Protection de l'Information Digitalisée

Performance des Processus d'Informatisation
IATIC 5 2019/2020

Clément LEFEVRE
Jérémy JULLIENNE
Mickaël LAMOTTE
Kyndra KANA-ZEBAZE

Encadré par :
M. Jean-Guy SAYOUS

ISTY

Table des matières

Table des figures

Problématique

A. Information digitalisée

L'information digitalisée est une **information sous forme numérique et électronique stockée**, **manipulée** et **affichée** par des **outils informatiques**. Elle **décrit un système** en fonction de **données** ou **d'événements discontinus**.
Des premières conceptions de données numériques primitives, aux récents volumes massifs de données binaires hautement sophistiquées, les données numériques cherchent à **capturer des éléments du monde physique** et à les **simuler** à des **fins technologiques**. Cela se fait de différentes manières, mais avec des techniques spécifiques pour capturer divers événements du monde réel et les convertir sous forme numérique.

En 2020, il y aura environ **40 billions de giga-octets de données** (40 zettaoctets). Cette statistique est d'autant plus impressionnante lorsque l'on sait que **90% des données ont été créées au cours des deux dernières années**.

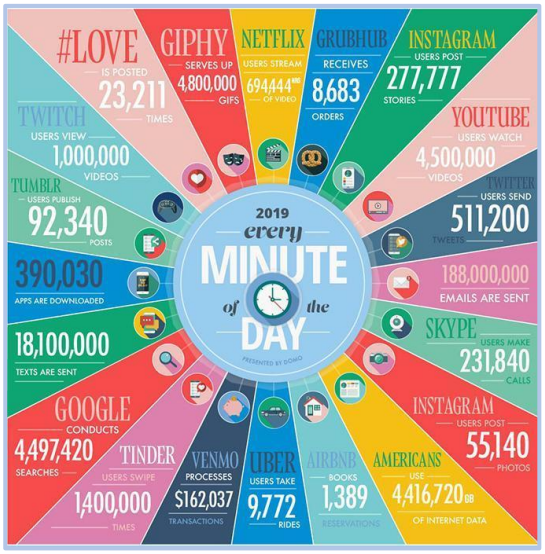

Figure 1 : Quantités de données manipulées chaque minute - Data Never Sleeps 7.0, DOMO

Nous consacrerons ce rapport principalement à la **protection des données à caractère personnel**, qui sont parmi les **informations digitalisées les plus sensibles**.
Une donnée personnelle peut être définie comme étant **toute information se rapportant à une personne physique identifiée ou identifiable directement** ou **indirectement**, qui **doit en conserver la maîtrise**.
Tout l'enjeu derrière la protection des données personnelles repose sur ces derniers mots, et nous amène à une première problématique : **Comment garantir à une personne la maîtrise de ses données personnelles lorsque l'on sait que chaque seconde passée sur internet génère plus d'1,7 Mo de données à son sujet ?**

B. Protection de l'information digitalisée

Ces dernières années, la protection des données est devenue une **problématique majeure pour les entreprises**. L'Union Européenne et d'autres pays dans le monde ont **révisé leurs lois** relatives à la protection des données, introduit des **règles plus strictes** afin de **protéger les droits des personnes** concernées, et des **sanctions importantes** en cas de non-respect de la législation. La **sensibilisation** et les **attentes des individus**, qu'ils soient consommateurs, employés, prestataires, partenaires commerciaux, ou mêmes autorités publiques, ont également **augmenté de manière significative**.

Pourtant, au cours du premier semestre 2019, plus de **4.1 milliards d'enregistrements de données** ont été **compromis**. **Les moyens mis en œuvre suffisent-ils à garantir la protection des données des personnes civiles et morales ?**

Enfin, alors que les infections globales par les **ransomwares** ont diminué de 52%, les **infections d'entreprise ont elles augmenté de 12% en 2018**. De plus, avec l'émergence de **nouvelles technologies**, telles que le Cloud, les **failles de sécurité ont augmenté de 11% depuis 2018 et de 67% depuis 2014**. **Quels sont les enjeux pour les entreprises, et comment sont-elles impactées dans leurs pratiques ?**

Législation

A. En France et en Europe

(i) Grandes lois

Loi *Informatique et Libertés* du 6 janvier 1978

La **loi *Informatique et Libertés***, adoptée le 6 janvier 1978, constitue le **fondement de la protection des données face aux traitements informatiques** en France. Bien qu'ayant subi **plusieurs modifications** profondes, cette loi est **toujours en vigueur aujourd'hui**.
Née d'un débat ayant nourri la décennie, notamment autour d'un projet du gouvernement d'identifier chaque citoyen par un numéro et d'interconnecter tous les fichiers de l'administration (projet SAFARI), cette loi est l'**une des premières d'Europe** à réglementer le traitement de données personnelles. Elle vise à **protéger les droits des individus**, en **encadrant les possibilités de traitements** de données à caractère personnel, notamment en **créant la CNIL** (Commission Nationale de l'Informatique et des Libertés).

Elle a par la suite été enrichie et complétée par plusieurs décrets, à l'image de la directive européenne du 24 octobre 1995, imposée par le développement de la micro-informatique avec pour ambition particulière de prendre en compte trois éléments d'évolution majeures :

- **La marchandisation des données**, obligeant les entreprises à placer le client au cœur de toute stratégie commerciale sur leurs données.
- **L'internationalisation des données**, visant à résoudre la problématique des données personnelles collectées en France, se retrouvant sur les réseaux d'entreprises de taille mondiale, et adressant les problématiques de contrôle des bases de données mises en œuvre par les autorités habilitées.
- **Le phénomène de traçabilité**, induit par le développement de la vidéosurveillance, des cartes à puces et reposant sur l'exploitation des données de connexion. Du fait du développement de technologies tels que les systèmes de paiements, de porte-monnaie électronique, la notion de fichier était rapidement devenue obsolète, car incapable de couvrir l'ensemble des usages. Pour pallier à cela, une **notion de trace**, plus générale, a été introduite.

Plusieurs dispositions sont comprises dans cette loi, à savoir :

- **L'obligation de déclarer** auprès de la CNIL les fichiers contenant des données personnelles
- **L'interdiction de collecter** des **données à caractère sensible**, c'est-à-dire relatives à la religion, la santé, la politique, etc.
- Le principe de **collecte loyale** de données
- L'obligation **d'assurer la sécurité** de l'ensemble des données collectées
- L'obligation **d'informer les individus concernés** de la collecte de leurs données
- Le **droit à l'accès**, la **modification** et la **suppression** des données en question

En somme, la Loi *Informatique et Libertés* du 6 janvier 1978 fait ainsi **référence aux droits des personnes** et non plus seulement aux fichiers informatiques, garantissant ainsi la **liberté individuelle et publique**.

Règlement Général sur la Protection des Données (RGPD)

Entré en vigueur dans l'ensemble de l'Union Européenne le **25 mai 2018**, le RGPD marque un véritable **changement de paradigme** en termes de protection des données personnelles. Il vise à **redonner à chaque citoyen le pouvoir sur ses données**. Avec ce dispositif, l'Union Européenne construit un **cadre juridique harmonisé** et **consolide son pouvoir** en matière de protection des données personnelles.

Le RGPD apporte également une certaine **modernisation** à la protection des données à caractère personnel, **face aux évolutions technologiques** (Cloud, Big Data, IoT, etc.), en **renforçant les droits des individus**. De plus, les **sanctions** prévues se veulent **plus dissuasives**, afin de s'affirmer contre les géants de la donnée.
Cette réglementation s'applique aux **entreprises**, aux **organismes publics** et aux **associations quelles que soient leur taille ou leur activité**, dès lors qu'ils **traitent des données personnelles de personnes physiques** se trouvant **sur le territoire de l'Union Européenne**. Les entreprises basées en dehors de l'Union Européenne traitant des données de citoyens européens sont donc elles aussi concernées.

Le RGPD défini plusieurs principes, détaillés ci-après :

1. **Licéité**, **loyauté** et **transparence**
   Les données doivent être collectées et traitées de manière **loyale**, **licite** et **transparente**. La **licéité** du traitement fait référence à son **fondement juridique** (obligation légale, obligation contractuelle, etc.), qui doit être défini dans l'article 6 du RGPD. La **loyauté** du traitement désigne elle les modalités selon lesquelles les données sont collectées. Enfin, pour répondre au principe de **transparence**, le responsable de traitement devra fournir une **information complète et compréhensible sur le traitement effectué**.

2. **Finalité**
   Les **objectifs** de la collecte et du traitement des données doivent être **annoncés en amont aux personnes concernées**. Les données personnelles collectées **ne peuvent être réutilisées pour une autre finalité** que celle prévue initialement.

3. **Pertinence** et **minimisation**
   Les données recueillies et traitées doivent être **pertinentes**, **adéquates**, et **limitées au regard de la finalité** pour laquelle elles sont traitées. Ainsi seules les données strictement nécessaires à la réalisation de l'objectif déterminé doivent être collectées.

