PLATEFORME **RSE**
Responsabilité sociétale des entreprises

Juillet 2020

Avis

Responsabilité numérique des entreprises

1. L'enjeu des données

FRANCE STRATÉGIE
ÉVALUER. ANTICIPER. DÉBATTRE. PROPOSER.

PLATEFORME RSE
Responsabilité sociétale des entreprises

Responsabilité numérique des entreprises
1. L'enjeu des données

Animatrice
Bettina LAVILLE – Comité 21

Co-rapporteurs
Ghislaine HIERSO – 4D / Les Petits Débrouillards
Geoffroy de VIENNE – CFTC

FRANCE STRATÉGIE

Juillet 2020

Secrétariat permanent
Gilles BON-MAURY, secrétaire permanent
Sandrine CADIC, chargée d'études
Garance PACOURET, chargée d'études
Etienne BRODEAU, stagiaire chargé d'études
plateformerse@strategie.gouv.fr

SOMMAIRE

AVANT-PROPOS

La Plateforme nationale d'actions globales pour la responsabilité sociétale des entreprises (Plateforme RSE) réunit depuis 2013 les parties prenantes de la RSE en France : entreprises, partenaires sociaux, organisations de la société civile, réseaux d'acteurs, chercheurs et institutions publiques.

La Plateforme RSE a décidé en 2018 de constituer un groupe de travail portant sur la « Responsabilité numérique des entreprises » (RNE) afin d'appréhender les questions soulevées par la transition numérique. La massification des données et les évolutions numériques constantes transforment le paysage dans lequel évoluent les entreprises. Souvent positifs, ces effets doivent être appréhendés avec éthique et dans le respect de l'environnement et des droits humains fondamentaux.

Le champ d'étude était considérable, et le groupe de travail a décidé de scander l'étude en deux temps. La Plateforme RSE s'est concentrée, dans un premier temps, sur les données collectées ou générées par les entreprises dans le cadre de leurs activités.

La prise en considération des défis sociaux et environnementaux par les entreprises sera examinée dans un second temps. Le sujet environnemental faisant l'objet de différentes études parlementaires attendues en juin 2020, la Plateforme RSE s'attachera à les consulter. De plus, la stratégie sur les données établies par la Commission européenne et dont les premiers éléments ont été publiés le 19 février 2020, permettra une analyse intéressante.

Dans le cadre de cette autosaisine, la Plateforme RSE a constitué un groupe de travail qui a mené dix-huit auditions afin d'élaborer un diagnostic et des propositions. En analysant le contexte numérique dans lequel évoluent les entreprises et en s'appuyant sur leurs pratiques, elle adresse ses recommandations aux pouvoirs publics, aux entreprises, aux syndicats de salariés, aux chercheurs et aux acteurs de l'évaluation extra-financière des entreprises.

SYNTHÈSE

Les entreprises à l'aune des transformations numériques

L'étendue des transformations technologiques, la massification des données et leur prise en compte à tous les niveaux de l'entreprise transforment le paysage dans lequel elles évoluent. À la fois une transformation technique, un enjeu stratégique et un bouleversement humain, le numérique engendre de nouveaux risques à appréhender et de nouvelles opportunités à explorer. Considéré comme l'un des atouts des plans de relance de l'économie à la suite de la crise sanitaire de la Covid-19, il doit s'inscrire dans la stratégie RSE des entreprises.

Face à la quantité de données engendrées par la transition numérique, les entreprises ont, aujourd'hui, une quadruple responsabilité dans la maîtrise de ces données et leur protection, juridique, managériale et éthique. La Plateforme RSE a constaté que si la responsabilité juridique était encadrée par la loi, l'ensemble des risques et responsabilités que soulève le numérique ne l'était pas au regard des pratiques de la RSE, alors que son utilisation soulève des questions prégnantes quant à ses impacts sociaux, environnementaux et sociétaux.

C'est pourquoi la Plateforme RSE propose une définition de la Responsabilité numérique des entreprises (RNE), ainsi libellée :

La RNE est un déploiement nouveau et incontournable de la RSE, qui se fonde sur les mêmes principes de confiance, de redevabilité, d'éthique et d'échanges avec les parties prenantes des entreprises. La transversalité du numérique et son omniprésence impliquent que la création de valeur qu'elle engendre soit comprise et partagée par tous, au regard des enjeux démocratiques, sociaux et sociétaux. Il s'agit d'un enjeu de confiance, d'une confiance à renouveler au regard des constantes évolutions des techniques.

La RNE s'exerce dans des champs nombreux liés à l'usage des moyens informatiques et digitaux dont disposent les entreprises. Une entreprise numériquement responsable

devrait ainsi répondre à plusieurs enjeux majeurs, en lien avec les objectifs de développement durable :

- la responsabilité réglementaire, liée à la protection des données et au respect du RGPD et des réglementations sectorielles ;
- la responsabilité éthique, liée aux logiciels relatifs à l'intelligence artificielle (IA) ;
- la responsabilité sociétale, relative à la gestion des données, à la transformation des modes de travail, au type de partage des données et à l'inclusion de toutes et tous ;
- la responsabilité environnementale, liée à l'utilisation des données dans la prise en considération des impacts environnementaux des activités des entreprises.

La Plateforme RSE s'est d'abord attachée à cerner la responsabilité des entreprises au regard des données qu'elles collectent, gèrent, conservent, et traitent. Cet avis est le premier d'un cycle dédié à la responsabilité numérique des entreprises, ainsi les profonds changements concernant le travail, les rapports entre salariés, dirigeants et parties prenantes, et l'aggravation notoire de l'empreinte environnementale par le numérique, seront étudiés ultérieurement.

Numérique et RSE, deux secteurs qui doivent se décliner ensemble dans l'entreprise

Encore peu développée en France, la notion de « responsabilité numérique des entreprises » (RNE) se révèle fondamentale. La protection des données, très encadrée par la loi, constitue un enjeu majeur pour les entreprises en matière de concurrence et de protection des droits humains, de valeur de l'entreprise et d'évolution des *business models* ; et s'inscrit dans une démarche responsable auprès des salariés, des parties prenantes ainsi que des clients et des utilisateurs.

Or, force est de constater que, même si la transition numérique impacte aujourd'hui toutes les entreprises, les enjeux numériques ne sont pas intégrés aux stratégies RSE, et inversement. Les auditions menées dans le cadre du groupe de travail de la Plateforme RSE ainsi que l'analyse des textes législatifs en vigueur témoignent de l'absence regrettable de coordination entre numérique et RSE. Les membres de la Plateforme RSE ne peuvent, ainsi, que recommander la coordination entre ces deux politiques, et la liaison entre les directions qui en ont la charge.

Les entreprises face à la massification des données

Depuis 1970, les traités internationaux, directives européennes et législations françaises se succèdent afin de réglementer l'usage des données par les entreprises et assurer la protection des données de tous les utilisateurs.

Au-delà des données personnelles, les entreprises possèdent une multitude de données avec lesquelles elles interagissent quotidiennement et dans tous les secteurs de leurs activités – marketing, relations clients, relations avec les parties prenantes, données commerciales, données comptables et financières, données de recherche, données

d'exploitation, etc. Néanmoins, la création, la détention ou encore la manipulation de données exposent les entreprises à des risques et des menaces protéiformes.

Par ailleurs, la numérisation croissante des entreprises participe à la construction d'un horizon numérique global qui doit porter en son sein des valeurs de respect des droits humains et d'intérêt collectif. L'intelligence artificielle (IA), en ouvrant la voie à de nouveaux services et en augmentant les capacités productives des entreprises, s'est rapidement imposée comme une technologie stratégique. Elle permet de renforcer la compétitivité des entreprises et sa mise en œuvre peut avoir un impact sur le bien-être des citoyens et sur l'environnement.

Au regard de la prégnance du numérique sur leurs activités, la Plateforme RSE estime qu'il est fondamental pour les entreprises de s'assurer de l'utilisation éthique des processus et de la responsabilisation des acteurs de l'IA.

La gouvernance des données au sein de l'entreprise

La maîtrise des données par les entreprises constitue aujourd'hui un moteur de développement et d'innovation, et est une clé de leur stratégie. La gouvernance des données se révèle fondamentale pour la transformation numérique pérenne des entreprises. Elle permet de définir de manière efficace les politiques, fonctions et procédures nécessaires au traitement des informations de l'entreprise. Elle doit assurer une protection des données personnelles et opérationnelles efficace, et relève par plusieurs aspects de la RSE. Dans le cadre de la loi Pacte, la gouvernance est invitée à prendre en compte les enjeux éthiques liés aux données dans la définition de leur raison d'être et ce, particulièrement dans les entreprises dont le modèle d'affaires est guidé par les données (*data driven*).

La gouvernance des données est une décision collégiale, planifiée et mise en œuvre par les délégués à la protection des données (DPD), avec le support opérationnel de la Direction des systèmes d'information (DSI), et le support stratégique des organes de direction.

Le Conseil européen de la protection des données (CEPD, ex G29) recommande que le DPD soit associé en amont à toutes les questions relatives à la protection des données, et le RGPD dispose que le DPD fasse directement rapport au niveau le plus élevé de la Direction. Toutefois, force est de constater que dans la plupart des entreprises, la gouvernance des données reste perçue comme une question de conformité et non de responsabilité. Or le respect de la réglementation est la responsabilité minimale des organisations, et elle n'est pas suffisante pour répondre aux attentes du public en matière de responsabilité sociétale, pour gérer les risques ou pour répondre aux attentes des parties prenantes.

Il apparaît à la fois que malgré les effets bénéfiques de la réglementation, les entreprises, en particulier les TPE et les PME, ont encore du chemin à parcourir pour dépasser la conformité et la lier à leur engagement sociétal global.

L'amélioration de l'accès aux données peut maximiser leur utilité sociétale et économique, à condition que tous les acteurs concernés (responsables de traitement et sous-traitants) respectent les différents mécanismes qui encadrent le transfert des données : *Binding Corporate Rules*[1], clauses contractuelles types ou encore *Privacy Shield*[2].

Ainsi, pour réellement intégrer la responsabilité numérique au cœur de leur stratégie, certaines grandes entreprises mettent en place un Comité de protection des données. En impliquant une multitude de parties prenantes, celui-ci peut avoir pour rôle d'intégrer les enjeux éthiques dans la gouvernance des données. Par ailleurs, le volume et la complexité des problématiques éthiques auxquelles vont être confrontés les futurs développeurs rend nécessaire leur formation pour lutter contre les biais discriminants.

Les pratiques de protection des données

Les menaces sur la cybersécurité se multiplient : les entreprises sont de plus en plus exposées aux violations de leurs données. Une violation de la sécurité se caractérise par la destruction, la perte, l'altération, la divulgation non autorisée de données transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite. Face à cette menace, la responsabilité sociétale des entreprises se trouve accrue du fait du caractère personnel ou stratégique des données impactées.

Les organismes traitant des données doivent anticiper et mettre en place des processus : détection d'une violation, capacité à l'endiguer, à appréhender les risques engendrés, et déterminer qui notifie cette violation. Ils doivent mettre en place un registre de violation des données ; à titre d'exemple, l'anonymisation des données, bien que faillible, permet d'empêcher l'identification : elle sécurise donc l'exploitation des données à caractère personnel et respecte les droits des individus dont les données sont traitées.

De nombreuses entreprises disposent d'une politique de sécurité des systèmes d'information. Mais au sein des TPE/PME, le manque de moyens et, souvent, le défaut de compétences en interne rend complexe la mise en place de politiques efficientes. La Plateforme RSE a été attentive à leur besoin de soutien pour assurer un niveau de protection suffisant. Les TPE et PME doivent ainsi être attentives à la responsabilité numérique, essentielle dans les relations qu'elles construisent avec les clients et les consommateurs, notamment en tant qu'acteurs des chaînes de valeurs.

Dans un contexte de développement du recours à des prestataires externes pour stocker et gérer leurs données, les entreprises doivent veiller à en garder le contrôle.

La Plateforme RSE a passé en revue lors de ses auditions les modalités de gestion des données par les entreprises

De nombreuses entreprises recourent à un progiciel de gestion intégrée (PGI), qui permet de gérer l'ensemble des processus d'une entreprise en intégrant dans une base

[1] Règles d'entreprises contraignantes, cf. p 100.
[2] Bouclier de protection des données, cf. p 104.

de données unique l'ensemble de ses fonctions, dont la gestion des ressources humaines, la gestion comptable et financière, l'aide à la décision, mais aussi la vente, la distribution, l'approvisionnement et le commerce électronique. Cette centralisation facilite la conformité au RGPD. Des outils tels que l'« échange de données informatisées » permettent une standardisation des données et donc une meilleure interopérabilité. De telles solutions se révèlent néanmoins coûteuses et complexes, ce qui peut constituer un frein à leur implémentation dans les TPE et PME.

La sous-traitance de la gestion et du stockage des données se généralise et devient cruciale dans le développement de l'économie des données. Elle ouvre l'accès aux technologies futures et émergentes telles que l'IA, et contribue fortement à la compétitivité, à la conquête des marchés adjacents et au développement de nouveaux marchés. Sur ce sujet, la France accuse un retard par rapport aux autres pays de l'Union européenne.

