UE, par le biais de biens et services offerts sur internet et donc, potentiellement, à destination d'un public présent sur le territoire européen. Ces entreprises seront donc amenées à récolter des données relatives à des citoyens européens qui pourront ensuite être traitées hors UE.

Il faudra attendre de voir comment pourront être exécutées les décisions qui seraient prises à l'encontre d'un Responsable du traitement situé hors de l'Union.

Ceci est d'autant plus vrai avec plusieurs responsables conjoints du traitement (notamment dans le cas où des sous-traitants seraient impliqués). La réponse pourra dépendre des règlements nationaux qui peuvent imposer un partage plus précis. A ce propos, la disposition ne prend en considération que l'hypothèse où les responsables conjoints sont soumis au même droit national, ce qui en pratique ne sera souvent pas le cas.

4.1.3.2. Responsabilité du responsable du traitement

Avec l'augmentation des moyens de contrôle de des sanctions en cas de non-conformité au GDPR, la responsabilité des responsables des traitements atteint un niveau jamais égalé : le degré de professionnalisation et de mise en œuvre de moyens (tant techniques qu'organisationnels) pour y faire face est sans commune mesure avec ce qui est prévu aujourd'hui.

L'estimation des risques à leur juste valeur afin d'y répondre par des mesures adaptées constituera le plus grand challenge pour l'équipe dirigeante.

Il faudra notamment :

- Revoir la conformité de tous les traitements existants et analyser les risques et donc les mesures correspondantes qu'il faut prendre,
- Revoir l'organisation des services (IT, juridique, RH, marketing…) et mettre en place une coordination renforcée entre eux,
- Renforcer la sécurité des traitements et la protection des données.

4.1.4. Aspects juridiques/contractuels

4.1.4.1. Nouvelles règles d'entreprises contraignantes

Les nouvelles règles d'entreprises contraignantes définie à l'article 47 du GDPR amèneront, n'en doutons pas, à revoir les règles internes d'entreprise (Binding Corporate Rules ou BCR en anglais) pour s'assurer qu'elles sont bien conformes. Cette adaptation nécessitera à son tour un effort pédagogique de sensibilisation de l'ensemble du personnel de l'organisation.

4.1.4.2. Sous-traitance

La précision et l'élargissement des mentions contractuelles (étendues aux liens de sous-traitance secondaire) imposent aux responsables de revoir toutes leurs relations à leurs sous-traitants et d'adapter les contrats existants.

Pour certaines sociétés, cette tâche risque fort de s'avérer longue et fastidieuse et d'autant plus compliquée si la relation client-fournisseur est fortement déséquilibrée en faveur du sous-traitant. Par ailleurs, en cas de doute, il incombera au responsable du traitement de faire la preuve que toutes les mesures ont été prises pour assurer la protection des DCP, y compris, si nécessaire, par des audits chez ses sous-traitants. Il doit donc se préparer à cette éventualité.

4.1.4.3. Notification d'une violation de DCP aux autorités de contrôle

Toute violation de DCP ne donne pas lieu à notification. Se pose alors nécessairement la question de la pondération du risque pour la violation des droits et libertés des personnes concernées. Le dirigeant de l'organisation devra en effet mettre en balance les sanctions dont son organisation pourrait faire l'objet avec la crainte du préjudice à son image et à la confiance que lui accordent ses clients et partenaires en cas de notification de violation aux autorités.

4.1.4.4. Notification d'une violation de DCP à la personne

Le responsable du traitement est tenu à notifier les individus victimes d'une violation de données uniquement si :

- La violation « est susceptible d'engendrer un risque élevé pour [ses] droits et libertés »[6],

En revanche, il n'a pas à le faire si :

- Il a mis en œuvre les mesures de protection techniques et organisationnelles appropriées (par exemple le chiffrement) pour les protéger,
- Il a pris des mesures ultérieures qui garantissent que le risque élevé n'est plus susceptible de se matérialiser,
- Cette notification exigerait des efforts disproportionnés.

[6] GDPR, Article 34

Les dirigeants seront à nouveau confrontés à un choix cornélien entre une communication à la personne et les conséquences qu'elle pourrait avoir et le risque d'une sanction de la part des autorités de contrôle.

4.2. Difficultés de gouvernance / organisationnelles

4.2.1. Réticences des partie prenantes

On peut s'attendre à ce qu'un projet d'une telle envergure soit l'objet de nombreuses réticences à travers de nombreux niveaux et services de l'organisation. Citons-en quelques-uns :

- En premier lieu **la direction** qui se voit imposer un projet complexe, chronophage, coûteux et dont l'objectif est, à priori, uniquement règlementaire. Néanmoins, au vu des sanctions encourues, cette réticence devrait être de courte durée. Un DSI éclairé saura en outre mettre en balance les opportunités offertes par le projet (voir chapitre suivant).
- **Les métiers** risquent quant à eux de faire grise mine lorsqu'on leur annoncera que les projets qu'ils considèrent comme stratégiques (et tant attendus) sont reportés pour cause de GDPR. Dès lors, ils risquent de trainer des pieds lorsqu'on leur demandera de coopérer et de mobiliser une partie de leurs ressources déjà trop rares pour y participer.
- Les **différentes directions** (métiers mais aussi juridique, RH, etc.) de l'organisation pourront, elles, craindre que ce projet n'empiète sur leur pré carré et que leurs si chères données ne leurs soient « subtilisées ». On peut alors douter de leur volonté de partager leurs connaissances. Un travail de pédagogie et une volonté forte de la direction seront nécessaires à les amadouer.
- Le **service IT**, enfin, pour qui ce projet représente un overhead peu soutenable et qui ne saura sans doute pas comment le mener. Un support sans faille de la direction et la mise à disposition des moyens et compétences nécessaires seront indispensables.

4.2.2. Réticences au changement

Comme nous l'avons vu, il faut s'attendre à ce que des changements organisationnels, de gouvernance soient nécessaires pour aligner l'organisation avec les exigences du GDPR. Les responsabilités du DPO risquent d'empiéter sur des activités attribuées jusqu'alors à d'autres fonctions. Enfin, les nouvelles exigences imposées à l'IT, notamment par la clause de « Privacy by design » risquent d'être mal perçues.