4. **Exactitude**
   Les données doivent être **exactes**, et **si nécessaire**, **tenues à jour**. Les détenteurs de données doivent donc prévoir des processus de correction, ou de suppression des données des sujets.

5. **Limitation de conservation**
   La **durée de conservation** des données doit être **limitée au strict minimum**. Dès la **finalité atteinte**, elles doivent être **supprimées**. Cette durée de conservation doit être **définie au préalable** par le responsable du traitement, en tenant compte des éventuelles obligations de conserver certaines données étant susceptibles de varier.

6. **Droits d'accès**, de **rectification**, de **suppression** et **d'objection**
   En plus du droit à l'information mentionné préalablement, les personnes dont les données personnelles sont collectées disposent également de certains droits qu'elles peuvent exercer auprès de l'entité détenant ces données. Par le **droit d'accès**, les personnes concernées sont en droit d'obtenir la **communication des informations personnelles les concernant**, sauf si les demandes sont manifestement abusives du fait de leur fréquence déraisonnable, de leur nombre ou de leur nature répétitive ou systématique. De plus, les personnes concernées ont le **droit de faire rectifier**, **modifier** ou **supprimer** les données à caractère personnel les concernant **lorsque celles-ci sont inexactes** ou **font l'objet d'un traitement contraire aux principes évoqués**.

7. La **sécurité** des données personnelles
   Le responsable de traitement doit **garantir la sécurité des données collectées** mais également leur **confidentialité**, afin que seules les personnes autorisées y accèdent. Ces mesures dépendent généralement des risques liés au fichier (sensibilité des données, finalité du traitement, etc.).

8. **Responsabilité** (Accountability)
   Enfin, le responsable du traitement des données doit être capable de **démontrer sa conformité avec la totalité des autres principes**, en tenant, par exemple, des registres de traitement, et en menant régulièrement des études d'impact sur la vie privée.

(ii) Acteurs de régulations

DPO

Le **DPO** (Data Privacy Officer ou Data Protection Officer) est l'acteur situé au cœur de la protection des données personnelles au sein d'un organisme. Il est de ce fait le **point de contact et de connexion entre l'organisme qu'il représente et l'autorité de contrôle nationale** telle que la CNIL en France. Membre de l'organisation ou consultant externe, ses missions sont clairement définies dans le RGDP (art. 38 et 39). Son rôle est de **conseiller de manière indépendante** et de **s'assurer que le RGDP est correctement respecté** au sein de l'organisme.
Ses missions lui incombent :

1. **D'informer** et de **conseiller** le responsable du traitement quant aux obligations en matière de protection des données personnelles, ce qui implique de **mener les actions de sensibilisation et de formation**.
2. De **contrôler le respect du RGDP** au travers d'**audits de mise en conformité**.
3. De **dispenser des conseils** sur demande.
4. De **gérer les interactions avec l'autorité de contrôle**.

La présence du DPO est **obligatoire dans trois cas de figure** :

- au sein **d'organismes publics** ou **autorités publiques**,
- au sein **d'organismes ayant un suivi à grande échelle de personnes**,
- au sein **d'organismes traitant des données sensibles** (e.g. santé, militaire) **à grande échelle**.

CNIL

La **CNIL** (Commission Nationale de l'Informatique et des Libertés) est une **autorité administrative indépendante française** (AAI) créée par la loi *Informatique et Libertés* du 6 janvier 1978. Son but est de veiller à ce que l'informatique respecte les droits de l'Homme, l'identité humaine, la vie privée et les libertés.
Elle accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits.
La CNIL possède **quatre grandes missions**, allant de la pédagogie au pouvoir de sanction.

- **Informer, protéger les droits** : Tout public (salariés, entreprises, particuliers) peut s'adresser à la CNIL afin de demander des renseignements en matière de protection des données personnelles. La CNIL met d'ailleurs à disposition des outils pratiques et pédagogiques, et mène régulièrement des actions de sensibilisation en ce sens.
- **Accompagner la conformité et conseiller** : La mise en conformité est l'objectif premier de la CNIL. Elle intervient dans les entreprises par le biais de correspondants informatique et liberté, et accompagne également quotidiennement le législateur en prenant position sur des projets de lois ou des décrets.
- **Anticiper et innover** : Les enjeux liés à la protection des données personnelles étant en constante évolution, la CNIL, par son comité de prospective, effectue un travail régulier afin d'évaluer l'impact de sujets émergents sur les libertés.

- **Contrôler et sanctionner** : La CNIL possède un rôle d'alerte, de conseil et d'information vers tous les publics, mais dispose également d'un pouvoir de contrôle et de sanction. En cas de contrôle, celle-ci peut accéder à tous les locaux professionnels, demander consultation de tout document, et accéder aux programmes informatiques et aux données. A l'issue d'un contrôle la CNIL dispose d'un large éventail de mesures, allant du simple avertissement aux sanctions administratives et/ou financières.

Bien que le RGPD soit une législation mise en place par l'Union Européenne, celui-ci n'impacte pas le rôle et l'influence de la CNIL. Celle-ci met d'ailleurs à disposition des entreprises de nombreux outils pour aider à la compréhension et l'application du RGPD.

CEPD

Le **CEPD** (Comité Européen de la Protection des Données) est un **organe européen indépendant** contribuant à **l'application cohérente des règles en matière de protection des données au sein de l'Union Européenne**. Sa principale mission est de garantir l'application du RGPD et de la directive (95/46/CE) sur la protection des données personnelles.
A l'instar de la CNIL, il possède un rôle de conseil envers les institution et organes de l'UE en matière de traitement des données personnelles, et se positionne sur les politiques et les textes législatifs à ce propos. Il contrôle également les activités de traitement de données personnelles par l'administration européenne, afin d'en vérifier la conformité avec la législation.
Enfin, il encourage la coopération entre autorités de l'Union Européenne chargées de la protection des données, et collabore avec eux afin d'assurer la cohérence en matière de protection des données.

B. Dans le monde

(i) Une mosaïque de législations

Dans un contexte de mondialisation, avec des flux qui ne cessent de croître, **les données personnelles représentent un enjeu stratégique pour le commerce international**. En effet, il est fréquent que les transactions commerciales soient accompagnées de données, parce qu'elles sont l'objet du commerce, ou sont incorporées au produit ou au service commercialisé.

Néanmoins, la circulation des données personnelles est complexe, puisque leur **protection est différenciée**, et encore **très faible à l'échelle mondiale**. Ainsi, comme le montre la carte présentée par la CNIL ci-après, **la majorité des états ne possède pas de législation**, ou celle-ci n'est **pas en adéquation avec le RGPD**.

Toutefois, le RGPD interdisant le transfert des données relatives aux citoyens européens d'une entreprise américaine ou asiatique ne garantissant pas une sécurité des données similaire à celle stipulée par le droit de l'Union Européenne, **de nombreux états mettent actuellement en place une législation fortement inspirée de celui-ci**.
Cependant, la **cohérence et la fiabilité de ce « *Privacy Shield* » posent questions**, puisque suite à des négociations commerciales, et malgré les contestations des régulateurs européens, **les États-Unis ont obtenu le droit de déroger à cette règle**, par la Commission Européenne.

Bien que l'Union Européenne fasse figure de proue, en proposant en mai 2019 à l'OMC (Organisation Mondiale du Commerce) un texte ayant pour ambition de mettre en place un cadre réglementaire à l'international sur la protection des données personnelles, **l'aboutissement d'un accord international n'est pas chose aisée**, puisque des grandes puissances telles que la Chine ou les États-Unis ne sont pas prêtes à accueillir favorablement une telle initiative.