Cependant, l'émergence de ce paradigme soulève deux enjeux majeurs : la perte de contrôle sur les données et une perte de contrôle sur la sécurité des données. Pour mettre en œuvre cette sous-traitance informatique, les entreprises ont de plus en plus recours à des outils de transfert de données vers de tierces parties, dans le cadre d'un contrat comportant des obligations vis-à-vis des données. Se pose ainsi la question de la délégation de responsabilités, spécifique à la RSE, qui s'applique entre une entreprise et son sous-traitant prestataire de services numériques – dont certaines obligations sont fixées par le RGPD et le *Privacy Shield*. L'éditeur de solutions numériques peut toutefois aller plus loin que le seul respect de la réglementation dans le traitement des données, en mettant en œuvre une démarche RSE fondée sur les meilleures pratiques.

Faire concilier outils de la RSE et enjeux numériques

Dans une démarche de conciliation de leurs effets, numérique et RSE peuvent enrichir les entreprises. La Responsabilité numérique des entreprises (RNE) engage la protection des données détenues par les acteurs économiques dans une perspective de protection des actifs de l'entreprise, de respect des droits, des libertés, de la vie privée mais également du bien-être des salariés, des consommateurs et des parties prenantes.

Dans un contexte d'évolution numérique constant, la protection des données et le respect des droits humains sont fondamentaux et constitutifs d'une démarche responsable des entreprises. La RSE offre des perspectives qui peuvent – et doivent – s'inscrire comme les vecteurs d'une responsabilisation accrue des entreprises dans leur appréhension du numérique.

Normes d'application volontaire, référentiels, outils d'autodiagnostic, chartes ou encore réseaux d'entreprises, tous ces outils sont autant de manières de faire concilier les enjeux numériques d'aujourd'hui et de demain avec les exigences sociétales et éthiques de la RSE.

Recommandations de la Plateforme RSE

La Plateforme RSE estime qu'il est nécessaire de renforcer la gestion des données détenues par les entreprises, que ce soit en matière de droits humains ou d'impact sur les modèles économiques. Elle encourage les nouveaux modèles dans le respect des cadres légaux.

À cet effet, la Plateforme RSE estime fondamental de former, dès le plus jeune âge, aux utilisations des nouvelles technologies et à leurs impacts potentiels sur la vie privée et les droits de manière générale. Les entreprises doivent s'inscrire dans une dynamique de formation aux enjeux numériques de toutes et tous – institutions publiques, dirigeants, salariés ou organisations syndicales – afin d'engager une responsabilité globale.

Partant du constat que les stratégies RSE et numérique restent éloignées dans la grande majorité des entreprises, la Plateforme RSE juge primordial d'adopter des stratégies communes et de se doter d'ambitions sociétales, sociales, environnementales et éthiques plus fortes et soutenables.

Elle affirme que le champ nouveau de la RSE est aussi d'ordre numérique, et que les textes européens à venir doivent en donner les perspectives et les cadres.

Considérant cet état des lieux, la Plateforme RSE recommande de rendre opérationnelle la définition de la Responsabilité numérique des entreprises (RNE) qu'elle propose, et formule des recommandations à l'attention des pouvoirs publics, des entreprises, des organisations syndicales, des chercheurs ainsi qu'aux acteurs de l'évaluation extra-financière afin d'engager la responsabilisation de toutes les entreprises sur les problématiques liées au numérique.

INTRODUCTION

Pour éduquer et enseigner, pour communiquer, pour faire reconnaître et défendre ses droits, pour travailler, pour se former ou bien pour se divertir, les outils numériques font partie du quotidien de la majorité des Françaises et des Français, qui se les sont appropriés en quelques années, aussi bien dans leur vie privée que professionnelle. Toutefois de profondes inégalités persistent, reflet des inégalités sociales, territoriales et générationnelles.

L'émergence de nouvelles possibilités technologiques – intelligence artificielle, objets connectés, *cloud*, *big data*, robotique, etc. – transforme le paysage dans lequel les entreprises évoluent. Le numérique représente aujourd'hui pour celles-ci à la fois un enjeu stratégique à maîtriser, de nouveaux risques à gérer et de nouvelles opportunités à explorer.

Si la transition numérique permet aux entreprises de développer leur activité à plus grande échelle, de faciliter les échanges, d'optimiser leurs activités tout au long de la chaîne de valeur et le travail de leurs salariés, de répondre au mieux aux attentes de leurs clients et actionnaires, de fournir des produits et services plus efficients, elle comporte aussi des risques, pour les entreprises et pour leurs parties prenantes.

De nombreux travaux parus ces dernières années sur cette thématique mettent en évidence, notamment, des enjeux liés à la gestion de ressources humaines, à l'éthique, au patrimoine numérique et à sa protection ou encore aux risques juridiques. Le numérique s'impose de plus en plus dans la définition du projet d'entreprise.

Face à la quantité de données que produit la transition numérique, les entreprises ont une responsabilité de maîtrise et de protection, notamment en matière de données personnelles. Il s'agit d'une obligation qui émane de la réglementation européenne, d'une obligation éthique ensuite, et d'une obligation sociétale. À ce titre, compte tenu des données dont les entreprises disposent et des possibilités ouvertes par le numérique, le respect des Objectifs de développement durable et la prise en considération des enjeux sociétaux constituent un autre volet de leur responsabilité. Cette responsabilité est

encadrée par la réglementation européenne, mais les entreprises doivent aussi assumer leurs responsabilités éthiques.

La responsabilité des entreprises dans leur exploitation des outils numériques se révèle multiple : responsabilité réglementaire, responsabilité éthique ou encore responsabilité sociétale et environnementale. Ainsi, partie intégrante de la responsabilité sociétale des entreprises (RSE), la responsabilité numérique soulève des enjeux de confiance, de redevabilité, de transparence, d'anticipation des impacts ou encore d'encadrement des pratiques.

Les acteurs de la (RSE) réunis au sein de la Plateforme RSE ont décidé, en 2018, d'inscrire les questions soulevées par la transition numérique à l'ordre du jour de leurs travaux. Ils ont constitué un groupe de travail[3] chargé de proposer un diagnostic et des recommandations relatives à la « Responsabilité numériques des entreprises ».

Plusieurs questions soulevées par la transition numérique des entreprises peuvent en effet être posées aux acteurs de la RSE. Trois thématiques distinctes ont ainsi été identifiées par la Plateforme RSE :

- la responsabilité des entreprises vis-à-vis de la production, des usages et de la protection des données collectées ou créées dans le cadre de leur activité ;
- la responsabilité des entreprises vis-à-vis des conditions de travail des salariés et des formes de travail non salarié, qui sont profondément transformées du fait de leur transition numérique ;
- la responsabilité des entreprises vis-à-vis de l'impact de leurs activités numériques sur l'environnement.

Compte tenu de l'étendue de chacune des trois questions soulevées, les membres de la Plateforme RSE ont décidé de les traiter successivement, dans le cadre d'avis distincts.[4]

[3] Cf. Composition du groupe de travail en annexe.
[4] Les membres de la Plateforme RSE ont pris le parti d'analyser la responsabilité des entreprises sous le prisme de la gestion des données auxquelles elles sont confrontées. Les problématiques liées à l'impact de la transformation numérique sur les formes de travail et l'environnement seront traitées ultérieurement. Cet avis est le premier d'un cycle dédié à la Responsabilité Numérique des Entreprises.

Responsabilité numérique des entreprises		
1. Les données	***2. Volet social***	***3. Volet environnemental***
A quels risques liés à l'utilisation des données sont exposées les entreprises ? Quelles données sont gérées, produites et valorisées par les entreprises ? Quel est le contexte juridique des entreprises face à l'exploitation des données ? Quelles sont les règles que l'entreprise respecte dans l'usage des données collectées auprès de ses parties-prenantes ? Quels sont les moyens dont disposent les entreprises pour valoriser la manière dont elles respectent ces règles, dans le cadre de leur politique RSE ?	Quel est l'impact de la transition numérique dans la vie interne de l'entreprise ? Quelle est la responsabilité de l'entreprise envers ses salariés face aux externalités négatives du développement des outils numériques ? Comment l'entreprise est-elle amenée à modifier sa gestion des ressources humaines dans un contexte de développement du numérique ? Que modifie le numérique dans la relation travailleurs / entreprise ? Quelles modifications du dialogue social à l'aune des transformations numériques ? Quel est l'impact de l'ubérisation de l'économique sur les relations avec les parties-prenantes de l'entreprise ? Comment les entreprises font-elles face à la fracture numérique ?	Comment les entreprises appréhendent-elles la transition numérique et les impacts de ces nouvelles activités sur l'environnement ? Comment les entreprises du secteur du numérique prennent-elles en compte les enjeux environnementaux croissants avec leurs pratiques ? Comment les entreprises publiques ou privés gèrent elles les données d'ans l'intérêt général (bien(s) commun(s)) et la protection du patrimoine environnemental

Le présent avis porte ainsi sur la thématique de la collecte, des utilisations et de la maîtrise des données produites et/ou collectées par les entreprises dans le cadre de leurs activités. Partant du constat que les textes juridiques relatifs au numérique ne font pas le lien avec les problématiques de la responsabilité sociétale des entreprises – et inversement –, la Plateforme RSE questionne le rôle des entreprises au regard de la gestion des données, notamment les données dites « personnelles », auxquelles elles sont confrontées. Aujourd'hui omniprésentes, les données deviennent des éléments stratégiques indispensables au fonctionnement des entreprises. La collecte de données par les entreprises est facilitée par la multiplication des outils – statistiques de consultation, données de caisse, objets connectés, données de géolocalisation, etc. – qui produisent des données sur les comportements de leurs parties prenantes, données que les entreprises utilisent ou valorisent. De même la création de données par les entreprises est facilitée par la numérisation de l'ensemble des processus de recherche,

de gestion de production, de gestion commercial et d'après-vente mis en œuvre par les entreprises.

Dans le contexte actuel de développement du volume des données, l'enjeu de l'éthique autour de l'utilisation de ces données est un volet important de leurs responsabilités numériques. Le questionnement sur l'éthique conduit à s'interroger sur les notions de protection des actifs de l'entreprise, de la vie privée, de surveillance, d'anonymat ou encore d'algorithmes.

La groupe de travail (GT) de la Plateforme RSE a, dans le cadre du présent avis, interrogé un certain nombre d'entreprises et d'acteurs afin de déterminer leur rôle et leurs objectifs au regard des données qu'ils collectent et produisent dans un contexte de transformation numérique en perpétuelle évolution. Dans le présent avis, le GT a établi une analyse du contexte réglementaire propre à la gestion des données ainsi qu'un état des lieux des grands enjeux auxquels sont confrontées les entreprises. Puis, s'appuyant sur l'étude des documents de référence des entreprises du CAC 40 et sur une série d'entretiens et d'auditions avec des acteurs du monde du numérique, le groupe de travail a analysé les pratiques des entreprises en matière de gestion des données en identifiant notamment les bonnes pratiques. Enfin, dans le contexte de la crise sanitaire liée à la Covid-19 intervenue en 2020, la Plateforme RSE a souhaité compléter ce diagnostic par une revue de la contribution de l'usage du numérique par les entreprises à la gestion de cette crise, et de son impact en matière de libertés publiques et de droits fondamentaux.

Pour établir ce diagnostic et formuler des recommandations, la Plateforme RSE a mené, de novembre 2019 à juin 2020, dix-huit auditions. Elle a rencontré des experts, praticiens et académiques, des entreprises et des acteurs de la société civile. Le présent avis représente la position partagée par l'ensemble des acteurs de la RSE réunis au sein de la Plateforme RSE. Il a été adopté en assemblée plénière le 6 juillet 2020.

I. CONTEXTE ET ENJEUX

1. Entreprises et numérique : de quoi parle-t-on ?

Histoire des données

Si les données sont devenues des éléments majeurs de l'économie seulement depuis une vingtaine d'années, leur collecte et leur stockage ne sont pas des problématiques nouvelles. Les transformations numériques majeures intervenues ces dernières années ont fait exploser la quantité de données produites et stockées et rendu plus aigus les enjeux liés à leur stockage et traitement.

C'est en 1884 que les premières données sont produites grâce à l'invention de la « tabulatrice à cartes perforées » d'Herman Hollerith afin de recenser la population américaine plus rapidement, faisant baisser de sept années la vitesse de recensement (de dix ans initialement à trois ans). Cette machine est à l'origine de la fondation de la Tabulating Machine Company, qui deviendra IBM en 1917.

En 1928, la cartouche magnétique, inventée par Fritz Pfleumer permettra de stocker davantage les données des entreprises. Une fois pleines, les cartouches étaient entreposées matériellement dans les locaux des entreprises.

En 1956 est créé le premier disque dur par IBM – l'IBM 350 Disk File –, conçu pour fonctionner avec l'ordinateur central IBM 305 RAMAC. Cette invention a permis aux entreprises de stocker leurs données en temps réel, et d'accéder aux données produites par l'impression de cartes perforées.