Si un DPO est nommé, il devra rester à l'écoute, tout au long du projet, des différents interlocuteurs de l'organisation et s'assurer que toutes les objections sont bien écoutées et, dans la mesure du possible, prises en compte. Il aura également fort à faire pour convaincre l'ensemble des parties prenantes et les amener à coopérer. En l'absence de la nomination d'un DPO, ce travail pédagogique devra être endossé par la personne désignée pour piloter le projet.

4.2.3. Manque de méthodologie / de compétences

Aujourd'hui, point de formation de DPO ni même de certification au GDPR. Les organisations devront donc identifier en leur sein ou recruter le bon profil pour mener la mise en conformité à bien. L'oiseau rare devra savoir faire preuve d'une grande polyvalence et avoir des connaissances métier de l'entreprise, une bonne maîtrise en gestion de projets IT, une forte sensibilité aux problématiques de sécurité et, si possible, posséder des bases juridiques … rien que ça.

Il devra en outre faire preuve de beaucoup de persévérance et faire montre d'indépendance pour rester inflexible sur l'application de la méthodologie à appliquer sur le projet afin d'obtenir un résultat à la fois exhaustif et exact.

4.2.4. Budgétaires

Une des grosses difficultés du GDPR est l'absence totale de visibilité sur le coût final du projet. Peut-être sera-t-il encore possible de faire une estimation grosses mailles du budget à engager pour réaliser la cartographie des traitements. Dans certaines grandes organisations disposant d'un système d'information hétérogène composé de nombreux sous-systèmes, parfois hérités de différentes fusions et acquisitions, cette estimation initiale sera déjà un challenge en soi. Il est en revanche absolument impossible d'anticiper les surprises qui pourront découler de cette étape. Même tante Irma ne saurait rassurer la DAF quant à l'étendue des dégâts à prévoir.

Par la suite, une fois identifiées les zones à risques il faudra se livrer à un délicat jeu d'arbitrage des chantiers à prioriser et trouver le bon équilibre entre un onéreux système « Plaqué or » et une solution qui pourrait exposer l'organisation à de lourdes sanctions.

En tout état de cause, ces dépenses « imprévues » vont peser sur la trésorerie du responsable du traitement pouvant le mettre en difficulté si sa marge de manœuvre était déjà ténue.

4.2.5. Délais

Rappelons-le : le responsable du traitement a jusqu'au 25 mai 2018, date d'entrée en vigueur du GDPR, pour se mettre en conformité. L'absence d'une règlementation transitoire et les délais de mise en application très serrés pour une telle transformation imposent une exécution du programme à pas forcés.

Heureusement, ces délais serrés s'appliquent également à la CNIL qui va devoir, elle aussi, subir une véritable révolution. C'est en effet à la fois son périmètre et son mode de fonctionnement qui évoluent : on passe d'une situation dans laquelle les responsables du traitement devaient effectuer des déclarations à la commission, sur une base de volontariat, à une situation où les responsables du traitement sont supposées être en conformité et où l'autorité de contrôle aura à aller « débusquer » les contrevenants. Il lui faudra pour cela des moyens adaptés et en particulier des ressources compétentes pour adresser ce nouveau règlement. A l'heure où l'Etat cherche à la fois à diminuer la voilure dans les administrations et à simplifier la vie aux entreprises, on peut se demander jusqu'où la CNIL poussera l'application du règlement?

On est également en droit de se demander si la France va appliquer le GDPR dans son intégralité ou si des lois d'application locale venant en modifier certains aspects seront promulguées – et dans quel sens : plus de souplesse ou, au contraire, plus de contraintes ?

On peut enfin espérer que les premiers verdicts prononcés seront plus cléments au vu de l'ampleur de la tâche à réaliser dans des temps très courts, pour autant que le responsable du traitement soit en mesure de démontrer sa bonne foi, soit déjà à un stade suffisamment avancé de son programme de mise en conformité et qu'il ait adressé les points les plus urgents.

4.3. Cas particulier : les transferts ou divulgations non autorisés par le droit de l'Union

L'UE semble légaliser sa doctrine issue de l'affaire « Swift »[7]. Même si elle n'a pas de pouvoirs sur les juridictions et autorités administratives étrangères, elle met les responsables du traitement ou sous-traitants établis en Europe en contrariété au Règlement dès lors qu'ils se soumettraient à des injonctions étrangères, ce qui peut créer des situations ingérables pour ceux-ci.

[7] Wikipédia :

L'accord **Swift** est un traité international entré en vigueur le 1er août 2010 entre l'Union européenne et les États-Unis. Il donne aux autorités américaines l'accès aux données bancaires européennes stockées sur le réseau de la Society for Worldwide Interbank Financial Télécommunication (SWIFT), dans le but de lutter contre le terrorisme, sous certaines conditions de protection de la vie privée des citoyens.

Depuis 2001, les États-Unis exploitaient secrètement les données du réseau Swift sans aucune base juridique. Cependant, la justice belge, où la société Swift est domiciliée, a estimé que celle-ci présentait des garanties suffisantes et a abandonné les poursuites judiciaires à son encontre. En novembre 2009, un premier accord est signé par les vingt-sept États membres de l'Union européenne, mais il a été rejeté par le Parlement européen qui estime qu'il ne protègerait pas suffisamment les données personnelles des citoyens européens.

Gageons que l'objectif soit plus politique que juridique.

Actualité (Les Echos) au 29/3/2017 : Le buzz des Etats-Unis : le Congrès abroge un texte protégeant la vie privée sur Internet : Les fournisseurs d'accès Internet pourront vendre les données de leurs clients à des tiers sans autorisation explicite.

> *Si Donald Trump promulgue la loi votée mardi, les fournisseurs d'accès comme Verizon ou Comcast pourront suivre les comportements de leurs clients sur Internet, et utiliser leurs données financières et personnelles sans leur autorisation pour pouvoir vendre de l'espace publicitaire particulièrement bien ciblé. Cela doit leur permettre de rivaliser plus équitablement avec Google ou Facebook, qui sont régulés par d'autres textes réglementaires et qui valorisent mieux l'information collectée pour s'imposer sur un marché de la publicité en ligne estimé à 83 milliards de dollars.*[1]

Si cette loi, diamétralement opposée aux principes du GDPR venait à passer, cela pourrait bien marquer une rupture avec l'approche plutôt accommodante de la Commission Européenne envers les Etats-Unis et un retournement de situation par rapport aux jurisprudences du type Swift.

Quoi qu'il en soit, si elle reste cohérente, il faut s'attendre à des réactions – l'avenir nous le dira.