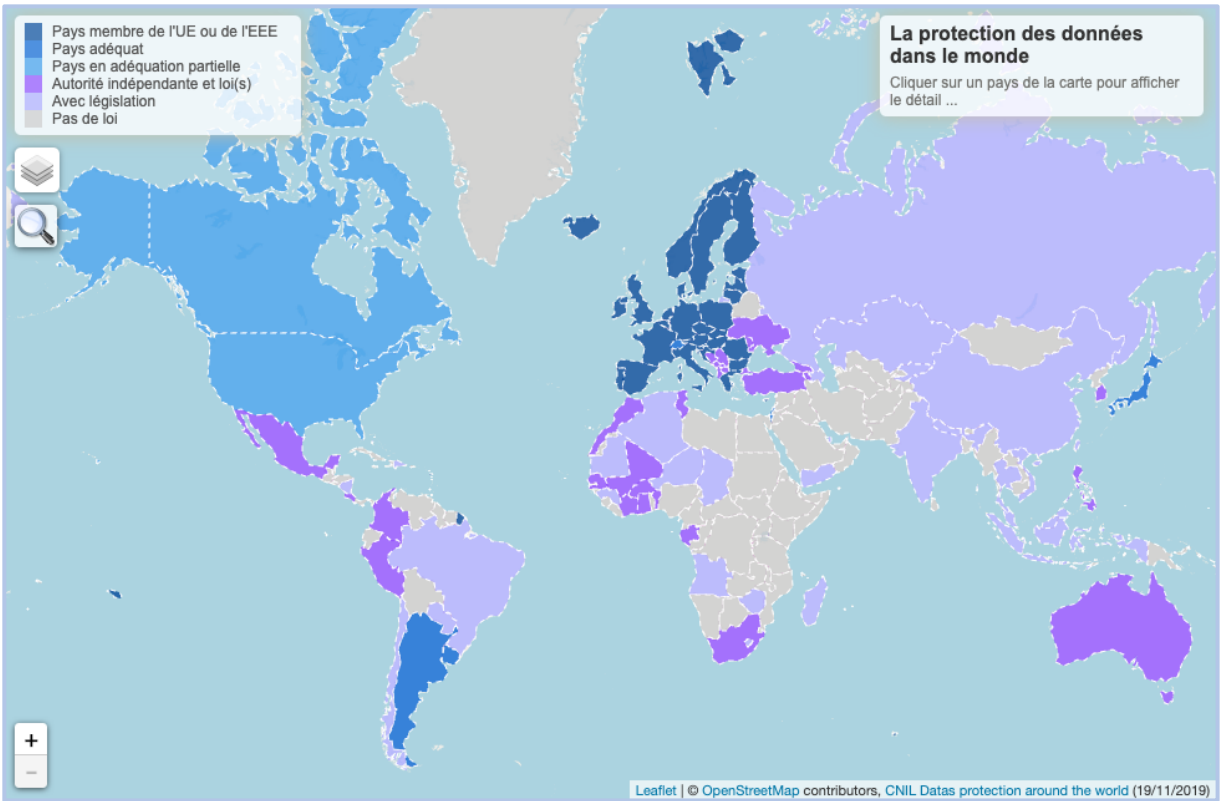

Figure 2 : Protection des données dans le monde - CNIL

(ii) Organisations mondiales

IAPP

L'**IAPP** (Internal Association of Privacy Professionals) est une **association à but non lucratif** fondée en 2000. Avec plus de **50 000 membres**, elle se présente comme la **plus grande communauté internationale de professionnels de protection des données**.

Par ses différentes actions, allant de l'organisation de conférences mondiales, à la formation, et la proposition de certifications, elle **sensibilise à la protection des données**.
L'IAPP est responsable du développement et du lancement d'un **programme mondial d'accréditation** en matière de confidentialité des informations. De plus, les **certifications** qu'elle propose – CIPM (Certified Information Privacy Manager), CIPT (Certified Information Privacy Technologist), et CIPP (Certified Information Privacy Professional) – sont **accréditées par l'ANSI** (American National Standard Institute), **et l'ISO** (International Organization for Standardization).

Solutions mises en place

A. Mise en conformité de l'existant

Avec l'entrée en vigueur du RGPD le 25 mai 2018, tous les organismes, qu'ils soient privés ou publics, ont dû se **mettre en conformité** avec cette nouvelle réglementation, **sous peine de s'exposer à des sanctions administratives** et des amendes pouvant atteindre 4% de leur chiffre d'affaire international.

Cette démarche a forcé certaines entreprises à **repenser la nature même de leurs modèles**, basés sur la collecte d'un large éventail de données personnelles, souvent à des fins non-définies. En conséquence, de nombreux aspects de l'entreprise, de la stratégie marketing au droit relatif à la protection de la vie privée, en passant par la conception des infrastructures techniques, ont dû être pris en compte.

Les étapes d'une démarche de mise en conformité, sont, de manière générale, les suivantes :

1. **Établissement d'une cartographie** de l'ensemble des traitements de données de l'entreprise ou de l'entité
2. **Vérification des spécificités** et des dispenses propres à l'activité ou au statut de l'établissement
3. **Analyse de chaque traitement** de données en profondeur, afin de vérifier sa **conformité** avec le règlement
4. **Tenue d'un registre** au sein duquel seront référencés les différents traitements des données à caractère personnel, conformes ou à modifier
5. Prise en compte de l'évolution de l'entreprise et s'assurer que la **conformité est maintenue**

Il est difficile d'évaluer le coût moyen de cette démarche, tant elle est liée au contexte de départ, au volume d'éléments à modifier, et au temps qui lui est accordé.
La CNIL, par le biais d'une formation en ligne ouverte à tous, intitulée « L'atelier RGPD » permet d'initier une mise en conformité et de sensibiliser les équipes.

B. AIPD

Dans le cadre de la mise en œuvre de **certains traitements**, notamment ceux **présentant un risque élevé pour les droits et les libertés des personnes physiques**, le RGPD impose de réaliser une **AIPD** (Analyse d'Impact relative à la Protection des Données), **préalablement à la mise en œuvre du traitement**. En effet, dans la mesure où les technologies évoluent rapidement, il est nécessaire de prévenir au maximum les risques d'un nouvel environnement de traitement pourrait occasionner sur les données analysées.
Les autorités de protection des données (APD) nationales, en concertation avec le comité européen de la protection des données peuvent fournir des listes de cas pour lesquels une AIPD serait nécessaire. La CNIL énumère les situations suivantes :

- les opérations de traitement des **données de santé par les établissements médicaux**,
- les opérations de traitement concernant les **données sensibles** (génétiques, de géolocalisation, hautement personnelles),
- les opérations de traitement des données de **personnes vulnérables** (enfants, personnes âgées),
- les opérations de traitement des données concernant le **profilage** (gestion, ressources humaines),
- les opérations de traitement des données concernant la **surveillance active et continue d'employés**,

- les opérations de traitement de données dans le cadre d'un **usage innovant** (nouvelle technologie),
- la collecte de données à **large échelle et leur croisement.**

L'AIPD se décompose généralement en trois parties :

1. Une **description détaillée du traitement** envisagé, de son **intérêt** et sa **finalité.**
2. Une **évaluation de la nécessité du traitement**, en fonction des risques encourus sur les droits des libertés des personnes concernées.
3. Les **mesures de sécurité** et les **garanties** envisagées afin de diminuer les risques évalués.

Si suite à l'analyse d'impact, les **risques** pour la sécurité des données **restent élevés**, le rapport doit être **transmis à la CNIL**. Celle-ci peut également initier cette vérification, en demandant de son propre chef l'accès à ce rapport.

Bien qu'elle puisse être perçue comme une contrainte pour les entreprises, l'AIPD représente tout de même une **opportunité dans le cadre juridique actuel**. En effet, elle offre un **cadre de travail précis** pour parvenir à la conformité aux directives du RGPD. De plus, elle permet aux entreprises de **réduire les craintes et les inquiétudes des personnes**, quant à l'utilisation de leurs données personnelles, et est une **preuve de sérieux**, souvent appréciée par d'éventuels partenaires, clients, etc.
En cas de non-respect des règles relatives aux études d'impact, les sanctions peuvent atteindre **10 millions d'euros**, ou **2% du chiffre d'affaire** de l'entreprise.

C. Accountability

L'Accountability désigne un nouveau principe du RGPD qui **introduit une logique de responsabilisation** et de **capacité à démontrer, à tout moment et de manière continue**, **la conformité d'une organisation au RGPD**. L'Entité doit établir une **démarche globale d'Accountability** visant à mettre en œuvre des mécanismes et des procédures internes permettant d'assurer et de démontrer à tout moment et de manière continue le respect des règles imposées par le RGPD. Concrètement, cette démarche se traduit par la **mise en place de mesures techniques et organisationnelles**, et la production d'éléments permettant de documenter et d'attester les actions effectuées.

Les obligations au titre du principe d'Accountability sont les suivantes :

- la **tenue d'un registre** relatif aux traitements de données à caractère personnel mis en œuvre,
- la mise en place des **procédures internes** au titre des principes de ***Privacy by design*** et de ***Privacy by default***,
- la réalisation d'**analyses** d'impact pour les traitements de données susceptibles d'entraîner un risque élevé pour les droits et libertés des personnes physiques,
- la désignation d'un **DPO** (Délégué à la Protection des Données),
- un **encadrement contractuel détaillé des relations de sous-traitance**,
- l'application d'une **politique de sécurité** et la **documentation de toute violation des données à caractères personnel**,
- l'application d'une **politique d'encadrement des transferts de données à caractères personnel hors Union Européenne**,
- la mise en place de **procédures permettant l'exercice des droits des personnes concernées**, y compris la fourniture d'informations.

Il est important de préciser que ces obligations, au titre du principe d'Accountability, **incombent aussi bien au responsable du traitement qu'aux éventuels sous-traitants**.