La véritable transformation se tiendra dans les années 1960 au travers de la massification de l'information. À cette période, les entreprises commencent à se doter de systèmes informatiques centralisés qui optimisent, notamment, leurs inventaires ou pour les banques, la tenue des comptes clients.

Dans les années 1970, sont conçus les premiers systèmes de planification des besoins en matériel pour aider les entreprises manufacturières à planifier et organiser leurs données.

Parallèlement, se développe une réflexion sur la gestion du traitement automatisé des systèmes d'information en Europe comme aux États-Unis. En France, c'est un article du journal *Le Monde* daté du 21 mars 1974, « SAFARI ou la chance aux Français », qui tire la sonnette d'alarme et positionne le débat sur la place publique. Le projet SAFARI (Système automatisé pour les fichiers administratifs et le répertoire des individus) entendait créer une base de données centralisée de la population française. Face au problème de société engendré par ce projet, le Premier ministre de l'époque, Pierre Messmer, le retire et crée une commission « Informatique et libertés ». La commission sortira un rapport en 1975 qui fondera la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Dans l'objectif de faire de l'informatique un outil au « service de chaque citoyen », la Commission nationale de l'information et des libertés (CNIL) est instituée. Elle constitue ainsi la première autorité administrative indépendante créée en France[5]. Par la suite, des autorités indépendantes de protection des données nationales verront le jour dans l'Union européenne et se regrouperont dans le réseau européen G29 (aujourd'hui : Conseil européen de la Protection des Données) institué par l'article 29 de la directive du 24 octobre 1995 sur la protection des données et la libre circulation.

La fin des années 1990 voit se profiler la systématisation des systèmes informatiques et logiciels dans les entreprises. Ces systèmes intègrent les domaines de la fabrication, la distribution, la finance, les ressources humaines ou encore la gestion des stocks.

Les données explosent avec le succès du World Wide Web. Avec ensuite le succès des réseaux sociaux et du « Web 2.0 », c'est l'avènement des données massives, dites *big data*, qui ouvre de nouvelles possibilités d'analyse basées sur l'intelligence artificielle.

Histoire de l'intelligence artificielle (IA)

L'intelligence artificielle est une science plus ancienne qu'il n'y paraît et qui a connu des développements majeurs au cours des dernières années.

En 1949, Warren Weaver se penche sur la traduction automatique des langues et émet l'idée qu'une machine pourrait effectuer une tâche qui relève originellement de l'intelligence humaine.

En 1950, le mathématicien Alan Turing publie un article « Computing Machinery and Intelligence » dans lequel il explore les problématiques de définition si une machine est consciente ou non. De cet article a découlé le « test de Turing », fondé sur la faculté d'une machine à imiter une conversation humaine.

Ce n'est pourtant qu'à l'été 1956 que l'intelligence artificielle est officiellement reconnue comme un véritable domaine scientifique, lors d'une conférence tenue au Dartmouth College. À la suite de cette conférence, certains participants se sont investis dans des

[5] Création de la Commission nationale de l'informatique et des libertés (CNIL), site du gouvernement (ici)

recherches sur l'intelligence artificielle. Ces programmes s'implanteront par la suite dans de prestigieuses universités comme Stanford, le Massachusetts Institute of Technology (MIT) ou encore Edimbourg.

Dans les années 1960, la recherche américaine était majoritairement financée par le ministère de la Défense, et des laboratoires s'ouvraient au niveau international. Néanmoins, les prédictions utopiques des chercheurs et l'échec de trop nombreux projets entraînent une réduction des fonds britanniques et américains sur la recherche en IA.

Les projets seront massivement relancés dans les années 80 avec le succès des systèmes experts – ordinateurs capables de se comporter dans un domaine précis comme un expert humain –, qui ont fait augmenter la valeur de marché de l'IA à un milliard de dollars.

Dans les années 1990 et 2000, la loi dite de Moore[6] permet d'anticiper le développement exponentiel des performances informatiques et l'exploitation de l'IA dans davantage de domaines.

En 1997, l'IA atteindra une reconnaissance mondiale lorsque « Deep Blue » créé par IBM battra Garry Kasparov, champion du monde d'échecs. Cette expérience sera renouvelée avec « Waston » d'IBM qui vaincra en direct les deux plus grands champions de « *Jeopardy* ».

Les années 2000 marquent ainsi un tournant. L'IA s'intègre davantage dans la société : les ordinateurs personnels deviennent accessibles, Internet se déploie sur les territoires, les *smartphone* émergent, etc. La question de l'éthique commence également à être posée par des chercheurs du monde entier – en 2007, la Corée du Sud dévoile une charte de l'éthique des robots et, en 2009, le MIT réunit des scientifiques afin d'élaborer les contours de la recherche dans le domaine.

Les années 2010 sont marquées par la médiatisation accrue des recherches relatives à l'IA. Les chercheurs développeront les concepts de « *machine learning* » et de « *deep learning* », qui lient l'IA aux données massives récoltées.

Aujourd'hui, les études sur le numérique à l'aune des enjeux sociétaux actuels fleurissent dans les institutions et les organisations spécialisées. Le numérique et, plus récemment, l'émergence de l'intelligence artificielle constituent des sujets au cœur de la société.

France Stratégie dispose d'une commission dédiée aux enjeux numériques et publie régulièrement des études faisant état des problématiques sociétales qu'ils impliquent :

[6] Loi empirique issue des constatations de Gordon E. Moore en 1965, qui évalue la puissance de calcul des ordinateurs et la complexité du matériel informatique. La loi affirme qu'à coût égal, la complexité des microprocesseurs doublait tous les deux ans. En 1975, il prédit que la croissance allait se poursuivre à ce rythme jusqu'en 2015.

Mutations digitales et dialogue social[7] en novembre 2017, *Les bénéfices d'une meilleure autonomie numérique*[8] en juillet 2018, *Les enjeux des blockchains*[9] en juin 2018, ou encore *Intelligence artificielle et travail*[10] en mars 2018. L'institution organise également de multiples conférences sur le sujet.

Les parlementaires interrogent également les transformations numériques à l'aune des textes législatifs en vigueur. Les Commissions des Lois et des Affaires économiques de l'Assemblée Nationale lancent une mission d'information commune à la Commission des Lois et à la Commission des Affaires économiques sur l'identité numérique, en novembre 2019, afin d'interroger les interactions entre pouvoirs publics et secteur privé et les moyens techniques mis en œuvre[11]. Dans le même temps, des groupes d'études réunissent les députés autour d'enjeux numériques actuels : la « cybersécurité et souveraineté numérique »[12] ou encore « internet et société numérique »[13]. Au Sénat, la Commission de l'aménagement du territoire et du développement durable a retenu, dans son programme pour l'année 2020, la création d'une mission d'information relative à l'empreinte environnementale du numérique afin d'évaluer les impacts environnementaux du digital en France et formuler des pistes d'actions pour les politiques publiques[14]. Des colloques réunissent également experts et parlementaires autour des enjeux territoriaux à l'image de la couverture numérique des territoires, et d'enjeux humains tels que les droits et la démocratie à l'ère numérique. Plus récemment, un rapport sur le devoir de souveraineté numérique a été publié dans le cadre d'une commission d'enquête[15]. Au Conseil économique, social et environnemental, ce sont les nouveaux rapports entre l'industrie et les services[16], les données numériques comme enjeu d'éducation et de citoyenneté[17] ou une politique de souveraineté européenne du numérique[18] qui sont évalués.

[7] À retrouver ici : https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/ns-fs-mutations-digitales-10-novembre-2017.pdf
[8] France Stratégie (2018), *Les bénéfices d'une meilleure autonomie numérique,* Antoine Baena et Chakir Rachiq
[9] À retrouver ici : https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-rapport-blockchain-21-juin-2018.pdf
[10] À retrouver ici : https://www.strategie.gouv.fr/sites/strategie.gouv.fr/files/atoms/files/fs-rapport-intelligence-artificielle-28-mars-2018_0.pdf
[11] À retrouver ici : http://www2.assemblee-nationale.fr/15/missions-d-information/missions-d-information-communes/identite-numerique/(block)/67684
[12] À retrouver ici : http://www2.assemblee-nationale.fr/instances/resume/OMC_PO746763/legislature/15
[13] À retrouver ici : http://www2.assemblee-nationale.fr/instances/resume/OMC_PO747007/legislature/15
[14] À suivre ici : http://www.senat.fr/commission/dvpt_durable/mission_dinformation_sur_lempreinte_environnementale_du_numerique.html
[15] À retrouver ici : http://www.senat.fr/rap/r19-007-1/r19-007-11.pdf
[16] Kotlicki M. (2015), *Les nouveaux rapports industrie/services à l'ère du numérique*, avis du CESE.
[17] Peres E. (2015), *Les données numériques : un enjeu d'éducation et de citoyenneté*, avis du CESE.
[18] Thieulin B. (2019), *Pour une politique de souveraineté européenne du numérique*, avis du CESE.

1. Définitions

Algorithme : Un algorithme définit une série d'instructions et opérations réalisées sur des données afin d'exploiter un système ; c'est-à-dire de produire un résultat ou résoudre un problème.

Anonymisation : L'anonymisation désigne un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, l'identification de la personne par quelque moyen que ce soit et de manière irréversible. Si l'anonymisation est effective, le RGPD ne s'applique pas aux données en question.

Base de données : Une base de données est définie par le Code de la propriété intellectuelle comme un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen. Elle est protégée par le droit d'auteur et le droit des producteurs de base de données. Celui-ci, formalisé au milieu des années 90 suite au développement du commerce électronique et des premières technologies de traitement des données, est issu de la directive communautaire du 11 mars 1996 et transposé dans le droit de la propriété intellectuelle français par la loi du 1er juillet 1998.

Big data : Souvent traduit comme « données massives », le *big data* s'est développé suite à la massification des nouvelles technologies, d'internet et des réseaux sociaux. Il répond, selon la CNIL, a trois caractéristiques principales : volume, vélocité, variété.

Le volume de données produites combiné aux capacités grandissantes de stockage et aux outils d'analyse en temps réel de plus en plus sophistiqués offrent, ainsi, des possibilités d'exploitation de l'information infinies.

Blockchain : Selon Blockchain France, la blockchain est une « technologie de stockage et de transmission d'informations transparente, sécurisée, et fonctionnant sans organe central de contrôle »[19] ; c'est une base de données contenant l'historique de tous les échanges effectués entre ses utilisateurs, depuis sa création. Cette base de données est sécurisée et partagée entre les utilisateurs, sans intermédiaire, afin que chacun puisse vérifier sa validité.

Cloud computing : Le *cloud computing* est un modèle qui permet un accès réseau omniprésent, pratique et à la demande à un ensemble partagé de ressources informatiques configurables (par exemple, réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement mobilisées avec un minimum d'efforts de gestion ou d'interaction avec les fournisseurs de services. [20]

[19] « Qu'est-ce que la blockchain ? », Blockchain France https://blockchainfrance.net/decouvrir-la-blockchain/c-est-quoi-la-blockchain/
[20] National Institute of Standards and Technology

Cybers**écurité** : L'ANSSI[21] désigne la cybersécurité comme un « état recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace, susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent »

Cycle de vie de la donnée : On identifie six phases dans le cycle de vie de la donnée : l'acquisition et la production ; le traitement ; l'analyse, l'informatique décisionnelle et l'IA ; l'accès, la sécurisation, l'intégrité et la confidentialité, la conservation, l'archivage et/ou l'effacement ; la réutilisation, la libération et les processus d'*open data*[22].

Données : En informatique, la donnée désigne la représentation d'une information dans un programme ; les données peuvent être créées ou récoltées par son détenteur.

Les différentes auditions menées dans le cadre de cet avis mènent à la définition de plusieurs types de données :

- Les données enrichies qui sont des données personnelles ayant subi une classification ;
- Les données statistiques et analytiques qui sont des données récoltées permettant d'établir des classements en fonction des habitudes des utilisateurs et d'influer les pratiques d'entreprises ;
- Les données horodatées qui sont un ensemble de données ordonnancées définissant la séquence selon laquelle chaque point de données a été capturée ou collectée. Ce type de données est utilisé lors de la collecte de données comportementales – actions de l'utilisateur sur un site web – elles permettent de prévoir le parcours d'un utilisateur ;
- Les données spatiotemporelles qui décrivent le lieu et l'heure d'un événement, des emplacements ponctuels ou des trajectoires complexes comme celles des véhicules ; elles comportent le temps valide et le temps de transaction ;
- Les données ouvertes (*open data*) qui sont des données ouvertes et mises à disposition par les entreprises et collectées dans un objectif de bien commun et de contribution à l'intérêt général. L'article 17 de la Loi du 7 octobre 2016 pour une République Numérique a imposé l'ouverture des données des entreprises exerçant une délégation de service public ;
- Les données relatives au fonctionnement de l'entreprises à l'image des données de recherche, des données marketing, des données comptables et financières, des données de production et d'observation ou encore des données de vente et d'après vente.