4.4. Restons positifs !

Comme nous venons de le voir, l'entrée en vigueur du GDPR et la mise en conformité des organisations à ce règlement ne va pas être une chose aisée. Heureusement, le GDPR ne comporte pas que des risques mais il offre également des opportunités d'envergure aux organisations qui sauront les saisir. C'est ce que nous aborderons dans le chapitre à venir.

5. OPPORTUNITES

Rappelons d'abord qu'en 1995 déjà, l'UE était un précurseur en matière de protection des données. Aujourd'hui, nombreux sont les pays à travers le monde qui disposent de lois relatives à la protection des données (voir **Erreur ! Source du renvoi introuvable.** - **Erreur ! Source du renvoi introuvable.Erreur ! Source du renvoi introuvable.**). Moins de la moitié d'entre eux sont des pays européens. A un moment où la confiance des personnes dans les entreprises et les gouvernements a été ébranlée par des révélations sur les violations de données et la surveillance de masse, la responsabilité des législateurs est considérable.

L'influence de la directive de 1995, avait largement dépassé les portes de l'UE et a même servi de base pour le libellé du droit à la protection des données à caractère personnel prévu à l'article 8 de la Charte des droits fondamentaux. Avec le GDPR, l'UE est à nouveau à la pointe dans le domaine : gageons que cela aura à nouveau un impact au-delà des frontières communautaires.

5.1. Une opportunité pour les Européens

Il ressort de l'Eurobaromètre 2015-431 sur la protection des données (étude commandée par la Commission Européenne) que les européens avaient une demande forte en termes de protection des données ainsi qu'une défiance vis-à-vis de leur collecte. Pour ne retenir que quelques chiffres :

- Pour **57 %** des Européens, la divulgation d'informations à caractère personnel pose un réel problème,
- **94 %** estiment nécessaire qu'un consentement explicite soit fourni pour autoriser la collecte de données personnelles (dont 74% dans tous les cas, 12% dans le cas de collecte de données sur internet et 8% dans le cas de collecte de données sensibles),
- **90 %** des Européens pensent qu'il est important de bénéficier des mêmes droits et de la même protection dans tous les pays de l'UE,
- **70 %** sont préoccupés à l'idée que des entreprises puissent utiliser des informations à des fins autres que celle pour laquelle elles ont été collectées,
- Seulement **15 %** ont le sentiment de contrôler totalement les informations qu'ils fournissent en ligne.

Le GDPR répond largement à leurs attentes : c'est un message fort s'adressant avant tout à la nouvelle génération européenne de « petites poucettes » (comme la nomme le philosophe Michel Serre), génération qui n'a jamais vécu sans une connexion internet et qui a aujourd'hui les « pouces » rivés sur leur écran de téléphone intelligent. Leurs ainés y verront également un gage face à un outil qui leur inspire encore (et à juste titre) des inquiétudes. C'est l'opportunité de voire se réduire le déséquilibre entre l'innovation, l'exploitation des DCP et leur protection, en renforçant l'efficacité des garanties au sein de notre société numérisée par des pratiques commerciales responsables, une ingénierie innovante et en donnant à l'individu les moyens de reprendre la main sur sa vie privée.

5.2. Une opportunité pour les Organisations Européennes

5.2.1. Reprendre la main sur la donnée

Partant du postulat que la donnée est le trésor numérique de toute organisation en ce début de siècle, on voit très clairement que le travail de remise à plat de tout le cycle de vie des données, qui aura été réalisé dans le contexte du GDPR, pourra donner un avantage certain à ceux qui sauront aller au-delà de la mise en conformité avec le règlement, dans le but de se démarquer de la concurrence. Cependant, si la donnée est aujourd'hui un atout capital, source de valeur et de pouvoir, elle n'a aucune valeur « a priori » et n'est d'aucune utilité si elle n'est pas maîtrisée. Ce sont les actions et traitements réalisés sur cette matière brute qui lui confèrent toute sa valeur. Ces nouvelles contraintes peuvent ainsi devenir une véritable opportunité de repositionnement dans un écosystème dans lequel les acteurs prénumériques n'ont plus leur place.

Par ailleurs, les transformations globales sont risquées et rebutent tant les DSI que les dirigeants des organisations qui rechignent à passer le cap. C'est le cas des programmes de transformation numériques qui ambitionnent de créer un SI « Data-centric » pour lequel il sera nécessaire de repenser l'architecture pour et par le digital. Or tout le monde s'accorde à convenir que l'entreprise de demain sera digitale ou ne sera pas. Pourtant, toutes n'ont pas aujourd'hui le même chemin pour y parvenir, loin s'en faut : un sondage Opinionway révèle qu'aujourd'hui, en France, 75% des dirigeants et managers d'entreprises interrogés se sont déclarés incapables de donner une définition précise du Big Data ; 86% avouent même que la notion leur paraît « floue ». Pire encore : plus de la moitié des TPE/PME ne sont toujours pas présentes sur le net ! Pourtant, d'après le rapport McKinsey réalisé fin 2014 sur l'intérêt d' « accélérer la mutation numérique des entreprises en France », l'impact de la transformation digitale sur le résultat opérationnel de l'entreprise est évalué à +/- 60% (de +40% en cas de succès à -20% en cas d'échec) ; mieux vaut faire les bons choix !

En parallèle, on note que les règlementations nouvelles, comme les ruptures technologiques sont de bons points de départ pour le lancement de tels programmes de transformation. C'est donc le moment où jamais d'agir puisque ces deux facteurs sont aujourd'hui réunis avec, d'une part, le GDPR et, d'autre part, des technologies comme le Big Data qui arrivent à maturité : il est à ce sujet intéressant de constater comme le Salon Big Data qui s'est tenu au palais des congrès les 6 et 7 mars 2017 a enfin passé le cap de la technologie (qui attirait l'essentiel des projecteurs sur les éditions précédentes) pour faire la part belle aux solutions et services proposés, alors que des projets ambitieux commencent à voir le jour et à porter leurs fruits.

Les travaux effectués dans le cadre du GDPR permettront donc, dans un premier temps, aux responsables du traitement de se réapproprier leurs données et, ensuite, d'en rationaliser le traitement. L'objectif sera alors d'en reprendre le contrôle, d'en maîtriser la fiabilité, d'en assurer l'unicité et la cohérence et de rationaliser les coûts de maintenance et les efforts opérationnels que cela engendre. On pourra par exemple étudier l'opportunité d'implémenter un système de gestion des données de références (Master Data Management ou MDM en anglais).