D. Privacy by Design et Privacy by Default

(i) Définition

Le principe de *Privacy by Design* (confidentialité par conception) est l'un des **principes clés du RGPD**. Il y est d'ailleurs prévu et mentionné par l'article 25, intitulé *Protection des données dès la conception et protection des données par défaut*.
L'idée derrière ce principe est d'**intégrer la protection des données dès la conception** d'un projet, d'un service, ou de tout autre biais manipulant des données personnelles. Ainsi, les risques d'un éventuel non-respect du RGPD sont particulièrement réduits, puisque les **mesures nécessaires au traitement des informations personnelles**, qu'elles soient techniques ou organisationnelles, **doivent être prises en amont** par l'entreprise.
Le principe de *Privacy by Design* **ne constitue pas une mesure de protection des données personnelles en tant que telle**, mais vise à rappeler aux entreprises la nécessité de prévoir, dès la conception d'un projet impliquant le traitement de données à caractère personnel, les mesures de protection élémentaires.

Le principe de *Privacy by Default* est le corollaire du *Privacy by Design*. Il désigne le responsable du traitement comme garant du plus haut niveau de confidentialité des données personnelles des personnes concernées.

(ii) Principes

Privacy by Design repose sur sept principes illustratifs fondamentaux :

1. **Principe de proactivité** : prise de mesures préventives à l'encontre des risques d'atteinte à la vie privée.
2. **Principe de protection par défaut** : protection systématique et implicite des données personnelles.
3. **Principe de protection par construction** : intégration du principe de protection des données dès la conception des systèmes et des pratiques internes.
4. **Principe de somme positive** : considération de la protection intégrée de la vie privée par tous les effectifs de l'organisme, et plus particulièrement par la fonction commerciale, comme une valeur ajoutée.
5. **Principe de protection de bout en bout** : sécurisation et protection des données sur la totalité de leur existence.
6. **Principe de visibilité et de transparence** : conformité aux objectifs établis, sous réserve de vérification indépendante.
7. **Principe de souveraineté de l'individu** : protection des intérêts des particuliers par des mesures implicites et strictes.

(iii) Mise en œuvre

En pratique, les principes évoqués précédemment nécessitent une **convergence des pratiques organisationnelles et des mesures techniques** qui assurent un niveau de protection des données élevé.
Pour l'aspect organisationnel, il est indispensable d'**allier les politiques, les processus et les procédures opérationnelles à une formation approfondie vers une culture prônant le respect de la vie privée**. C'est d'ailleurs le cas de certaines des entreprises au sein desquelles nous évoluons actuellement, dans le cadre de notre contrat de professionnalisation, qui sensibilisent très rapidement les nouveaux arrivants à ces problématiques, par le biais de formations en ligne.

Techniquement, une des approches possibles afin de mettre en œuvre le principe de *Privacy by Design* peut être la **pseudonymisation des données** (le remplacement de certaines données à caractère personnel par un pseudonyme). Ainsi, la personne concernée par les données est

inidentifiable, sa **vie privée est protégée** tout en permettant à l'entreprise d'**utiliser les données aux finalités souhaitées**. Les données sont ainsi **dissociées de l'identité** de la personne.
D'autres pratiques, telles que la **minimisation des données** (utilisation de données personnelles, adéquates, pertinentes et limitées au vu de la finalité) ou leur **chiffrement** permettent de protéger les données personnelles dès la conception.

Enfin, afin de mettre en œuvre le principe de *Privacy by Default*, les entreprises doivent **paramétrer par défaut** leurs produits avec **un haut niveau de protection**.
Les bonnes pratiques consistent ainsi à **assurer la confidentialité des données dès la première utilisation**, à **l'informer des risques encours** s'il souhaite bénéficier de fonctionnalités nécessitant l'accès à ses données, mais également à lui **permettre de modifier lui-même le paramétrage**.

Open Data

A. Définition

Le terme d'Open Data désigne des **données publiques**, auxquelles **tout un chacun peut accéder**, mais aussi **utiliser et partager**. L'Open Knowledge Foundation fournit une définition basée sur **trois critères** essentiels :

- La **disponibilité et l'accès** : Les données doivent être **pleinement accessibles**, moyennant un **coût de reproduction raisonnable**. De préférence, elles sont téléchargeables sur Internet. La forme doit être confortable et modifiable.
- La **réutilisation et la redistribution** : Les données doivent être fournies sous des conditions **permettant la réutilisation et la redistribution**, incluant le mélange avec d'autres ensembles de données.
- La **participation universelle** : Tout le monde doit être en mesure d'**utiliser**, de **réutiliser** et de **redistribuer les données**. Il ne doit y avoir **aucune discrimination** concernant les fins d'utilisation, ou contre des personnes ou des groupes. Par exemple, des restrictions non commerciales qui empêchent l'utilisation commerciale, ou les restrictions d'usage à certains secteurs, ne sont pas compatibles avec l'Open Data.

Du fait de leur **accès et exploitation libres de droits**, ces données offrent de nombreuses opportunités en termes de connaissance humaine, permettant entre autres la création de services qualitatifs et de nouveaux produits.
Par sa nature, l'Open Data est basée sur une **interopérabilité**, c'est à dire un principe fondamental de **mise en commun des données**, essentiel pour tirer des bénéfices de l'ouverture de nombreuses sources d'information au public. Ces données doivent donc permettre à différentes organisation et systèmes de travailler ensemble, en partageant leur savoir, et en utilisant un langage commun.

L'Open Data s'inscrit donc dans une tendance qui considère **l'information publique comme un bien commun** dont la **diffusion est d'intérêt public et général**. Cette philosophie a été renforcée en 2016 par la **loi Lemaire**, qui a consacré l'obligation pour les administrations de mettre à disposition les données qu'elles détiennent. Ainsi, l'ensemble des données produites et collectées par les administrations doit désormais être mis à disposition de manière spontanée et large.

B. Conciliation avec le RGPD

Le RGPD définissant de manière relativement large ce qu'est une donnée à caractère personnel, et donc devant être protégée par une série de mesures, il pourrait sembler **complexe de concilier les principes de l'Open Data avec ceux du RGPD**. En effet, l'addition de ces deux dispositifs, par principe opposés, pourrait **ralentir la mise en Open Data des données publiques**. De plus, comment les collectivités, ne touchant aucune dotation particulière pour la mise en œuvre du RGPD, feront-elles face aux coûts liés à l'anonymisation des données et au risque de se voir infliger en cas de violation du Règlement ? Demeure-t-il un intérêt à consulter une donnée privée de toutes informations personnelles ?
Les enjeux derrière ces deux principes simples que sont l'**obtention de données publiques transparentes pour davantage de démocratie** et la **protection des données à caractère personnel des citoyens**, sont fondamentaux, certains étant même de nature politique et démocratique, à l'image du contrôle citoyen des usages publics de la data.

Pour concilier ces deux principes, une des solutions serait le recours aux nouveaux principes introduits par le RGPD, notamment celui de *Privacy by Design*, qui incite les collectivités à prendre en compte la notion de vie privée préalablement à la collecte et au traitement, au regard des obligations futures auxquelles elles devront se soumettre lors de la diffusion des données publiques.

Une solution complémentaire éventuelle consisterait à **distinguer des groupes d'utilisateurs**, qui disposeraient de **droits de lecture et d'accès aux données différents** :

1. Le service émetteur de l'administration concernée (habilité à une consultation totale)
2. L'administration émettrice (habilité à une consultation partielle du document, quelle que soit la nominativité)
3. Une autre administration (locale ou nationale), via convention avec l'administration émettrice
4. Les ré-utilisateurs habilités, via un contrat de licence
5. Les autres utilisateurs, dans une configuration Open Data générale

Cette vision, bien que moins manichéenne que la vision de l'Open Data en France, pourrait permettre à la donnée de s'affirmer comme outil de développement de l'économie numérique et de transparence de l'action publique.

Limites

A. Violations de données à caractère personnel

(i) Définition

Une violation de données à caractère personnel est caractérisée par une **violation de la sécurité** entrainant **la destruction**, **la perte**, **l'altération**, la **divulgation non autorisée** de données à caractère personnel transmises, qu'elles aient été **conservées ou traitées d'une autre manière** ; ou **l'accès non autorisé** à celles-ci, de manière **accidentelle ou illicite**.

A titre d'exemple, l'exposition sur internet d'une base de données contenant des données personnelles relatives à des clients, en raison d'une faille de sécurité ou vulnérabilité, constitue une violation de donnes à caractère personnel. De la même manière, le vol ou la perte d'un support informatique contenant des données à caractère personnel en est également une.

(ii) Exemples

Les **cyberattaques** constituent un premier axe de violations de données à caractère personnel. **La plus importante de l'histoire a touché l'entreprise *Yahoo!* en 2013**, dont **l'ensemble des 3 milliards de comptes a été piraté**. Des informations personnelles telles que les noms, adresses électroniques, numéros de téléphones, dates de naissances et mots de passe des utilisateurs ont été dérobées.