Par ailleurs, la protection des données détenues par les entreprises est régie par la loi n°2018-670 du 30 juillet 2018 sur le secret des affaires, notamment au regard de la

[21] Glossaire, ANSSI
[22] FNCCR (2019) *Etude sur le cycle de la donnée dans la conception et la mise en œuvre des services et usages numériques des collectivités territoriales*

protection de la sphère privée des entreprises, c'est-à-dire des connaissances stratégiques ou des informations sensibles.

Le terme anglo-saxon *data* peut également être utilisé pour mentionner les données.

Données à caractère personnel : Pour la CNIL, « toute information se rapportant à une personne physique identifiée ou identifiable » est une donnée à caractère personnel. Une personne physique identifiable est « une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. »[23]

La CNIL distingue trois types de données à caractère personnel :

- Données à caractère personnel courantes : état-civil, données d'identification, situation familiale, CV, situation financière, données GPS, etc.
- Données à caractère personnel perçues comme sensibles : numéro de sécurité sociale, données biométriques, données bancaires, etc.
- Données à caractère personnel sensibles au sens de la Loi Informatique et Libertés : opinions philosophiques, politiques, religieuses, origines raciales ou ethniques, vie sexuelle, données de santé, condamnations, etc ;
- Données et informations produites par l'entreprise : mesures et inventaires écologiques, consommations énergétiques, déplacements, etc.

Ces données dites sensibles, forment une catégorie particulière de données personnelles[24]. Les données sont des informations qui révèlent *« la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophique ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique »*. Les données de santé ou concernant la vie sexuelle et l'orientation sexuelle d'une personne entrent également dans ce champ.

Il existe, selon la CNIL, sept grands principes de la protection des données à caractère personnel :

- Limitation des finalités ;
- Minimisation des données ;
- Licéité, loyauté, transparence ;
- Exactitude ;
- Limitation de la conservation ;
- Intégrité et confidentialité ;
- Respect des droits des personnes : information, consentement, rectification, accès et portabilité.

[23] Audition de Mme Sophie Nerbonne, direction de la co-régulation économique de la CNIL
[24] Données sensibles, CNIL

Données d'intérêt général : La Plateforme RSE se réfère à la notion de données d'intérêt général introduite par la Loi pour une République numérique (Loi n°2016-1321 du 7 octobre 2016, article 17). Les données d'intérêt général sont des données de nature privée qui bénéficient d'une ouverture à tous en raison de leur intérêt à l'amélioration des politiques publiques.

Le groupe de travail a souvent évoqué, comme ce fut le cas lors des discussions autour de la Loi pour une République Numérique, une définition souhaitable de « données de bien commun », mais a repoussé cette définition, et éventuelle recommandation, à la fin de ses travaux, afin de la confronter aux problématiques environnementales.

Économie de la donnée : L'économie de la donnée se définit comme un univers d'initiatives, d'activités et/ou de projets dont le modèle économique est basé sur l'exploration et l'exploitation des structures des bases de données pour identifier les possibilités de générer des produits et des services.

Fracture num**érique** : La fracture numérique décrit les inégalités humaines et territoriales dans l'accès aux technologies de l'information et de la communication (TIC), à leur utilisation et à leur impact. Deux niveaux de fracture peuvent être délimités : l'accès (fracture de premier degré) et l'usage (fracture de second degré).

Intelligence artificielle (IA) : L'IA désigne la mise en œuvre de techniques visant à permettre aux machines d'imiter une forme d'intelligence réelle. La notion voit le jour dans les années 1950 grâce au mathématicien Alan Turing. Dans son livre *Computing Machinery and Intelligence*, il décrit le « Test de Turing » dans lequel un sujet interagit à l'aveugle avec un autre humain puis avec une machine programmée pour formuler des réponses sensées : si le sujet ne fait pas la différence, la machine a réussi le test et peut être considérée comme intelligente[25]. L'IA réunit des sciences théoriques et techniques afin de parvenir à « faire imiter par une machine les capacités cognitives d'un être humain. »[26]

Internet des objets (IdO) *Internet of Things* ***(IoT)*)** : Selon l'Union Internationale des Télécommunications[27], l'IdO est une « infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution. »

D'un point de vue conceptuel, l'IdO caractérise des objets physiques connectés avec une identité numérique propre et capables de communiquer les uns avec les autres. D'un point de vue technique, l'IdO consiste en l'identification numérique directe et normalisée (adresse IP, protocoles smtp, http…) d'un objet physique grâce à un système de communication sans fil.

[25] FuturaTech « Intelligence artificielle » https://www.futura-sciences.com/tech/definitions/informatique-intelligence-artificielle-555/
[26] Conseil de l'Europe « L'IA, c'est quoi ? » https://www.coe.int/fr/web/artificial-intelligence/what-is-ai
[27] Arcep (2019), « L'internet des objets », Grand dossier, mis à jour le 10 avril 2019

Les objets connectés créent ainsi de nouveaux usages et de nouveaux services dans tous les secteurs – déplacements, vie quotidienne, logement, soins – et leur déploiement constitue un nouvel enjeu pour l'aménagement numérique des territoires.

Interopérabilité des données : L'interopérabilité des données est rendue possible par des systèmes capables de s'adapter et collaborer avec d'autres systèmes indépendants, compatibilité facilitant le transfert de données provenant de systèmes différents.

Principe de sandbox (bac à sable) : Le principe de *sandbox* est un mécanisme de sécurité informatique prévoyant l'isolation de logiciels par rapport au système d'exploitation hôte. Ce principe est notamment utilisé pour permettre l'exécution d'un code non testé pouvant potentiellement impacter le système. La *sandbox* est également utilisée pour faire référence à un environnement de test pour logiciels ou sites web.

En France, la Loi n°2016-1321 pour une République numérique permet à l'ARCEP d'expérimenter les *sandbox* règlementaires sur une durée maximale de deux ans dans le domaine des communications électroniques[28].

Pseudonymisation : La pseudonymisation est un traitement qui consiste à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans avoir recours à des informations supplémentaires. Elle permet de remplacer les données directement identifiables par un jeu de données indirectement identifiables.

Responsabilité numérique des entreprises (RNE) : Tout au long de ce rapport, les membres de la Plateforme RSE se sont efforcés à définir ce que représente la RNE. À l'aune des recherches, analyses et auditions menées, la Plateforme RSE définit la RNE comme un déploiement nouveau et incontournable de la RSE, qui se fonde sur les mêmes principes de confiance, de redevabilité, d'éthique et d'échanges avec les parties prenantes des entreprises. La transversalité et l'omniprésence du numérique impliquent que la création de valeur qu'elle engendre soit comprise et partagée par tous, au regard de ses enjeux démocratiques, sociaux, sociétaux et environnementaux. Les enjeux auxquels doit répondre une entreprise responsable seront explicités à la fin de ce rapport.

Small data : Le concept de *small data* désigne des quantités de données limitées, faciles à stocker et à utiliser (les PME et TPE peuvent facilement les stocker et les réutiliser). Définies comme plus humaines, les *small data* permettent de personnaliser et d'améliorer les relations avec les parties prenantes en utilisant les propres données de l'entreprise ; le traitement des données n'étant pas effectué par une machine comme pour les *big data*.

Tracing : Le *tracing* ou traçage est un dispotif qui a pour objectif d'identifier, par des moyens numériques, les activités des individus et leur contact potentiels avec d'autres

[28] CNIL (2020), Rapport d'activité « Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles »

individus. Développé par dans cadre de la crise sanitaire de la Covid-19, le contact tracing a porté de nombreux débats[29].

Tracking : Le tracking est une stratégiecommunicationnelle et marketing visant, pour les prestataires de services informatiques, à repérer les potentiels clients et à cibler leurs attentes.

Traitement de données personnelles : Le traitement des données personnelles désigne les opérations portant sur des données personnelles, quel que soit le procédé utilisé : collecte, enregistrement, conservation, extraction, diffusion, rapprochement. L'opération a pour objectif de recueillir les données et de les exploiter.

Transformation numérique : La transformation numérique – ou digitale – désigne un processus qui consiste, pour une entreprise ou une organisation, à intégrer les technologies numériques dans ses activités.

Transition numérique : La transition numérique est née de l'intégration des technologies digitales dans les processus de l'entreprise, et de la transformation de toutes les composantes de l'entreprise (processus, métiers, culture, organisation, etc.) sous l'influence des TIC.

Elle se compose de plusieurs éléments : la digitalisation, l'automatisation des processus, les outils de travail collaboratifs, la massification des applications mobiles, l'analyse des données, les *chatbots*[30], les objets connectés, la densification des sites web et de leurs possibilités et l'ouverture des possibilités de la *blockchain.*

2. Chiffres clés

Le volume des données produites

Les chiffres disponibles autour de la production de données au cours des dernières années représentent un marqueur fort de la croissance des nouvelles technologies et de la transformation numérique opérée au sein de nos sociétés. Ainsi, l'analyse et la gestion de volumes de données sont aujourd'hui une préoccupation majeure pour de nombreuses entreprises.

Le volume de données crées quotidiennement est de 2,5 quintillons[31], ce sont ainsi 50 000 Go de données qui sont créés chaque seconde[32] et plus précisément, 1,7 Mo produites par personne chaque seconde[33]. Néanmoins, 88 % des données disponibles ne sont pas analysées[34].

[29] Cf p 57
[30] Robot logiciel capable de dialoguer avec un individu.
[31] https://www.markentive.com/fr/blog/infographie-chiffres-cles-big-data
[32] https://www.engie-cofely.fr/dossiers-thematiques/histoire-data/
[33] Chiffres Big Data, Le Big Data, janvier 2018
[34]https://www.engie-cofely.fr/dossiers-thematiques/histoire-data/

Les données personnelles représentent 75 % des données produites[35] et constituent une valeur fondamentale pour les entreprises ; à ce titre, certaines entreprises ont créé des alliances afin de récolter davantage de données.

Le poids des données

Le poids estimé du marché mondial du *big data* en 2020 est de 203 milliards de dollars[36].

Les entreprises tendent à s'inscrire dans une démarche vertueuse dans l'utilisation de leurs données, poussées par toutes les parties prenantes. Une étude d'Accenture a montré que 77 % des entreprises s'accordent pour affirmer que la responsabilité en termes d'utilisation des données est un élément stratégique de leur modèle économique[37] .

Considérant que 54 % des individus sont davantage attirés par les marques et entreprises transparentes sur leur gestion des données et que 48 % d'entre eux estiment qu'ils seraient plus à même de consommer auprès de ces entreprises[38], la gestion éthique des données s'implante comme un argument majeur de la stratégie de l'entreprise.

La maturité numérique des entreprises du CAC 40[39]

Chaque année, les *Echos executives* et Gilles Babinet, Digital Champion de la France auprès de la Commission européenne réalisent un classement évaluant la maturité numérique des entreprises du CAC 40.

Alors que les secteurs de la banque et des assurances faisaient partie du haut du classement, en 2019 le secteur industriel tend à s'aligner – à la suite d'un investissement sur la transformation interne plutôt que sur l'image externe. Ainsi, en 2019, Air Liquide prend la première place qu'occupait la Société Générale depuis plusieurs années. Le PDG de ce distributeur de gaz affirme, en ce sens, que le digital constitue un accélérateur et un levier permettant d'aller en profondeur et de concrétiser des projets ; par ailleurs, cette réussite passe par une gouvernance en réseau ainsi que l'entrée dans les métiers d'Air Liquide de l'intelligence artificielle, des algorithmes et de l'IdO.

Orange occupe la seconde place, à la suite de la réorganisation du management et de l'appropriation effective des technologies digitales. Le groupe Accor, qui se tenait au 21ème rang en 2018, obtient la cinquième place en 2019 grâce à une culture managériale revue et une stratégie digitale intégrée à la gouvernance.

[35] https://www.accenture.com/us-en/insight-outlook-doing-well-doing-good
[36] Cabinet IDC, 2016
[37] https://www.accenture.com/us-en/insight-outlook-doing-well-doing-good
[38] https://www.accenture.com/us-en/insight-outlook-doing-well-doing-good
[39] Datiche N. (2019), « Classement eCAC40 2019 : et les champions du numérique sont… », LesEchos.fr

De manière générale, l'étude témoigne d'une prise de conscience de l'urgence numérique, de la nécessité de transformer les organisations et d'engager des changements dans les modes de gouvernance.

L'IA en France

Le Cabinet IDC[40] identifie trois secteurs consommant le plus d'intelligence artificielle en 2017 : le commerce de détail (27 %), l'industrie (14 %) et le secteur bancaire 13 %). Aujourd'hui, la tendance se poursuit vers les secteurs de la santé et des télécommunications.