Quoi qu'il en soit, il est impératif de casser les silos de données que l'on retrouve traditionnellement dans les organisations qui vont à l'encontre de ces principes de rationalisation et ont un effet délétère sur son fonctionnement. En contrepartie d'une certaine perte de contrôle (du moins ressentie) sur leurs données propres, il faudra démontrer aux différents services tous les bénéfices qu'ils pourront tirer d'avoir accès à une vision globale, enrichie et épurée de l'information. Il est temps de donner le pouvoir aux métiers et ça tombe bien car les outils « self-service », qui leur apportent de la valeur directe (aux métiers et donc à toute l'entreprise) et allègent la charge des DSI sont maintenant à maturité pour être généralisés, tels que :

- **Data Preparation** : logiciels d'aide à la préparation (nettoyage, qualité, homogénéité) des données,
- **Data Discovery** : logiciels d'exploration des données disponibles au sein de l'entreprise,
- **Data Governance** : Logiciels de gouvernance trans-organisationnelle de la données donnant la possibilité d'automatiser un grand nombre de tâches nécessaires et de la rendre disponible,
- **Dataviz** : logiciels de représentation graphique de données statistiques ou visualisation de données statistiques,
- **Data Science** : toutes les applications de Business Intelligence (BI) & Artificial Intelligence (AI) permettant l'extraction de connaissance à partir des données.

Ces utilisations en self-service devront cependant toujours rester en adéquation avec les principes du GDPR et donc rester sous la supervision soit d'une « cellule DPO », soit d'un point de contact au sein du service que l'on aura pris soin de former aux exigences de la règlementation.

La cible à garder en vue est bien entendu de donner un maximum de valeur aux données de l'entreprise comme levier pour :

- **Accroitre le revenu** : en améliorant l'image de marque, accroissant la satisfaction client en lui offrant une expérience personnalisée, le fidélisant et possiblement en générant de nouvelles opportunités de vente,
- **Réduire les risques** : par la mise en conformité au règlement, une meilleure prise en considération de la vie privée, une détection proactive de la fraude et une réduction des risques financiers,
- **Optimiser les coûts** : coûts opérationnels et coûts de marketing et d'analytiques.

Cette reprise de la maîtrise des données pourra permettre d'identifier des bénéfices similaires en interne pour viser à accroitre la satisfaction des employés et donc à la fois leur motivation, leur adhésion aux valeurs nouvelles de l'organisation et, in fine, leur productivité et leur rétention.

Le spectre des possibilités en matière de traitement des données et plus généralement dans une approche de transformation digitale est très large. Reste au DSI à faire les bons choix pour son organisation en justifiant du ROI des solutions envisagées et, ainsi, à gagner l'adhésion des métiers et de sa direction, en s'adossant sur une approche agile, par prototypage. Il faudra

cependant qu'il garde en permanence à l'esprit de toujours faire un usage éthique de la donnée et n'abuse pas du pouvoir qu'elle lui confère. Un autre point à surveiller de près concerne la minimisation des risques et la sécurisation de la donnée dont nous allons traiter dans le paragraphe suivant.

5.2.2. Reprendre la main sur la sécurité du SI

En simplifiant, harmonisant et assainissant la gestion des données dans les différents pays de l'Union Européenne, le GDPR entend permettre plus de transparence et donc de confiance dans le monde numérique. Ce facteur confiance est un élément décisif dans les relations avec les clients et partenaires et en particulier dans le développement des activités en ligne où elle est tout autant, voire plus importante encore que la qualité du produit ou du service.

Les entreprises ignorent cet aspect ou, du moins, le sous-estiment-elles trop souvent. Des études menées par Symantec en 2015 et 2016 [8] nous enseignent en effet que 75 % des entreprises ignorent que l'expérience qu'elles offrent en matière de protection de la vie privée fait partie des trois critères recherchés en priorité par les clients et que 88 % des consommateurs en ligne considèrent même la sécurité des données comme LE facteur le plus important lorsqu'ils choisissent de traiter avec une entreprise.

Se conformer aux exigences du GDPR est certes une obligation ; c'est également et surtout un investissement dont le retour s'avèrera à la fois rapide et pérenne pour autant que l'organisation sache le mettre en avant. C'est enfin une opportunité à ne pas manquer de remettre à plat la sécurité de son système d'information pour le renforcer et tenter de parer à des attaques qui peuvent s'avérer être extrêmement préjudiciables, voire même fatales à l'organisation. L'ANSSI (Agence nationale de la sécurité des systèmes d'information, rattachée au Secrétariat général de la défense et de la sécurité nationale (Premier ministre)) n'hésite pas aujourd'hui à parler de véritable guerre informatique. En la matière, l'attaque informatique ayant affecté la chaîne de télévision TV5 Monde en avril 2015 est un véritable cas d'école qui a bien failli mener à la fermeture de la chaine[9].

Si l'on peut s'attendre à de telles attaques contre les médias et les grandes entreprises, toutes les organisations ainsi que toutes les personnes physiques peuvent être concernées. A titre d'exemples, en 2016, 24 000 attaques externes ont été bloquées par les dispositifs de sécurité

---

[8] Rapport State of Privacy Symantec de 2015 / Enquête State of European Data Privacy Survey Symantec de 2016

[9] Wikipédia : TV5 Monde est une chaîne de télévision généraliste francophone internationale créée le 2 janvier 1984 et détenue conjointement par des sociétés audiovisuelles publiques françaises, belges, suisses, canadiennes et québécoises. Elle est l'un des trois plus grands réseaux mondiaux de télévision, accessible auprès de 291 millions de foyers à travers 200 pays et territoires. Elle diffuse 10 signaux régionalisés distincts, 2 chaînes thématiques et 2 web TV.

L'attaque s'est déroulée en 3 étapes :

1. Envoi d'un e-mail de "phishing" à l'ensemble des employés. Seuls 3 journalistes y ont répondu, permettant aux "hackers" de pénétrer dans le système de la chaîne par des logiciels de type "Cheval de Troie"
2. Un virus a ensuite contaminé plusieurs serveurs
3. Dans la nuit du 8 au 9 avril, l'offensive commence, avec l'attaque des serveurs, pendant plusieurs heures, puis des réseaux sociaux.

Tout le système informatique de TV5 Monde s'est ainsi retrouvé bloqué, obligeant la chaîne à interrompre la diffusion de sa chaine et ses communications sur les réseaux sociaux.