Aux États-Unis, une **erreur humaine** est à l'origine du **vol des données de 143 millions d'utilisateurs d'*Equifax***, une **agence de crédit**. Les informations récupérées ne se limitent pas ici à de simples adresses mail, puisque l'on dénombre également des numéros de sécurité sociale, adresses postales, et des numéros de permis de conduire. De plus, les numéros de cartes de crédit de 209 000 consommateurs ont été volées, ainsi que les documents administratifs personnels d'environ 182 000 personnes.

On peut également citer le scandale d'AOL, ayant rendu public par inadvertance plus de 20 millions de recherches de mots clés effectuées par des centaines de milliers d'utilisateurs entre mars et mai 2006. Après enquête, il est apparu que les données contenaient également des numéros de carte de crédit, des numéros de carte de sécurité sociale, des noms et des adresses. Toutes les données exposées étaient celles des utilisateurs d'AOL aux États-Unis.

Enfin, la **fuite de données de *Facebook-Cambridge Analytica*** est également un autre exemple de violation de données à caractère personnel à grande échelle. *Cambridge Analytica* (*CA*), une société de profilage politique, a en effet **recueilli les données de plus de 87 millions d'utilisateurs Facebook**, **sans leur consentement**, à partir de 2014, dans le but d'**influencer les intentions de votes** en faveur d'hommes politiques ayant retenu les services de *CA* (notamment l'élection

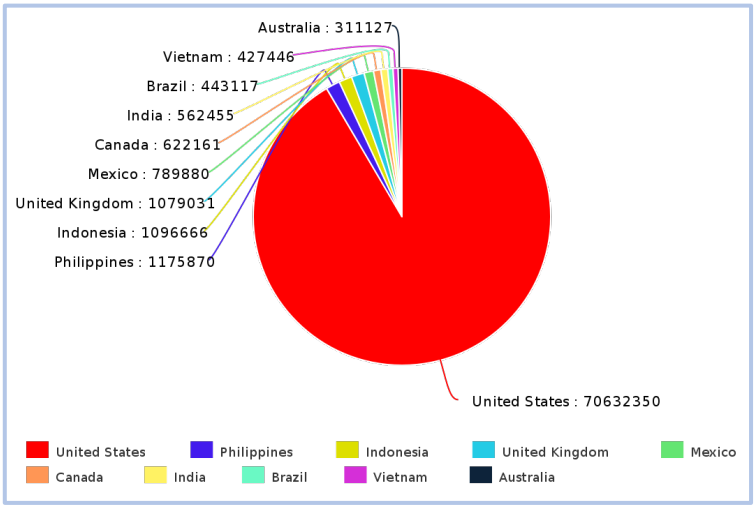

Figure 3 : Nationalité des victimes de la fuite de données Facebook-Cambridge Analytica

présidentielle américaine de 2016, et le référendum sur l'appartenance du Royaume-Uni à l'Union Européenne).

Pour ce faire, l'entreprise a agît par le biais d'une application développée sur la plateforme, sous la forme de tests psychologiques, ayant ainsi accès aux données personnelles des utilisateurs et de leurs amis.
Bien que n'ayant pas délibérément donné les données personnelles de ses utilisateurs à *CA*, Facebook est **mis en cause pour la conservation et la protection des données**. L'entreprise n'aurait également pas vérifié que toutes les données obtenues par CA aient été supprimées. Si le RGPD avait été en vigueur, Facebook aurait été coupable d'avoir communiqué des données personnelles à un tiers sans le consentement des utilisateurs mais également d'avoir manqué à son obligation d'informer les personnes concernées de ces transferts de données, et aurait encouru une amende pouvant atteindre 4% de son chiffre d'affaire.

(iii) Insuffisance face aux géants ?

Le 28 mai 2018, suite à l'entrée en vigueur du RGPD, l'association la *Quadrature du Net*, défendant et promouvant les droits et libertés des internautes, a déposé **cinq plaintes collectives** regroupant **12 000 personnes** contre Google, Amazon, Facebook, Apple et Microsoft. Derrière ces plaintes est dénoncée, entre autres, **la stratégie du "à prendre ou à laisser"** (soit l'utilisateur accepte les conditions d'utilisation et donc cède ses données personnelles, soit il n'a plus accès au service), qui est **interdite par le RGPD**.

Le 21 janvier 2019, suite à des activités non-conformes, **Google est condamné par la CNIL** à une **amende record de 50 millions d'euros**, pour **manquement à ses obligations de transparence et d'information dans le traitement des données des internautes européens** et pour **recueil insuffisant du consentement des internautes dans le cadre du traitement de leurs données à des fin de personnalisation de la publicité**.

On peut donc rester sceptique quant à la conformité des GAFAM en matière de protection des données personnelles. En effet, tout étant question de priorité dans l'évaluation de l'intérêt, on peut alors penser que si l'intérêt pécuniaire que tirent les GAFAM du traitement illégal est supérieur au montant des sanctions perçues, alors il est d'autant plus logique qu'ils demeurent dans cette volonté de non-conformité dès lors qu'ils réalisent toujours des bénéfices au vu la valeur sans cesse grandissante des données personnelles.
Reçus en septembre 2019 devant la Commission du commerce, des Sciences et du Transport, les représentants des géants américains du web et des télécoms, invités à donner leur avis sur le RGPD, ont affirmé leur attachement à la vie privée des utilisateurs, en plaidant néanmoins pour un **cadre plus souple**.

B. Enjeux de souveraineté

Si les données ont vocation à circuler, des tensions apparaissent dès lors que la frontière entre traitement des données à des fins commerciales et sécuritaires devient perméable, à l'image de l'affaire *Max Shrems*. A l'origine de cette affaire se trouve la découverte d'un **transfert de données personnelles massif** par Facebook, sans filet, **depuis l'Irlande vers les États-Unis**, où elles étaient ensuite **accessibles aux autorités américaines** notamment dans un contexte de lutte contre le terrorisme.
L'issue de l'affaire a été l'**invalidation spectaculaire du *Safe Harbor***, dispositif qui organisait le transfert des données de l'Union Européenne vers les États-Unis.

Le **Cloud Act** (Clarifying Lawful Overseas Use of Data Act), ratifié le 23 mars 2018 sous l'impulsion de Donald Trump, est une loi visant à **autoriser les autorités américaines à manipuler des données étrangères**. Il succède ainsi au **Patriot Act**, la loi antiterroriste évoquée au sein du paragraphe précédent.
Avec son adoption, les **opérateurs numériques et prestataires de services américains** sont tenus dans l'**obligation de divulguer les données personnelles de leurs utilisateurs**, dès lors que les autorités américaines le leur demandent, et ce **sans que les utilisateurs eux-mêmes en soient informés**.
Plus grave encore, le texte de loi précise que les informations personnelles doivent être transmises aux autorités américaines, et ce **même lorsqu'elles sont stockées en dehors du territoire national**. Ainsi, des entreprises telles que les GAFAM, qui détiennent à elles-seules 85% des données personnelles mondiales, ne sont plus en mesure d'assurer à leurs utilisateurs la confidentialité de leurs données personnelles.

Pourtant, deux ans auparavant, le RGPD avait été adopté par le Parlement Européen, imposant un cadre juridique nouveau, pensé pour garantir la confidentialité des données personnelles, en limitant les impacts des piratages et fuites d'informations professionnelles, et dont l'application était destinée aux sociétés, administrations et associations des pays du monde entier collectant des informations personnelles d'internautes européens.
Cette réglementation a malheureusement été contrée par l'adoption du Cloud Act aux États-Unis, remettant ainsi en cause le principe fondamental de protection des données personnelles, et visant à imposer une certaine forme **d'impérialisme numérique**, en transformant le **cyberespace en un terrain où s'affrontent des souverainetés**.
Certaines craintes s'avèrent donc être légitimes, en particulier celles de voir des pays moins démocratiques œuvrer pour que leurs lois régulent l'information de manière globale et/ou pour annihiler les autres réglementations.

Il apparaît aujourd'hui que **le cyberespace est devenu un lieu de pouvoir**, où s'affrontent intérêts privés, États, et multinationales.
L'Europe n'est pas obligée de se soumettre ni à une doctrine asiatique dont la conception des libertés individuelles est profondément différente, ni au pouvoir de l'administration débordante des États-Unis qui vient contrecarrer l'équilibre judiciaire et administratif des pays européens. A l'image du Cloud Act, de plus en plus de dispositions américaines sont extraterritoriales, car les grandes entreprises américaines dominent outrageusement le marché mondial. Afin de riposter à cette extraterritorialité américaine, la France et ses partenaires européens doivent s'organiser et se structurer ensemble, afin de mettre en place une nouvelle législation. Le Cloud Act représente une bataille idéologique, juridique, politique et stratégique que l'Europe doit mener afin de faire respecter sa souveraineté numérique, et ainsi, sa souveraineté nationale.