L'étude distingue cinq raisons poussant les entreprises à investir dans des logiciels d'intelligence artificielle :

- La réduction des coûts par une amélioration de la productivité et de l'efficacité (74 % des répondants)
- L'accroissement de la qualité des produits et des services (72 % des répondants)
- L'amélioration du support clients (68 % des répondants)
- L'amélioration de l'efficacité des systèmes IT (68 % des répondants)
- L'amélioration des opérations de marketing via la connaissance des clients et leur ciblage (58 % des répondants)

Le rapport Villani[41]éclaire le fait que la France compte parmi les 4 premiers pays au monde pour la production mondiale d'articles sur l'intelligence artificielle, avec la Chine, les États-Unis et le Royaume Uni. Avec 81 écoles d'ingénieurs, 38 universités délivrant 138 cours dédiés à l'IA et 18 diplômes de mastères spécialisés en IA, la France connaît une augmentation des cursus dédiés préparant les futurs ingénieurs du numérique. La France dispose ainsi de 268 équipes de recherche dédiées comprenant 5 300 chercheurs dédiés à l'IA ; les financements publics pour la recherche en IA s'élèvent à 400 millions d'euros par an.

Un accès inégal aux données

L'économie européenne n'est digitalisée qu'à 12 %, contre 18 % pour les États-Unis[42]. Il existe de grandes disparités entre les États-membres mais également entre les secteurs et les entreprises nationales.

Les profondes transformations en cours et à venir ainsi que les réorientations des enjeux de l'entreprise constituent des opportunités à saisir. Les secteurs les moins digitalisés – agriculture, construction, immobilier – pourraient ainsi connaître des changements conséquents.

[40] https://idc.fr/infographies/index/lia_en_france_tendances_et_chiffres_cles
[41] Villani C. (2018), *Donner un sens à l'intelligence artificielle, pour une stratégie nationale et européenne*, rapport au Premier ministre
[42] Source : https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-europe-realizing-the-continents-potential

Données et développement territorial

Les dispositifs du Code des relations entre le public et l'administration imposent certaines obligations de publication en ligne des documents administratifs aux collectivités Depuis le 7 octobre 2018, les collectivités territoriales de plus de 3500 habitants et employant plus de 50 agents sont tenues de mettre en ligne[43] :

- Les documents qu'elles communiquent en application des procédures prévues par le Code des relations entre le public et l'administration ;
- Les documents qui figurent dans le répertoire des bases informations publiques (RIP) ;
- Les bases de données, mises à jour régulièrement, qu'elles produisent ou qu'elles reçoivent et qui ne font pas l'objet d'une diffusion publique par ailleurs ;
- Les données, mises à jour régulièrement, dont la publication présente un intérêt économique, social, sanitaire ou environnemental ;
- Les règles définissant les principaux traitements algorithmiques utilisés dans l'accomplissement de leurs missions, lorsque ces traitements fondent des décisions individuelles.

Les données constituent aujourd'hui un levier de la transformation numérique des entreprises mais également un enjeu de création de valeur. Au niveau territorial, les usages numériques constituent des enjeux conséquents, notamment dans le cadre du développement de nouveaux bassins de vie. Les plateformes de données mutualisées permettent, par exemple, d'accélérer les regroupements de moyens.

Les collectivités appréhendent de manière progressive l'ère du digital[44], elles sont elles aussi concernées par la massification des données produites chaque jour. Selon le niveau de collectivité sur lequel on se positionne, de multiples données peuvent en effet être produites et/ou collectées : démographie, climat, consommation énergétique, utilisation des transports, fréquentation des lieux publics, commande publique, etc[45].

À titre d'exemple, l'entreprise Atos a structuré sa stratégie de développement auprès des collectivités autour des plateformes de données mutualisées. L'objectif est ainsi d'organiser le choix, la récupération et le traitement des données produites via diverses sources. Le directeur du Marché Collectivités Territoriales d'Atos, explique que les données sont *« choisies par rapport à un besoin stratégique »* – comme le choix d'un emplacement pour une zone commerciale ou bien la sensibilisation d'un public choisi sur sa consommation énergétique – puis organisées pour produire une information. Pour Atos, l'objectif d'un tel processus est de parvenir à la formation d'un service à destination des collectivités mais également des associations, des entreprises ou des citoyens. Se développe ici une « nouvelle manière d'aborder la performance du service public », au travers de pratiques en lien avec les usages numériques des acteurs locaux. Il considère ainsi que les plateformes de données *« apparaissent comme une véritable opportunité*

[43] CNIL
[44] Mon mandat Local (2019), « De la donnée mutualisée aux services : des plateformes de confiance pour le développement du territoire »
[45] Idem

de renforcer la coopération, de préparer conjointement l'avenir et d'envisager une utilisation de la donnée plus transverse et à plus grande échelle. »

Cependant, mettre en place de tels services nécessite que les collectivités s'adaptent aux transformations numériques – à l'heure où nombre d'entre elles sont encore à la marge. À ce propos, Marie-Hélène Thoraval, maire de Romans-sur-Isère et vice-présidente Attractivité de Valence Romans Agglo estime que *« les communes ne pourraient pas obtenir des informations venant des données seules, c'est en mutualisant que l'efficience voit aussi le jour dans nos territoires. Grâce au numérique, nous devons développer une approche process dans nos communes pour que le service public soit plus efficace. »*

Au niveau des territoires, les enjeux des données et de la plateformisation de la société peuvent, ainsi, être envisagés sous de multiples dimensions[46] :

- Le développement de nouveaux services pour la population. Dans un contexte de « désertification des territoires ruraux », la plateformisation pourrait permettre la mise en commun de ressources de santé et d'éducation ainsi qu'un meilleur usage des données publiques ;
- Le développement d'activités nouvelles, par création ou relocalisation. La mise en place de nouveaux champs d'activités sur les territoires peut résulter du développement de nouveaux services et de processus de relocalisation d'activités induits par l'attractivité des territoires et l'amélioration des infrastructures numériques ;
- La mise en grappes d'activités existantes. La mise en relation d'activités constitue, de facto, une caractéristique aujourd'hui fondamentale du numérique ;
- La facilitation des processus de socialisation au travers de nouveaux circuits économiques. Dans un contexte local, de circuits courts, le développement des plateformes peut contribuer à la facilitation des processus de partage de biens et services ;
- La facilitation d'articulation entre les activités locales et les activités des entreprises mondiales. La « plateformisation » permet de mettre en relation les activités intensives en connaissances et peut également permettre la valorisation de marques locales et de savoir-faire locaux.

La Chaire européenne de l'immatériel[47] estime que l'innovation numérique au niveau territorial est importante. À ce titre, la « plateformisation » *« appelle à innover dans les règles de fonctionnement des institutions, en particulier en ce qui concerne l'adoption de rôles différenciés et contextualisés par les collaborateurs et les institutions concernées. »*

Par ailleurs, en septembre 2018, l'association Opendata France – qui promeut notamment l'ouverture des données au niveau local – estimait que seuls 300 communes, départements et régions avaient publié au moins un jeu de données sur les 4500

[46] « 5ème conférence sur les actifs immatériels territoriaux – Plateformes, données et développement territorial », Conférence du 28 novembre 2019
[47] Site web à retrouver ici : http://www.chairedelimmateriel.universite-paris-saclay.fr/

collectivités territoriales soumises à l'*open data* suite à la loi pour une République numérique. En mars 2019, l'association en comptabilisait 512[48].

3. RSE et numérique, deux mondes qui ne se croisent pas encore

Force est de constater que même si la transformation numérique impacte, aujourd'hui, toutes les entreprises, elle demeure peu intégrée dans les enjeux de la RSE – et inversement. Malgré des attributs communs liés à l'éthique, à la temporalité ou encore aux enjeux démocratiques – et bien que la transformation numérique et les enjeux de durabilité soient deux enjeux actuels majeurs – ce sont deux mondes qui s'ignorent encore.

Les auditions menées par le Groupe de Travail et l'analyse du cadre normatif règlementant l'utilisation des outils numériques par les entreprises témoignent de l'absence de liaison entre le numérique et la RSE. Les experts du numérique s'attellent à la protection des données, à l'analyse des données détenues ou encore à la conformité de leur politique aux textes en vigueur sans intégrer ces problématiques à celles soulevées par la RSE.

L'analyse des enjeux environnementaux intègre progressivement le numérique. Néanmoins, les enjeux relatifs à la collecte, la gestion et le traitement des données dont disposent les entreprises ne sont pas encore intégrés aux stratégies globales RSE, alors même que les parties prenantes de l'entreprise dont le salariés et les clients attendent qu'elle soit responsable et rende compte de son action en la matière. Au regard de la RSE, la protection des données s'inscrit impérativement dans une démarche responsable.

Il devient ainsi difficile pour les entreprises d'évoluer dans un univers numérique ne répondant pas aux enjeux règlementaires ; au regard de la RSE, la protection des données est un enjeu pour les parties prenantes et dans une perspective de responsabilisation des entreprises.

La protection des données personnelles dans une optique de conformité au RGPD est aujourd'hui un sujet qui, s'il n'est pas correctement abordé par les entreprises, peut avoir un impact matériel sur la valeur de leurs investissements[49]. Ainsi, pour les entreprises, le rattachement de la protection des données qu'elles détiennent à la politique RSE s'avère stratégique ; le RGPD exige, en ce sens, au titre du principe de responsabilité, de répondre à de nombreux critères relevant de la RSE : loyauté, transparence de l'information auprès des individus dont les données personnelles sont collectées, conformité, sécurité, etc.. Les leviers de confiance que constituent la RSE et le RGPD doivent ainsi être mieux articulés afin de renforcer et d'expliciter une meilleure gouvernance à tous les échelons de l'entreprise.

[48] « République numérique : qu'à changé la loi du 7 octobre 2016 ? » (2019), Vie-publique.fr
[49] Propos recueillis auprès de Mme Sophie Nerbonne, directrice de la co-régulation économique de la CNIL

Il est donc essentiel que la protection des données s'inscrive comme un critère supplémentaire de la politique RSE. Ainsi, les entreprises gagneraient à inclure dans leur politique RSE les critères 1 et 4 du RGPD *« la protection des données à caractère personnel est un droit fondamental »*, *« le traitement des données à caractère personnel devrait être conçu pour servir l'humanité »* : pour montrer qu'elles répondent et se saisissent d'enjeux sociaux et sociétaux forts.

La transparence et la confiance s'imposent comme des fondements sur lesquels les entreprises doivent s'appuyer pour se pérenniser ; et ce en cohérence avec les engagements économiques, sociaux et environnementaux auxquels elles répondent.

La revision de la Directive européenne de 2014/95/UE sur la publication d'informations non financières par la Commission européenne, dans le cadre du Pacte Vert et de la Taxonomie, pourrait voir l'introduction de la protection et de la sécurité des données dans un futur standard de reporting extra-financier européen. Dans un contexte de digitalisation grandissante de l'économie, de tels engagements seraient l'occasion de valoriser la politique de l'entreprise et d'engager la confiance des clients et des citoyens.

L'entreprise construit l'horizon numérique par les choix et les usages qu'elle en fait. Ainsi, considérant la massification des données, des outils numériques et des possibilités offertes à l'entreprise dans ses relations avec ses salariés et ses parties prenantes, les entreprises bénéficieraient d'une politique alliant stratégie numérique et stratégie RSE.

Interroger les termes
Les plateformes numériques[50]

L'économie numérique est, aujourd'hui, au cœur de la société. Néanmoins, on assiste à un flottement sémantique dû à l'interchangeabilité des termes entre eux : économie du partage, *sharing economy*, économique collaborative, économie numérique ou encore plateformisation. La multiplicité des termes pose question et peut altérer la régulation des plateformes numériques.

La loi pour une République Numérique définit les plateformes numériques comme suit :

« *Est qualifiée d'opérateur de plateforme en ligne toute personne physique ou morale proposant, à titre professionnel, de manière rémunérée ou non, un service de communication au public en ligne reposant sur :*

1° Le classement ou le référencement, au moyen d'algorithmes informatiques, de contenus, de biens ou de services proposés ou mis en ligne par des tiers ;

2° Ou la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service. »

Ainsi, cette définition entraine des obligations règlementaires en matière :

- fiscale : les plateformes doivent fournir une information claire, loyale et transparente aux utilisateurs à chaque transaction ;

- d'information : les plateformes doivent fournir une information claire, loyale et transparente aux consommateurs au regard des conditions générales d'utilisation, de la qualité de l'annonceur ou encore sur les droits et obligations des parties en matière civile et fiscale ;

- sociales : les plateformes qui déterminent les caractéristiques de la prestation de services fournie ou du bien vendu ont une responsabilité sociale – concernant les accidents du travail et la formation – à l'égard des travailleurs concernés.

Il est pertinent de se demander si ces obligations globales portent le même sens pour l'économie du partage, l'économie collaborative ou encore l'économie des services à la demande.

Dans le contexte de la future discussion sur le Digital Services Act en Europe, Renaissance Numérique a publié, en mai 2020, une note[51] appelant à une « plateformisation de la régulation ». À ce titre, cette structure recommande aux régulateurs et législateurs européens d'intégrer les caractéristiques des plateformes numériques. Renaissance Numérique estime, notamment, que sans une volonté politique forte, la régulation par les données restera ineffective, que la régulation des plateformes « structurantes » nécessite une définition « robuste et partagée » et que les utilisateurs – en tant que co-contributeurs à la création de valeur sur les plateformes – doivent être intégrés aux processus de régulation.