Au total, cette opération a coûté à TV5 Monde plus de 5 M € pour la première année suivie de 3 M € l'année suivante pour investir dans de nouveaux systèmes de protection puis d'un investissement complémentaire de 10 M € et a perturbé le fonctionnement de la chaine pendant de longs mois.

du ministère de l'intérieur et ce chiffre double chaque année ; 80% des entreprises auraient été visées par des attaques. Enfin, en 2015, le coût de la réparation de ces attaques informatiques a dépassé les 3,3 Milliards d'euros en France. Selon le rapport de l'éditeur en sécurité McAfee[10], filiale du groupe Intel, épaulé par le « Center for Strategic and International Studies » (CSIS), au niveau mondial, les pertes liées aux incidents de cybersécurité se chiffreraient en centaines de milliards de dollars (entre 375 milliards de dollars pour la fourchette basse à 575 milliards de dollars pour la fourchette haute).

La sécurisation de systèmes d'informations n'est donc plus une option et est même devenue une urgence.

On peut décliner la sécurisation des systèmes d'information en quatre phases :

- La première consiste à définir la **stratégie de gestion des risques** à mettre en place après avoir identifié les vulnérabilités potentielles de l'infrastructure,
- La deuxième est la protection, qui consiste à développer et à m**ettre en place des garde-fous** à l'échelle de l'infrastructure, des informations et des identités, pour limiter in fine la portée et les conséquences d'une attaque,
- La troisième étape est la **détection**, pour laquelle les entreprises ont besoin de services de surveillance et de solutions performantes d'identification des menaces. On considère qu'il faut en moyenne 229 jours à une entreprise pour déceler une attaque : la fuite de données a tout le temps d'être effective et plus cette durée s'allonge, plus les conséquences seront importantes,
- La dernière étape consiste à mettre en place les **procédures correctives** en cas d'attaque.

Cette sécurisation peut s'avérer extrêmement onéreuse ; cependant c'est aujourd'hui le prix à payer pour la sauvegarde du business. Se mettre en conformité avec le GDPR, c'est sécuriser les DCP : autant en profiter pour repenser la sécurité de son SI !

5.3. L'opportunité d'opter pour une architecture plus ouverte

Nous l'avons vu, le droit à la portabilité qui est l'un des principes novateurs du GDPR pourra amener certaines branches à normaliser leurs interfaces pour automatiser le processus. Sans attendre de telles initiatives, il s'agira de chercher à tirer profit d'un écosystème de plus en plus ouvert (on pense notamment aux initiatives d'Open Data) et, éventuellement, à lier des relations avec les partenaires (clients, fournisseurs, administrations), voire même éventuellement les concurrents.

Les technologies actuelles permettent en effet la mise en place ou l'utilisation extrêmement rapide d'interface (APIs) qui pourront permettre de s'ouvrir vers de nouveaux horizons.

Cette ouverture vers l'extérieure nécessitera cependant une vigilance extrême quant aux aspects de sécurité.

[10] McAfee : Net Losses: Estimating the Global Cost of Cybercrime (June 2014)

5.4. Une opportunité pour les acteurs du Big Data Européens

Bien sûr, toutes les données traitées dans les Big Data ne sont pas des DCP; mais, comme on a pu le voir, dès lors que ces données permettent d'identifier directement ou indirectement une personne, les principes d'analyse prédictive et prescriptive à grande échelle attendues du Big Data sont aux antipodes des règles de protection des données édictées par le GDPR. La dénomination même de Big Data fait référence au principe de collecte d'informations hétérogènes venant de tous types de sources, pour tenter d'extraire la substantifique moelle d'un volume de données maximal, sans se soucier des principes attendu par le GDPR (minimisation, anonymisation ou tout autre traitement préalable de l'information pour la décorréler de la personne physique qu'elle concerne). En outre, le Big Data utilise des sources plus ou moins maîtrisées et sécurisées (réseaux sociaux, IOT, BYOD, etc.) et la nécessité de traiter les données en temps réel ou quasi temps réel en rend le contrôle d'autant plus complexe.

Enfin, la logique, les conséquences et la finalité même des traitements de Big Data se caractérisent par une opacité, à l'opposé elle aussi des principes du GDPR.

Les techniques de « Privacy by Design » ne sont aujourd'hui pas applicables à l'échelle des Big Data et au-delà du stade expérimental, les entreprises intègrent rarement la protection des données par défaut dans les solutions de Big Data.

Tout reste à inventer à ce sujet mais espérons que les acteurs européens, les premiers et les plus exposés à ces problématiques, sauront attraper la balle au bond pour générer un avantage concurrentiel sur le marché européen dans un premier temps et pourquoi pas, par la suite, au-delà des frontières de l'UE.

Les premiers acteurs du cloud, les Entreprises de Service Numérique (ESN) et, d'une façon générale, toute entreprise amenée à agir en qualité de sous-traitant qui se mettront en conformité avec le règlement auront eux aussi un net avantage face à la concurrence. Gageons que, là encore que les acteurs européens seront les mieux préparer pour y faire face.

5.5. Et demain ?

5.5.1. Vers le « Privacy by Using » ?

Le GDPR n'en est qu'à ses prémices et l'on doit s'attendre à ce que des ajustements y soient apportés. Déjà le G29 travaille à clarifier certains points. La CNIL et, plus généralement, les institutions françaises doivent, quant à elles, encore définir leur position : de nouvelles dispositions à portée nationale seront-elles prises pour adapter la règlementation ? Quoi qu'il en soit, remettre l'individu au centre des décisions, le sensibiliser, lui donner la maîtrise de l'utilisation des données le concernant et lui permettre de bénéficier de l'utilisation de ses données est clairement un modèle gagnant-gagnant que certains souhaiteraient voir évoluer vers ce qu'ils appellent la « Privacy by Using », ouvrant certainement la porte aux entreprises qui, à nouveau, seront les plus agiles à s'adapter et proposeront les services adéquats.

Avec le Privacy by Using, l'individu a un contrôle total sur les informations (et niveaux de consentement) qu'il communique aux différents acteurs économiques notamment via une interface web que l'on peut imaginer ressemblant à ceci :

Figure 5-1 : Privacy by Using

Source: (businessdecision.com : GDPR Nouvelles contraintes & opportunités)

5.5.2. L'identifiant numérique unique

Sur internet, il peut être compliqué à un individu de contrôler son identité et, vice-versa, aux organisations de confirmer la véracité des informations fournies par leurs clients : quoi de plus aisé pour un mineur par exemple que de modifier sa date de naissance pour pouvoir commander en ligne de l'alcool ou autres produits réservés aux adultes ?