Conclusion

A l'heure où la dématérialisation des services et des procédures s'accélère, les flux de données se multiplient dans le monde, et les pratiques liées à la manipulation des données personnelles semblent être devenue monnaie courante.

L'âge, le sexe, la localisation, l'historique de navigation, ou encore l'adresse IP, sont des informations qui peuvent sembler anodines au premier abord. Toutefois, un usage déraisonné de ses informations peut s'avérer problématique et dangereux pour les libertés fondamentales.

C'est en ce sens qu'émergent de nouvelles législations, à l'image du RGPD, visant à renforcer l'encadrement juridique en matière de traitement de données à caractère personnel au niveau européen, afin d'assurer une protection à tous les citoyens de l'Union Européenne.

Le RGPD apparaît donc comme une législation utile mais qui présente le défaut de ne pas responsabiliser l'individu, d'une part, et qui récompense dans la compétition ceux qui y échappent, c'est-à-dire les GAFAM, d'autre part.

En effet, les utilisateurs, conscients théoriquement de l'importance de protéger leur vie privée ont en réalité un comportement généralement opportuniste et négligeant dans leur exercice intime des plateformes digitales, c'est le "paradoxe de l'intimité". Le RGPD ne permet pas aux utilisateurs de saisir la richesse des données qu'ils détiennent, et donc, de les inciter à un comportement individuel responsable.

Par ailleurs, la récolte massive d'informations personnelles apparaît comme un élément clé de développement économique pour les entreprises.
Aussi, les entreprises européennes, soumises à cette législation, encaissent un retard de compétitivité majeur sur leurs concurrentes faute de pouvoir stocker et analyser de vastes corpus de données privées, qui ont une importance primordiale pour des technologies telles que l'Intelligence Artificielle. Ce retard menace donc d'être fatal à notre innovation et notre compétitivité, face à des géants toujours plus puissants.

A l'image de notre mode de consommation, qui a tend à redevenir plus local, une prise de conscience autour de la gestion de nos données personnelles s'impose. Il est important de mettre en avant et d'utiliser en premier lieu des solutions développées par des entreprises françaises ou européennes, en conformité avec le RGPD. Les enjeux autour de cette prise de conscience sont fondamentaux, et concernent, à différentes échelles, à la fois les libertés individuelles et la souveraineté nationale.

Bien que ces changements puissent ne pas sembler évidents à mettre en œuvre au premier abord, de nombreuses alternatives aux services proposés par les GAFAM ont émergé ces dernières années, portées par des entreprises telles que *Mozilla*, principalement connue pour son navigateur web (*Firefox*), mais qui propose également d'autres solutions telles qu'un système d'exploitation mobile (*Firefox OS*), *Qwant*, un moteur de recherche français respectant la vie privée de ses utilisateurs, ou encore *Open Street Map*, une solution de cartographie libre de droits.

Acronymes

AIPD : Analyse d'Impact relative a la Protection des Donnees

ANSI : American National Standards Institute

CEPD : Comite Europeen de la Protection des Donnees

CNIL : Commission Nationale de l'Informatique et des Libertes

DPO : Data Protection Officer

ISO : International Organization for Standardization

RGPD : Reglement General sur la Protection des Donnees

UE : Union Europeenne

Sources

PROTECTION DES DONNEES DANS LE MONDE – CNIL
https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

AIPD - CNIL
https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd

COMPRENDRE LE RGPD - CNIL
https://www.cnil.fr/fr/comprendre-le-rgpd

DATA NEVER SLEEPS - DOMO
https://www.domo.com/learn/data-never-sleeps-7

RGPD – MINISTERE DE L'ECONOMIE ET DES FINANCES
https://www.economie.gouv.fr/entreprises/reglement-general-sur-protection-des-donnees-rgpd

ALTERNATIVES AUX GAFAM – KORII (SLATE)
https://korii.slate.fr/et-caetera/surveillance-donnees-personnelles-protection-vie-privee-alternatives-google-chrome-whatsapp-messenger

OPEN DATA - CNIL
https://www.cnil.fr/fr/publication-en-ligne-et-reutilisation-des-donnees-publiques-open-data
https://www.cnil.fr/fr/open-data-la-protection-des-donnees-comme-vecteur-de-confiance

Synthèses des séminaires

L'entreprise libérée

Ce document se veut une synthèse de l'intervention de M. Fabrice REBY, président de la société *Excilys*, traitant de la thématique l'Entreprise Libérée, dans le cadre du module *Performance du Processus d'Informatisation*, encadré par M. Jean-Guy SAYOUS.

L'entreprise libérée est un nouveau **modèle d'organisation**, dont le principe est de **laisser les salariés prendre des initiatives individuelles, plutôt que de leur imposer des directives et des contrôles**. L'idée derrière cette approche est de **ramener les décisions de vie qui impactent les salariés à leur niveau**.
Ainsi, l'entreprise libérée **prône la confiance en l'Homme**, en se basant sur la théorie Y de Douglas McGregor, selon laquelle l'homme aime travailler.
Le principal but de l'entreprise libérée est de **rendre le salarié libre**, **dans la limite des contraintes réelles**. Cette liberté se situe surtout dans la façon d'interagir avec les autres, afin **d'amener plus de valeur ajoutée dans le cœur du métier**.

En retraçant son parcours de vie, depuis sa scolarité, jusqu'à sa présidence d'*Excilys*, en passant par ses succès et échecs professionnels, M. REBY a soulevé de nombreuses thématiques importantes, liées à la notion d'entreprise libérée.
Ainsi, M. REBY a souligné à plusieurs reprises l'importance de **comprendre le monde qui nous entoure**. En effet, en termes de perspectives professionnelles, l'un des points les plus important en entreprise est d'apprendre des autres, et de comprendre leur comportement. Les réflexes craintifs (isolation, peur de l'autre, etc.), ancrés dans la nature de l'Homme, ne doivent pas nuire à son évolution, qu'elle soit personnelle ou professionnelle.
Une autre thématique évoquée à plusieurs reprises par M. REBY, intimement liée à la précédente, est **l'apprentissage de ses erreurs**, et des erreurs des autres.
Enfin, l'entreprise étant à l'image de la société, un des principaux défis à relever concerne notre état d'esprit. La **bienveillance doit émerger de chacun de nous tous**, un changement d'état d'esprit permet bien plus que de simples réformes. L'idée est de **changer le monde par nos attitudes et nos choix**.

L'entreprise libérée offre de nombreux bénéfices, tels que la **mise en avant du travail collaboratif**, des **salariés plus impliqués**, **plus motivés** et donc indéniablement **plus performants**. En laissant s'exprimer les idées et les initiatives de chacun, le **collectif se trouve renforcé**, et **le caractère innovant de l'entreprise est développé**.
Néanmoins, on peut se questionner quant aux **défis** liés à la mise en place d'un tel système organisationnel, dans une culture française où le **modèle pyramidal traditionnel est fortement ancré**. Ainsi, on peut se demander si les salariés souhaitent, et sont préparés aux responsabilités amenées par ce système, puisque celles-ci apportent également une **charge de travail et un stress supplémentaire**.

Enfin, il convient d'étudier la **transformation d'une entreprise vers ce modèle libéré**. Comment passer d'une structure hiérarchique pyramidale, à ce modèle ? Le défi concerne les collaborateurs, qui se voient chargés de nouvelles responsabilités, mais également les dirigeants, qui doivent eux accepter la réduction de leurs pouvoirs. Il est certainement préférable que cette **transition ait lieu de manière incrémentale**, en augmentant progressivement l'autonomie des collaborateurs.

Parmi tous les défis mentionnés au sein de cette synthèse, le principal demeure ici le **changement de culture** (qui peut être illustré comme étant le passage de chasseur à cultivateur). Pour amener ce changement, il serait intéressant de mettre en place des **formations**, et des **ateliers** au sein de l'entreprise, pour **permettre à chacun d'exprimer ses idées et d'évoquer ses réserves**.

Le DevOps

Ce document se veut une synthèse de l'intervention de cinq employés du *Crédit Agricole CIB*, traitant de la thématique du DevOps, dans le cadre du module *Performance du Processus d'Informatisation*, encadré par M. Jean-Guy SAYOUS.

Le terme **DevOps** est issu de la contraction des deux mots anglais Development (développement) et Operations (exploitation). Apparu en 2009, par l'initiative de Patrick Debois, consultant en informatique belge, la notion de DevOps vise **à améliorer la collaboration**, jusqu'alors étroite, **entre les équipes de développeurs (Devs), et les équipes d'exploitants (Ops)**. En effet, cette relation est souvent symbolisée par un **mur de la confusion**, dénonçant le fossé entre les **Devs**, constamment **à la recherche de changements**, et les **Ops**, qui **recherchent eux la stabilité**.
Le DevOps vise donc à **créer une culture et un environnement au sein desquels la conception, les tests, et la diffusion de logiciels peuvent être réalisés rapidement, fréquemment, et efficacement**. Il ne s'agit donc pas d'une simple méthodologie, mais d'une réelle **philosophie de travail**.