[50] *Mais au fait, c'est quoi une Plateforme ?,* Droit du Partage, février 2017
[51] « Réguler les plateformes numériques : Pourquoi ? Comment ? », Renaissance Numérique, 11 mai 2020

2. Cadre normatif

Cette partie entend établir un tour d'horizon de la législation en vigueur au regard de la protection des données. On notera que ce cadre concerne majoritairement les données personnelles. Vous trouverez l'explicitation des textes en annexe 1.

2.1. Droit international

2.1.1 Nations unies

Pacte international relatif aux droits civils et politiques, entré en vigueur le 23 mars 1976

L'article 17 garantit que « *Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.* » et que « *Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.* »

Principes directeurs pour la règlementation des fichiers informatisés contenant des données à caractère personnel proclamés lors de la quarante-cinquième session de l'Assemblée générale des Nations Unies dans sa résolution 45/95 du 14 décembre 1990

Le 14 décembre 1990, les Nations Unies ont adopté des principes directeurs relatifs à la règlementation des fichiers informatisés contenant des données à caractère personnel. Les modalités d'application ont été laissées à la libre initiative des Etats sous réserve du respect de plusieurs principes : licéité, loyauté, exactitude, finalité, accès, non-discrimination, dérogation, sécurité, contrôle et sanctions et de flux transfrontaliers des données.

Rapporteur spécial des Nations unies sur le droit à la vie privée[52]

Un rapporteur spécial des Nations unies est un expert indépendant chargé par le Conseil des droits de l'homme d'étudier la situation d'un pays ou un thème spécifique relatif aux droits humains.

Le premier Rapporteur spécial sur le droit à la vie privée a été nommé en 2015. Le poste a été occupé, depuis sa création, par Joseph Cannataci[53].

Le Rapporteur spécial a pour missions de :

- Recueillir des informations sur les pratiques et les expériences nationales, étudier les tendances et les problèmes concernant le droit à la vie privée et de faire des recommandations afin d'en garantir la promotion et la protection ;

- Solliciter des renseignements des Etats, de l'ONU et organismes, programmes et fonds des Nations unies, des institutions nationales des droits humains, des organisations de la société civile, du secteur privé et de tout autre partie prenante ou concernée ;

- Identifier les obstacles pouvant se poser à la promotion et à la protection du droit à la vie privée, d'identifier, d'échanger et de promouvoir les principes et les pratiques optimales aux niveaux national, régional et international et de soumettre au Conseil des droits de l'homme des propositions et des recommandations à cet égard ;

- Participer aux conférences et manifestations internationales pertinentes et contribuer à leurs travaux dans l'intention de faire prévaloir une approche systématique et cohérente des questions relevant du mandat ;

- Faire mieux comprendre qu'il importe de promouvoir et protéger le droit à la vie privée notamment au vu des défis qui se posent à l'ère du numérique

- Intégrer une perspective de genre dans toutes les activités relevant du mandat ;

- Signaler les violations présumées, en quelque lieux qu'elles se produisent, du droit au respect de la vie privée, tel qu'il est énoncé à l'article 12 de la Déclaration universelle des droits de l'homme et à l'article 17 du Pacte international relatif aux droits civils et politiques, y compris dans le contexte des défis que posent les nouvelles technologies et d'appeler à l'attention du Conseil et du Haut-Commissaire des Nations unies aux droits de l'homme sur les cas particulièrement préoccupants. Le rapporteur spécial soumet un rapport annuel au Conseil des droits de l'homme et à l'Assemblée générale des Nations unies.

[52] https://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx

[53] Le 17 novembre 2017, le Rapporteur spécial a effectué une visite en France au sujet du droit à la vie privée
https://www.ohchr.org/FR/NewsEvents/Pages/DisplayNews.aspx?NewsID=22410&LangID=F

Par ailleurs, en 2016, le Conseil des droits de l'homme a défini une série de mesures que les gouvernements devraient prendre afin de promouvoir et de protéger les droits humains et les libertés fondamentales en ligne, demandant notamment aux États « d'adopter et de mettre en œuvre des lois, réglementations, politiques et autres mesures relatives à la protection des données personnelles et de la vie privée en ligne[54] »

2.1.2 Conseil de l'Europe

Article 8 de la Convention européenne de sauvegarde des Droits de l'Homme et des Libertés fondamentales de 1950

L'article 8 garantit que « *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. »* Il exprime également qu'il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit, sauf si celle-ci est prévue par la loi et qu'elle constitue une mesure nécessaire à la *«* sécurité nationale *à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre, à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui. »*

Résolution 428 du Conseil de l'Europe portant déclaration sur les moyens de communication de masse et les droits de l'homme, adoptée en janvier 1970

L'article 19 de la Résolution 428 du Conseil de l'Europe souligne l'importance du droit à la vie privée, et édicte que : « *Lorsque des banques régionales, nationales ou internationales de données informatiques sont instituées, l'individu ne doit pas être rendu totalement vulnérable par l'accumulation d'informations concernant sa vie privée. Ces centres doivent enregistrer uniquement le minimum de renseignements nécessaires aux questions, telles qu'impôts, systèmes de retraites, Sécurité sociale, etc.* »

La Convention 108 du Conseil de l'Europe du 28 juillet 1981

La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dite Convention 108, du Conseil de l'Europe a été ratifiée le 28 janvier 1981 et est entrée en vigueur le 1er octobre 1985. À ce jour, elle a été ratifiée par les 47 États membres du Conseil de l'Europe, ainsi que l'Île Maurice, le Sénégal, l'Uruguay et la Tunisie. D'autres pays participent, à titre d'États observateurs, aux travaux du Comité de la Convention : le Canada, les États-Unis, l'Australie, la Corée, le Chili, le Ghana, le Japon, l'Indonésie, Israël et la Nouvelle-Zélande.

Elle constitue le premier instrument international contraignant visant à protéger les personnes contre l'usage abusif du traitement automatisé des données à caractère personnel. Elle a pour objectif de réglementer les flux transfrontaliers des données et interdit le traitement des données 'sensibles' relatives à l'origine raciale, aux opinions politiques, à la santé, à la religion, à la vie sexuelle ou encore aux condamnations pénales.

[54] Conseil des droits de l'homme, La promotion, la protection et l'exercice des droits de l'homme sur Internet, doc. ONU Doc A/HRC/38/L.10/Rev.1

Recommandation CM/Rec(2020)1 du Comité des Ministres aux États membres sur les impacts des systèmes algorithmiques sur les droits de l'homme, adoptée le 8 avril 2020

Considérant les évolutions technologiques majeures, leur ampleur dans la vie quotidienne, l'engagement des Etats membres à la garantie des droits et libertés, le Conseil de l'Europe établit une liste de recommandations aux gouvernements des **É**tats membres afin de contrôler les impacts des systèmes algorithmiques sur les droits humains.

2.1.3 Organisation de Coopération et de Développement Economique (OCDE)

Recommandations de l'Organisation de Coopération et de Développement Économiques concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontaliers des données à caractère personnel du 23 septembre 1980

Le 23 septembre 1980, l'OCDE émettait des recommandations en vue de favoriser la libre circulation de l'information entre les pays membres et d'éviter la création d'obstacles injustifiés au développement des relations économiques et sociales entre les pays. Le texte énonce des principes fondamentaux applicables au plan national[55] : limitation en matière de collecte des données, qualité des données, limitation de leur utilisation, garanties de sécurité, responsabilité, participation individuelle.

Dans le même temps, les recommandations s'intéressent au niveau international en appelant à la prise en considération des conséquences pour d'autres pays membres d'un traitement effectué sur leur propre territoire et de la réexportation des données à caractère personnel, de la sécurité des flux transfrontaliers et de l'absence d'obstacles à la circulation transfrontalière des données.

Recommandations de l'Organisation de Coopération et de Développement Économiques concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontaliers des données à caractère personnel 11 juillet 2013

Constituant une mise à jour des recommandations du 23 septembre 1980, ce rapport entend appuyer ces positions sur les pratiques de protection de la vie privée au travers d'une approche de management des risques et sur le besoin de donner une ampleur internationale à la protection via une interopérabilité améliorée. Les experts de l'OCDE considèrent également que plusieurs thématiques devront être abordées dans le futur : les stratégies de protection nationales, les programmes de management des risques et des recommandations sur les violations de données.

[55] OCDE, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel (lien)

Global Privacy Assembly

La « Global Privacy Assembly », anciennement appelée « International Conference of Data Protection and Privacy Commissioners », est un forum global de premier plan, né en 1979. L'Assemblée cherche à jouer un rôle moteur au niveau international en matière de protection des données et de la vie privée. Elle y parvient en reliant les efforts de plus de 130 autorités de protection des données et de la vie privée du monde entier.

La vision de l'Assemblée est celle d'un environnement dans lequel les autorités de protection de la vie privée et des données du monde entier sont en mesure de remplir efficacement leurs mandats, à la fois individuellement et de concert, grâce à la diffusion des connaissances et à des liens de soutien. Les missions de cette Assemblée incluent également de fournir du leadership au niveau international en protection des données et de la vie privée, ainsi que de soutenir les autorités à mieux protéger celles-ci.

Des exemples de résolutions adoptées ayant trait au présent avis :

- la Déclaration de Montreux de 2005[56], qui a reconnu la nécessité d'une reconnaissance mondiale des droits à la protection des données personnelles et à la vie privée, et qui a expressément demandé « aux Nations unies d'élaborer un instrument juridique contraignant qui énonce clairement et en détail les droits à la protection des données et à la vie privée en tant que droits de l'homme opposables »
- La « Résolution sur la nécessité urgente de protéger la vie privée dans un monde sans frontières, et de parvenir à une proposition commune pour établir des normes internationales sur la vie privée et la protection des données personnelles », adoptée à Strasbourg en 2008.57
- La « Résolution de Madrid » est une convention qui définit les principes qui devraient renforcer le caractère universel du droit à la protection de la vie privée et des Données personnelles de tous les citoyens (y compris les enfants ou personnes vulnérables, et notamment sur Internet). Adoptée en 2009, elle demande aux Etats d'élaborer en commun, par exemple sous l'égide de l'ONU, une norme commune internationale de protection des données, notamment sur Internet, en respectant quelques principes tels que la transparence, la responsabilité, les droits à l'accès à l'information, le droit à la rectification.

[56] Déclaration de Montreux (2005), *Dans un monde globalisé, un droit universel à la protection des données personnelles et à la vie privée dans le respect des diversités*
57 https://www.lda.brandenburg.de/media_fast/4055/resolution_international_standards_en.pdf

2.2. Droit de l'Union européenne

2.2.1 Traités

Charte des droits fondamentaux de l'Union européenne

L'article 8 garantit que « T*oute personne a droit à la protection des données à caractère personnel la concernant. »* et que les données doivent être traitées *« loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. »* De même, *« toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. » et* « l*e respect de ces règles est soumis au contrôle d'une autorité indépendante. »*

2.2.2 Directives

Directive 2002/58-CE du 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques, dite e-privacy

La Directive 2002/58-CE vise à protéger de façon spécifique la vie privée sur internet en couvrant certains aspects mis de côté par la Directive 95/46/CE. Elle interdit le spam en instaurant les principes « d'*opt-in* » – voulant qu'un opérateur obtienne le consentement du destinataire avant de lui envoyer tout message à caractère commercial – et « d'*opt-out* » permettant de se retirer d'une liste d'envoi. Ces deux principes ont été transposés dans le droit français au travers de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Directive (UE) 2016/1148 du 6 juillet 2016 sur la sécurité des réseaux et des systèmes d'information (Directive NIS)

Le Parlement européen et le Conseil de l'Union européenne ont adopté le 6 juillet 2016 la directive sur la sécurité des réseaux et des systèmes d'information, également appelée en anglais la directive NIS (Network and Information System Security). La France a transposé cette directive par différents textes en 2018[58]. Celle-ci est structurée autour de quatre axes[59] : le renforcement des capacités nationales de cybersécurité, l'établissement d'un cadre de coopération volontaire entre les États membres de l'UE, le renforcement de la cybersécurité des opérateurs de services essentiels au fonctionnement de l'économie et de la société et l'instauration de règles européennes communes en la matière.

[58] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033122937
[59] https://www.ssi.gouv.fr/actualite/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/

2.2.3 Règlements

Règlement n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000

Le règlement n°45/2001 du 18 décembre 2000 est relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données. Une de ses dispositions promulgue des mesures de conservation des données à une fin de police préventive. Elle introduit le nécessité de traiter les données à caractère personnel de manière loyale, licite, exacte, et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement.

Règlement n°2016/679 dit Règlement Général sur la Protection des Données (RGPD)

Le règlement n°2016/679 dit Règlement Général sur la Protection des Données (RGPD) est un règlement du Parlement européen et du Conseil constituant l'un des textes de référence en matière de protection des données. Adopté le 14 avril 2016, il est entré en vigueur le 27 avril 2016 et ses dispositions sont obligatoirement et directement applicables dans l'ensemble des 28 États-membres de l'Union européenne depuis le 25 mai 2018.

La conception du RGPD a été pensée autour de 3 objectifs : le renforcement des droits des personnes physiques, la responsabilisation des acteurs traitant des données et la crédibilisation de la régulation grâce à la coopération renforcée entre les autorités de protection des données.