Certains Tiers de Confiance, comme La Poste ou la Direction générale des finances publiques en France proposent un service d'identité numérique pour certaines utilisations. Les « Nordic Posts » du Danemark et de la Suède proposent une application d'identification et de signature numérique bien plus avancée, et ce depuis les années 1990, avec leur service e-Boks. Aujourd'hui l'Europe (via l'association ÆTERNAM qui collabore avec l'AFNOR (France), le DIN (Allemagne) et le CEN (Europe)) travaille sur un code d'identifiant unique : l'ISÆN ou **I**ndividual **S**ocial data **A**uditable addr**E**ss **N**umber, qui permettra à un individu de s'identifier de manière sécurisée.

Cet identifiant numérique lui permettra en outre de communiquer une information suffisante et uniquement l'information nécessaire auprès des acteurs économiques.

En reprenant l'exemple de la commande de spiritueux, une fois identifié, le client (majeur) pourra passer sa commande et finaliser sa transaction par un paiement : seules les informations de la majorité du client et celles nécessaires au paiement seront échangées avec le vendeur. Il suffira alors au vendeur de communiquer l'identifiant numérique de son client au livreur qui seul connaitra l'adresse de livraison du colis sans en connaitre la contenance.

5.5.3. Les objets connectés, robots & le GDPR

Avec une estimation de 26 milliards d'objets connectés et plus de 300 milliards de dollars de chiffre d'affaire en 2020, on ne pouvait pas ne pas aborder la problématique des objets connectés (Internet Of Things ou IOT en anglais).

Dans la foulée, on s'attend à ce que les applications type Big Data appliquées aux données des IOT génèrent de Big revenus, le volume des données générées par ces myriades d'objets étant potentiellement stratosphériques, permettant d'acquérir en temps réel une emprise inégalée du fonctionnement de l'organisation mais aussi une grand proximité (on peut même parler d'intimité) avec ses employés et clients dont on pourra littéralement suivre chacun de leurs gestes. On comprend alors les conflits que cela va inévitablement générer avec les principes du GDPR : il va falloir définir en urgence la ligne rouge à ne pas franchir ; peut-être l'un des prochains sujets de travail pour le G29 ?

Ensuite, très à la mode aujourd'hui, le marché de l'IOT est en plein boom et se développe de façon incontrôlée : c'est à celui qui arrivera le premier sur le marché avec un objet novateur et fonctionnel. L'objet doit effectivement proposer une fonctionnalité mais, si novatrice soit-elle, cela ne devrait pas se faire au détriment d'un certain nombre de principes fondamentaux, ce qui est malheureusement le cas aujourd'hui. Nous aborderons deux de ces principes, particulièrement cruciaux dans le cadre du GDPR :

- L'un des challenges des objets connectés repose sur leur principe même qui consiste à échanger de la donnée pour qu'elle puisse être traitée. Or, en l'absence de norme et d'intentions claires et prédéfinies de traitement, les objets connectés tendent à transmettre des flots de données importants, sous des formats souvent propriétaires. Or plus de données impose plus de gouvernance, surtout dans le contexte du GDPR, et, un prérequis fondamental, en est la qualité pour éviter que les « Lacs de Donnée » (Data Lakes) sur lesquels reposent le Big Data ne se transforment en « Marais de Donnée » (Data Swamps) inexploitables. C'est certainement ici l'occasion de mettre en pratique le principe de Privacy by Design pour ne récolter que les données nécessaires, en veillant peut-être à ce qu'elles soient formatées avant stockage …
- L'autre enjeu majeur et qui doit être considéré comme critique concerne les aspects de confiance et de sécurité. La confiance d'abord : en effet, avec la multiplication des objets connectés, les écosystèmes qui nous entourent risquent fort de reposer non plus sur un partenaire clairement identifié mais sur tout une chaine de partenaires (fournisseurs d'objets "inter"-connectés, fournisseur de services réseau, fournisseur cloud, etc.). En cas de défaillance au sein de cette chaine, l'identification de la responsabilité risque d'être longue et laborieuse, mettant à mal la fiabilité et la confiance de l'utilisateur. Enfin, le risque principal de cette interconnectivité, via internet ou une technologie sans fil quelconque, est l'accès non autorisé au système embarqué : connecter un équipement quel qu'il soit à un réseau, c'est mettre une porte d'entrée sur son système. Or, soit poussées par l'urgence de mettre leur nouvel objet star sur le marché avant la concurrence, soit par manque de compétences en la matière, les firmes tendent à négliger bien trop souvent les aspects de sécurité. C'est d'autant plus critique que la menace est permanente et toujours plus poussée. Une fois encore, l'absence de standards matures dans les IOT et la soif d'innovations de leurs concepteurs exacerbent cette problématique.

Ces aspects sont cruciaux pour le développement des IOT et pourraient leur être fatals s'ils ne sont adressés avec toute la détermination qui s'impose. Que se passera-t-il en effet si demain, en raison d'une faille de sécurité, des hackers parviennent à pénétrer de façon « industrielle » un système d'alarme depuis une simple connexion WiFi depuis un PC pour en prendre la main, mettant non seulement à mal le système lui-même mais donnant possiblement accès à tout le réseau de l'organisation ? Les individus continueront-ils à se jeter sur les derniers gadgets à la mode avec la même frénésie s'ils s'aperçoivent que cela ouvre grandes les portes de leur vie privée, jusqu'aux détails les plus intimes ?

« Ne parlez pas de choses trop personnelles ou trop sensibles devant votre télévision, parce que celle-ci vous écoute ! » nous avertissait récemment Samsung, le géant sud-coréen de l'électronique, au sujet de ses « smart TV », ces télés connectées en permanence à Interne.

Il est urgent d'éteindre les incendies qui couvent au cœur même de la communauté IOT !

La littérature concernant les robots est quant à elle pléthorique. Isaac Asimov a été l'un des pionniers au travers de ses œuvres de science-fiction à évoquer la nécessité de règlementer les actions des robots au travers de ses trois lois. Avec les percées récentes en matière d'intelligence artificielle (IA), la science-fiction d'hier est en passe de devenir réalité. Aussi, beaucoup de questions se posent-elles au sujet de la cohabitation de l'homme avec ses cyber-égos et de la protection de la vie privée des uns (et peut-être des autres ?). Le sujet est bien entendu en filigrane dans le GDPR mais tout reste à faire en la matière. Des députés visionnaires exhortent la Commission à envisager la création d'une agence européenne pour la robotique et l'intelligence artificielle dans l'optique de créer un droit des robots.