Après une introduction détaillant les enjeux du DevOps au sein du *Crédit Agricole CIB*, notamment en matière de gestion d'une infrastructure particulièrement imposante (11 000 environnements, 1 350 applications, et 9 000 serveurs), et d'internationalisation des effectifs (21% des salariés sont basés à l'étranger), l'intervention s'est décomposée en plusieurs parties.

La première présentation visait à expliciter la notion **d'usine logicielle**, en détaillant les technologies associées au DevOps, sur l'ensemble du cycle de vie du logiciel (du développement, à la livraison automatisée, en passant par le packaging et les tests). Cette présentation a souligné la **place importante, mais non exclusive, qu'occupent les technologies**, notamment pour **l'aspect CI/CD** (intégration et déploiement continus), au sein du DevOps.
Le **respect des principes et des règles de développements** est également particulièrement important, dans la mesure où la qualité du code impacte fortement la sécurité et les performances du produit. Le principe **KISS** (Keep It Simple, Stupid), qui **préconise la simplicité dans la conception**, adresse cette problématique de complexité, en soulignant les problématiques liées à celle-ci (maintenabilité coûteuse, source potentielle d'erreur, etc.).
Enfin, la notion de **veille technologique**, qui sera primordiale au cours de nos carrières professionnelles, a également été mise ne lumière durant cette présentation. Face à l'évolution, et l'émergence de nouvelles technologies, nous devrons **demeurer d'éternels apprenants**, afin de demeurer **performants** et **compétitifs**.

Les deux présentations suivantes nous ont offerts deux retours d'expériences liés au DevOps, le premier côté Dev, et le second côté Ops. Ces deux présentations étaient principalement axées sur les **méthodes agiles**, et donc sur le plan managérial et relationnel, complétant ainsi parfaitement la première.
Les quatre valeurs pionnières issues du manifeste agile, sont les suivantes :

- **Individus et interactions** plutôt que processus et outils
- **Fonctionnalités opérationnelles** plutôt que documentation exhaustive
- **Collaboration avec le client** plutôt que la contractualisation des relations
- **Acceptation du changement** plutôt que la conformité aux plans

Afin de faire écho à la première présentation, il est important de rappeler **que l'agilité prône l'excellence technique**, et bien qu'elle soit synonyme de flexibilité, elle nécessite beaucoup de rigueur, et **ne doit pas nuire à la vision long terme du projet**.

Le DevOps est donc un **enjeu de transformation vitale pour la compétitivité des entreprises**. Bien que sa mise en œuvre ait un coût non-négligeable pour l'entreprise, et amène avec elle de nouvelles pratiques, induisant un changement de culture en son sein, ceci ne doit pas être un frein, puisque les bénéfices apportés sont réels, que ce soit en termes **d'amélioration des dynamiques internes et externes**, ou **d'amélioration de la qualité de production**.

Architecture d'Entreprise

Ce document se veut une synthèse de l'intervention de M. Alain GUERCIO, Consultant Business Manager au sein de la société *MEGA International*, traitant de la thématique de l'Architecture d'Entreprise, dans le cadre du module *Performance du Processus d'Informatisation*, encadré par M. Jean-Guy SAYOUS.

Dans un **contexte de transformation digitale**, les entreprises subissent de **nombreux changements**, **impactant aussi bien leur modèle économique, leur stratégie, que leurs organisations et modes de fonctionnements**. En effet, si préalablement l'objectif était principalement la **productivité**, avec des marchés d'offre, de produits, locaux, stables et simples, désormais, il est à la **compétitivité**, avec des marchés de demande, de services, internationaux, instables et complexes.
Ces changements, souvent associés à la notion **d'*Uberisation*** (du nom de l'entreprise *Uber*) des marchés, de l'économie, impliquent de **profondes reconfigurations pour les entreprises et leurs Systèmes d'Informations**.

L'Architecture d'Entreprise (AE) est un **levier majeur pour la définition de ces transformations**, **et leur pilotage**. Elle vise à aligner l'ensemble des couches de l'entreprise (Métier, fonctionnelle, applicative, etc.) avec la stratégie d'entreprise, par la **réduction de la redondance**, **de la complexité**, **des silos d'informations et des risques commerciaux associés aux investissements**.
Les Architectes d'Entreprise sont chargés d'effectuer l'analyse de la structure et des processus de l'entreprise et doivent tirer des conclusions des informations collectées pour atteindre les objectifs de l'Architecture d'Entreprise : **l'efficacité**, **l'efficience**, **l'agilité** et la **continuité** des opérations.

Afin de mettre en cohérence les différentes visions du Système d'Information, l'Architecture d'Entreprise doit s'appuyer sur un **cadre de référence** (ou framework), visant à **organiser les différentes vues et identifier leurs articulations**. On distingue les cadres de référence **orientés modèles**, tels que *MERISE*, *Zachman*, de ceux **orientés méthodes**, tels que *TOGAF*.
Considéré par beaucoup comme le cadre fondateur de l'Architecture d'Entreprise, le framework ***Zachman,*** apparu à la fin des années 1980s, permet **d'identifier et de structurer les différents concepts constituant les briques utilisées pour réaliser les modélisations décrivant l'entreprise**. Il fournit un méta-modèle complet permettant de décrire l'entreprise sur différents niveaux, à différents points de vue, représenté par une matrice croisant les six interrogations de base (Quoi, Comment, Où, Qui, Quand et Pourquoi, avec six groupes de parties prenantes (Visionnaire, Propriétaire, Concepteur, Réalisateur, Sous-traitant et Exécutant).
Aujourd'hui, le cadre de référence le plus adopté par les entreprises est ***TOGAF*** (*The Open Group Architecture Framework*), actuellement dans sa version 9.2. Ce framework propose une **démarche de conception et de gouvernance des architectures d'entreprise ainsi qu'un recueil de meilleures pratiques**. Il fournit un modèle générique, centré sur la gestion des exigences, indépendant du modèle de formalisation de l'architecture et au périmètre adaptable.

Avec l'accélération de la compétition, et **l'émergence du syndrome *winner-takes-all***, les entreprises prennent conscience de l'importance du système des Systèmes d'Informations, et s'interrogent sur les évolutions techniques (telles que l'émergence du Big Data, du Cloud, du Deep Learning, etc.) pour rester dans la course. C'est dans ce contexte que le ***DevOps***, et particulièrement son aspect *CI* (*Continuous Integration*), trouve toute son importance, en permettant l'intégration des différents composants d'un projet le plus rapidement possible.
Pour s'adapter, les entreprises doivent procéder à des évolutions de plus en plus rapides, et maîtrisées, c'est **l'Architecture Continue**, qui vise à **créer une organisation robuste autour d'une démarche industrialisée d'architecture d'entreprise**. Cette problématique concerne autant les startups que les grandes entreprises à la recherche de réactivité face à l'accélération des évolutions du marché.
Ainsi, l'une des solutions adoptées par celles-ci est le **passage à l'échelle des pratiques Agile** (*Agile at scale*), dont un des cadres de référence les plus appliqué est ***SAFe*** (*Scaled Agile Framework*).

Impacts environnementaux du numérique

Ce document se veut une synthèse de l'intervention de M. Nicolas BROGNÉ, Product Manager au sein du *Crédit Agricole GIP*, traitant de la thématique de l'impact environnemental du numérique, dans le cadre du module *Performance du Processus d'Informatisation*, encadré par M. Jean-Guy SAYOUS.

Les activités humaines sont pour une très grande part responsable du dérèglement climatique auquel nous faisons face aujourd'hui. Les pires scénarios sont régulièrement revus à la hausse, et la teneur en gaz carbonique et en méthane n'a jamais, sur 800 000 ans, été aussi élevée.
De nombreux états semblent enfin saisir la mesure de l'impact de l'Homme sur le réchauffement climatique, et s'organisent pour le réduire, à l'image de l'accord de Paris sur le climat de 2015.
Le transport, l'énergie, l'agriculture sont souvent présentés, à raison, comme les principaux leviers sur lesquels agir. Le numérique, du fait notamment de son aspect dématérialisé qui l'accompagne, est souvent omis. Pourtant, il est aujourd'hui **responsable de davantage d'émission de gaz à effet de serre mondial que le transport aérien civil**. Et les **impacts environnementaux du numériques** ne se limitent pas au **réchauffement climatique global**, puisqu'il se traduisent également par un épuisement des ressources abiotiques et une consommation d'eau et d'énergies primaire accrue.
Ces impacts ne vont cesser d'augmenter, puisqu'on estime que le **volume de données mondial sera multiplié par 45 entre 2020 et 2035**.