Comparaison du RGPD et du California Consumer Privacy Act :

Le RGPD a inspiré de nouvelles législations dans d'autres pays. Ainsi, le *California Consumer Privacy Act* adopté le 28 juin 2019 et entré en application le 1er janvier 2020 s'inspire des acquis européens. Ce texte visant à renforcer la maîtrise et le contrôle des personnes sur leurs données constitue la première législation de ce type aux États-Unis. Il donne le droit aux californiens de demander aux entreprises quelles données sont collectées, comment elles sont utilisées, avec quelles tierce-parties elles sont partagées, qu'elles soient supprimées mais aussi de refuser que leurs données soient utilisées à des fin commerciales. Pour les enfants de 13 à 16 ans, les données ne peuvent être vendues sans leur accord explicite préalable et pour les enfants de moins de 13 ans, l'accord d'un adulte est nécessaire.

La législation californienne contient des différences notables avec le RGPD :

Règlement Général sur la Protection des Données	California Consumer Privacy Act
« Toute information se rapportant à une personne physique identifiée ou identifiable » (article 4) Distinction entre les données classiques et les données dites sensibles	« Informations qui identifient, se rapportent à, décrivent, sont susceptibles d'être associées à, ou pourraient raisonnablement être liées, directement ou indirectement, à un consommateur ou un ménage particulier » Pas de distinction entre les données Les données des salariés ne sont pas considérées comme des données à caractère personnel
Le RGPD contraint les entreprises à demander l'autorisation aux internautes avant de collecter leurs données	Les entreprises ne sont pas obligées de demander l'autorisation aux internautes avant de collecter leurs données
La protection s'applique sans distinction à tout organisme privé ou public disposant de données à caractère personnel. Il dispose d'un caractère extraterritorial puisqu'il ne s'applique pas seulement aux personnes présentes sur le territoire de l'Union européenne.	Exclusion des informations contenues dans un fichier tenu par un organisme public fédéral, étatique ou local et qui seraient rendues publiques La protection ne bénéficie qu'aux résidents de l'État de Californie et elle ne s'applique pas aux traitements de données liés à des activités commerciales réalisées intégralement hors de Californie. Le California Consumer Pivacy Act s'applique aux entreprises qui génèrent un chiffre d'affaires supérieur à 25 millions de $ sur le sol californien, achètent, reçoivent ou vendent les données de 50 000 consommateurs
	Autorise le responsable de traitement à créer des programmes d'incitation, notamment financières, au bénéfice de la personne qui accepte la collecte ou la revente de ses données personnelles
N'ouvre pas la possibilité d'engager des poursuites au civil	Ouvre la possibilité aux individus d'engager des poursuites au civil

Le Conseil européen de protection des données, ex-G29

Le G29 ou Groupe de travail Article 29 sur la protection des données est un ancien organe consultatif de l'Union européenne indépendant sur la protection des données et de la vie privée. Sa dénomination est tirée des articles 29 et 30 de la directive 95/46/CE, qui définit son organisation et ses missions. À compter de l'entrée en application du Règlement général sur la protection des données en mai 2018, il est remplacé par le Comité européen de la protection des données.

Il se compose de représentants des autorités nationales chargées de la protection des données et du Contrôleur européen de la protection des données (CEPD).

Celui-ci est chargé de :
- Fournir des orientations générales (y compris à travers des lignes directrices, des recommandations et des bonnes pratiques) pour clarifier la législation ;
- Conseiller la Commission européenne sur toute question liée à la protection des données à caractère personnel et sur les nouvelles propositions de législation dans l'Union européenne ;
- Adopter des conclusions relatives à la cohérence sur des questions de protection de données transfrontalières ;
- Promouvoir la coopération ainsi que l'échange efficace d'informations et de bonnes pratiques entre les autorités de contrôle nationales[60].

Règlement du Parlement européen et du Conseil du 10 janvier 2017 concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »)[61]

La Commission européenne a publié une proposition de règlement du Parlement européen et du Conseil de l'Union européenne le 10 janvier 2017 afin d'élargir le champ d'application de la Directive 2002/58-CE et aligner ses dispositions avec le RGPD. Néanmoins, les États-membres peinent à s'accorder et deux dispositions font débat : la notion de consentement préalable et la géolocalisation de la clientèle par les entreprises.

En mai 2017, les éditeurs de presse ont adressé une lettre ouverte[62] à l'Union européenne afin d'alerter les pouvoirs publics sur la notion de consentement préalable qui avantagerait les entreprises qui contrôlent 90 % de l'accès à Internet sur le territoire européen – Google, Apple, Microsoft et Mozilla – et renforcerait l'asymétrie entre les éditeurs de presse et les portails numériques mondiaux.

Dans le cadre de sa présidence du Conseil de l'Union européenne, du 1er janvier au 30 juin 2020, la Croatie a relancé les débats avec la proposition d'un nouveau compromis.

[60] https://edpb.europa.eu/about-edpb/about-edpb_fr
[61] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52017PC0010&from=FR
[62] https://www.lapresse.be/wp-content/uploads/2018/03/Definitive-Open-letter-ePR-v05032018-VF_2PAGES.pdf

Règlement 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne

Le règlement 2018/1807 vise à assurer le libre flux des données autres que les données à caractère personnel au sein de l'Union européenne. Pour cela, il établit des règles concernant les exigences de localisation des données, leur disponibilité pour les autorités compétences et le portage des données pour les utilisateurs professionnels.

2.2.4 Jurisprudences

Arrêt de la CJUE, grande chambre, 8 avril 2014, relatif à la directive 2006/24/CE du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications

Rendant décision dans le cadre d'un procès entre Digital Rights Ireland Ltd, cet arrêté du 8 avril 2014 condamne « *Une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne »,* d'une si *« vaste ampleur »* qu'elle *« doit être considérée comme particulièrement grave ».* En effet, *« la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soit informé »,* ce qui génère *« le sentiment que* [sa] *vie privée fait l'objet d'une surveillance constante ».*

La Cour de Justice de l'Union européenne précise la notion de « consentement libre et informé »

En mars 2020, l'avocat général de la Cour de Justice de l'Union européenne a rendu ses conclusions dans une affaire impliquant l'opérateur mobile et internet roumain « Orange România » en précisant la notion de « consentement libre et informé » dans le cadre du traitement des données à caractère personnel.

Orange România a conclu des contrats avec ses clients, dans lesquels ils ont accepté que l'opérateur traitent leurs données à caractère personnel en cochant une case dans la documentation contractuelle. Ce traitement consistait, notamment en la collecte et la conservation de copies de leurs pièces d'identité.

Considérant que ce mode opératoire ne constituait pas une expression viable du consentement, l'autorité roumaine de surveillance du traitement des données à caractère personnel a infligé une sanction à l'entreprise. Le Tribunal de Grande Instance de Bucarest[63] a donc interrogé les juges du plateau de Kirchberg afin de connaitre les conditions devant être remplies pour qu'une manifestation de volonté soit considérée comme « spécifique et informée » et librement exprimée.

Selon la CJUE, il est légitime que des entreprises demandent à leurs clients de fournir certaines données personnelles, et notamment de donner leur identité aux fins de l'établissement d'un contrat. Néanmoins, le parquet général considère qu'exiger d'un client qu'il consente à la collecte et à la conservation de copies de sa pièce d'identité « semble aller au-delà de ce qui est nécessaire à l'exécution du contrat ».

Dans le cas précis d'Orange România, la CJUE a estimé que les clients ne donnent pas leur consentement libre, notamment car il n'est pas indiqué au client que le refus de la collecte et de la conservation de sa carte d'identité ne compromet pas l'exécution du contrat. Ainsi, en n'ayant pas connaissance des conséquences de son refus, le client n'effectue pas son choix de manière éclairée.

2.3. Droit français

Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi « informatique et libertés », est une loi française règlementant la liberté de traitement des données personnelles. Elle prévoit des obligations à la charge des détenteurs de données à caractère personnel sur plusieurs niveaux : collecte de données à caractère personnel, finalité des traitements, durée de conservation, mesures de sécurité et confidentialité.

[63] Le législateur roumain n'a pas transposé le RGPD dans son entièreté. En droit roumain, la partie de la directive prévoyant que le consentement désigne « toute manifestation de volonté libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fassent l'objet d'un traitement » n'a pas été transposée.

La loi rappelle que les personnes ont des droits sur leurs données. Le responsable des données à caractère personnel permet aux individus d'exercer leurs droits et doit leur donner la possibilité d'obtenir les informations sur leur identité, la finalité de traitement de leurs données, le caractère obligatoire ou facultatif des réponses, l'existence de leurs droits et les transmissions envisagées.

La loi institue enfin la Commission nationale de l'informatique et des libertés (CNIL). Elle constitue l'autorité indépendante garante de la protection des données à caractère personnel. Ainsi, certains traitements de données doivent être déclarés auprès de la CNIL ou être autorisés par celle-ci.

Les décrets n°2018-687 du 1er août 2018 et n°2019-536 du 29 mai 2019 ont permis de renforcer la loi n°78-17 et de l'adapter aux obligations du RGPD.

La loi du 7 octobre 2016 pour une République numérique

La loi n°2016-1321 prépare la France aux enjeux de la transition numérique en créant de nouveaux droits afin de permettre aux individus de mieux maitriser leurs données personnelles. Elle renforce également les pouvoirs de la CNIL et entend promouvoir une meilleure ouverture des « données publiques ».

Les dispositions prévues anticipaient le RGPD, ainsi la loi façonne de nouveaux droits pour les personnes[64] : maîtrise des données, droit à l'oubli pour les mineurs, organisation du sort de ses données après la mort, exercice de droits par voie électronique, informations sur la durée de conservation des données.

Loi du 20 juin 2018 relative à la protection des données personnelles

La loi n°2018-493 reprend les dispositions du RGPD. Certains articles du règlement renvoient aux législations nationales afin qu'elles soient en mesure d'adapter et de clarifier certaines dispositions au regard de leurs spécificités, cette loi apporte des précisions complémentaires aux règles européennes.

Elle renforce ainsi le domaine de compétences de la CNIL qui est désormais un organe certificateur en mesure de certifier des personnes, produits, systèmes de données ou des procédures afin de reconnaitre leur conformité au RGPD. La majorité numérique est également fixée à 15 ans, c'est-à-dire l'âge à partir duquel un adolescent a la faculté de consentir seul, sans autorisation parentale, au traitement de ses données.

[64] https://www.cnil.fr/fr/ce-que-change-la-loi-pour-une-republique-numerique-pour-la-protection-des-donnees-personnelles

Règles spécifiques propres aux codes législatifs

La protection des données à caractère personnel est également régie au travers de codes législatifs précis. En voici quelques exemples :

Code de la Route[65]

Le Code de la Route prévoit que dans le cas de certaines infractions relevées sans interpellation physique du conducteur et commises avec un véhicule dont le titulaire du certificat d'immatriculation est une personne morale telle une entreprise, le représentant légal doit indiquer l'identité de la personne physique conduisant le véhicule.

A cet effet, les données personnelles sur les conducteurs sont stockées et transmises par l'entreprise, à destination des autorités compétences ; l'entreprise qui met en œuvre un tel traitement de données personnelles des salariés doit effectuer un engagement de conformité auprès de la CNIL afin d'assurer le respect des dispositions prévues par l'autorisation unique n°AU-10. Cette autorisation permet aux organismes publics ou privés recevant des procès-verbaux d'infractions au Code de la Route de désigner auprès de l'Agence Nationale de Traitement Automatisé des Infractions la personne qui conduisait ou était susceptible de conduire le véhicule lors de la contravention constatée. Les durées de conservations des données personnelles ne peuvent, cependant, pas excéder 12 mois à compter de la réception de l'avis de contravention.

Code du Travail[66]

Renforcé par le RGPD, le Code du Travail comprend plusieurs dispositions en vue de la protection des données des salariés.

Au moment du recrutement, les articles L.1221-6 et L.1221-7 prévoient que les informations demandées à un candidat doivent avoir un lien direct et nécessaire avec le poste en question ou avec l'évaluation des aptitudes du candidat. Le principe du RGPD de *Privacy by default* autorise la collecte de données strictement nécessaires. Par ailleurs, le Code du Travail prévoit que les informations concernant les candidats ne peuvent être collectées par un dispositif qui n'a pas été porté préalablement à leurs connaissance (articles L.1221-8 et L.1221-9). Les questionnaires d'embauche doivent ainsi mentionner : l'identité du responsable du traitement, la finalité poursuivie par le traitement auquel les données sont destinées, le caractère obligatoire ou facultatif des réponses, les droits des personnes à l'égard des traitements de données à caractère personnel.

Durant l'exécution du contrat de travail du salarié, l'employeur ne peut recourir à des moyens clandestins de contrôle du salarié – géolocalisation, accès biométrique, contrôle de la messagerie, suivi des activités extra-professionnelles – s'ils se sont pas conformes au RGPD ; l'employeur pourrait être poursuivi par le salarié pour violation de l'obligation de loyauté selon l'article L.1222-1 du Code du Travail.