Sujet à suivre donc . . .

Ironiquement, certains "robots" (ou du moins l'IA) pourraient bien venir au secours des responsables du traitement dans la mise en place du GDPR avec des solutions telles que celle proposée par la société britannique RAVN qui propose de débusquer, classifier et créer des rapports sur les DCP au sein du système d'information de l'entreprise.

6. CONCLUSION

"La plupart des gens passent à côté d'une opportunité parce qu'elle porte un bleu de travail et ressemble au travail" a dit un jour Thomas A. Edison. Le GDPR peut en effet être perçu comme une corvée, une obligation légale de plus à implémenter. Il serait cependant dommage de n'en conserver que cet aspect et de ne pas profiter des opportunités qu'elle offre pour, notamment, engager son organisation dans la voie du numérique ou, d'en accélérer la transformation et de revoir et renforcer la sécurité de son système d'information.

Le GDPR a un double objectif fort louable de renforcer les droits en matière de protection de la vie privée des citoyens européens et d'en harmoniser son application au sein de l'UE pour instaurer d'un climat de confiance sur un marché digital qui en avait bien besoin. Les organisations qui sauront mettre à profit sa mise en application pour effectuer leur mutation digitale ou simplement vendre leur nouvelle virginité numérique en sortiront renforcées. Les autres auront en effet investi des sommes non négligeables en pure perte, risquant de fragiliser un peu plus leur position face à la concurrence.

Pour celles enfin qui n'auront pas produit les efforts nécessaires, elles pourront toujours invoquer Sainte Rita pour être épargnées : au vu des sanctions maximales proposées, on ne peut douter de la volonté de grande rigueur de la part des autorités. Même si ces dernières font, dans un premier temps, preuve d'une certaine clémence, ne doutons pas que les condamnations, toutes magnanimes qu'elles soient, auront une portée médiatique forte et seront donc accompagnées d'une sanction immédiate de la part des clients.

Je suis convaincu qu'il faudra du temps (au-delà de la date fatidique du 25 mai 2018) pour que l'ensemble des états membres de l'UE appliquent pleinement le GDPR et un certain nombre d'itérations pour achever d'en préciser les contours. Le bon sens et la prudence doivent cependant être de rigueur et inciter les dirigeants à s'engager vigoureusement sur le chemin de la mise en conformité.

Cela laisse de beaux jours aux consultants qui auront su acquérir une connaissance du sujet pour faire fructifier le fruit de leurs expériences. Futurs DPOs et autres CDOs pourraient fort bien tirer leur épingle du jeu.

ANNEXE 1 : NON-CONFORMITE AU GDPR : LES ENTREPRISES CRAIGNENT DE METTRE LA CLE SOUS LA PORTE

Article de Laurent Leloup, paru sur finyear.com.

Près de la moitié des entreprises du monde entier redoutent de ne pas être prêtes à répondre aux exigences de la réglementation, la mise en place de technologies adaptées étant citée comme le principal défi de la mise en conformité.

Non-conformité à GDPR : les entreprises craignent de mettre la clé sous la porte

Une étude menée à l'échelle mondiale par Veritas Technologies, leader mondial de la gestion de l'information, révèle que 86% des entreprises dans le monde sont inquiètes des répercussions qu'un défaut de conformité au règlement général sur la protection des données (GDPR) [11] pourrait entraîner sur leur business. Parmi elles, près de 20%, soit une entreprise interrogée sur cinq, craignent de devoir mettre la clé sous la porte en cas de non-conformité. En effet, les pénalités peuvent atteindre 20 millions d'euros ou représenter 4% du chiffre d'affaires annuel, le montant le plus élevé étant retenu.

Destiné à harmoniser la gouvernance des informations personnelles au sein des pays membres de l'Union européenne, le GDPR impose de savoir précisément où et comment les données sensibles sont stockées et transférées et comment leur accès est encadré et contrôlé par les entreprises. Ces données concernent aussi bien les informations personnelles que les cartes de crédit ou encore les coordonnées bancaires et les données de santé. La réglementation, qui entrera en vigueur le 25 mai 2018, ne concerne pas uniquement les entreprises au sein de l'UE, la réglementation s'applique mondialement à toute entreprise proposant des biens et des services aux citoyens de l'UE ou analysant leur comportement en surveillant par exemple leurs habitudes d'achat. L'étude indique que 47% des entreprises interrogées dans le monde redoutent de ne pas être en mesure de répondre aux exigences de la réglementation en temps et en heure.

Les résultats sont issus du rapport Veritas 2017 GDPR Report pour lequel 900 décideurs ont été interrogés en 2017 en Europe, aux Etats-Unis et en Asie Pacifique. Ils mettent également en évidence que 18% des entreprises craignent qu'un défaut de conformité ne les pousse à mettre fin à leurs activités. De plus, 21% se montrent très préoccupées par les amendes potentielles qui pourraient entrainer des réductions de personnel afin de compenser le montant des pénalités infligées en cas de non-conformité à GDPR.

[11] https://www.cnil.fr/fr/reglement-europeen-sur-la-protection-des-donnees-ce-qui-change-pour-les-professionnels

Figure 1 : « Quelles potentielles répercussions craignez-vous en cas de non-conformité de votre organisation avec GDPR ? »

Les entreprises s'inquiètent également des répercussions qu'un défaut de conformité pourrait entrainer sur leur image de marque, plus particulièrement si un incident venait à être rendu publique, la nouvelle réglementation imposant en effet de notifier toute violation de données aux personnes concernées. 19% des personnes interrogées se montrent préoccupées par les éventuelles couvertures négatives dans les médias et sur les réseaux sociaux qui pourraient les amener à perdre des clients. De plus, une sur dix (12%) se dit très inquiète de la dévalorisation que pourrait engendrer ces couvertures négatives sur leur marque.

Le manque de technologie appropriée freine la préparation à GDPR

L'étude souligne également que beaucoup d'entreprises peinent à déterminer quelle est la nature des données dont elles disposent, à savoir où elles sont localisées et à évaluer quelle est leur pertinence business. Des critères pourtant essentiels pour assurer les premières étapes de mise en conformité avec GDPR. Selon les résultats de l'étude, elles auraient des difficultés à résoudre ces problématiques car elles ne seraient pas équipées des technologies adéquates pour répondre aux exigences de la réglementation.