En 2019, 4% des gaz à effet de serre ont été produis par le numérique, et on estime que cette valeur aura doublée d'ici 2025. Sur ces 4%, environ **un quart est issu des data-centers**, **un autre quart des infrastructures réseau**, mais la **majorité (47%) est due aux équipements utilisateurs**.
L'un des moyens de réduire son empreinte numérique est donc d'**allonger la durée de vie de ses équipements**, en conservant le plus longtemps possible ses terminaux. Des initiatives fleurissent en ce sens, à l'image du *FairPhone*, un smartphone qui se veut responsable, durable, maintenable et évolutif.
La **sobriété numérique** est une démarche visant à réduire l'impact environnemental du numérique, en **concevant des services numériques plus sobres** et en **modérant les usages numériques quotidiens**.
En 2018, **80% des flux de données** concernaient le **streaming vidéo**, représentant à lui seul l'équivalent des émissions de CO2 d'un pays comme l'Espagne. A titre d'exemple, être « numériquement sobre » dans sa consommation de vidéo en ligne, consiste à diminuer sa consommation, et utiliser la plus faible résolution qui permette de profiter du contenu.
Dans un monde sous contrainte climatique, la **priorisation des usages** est donc l'un des **enjeux clés** des débats. La dimension mondiale du système numérique nécessite la **mise en place d'outils de régulation et de sensibilisation nationaux et internationaux**.

Pour les entreprises, la rédemption peut passer par **l'écoconception**, qui consiste à intégrer l'environnement dès la conception d'un produit ou service, et sur la totalité de son cycle de vie. Cette écoconception s'appuie sur un **recueil de bonnes pratiques**, à intégrer à la fois dans la fonction d'Architecture, dans le rôle de Product Management, et dans la démarche Agile de l'entreprise.
Le **recyclage** et le **réemploi**, sont également à considérer, afin de lutter contre l'obsolescence programmée. Ainsi, le **low-tech**, promouvant une **sobriété de consommation et de production** grâce à des technologies simples d'usages et à faible impact environnemental est à préférer au high-tech.
Il est également important de considérer l'idée d'***IT for Green***, selon laquelle les **technologies du numériques pourraient agir comme catalyseur du développement durable**. En effet, à l'image de Google, ayant réduit de 30% la consommation en énergie de ses Data Centers grâce à l'intelligence artificielle, **le numérique peut participer à la réduction de gaz à effet de serre**, et ce dans d'autres secteurs également. En somme, l'intelligence artificielle aura donc, à terme, un impact particulièrement positif sur l'environnement.
Enfin, d'autres leviers existent, à l'image de la **comptabilité sociale et environnementale**, qui vise à intégrer à la comptabilité l'impact de l'entreprise sur l'environnement et la société, ou encore la **compensation carbone**, qui consiste à essayer de contrebalancer les émissions de CO_2 par le financement de projets de réduction d'autres émissions ou de séquestration de carbone.

Cybersécurité

Ce document se veut une synthèse de l'intervention de M. Gilles CASTERAN, directeur exécutif au sein d'*Accenture Security*, traitant de la thématique de la cybersécurité, dans le cadre du module *Performance du Processus d'Informatisation*, encadré par M. Jean-Guy SAYOUS.

L'émergence des cyber-systèmes marque une **quatrième révolution industrielle**, après celles amenées par la mécanisation, l'électrification, et l'électronique. A l'image des précédentes, cette nouvelle révolution, dont la **matière première serait la donnée**, induit de **profondes modifications des pratiques**, demande de **nouvelles compétences**, mais est également accompagnée d'un certain nombre de **menaces** et de **risques**. Le monde s'en trouve également transformé, avec la domination de **deux superpuissances** que sont les **États-Unis** et la **Chine**, dominant le marché par le biais de géants du web : les **GAFAM** (*Google*, *Apple*, *Facebook*, *Amazon* et *Microsoft*) pour la première, et les **BATX** (*Baidu*, *Alibaba*, *Tencent* et *Xiaomi*) pour la seconde.

Espionnage, vol de données sensibles, déstabilisation, dégradation, les **motifs des cyberattaques** et piratages sont **de plus en plus nombreux** et leurs cibles le sont tout autant. Ainsi, un simple groupe de personnes est désormais en capacité de **déstabiliser des entreprises, des États**. Ces attaques peuvent être menées de différentes manières, allant la saturation du réseau informatique par déni de service (DDoS), aux logiciels malveillants (*ransomware*, *spyware*, etc.), en passant par l'hameçonnage (*phishing*). Ces dernières années, on assiste à un **bouleversement des pratiques des cybercriminels**, puisque les **cyberattaques deviennent de plus en plus indirectes**. En effet, à l'image d'Airbus, visé par la cyberattaque menée sur Altran, les attaques sont de plus en plus ciblées sur des sous-traitants, clients, afin de nuire indirectement à l'entreprise.
Les **menaces**, de plus en plus **nombreuses**, **sophistiquées**, **ciblées**, et **dévastatrices**, du fait de leurs conséquences financières élevées, **doivent donc être adressées par les entreprises**, c'est tout l'enjeu derrière la **cybersécurité**.

La cybersécurité est l'ensemble des **moyens techniques et non techniques** permettant d'assurer la **disponibilité**, **l'intégrité** et la **confidentialité des informations utilisées**, **transmises** et **stockées**.
Les grandes activités de la cybersécurité comprennent **l'identification**, la **protection**, la **détection**, la **réponse** et le **rétablissement** des attaques. Elle adresse une véritable **problématique de gestion de risques au sein de l'entreprise**.
Un risque peut être défini comme étant **l'éventualité qu'une menace parvienne à exploiter une vulnérabilité sur un actif métier en contournant les mesures de protection**. Il est donc fonction de trois paramètres, que sont la **vulnérabilité**, la **menace** et **l'impact**.
Il peut être traité de différentes manières : **accepté**, **annulé**, **transféré** ou **réduit**. Ainsi, pour les fournisseurs d'accès au Cloud, l'un des grands enjeux futurs, la réversibilité, correspond ici au transfert.
Les risques induits par les cyberattaques sont distingués à **différentes échelles** : **l'individu**, **l'entreprise**, et **l'état**, et **doivent être identifiés, cartographiés, et classifiés**.

Loin de faiblir, le **risque cyber devient de plus en plus prégnant**. La **transformation numérique** et ses corollaires (dépendance accrue aux outils, interconnectivité des systèmes d'information, généralisation du stockage dans le Cloud, émergence de l'IoT, etc.) ont généré un **ensemble de nouveaux risques** contre lesquels les entreprises ne sont pas suffisamment armées. Ainsi, le **cyber-incident** arrive en **deuxième position des risques les plus redoutés** par les organisations, devant les catastrophes naturelles, et juste **derrière l'interruption d'activité, avec laquelle il est interdépendant**. En effet, les incidents informatiques ont souvent pour conséquence une interruption ou un ralentissement de l'activité, du fait de l'interconnexion entre l'entreprise et son Système d'Information.

D'après une étude menée par *Accenture*, **les violations de sécurité ont augmentées de 11% sur 2 ans**, et de **67% sur 5 ans**. Toutefois, la même étude montre également une **amélioration de la défense** mise en place par les entreprises, puisqu'**en 2018**, **87% des attaques ont été déjouées**, contre 70% en 2017.
En ce sens, **un des axes de maturité face aux cyberattaques concerne leur détection**. En effet, si l'on pourrait penser que **la capacité de détection des entreprises s'améliore considérablement**, avec **23% de celles-ci détectant plus de 76% des attaques**, il ne faut pas oublier qu'à l'inverse, **24% des entreprises en détectent moins de la moitié**. Pour pallier à cela, les entreprises doivent s'inspirer des leaders, qui mettent en place des solutions telles que le **déploiement de la sécurité à l'échelle**, la **formation**, permettant ainsi d'introduire au sein de l'entreprise une certaine **culture de la sécurité**, ou encore la **collaboration**, apportant une réelle valeur ajoutée.

Les organisations doivent désormais partir du principe qu'elles **seront victimes d'une attaque**, puisqu'on estime que **80% d'entre-elles ont subi une cyberattaque en 2019**.
Une approche complémentaire à la cybersécurité, devrait donc être de **planifier une stratégie de cyber-résilience** afin de limiter l'impact d'une attaque. La cyber-résilience est la **capacité** que possède l'entreprise de **continuer son activité opérationnelle lorsqu'elle subit, ou a subi une attaque**.
Elle vise à gérer la sécurité en adoptant une **approche globale** impliquant à la fois les **individus**, les **processus** et la **technologie**. Elle impose une **méthodologie** à la fois **solide** et **évolutive** de **gestion**, **d'analyse** et **d'optimisation des risques.**

Les cinq sujets essentiels, qui doivent être adressés dans la cybersécurité de nouvelle génération sont donc la **confiance numérique**, **l'éthique**, qui permet de l'accentuer, la **souveraineté**, la **solidarité**, et la **cyber-résilience**.