Près d'un tiers des répondants (32%) redoutent que les technologies actuellement en place dans leur entreprise ne soient pas capables de gérer leurs informations efficacement ce qui pourrait entraver la recherche, la découverte et la vérification des données, des critères clés pour garantir la conformité avec GDPR.

De plus, 39% des répondants estiment que leur entreprise n'est pas en mesure d'identifier et de localiser correctement les données pertinentes. Pourtant, la réglementation exige que les entreprises transmettent à toute personne qui en ferait la demande une copie des données la concernant ou procèdent à leur suppression sous un délai de 30 jours.

La conservation des données est également une préoccupation majeure. 42% des entreprises admettent qu'aucune démarche n'est mise en place pour déterminer quelles données doivent être sauvegardées et quelles sont celles à supprimer (en fonction de leur valeur). Dans le cadre de GDPR, les entreprises peuvent conserver des données personnelles seulement si celles-ci sont toujours utilisées pour les raisons notifiées auprès des individus au moment de la collecte

de leurs données. En revanche, elles doivent être supprimées si leur utilisation n'est plus nécessaire pour les raisons invoquées au moment de la collecte.

Les investissements pour assurer la conformité à GDPR

L'étude de Veritas met en évidence que moins d'un tiers des répondants (31%) pensent que leur entreprise est en conformité avec GDPR. Pour celles travaillant actuellement à la mise en conformité, des investissements à près de 7 chiffres sont envisagés. En moyenne, les entreprises prévoient de dépenser plus de 1,3 millions d'euros.

Les défis rencontrés en fonction des pays interrogés

Le chemin vers la conformité est encore long pour de nombreuses entreprises partout dans le monde :

- Du retard dans la préparation : le rapport souligne d'importantes disparités en fonction des pays en matière de préparation à GDPR. Singapour, le Japon et la République de Corée sont les plus en retard. 56% des répondants à Singapour craignent ne pas pouvoir répondre aux exigences de la réglementation dans les temps. La situation est pire au Japon et en République de Corée où ce pourcentage dépasse les 60%.
- La crainte de mettre la clé sous la porte : c'est aux Etats-Unis et en Australie que les entreprises redoutent le plus la faillite en cas de défaut de conformité. Près de 25% des répondants dans ces deux pays craignent que la non-conformité ne menace la pérennité de leur entreprise.
- La peur des licenciements : de même, c'est aux Etats-Unis et en Australie que la crainte des licenciements pour compenser le montant des amendes appliquées en cas de défaut de conformité est la plus élevée. 26% des répondants aux Etats-Unis s'inquiètent des réductions de personnel et ce pourcentage atteint 30% en Australie. C'est également la principale préoccupation en République de Corée, où 23% des répondants redoutent des licenciements.
- Inquiétudes concernant l'image de marque : en Asie Pacifique, les entreprises se montrent particulièrement soucieuses de l'impact qu'un défaut de conformité pourrait avoir sur la réputation de leur marque. 20% des répondants à Singapour craignent de perdre des clients suite à une couverture médiatique négative ou à une mauvaise publicité sur les réseaux sociaux. Un chiffre qui atteint les 21% au Japon et en République de Corée.

« Il reste à peine plus d'un an avant que GDPR n'entre en vigueur, mais l'attitude qui consiste à se dire « j'ai encore le temps » persiste dans les entreprises du monde entier. Pourtant, que vous soyez localisés au sein de l'Union européenne ou non, importe peu. A partir du moment où votre entreprise a des activités dans la région, la réglementation s'applique à vous » rappelle Mike Palmer, Executive Vice President et Chief Product Officer chez Veritas. « Pour ces entreprises, il est temps qu'elles sollicitent les bons conseils pour déterminer précisément leur niveau de préparation et pour les aider à établir une stratégie précise afin d'assurer leur conformité. Car un défaut de conformité pourrait bien mettre en péril les emplois, l'image de marque et la pérennité des entreprises ».

Pour comprendre comment les entreprises peuvent garantir leur conformité à GDPR, visitez veritas.com/gdpr.

Méthodologie

Veritas a confié au cabinet d'études indépendant Vanson Bourne la réalisation de cette étude. Au total, 900 décideurs d'entreprise ont été interrogés en février et mars 2017 aux États-Unis, au Royaume-Uni, en France, en Allemagne, en Australie, à Singapour, au Japon et en République de Corée. Les répondants faisaient partie d'entreprises comptant au moins 1 000 employés et appartenant à tout type de secteur. Pour être admissibles à la recherche, les répondants devaient travailler dans des entreprises ayant des activités au sein de l'UE et détenant ainsi des données personnelles sur les citoyens de la zone.

REMERCIEMENTS / REFERENCES

Je tiens à remercier Mr. Antoine Vigneron, enseignant au CNAM.

Les documents et sites suivants ont été principalement utilisés pour la réalisation de cette synthèse. D'autres sources secondaires ont également été utilisées. Elles ont été précisées au cas par cas tout au long du document.

REFERENCE	LIRE EN LIGNE
Conseil Européen - Le règlement général sur la protection des données	http://www.consilium.europa.eu/fr/policies/data-protection-reform/data-protection-regulation/
CNIL (Commission nationale de l'informatique et des libertés)	https://www.cnil.fr/professionnel
CIGREF - Valorisation des données dans les grandes entreprises - Maturité, pratiques et modèle	http://www.cigref.fr/wp/wp-content/uploads/2016/11/CIGREF-Valorisation-des-donnees-Pratiques-Modele-2016.pdf
gdpr.expert	https://www.gdpr-expert.eu/#textesofficiels
GlobalSecurityMag.fr - GDPR : 5 changements majeurs pour les entreprises	http://www.globalsecuritymag.fr/GDPR-5-changements-majeurs-pour,20170227,69261.html
NOVENCIA - 10 questions pour comprendre le GDPR	https://www.novencia.com/gdpr-10-questions/
BusinessDecision.com – Big Data & Blog Digital	http://blog.businessdecision.com/bigdata/2016/11/gdpr-nouvelles-contraintes-opportunites/
CIL consulting	http://www.protection-des-donnees.fr/gdpr-pourrait-bien-booster-croissance-acteurs-europeens-big-data/