[65] *Autorisation unique AU-10, Recouvrement des contraventions routières*, CNIL
[66] Juritravail (2018), *Le contrôle du travail des salariés est-il remis en cause avec le RGPD*

Code de la Santé publique[67]

Le traitement des données personnelles de santé est soumis au droit commun du traitement des données à caractère personnel du RGPD. L'article 9 définit les données de santé comme sensibles et interdit leur traitement ; toutefois, des exceptions sont possible si la personne concernée y consent et si le traitement de ces données est rendu nécessaire à des fins médicales de médecine préventive, de diagnostic médicaux, d'administration de soins ou de traitement dans l'intérêt public.

Le Code de la Santé publique soumet ainsi le traitement des données personnelles de santé à des obligations renforcées de sécurité, de confidentialité et d'information de la personne concernée. Par ailleurs, les données personnelles de santé traitées par un professionnel de santé sont soumises au secret médical.

Le partage d'information en milieu médical est également encadré par l'article L.1110-4 du Code de la Santé publique. À ce titre, un professionnel de santé peut échanger avec d'autres professionnels de santé identifiés des informations relatives à un patient à condition qu'ils participent tous à la prise en charge du patient et que ces informations soient strictement nécessaires à la coordination ou à la continuité des soins ou de son suivi médico-social. L'article L.1111-8 prévoit que les données de santé soient hébergées auprès d'hébergeurs agréés ou certifiés et par un organisme accrédité par le Comité France d'Accréditation. Il est ainsi interdit de procéder à une cession ou à l'exploitation commerciale des données de santé (article L.4113-7).

Code de la Propriété intellectuelle[68]

Les bases de données peuvent constituer des éléments essentiels dans la valorisation des entreprises.

Définies à l'article L.112-3-2 du Code de la Propriété intellectuelle comme « un recueil d'œuvres, de données ou d'autres éléments indépendants, disposés de manière systématique ou méthodique, et individuellement accessibles par des moyens électroniques ou par tout autre moyen », les bases de données sont soumises à une protection double :

- La protection du droit d'auteur qui protège la structure de la base de données – manière dont les données sont organisées – et confère le droit exclusif de faire ou d'autoriser la reproduction, la traduction, l'adaptation ou l'arrangement, toute forme de distribution et de communication sur la base en question ;
- La protection de droit *sui generis* du producteur de la base de données – sous couvert d'un investissement matériel, financier ou humain – qui protège le contenu de la base de données et qui peut interdire l'extraction et la réutilisation de la totalité ou d'une partie substantielle de la base de données.

[67] *Données personnelles de santé*, Sédallian Avocats
[68] *Bases de données : quelles protections ?,* Mathias Avocats, décembre 2016

Les régulateurs du numérique en France

La CNIL - Commission nationale de l'informatique et des libertés - Régulatrice des données personnelles

Fondée en 1978, la CNIL dispose de quatre missions principales :

- Accompagner les professionnels dans leur mise en conformité ;
- Aider les particuliers à maîtriser leurs données personnelles et exercer leurs droits en la matière ;
- Contrôler et sanctionner : la CNIL peut contrôler les organismes - cas de manquements constatés, elle peut décider de les mettre en demeure ou de les sanctionner ;
- Anticiper et Innover : dans le cadre de son activité d'innovation et de prospective, la CNIL se penche sur les signaux faibles et les enjeux émergents.

En 2016, la CNIL s'est dotée d'un plan triennal d'orientations stratégiques et opérationnelles. Ce plan avait deux objectifs principaux :
- Faire de la CNIL, confrontée à une très forte pression quantitative et qualitative du fait du basculement de la société dans l'ère numérique, un régulateur complet, agile et investi dans la co-régulation et l'inter-régulation ;
- Dessiner un projet pour une période sans précédent pour l'institution, celle de l'adoption puis de l'entrée en application du règlement européen sur la protection des données (RGPD)

D'ici 2021, la CNIL s'organise autour de cinq axes stratégiques déclinés en grands objectifs :
- Donner la priorité aux enjeux numériques de la vie quotidienne : faciliter le traitement des saisines des particuliers, enrichir l'offre éditoriale à destination des particuliers, être plus lisible ;
- Renforcer la place du quotidien numérique dans toutes les actions de la CNIL : assumer une régulation équilibrée de la protection des données à l'heure du RGPD, mieux cible et valoriser l'offre d'accompagnement, s'adapter à la maturité et aux besoins variables des professionnels, rendre l'action répressive plus lisible, mieux articuler sanction et accompagnement ;
- Promouvoir une diplomatie de la donnée : ancrer la coopération européenne dans le travail de la CNIL au quotidien, jouer un rôle moteur au sein du collectif européen, porter la voix de la CNIL à l'international ;
- Offrir une expertise publique de pointe sur le numérique et la cybersécurité : approfondir l'expertise technique de la CNIL, promouvoir la vision de la CNIL du numérique e de l'innovation, rendre plus concrète l'inter-régulation, diffuser l'approche éthique ;
- Incarner un service public innovant et rassemblé autour de ses valeurs : être encore davantage à l'écoute de ses publics, mieux se connaitre, mieux intégrer, améliorer le travail collectif au sein de la CNIL, créer une « marque employeur » CNIL.

L'ARCEP (Autorité de Régulation des communications électroniques, des postes, et de la distribution de la presse) - autorité administrative indépendante (AAI) architecte, régulatrice et gardienne des réseaux d'échanges internet, fixes, mobiles et postaux[69]

[69] https://www.arcep.fr/

Fondée en 1997, l'ARCEP a vu ses missions s'élargir au fil des années :
- Régulation du secteur postal en 2005
- Protection de la neutralité en 2015
- Loi pour une République numérique en 2016
- Aménagement numérique des territoires avec les dispositions de la loi Elan pour accélérer la couverture numérique du territoire en 2018
- Loi sur la modernisation de la distribution de la presse en 2019

L'objectif de cette AAI est de s'assurer que les dynamiques et intérêts des opérateurs privés correspondent aux objectifs de connectivité du territoire, de compétitivité et de concurrence effective et loyale entre les opérateurs, au bénéfice des utilisateurs finaux. Le cadre juridique des communications électroniques et les compétences de l'Arcep découlent ainsi très largement des règles européennes. À cet effet, l'Arcep doit pouvoir apporter son concours aux autorités françaises sur les questions internationales et européennes. Sa relation directe avec la Commission européenne en fait un acteur essentiel de la régulation numérique en France.

Le Secrétariat d'État chargé du numérique[70]

Le rôle du Secrétariat d'État chargé du numérique est de préparer et coordonner la politique de transformation numérique de l'**É**tat – de manière conjointe avec le Ministère de l'Action et des Comptes publics.

A cet effet, il dispose de plusieurs compétences :
- Le suivi du développement et de l'amélioration des usages et services numériques et de la politique d'ouverture et de circulation des données ;
- Le traitement des questions relatives au système d'information de l'**É**tat ;
- La participation à l'élaboration du cadre juridique relatif au numérique à l'échelle nationale, européenne et internationale ;
- La participation à la mise en œuvre du programme des investissements d'avenir dans le domaine du numérique ;
- La promotion de la transformation numérique de l'économie, de l'action publique et des territoires ;
- Le respect des droits et libertés fondamentales dans le monde numérique (éthique des technologies, inclusion, accessibilité, médiation numérique) ;
- Le traitement des questions relatives aux communications électroniques, au développement de l'économie numérique et à la transformation numérique des entreprises ;
- Le traitement des questions relatives à la promotion et à la diffusion du numérique, à la gouvernance de l'internet, à la sécurité des échanges et des systèmes d'information mais aussi aux infrastructures, équipements, services, contenus et usages numériques ;
- Le traitement des questions relatives à l'éducation et à la formation au numérique et les mutations numériques du travail.

[70] https://www.gouvernement.fr/le-secretariat-d-etat-charge-du-numerique

3. Enjeux et risques liés aux données

Les entreprises possèdent une multitude de données avec lesquelles elles interagissent dans toutes leurs activités – marketing, reporting, gestion des stocks, relations clients, relations fournisseurs, relations avec la sous-traitance, relations avec les parties prenantes, dialogue social, gestion financière et comptable, ressources humaines – néanmoins, la création, la détention ou encore le traitement de données au cœur du business exposent les entreprises à des risques spécifiques et les contraint à se saisir d'enjeux majeurs.

Aujourd'hui, les risques et les menaces s'avèrent sous-estimés et les enjeux sont sous-évalués voire mal-appréhendés par les entreprises.

1. Posséder et gérer les données

L'utilisation du numérique entraine des impacts notables sur les pratiques des entreprises et sur leurs relations avec les parties prenantes. Cette utilisation grandissante soumet par ailleurs les entreprises à des menaces et des risques qu'il leur faut prendre en considération.

Les impacts et les bénéfices de l'utilisation numérique

Cinq impacts internes liés à la transition numérique sur les entreprises peuvent être identifiés[71].

Ainsi, la multiplication des outils numériques permet, entre autre, aux entreprises d'avoir une meilleure connaissance de leurs clients et, de ce fait, de capitaliser sur leurs attentes et les tendances de marché. Dans le même temps, les nouvelles techniques et technologies permettent d'engendrer de nouveaux outils capables d'exploiter les potentialités de l'analyse des données et de l'intelligence artificielle au profit du business model de l'entreprise.

Les ressources humaines se voient, dès lors, impactées par la nécessité d'une part de recruter de nouveaux profils aux compétences variées et adaptées et d'autre part de former les salariés aux nouvelles technologies. Cette nécessité conduit à l'émergence de nouveaux postes – *chief data officer*, *data protection officer*, *data analytics* – pour permettre à l'entreprise de répondre aux nouveaux enjeux numériques.

Les impacts externes sont également des sources de risques à prendre en considération dans une approche RSE de la transformation numérique. Les entreprises ont pour responsabilité de limiter leurs impacts sur l'environnement[72] ; dès lors, le stockage des

[71] Audition de M. Rémi Dusaud, Data Analytics BDO

[72] Cette problématique spécifique fera l'objet d'un rapport ultérieur de la Plateforme RSE, comme mentionné en introduction. Les membres de la Plateforme RSE ont pris le parti d'analyser la responsabilité des entreprises sous le prisme de la gestion des données auxquelles elles sont confrontées. Les problématiques liées à l'impact de la transformation numérique sur les formes de travail et l'environnement seront traités ultérieurement. Cet avis est le premier d'un cycle dédié à la Responsabilité Numériques des Entreprises.

données et la consommation massive d'outils numériques doivent être questionnés et régulés. L'accroissement des utilisations numériques entraine des impacts sur la sécurité et le respect de la vie privée des personnes – aussi bien au niveau des salariés, que des parties prenantes – dont les données personnelles détenues par les entreprises peuvent être utilisées et/ou divulguées à mauvais escient et dans des conditions contraires aux règlementations. Sur ce point, la Ligue des droits de l'homme (LDH)[73] considère que, si les technologies numériques constituent des avancées considérables en matière d'accès à la connaissance, à l'information et à tout type d'échanges, elles peuvent devenir des *« outils de surveillance et parfois d'oppression. »* Enfin, la bonne gestion des données quelle qu'elles soient (personnelles ou économiques)au regard des enjeux sociaux, environnementaux et sociétaux doit s'inscrire dans la politique RSE de l'entreprise.

La révolution numérique constitue un défi pour les ONG. En 2016, la Conférence internationale des ONG organisée par l'UNESCO portait sur « les défis de la révolution numérique pour les ONG »[74]. Soulignant les enjeux majeurs que constituent la disqualification de l'action humaine au travers de l'intelligence artificielle ou les risques de marchandisation des données personnelles, les ONG présentes ont rappelé le rôle majeur des organisations non gouvernementales dans la sensibilisation des populations, la responsabilisation des acteurs économiques et des individus. Les débats ont fait ressortir la nécessité de soutenir les ONG qui agissent comme modératrices et médiatrices pour prévenir, identifier et limiter les risques numériques sur les populations, en complément de l'action des autorités dédiées.

Amnesty International dénonce même *« le modèle économique fondé sur la surveillance mis en place par Facebook et Google »* en indiquant qu'il est par nature incompatible avec le droit à la vie privée et représente une menace pour toute une série d'autres droits : droits à la liberté d'opinion, d'expression et de pensée, droits à l'égalité ou encore droit à la non-discrimination. Les entreprises des Gafam[75] et des Batx[76] ont accumulé un pouvoir inégalé sur la sphère numérique en collectant et monétisant les données personnelles de milliards d'utilisateurs. Amesty estime, en ce sens, que le contrôle insidieux de nos vies numériques sape le fondement même de la vie privée et c'est l'un des défis majeurs de notre époque en termes de droits humains[77].

Les impacts sur les relations avec les parties prenantes

Les liens des entreprises avec leurs parties prenantes se voient également modifiés par la massification des outils et processus numériques.

La digitalisation transforme les relations avec les salariés et les modes de fonctionnement et de management internes à l'entreprise. À titre d'exemple, les bulletins

[73] Artiguelong M. (2018) « Numérique, vie privée et libertés », *Hommes et Libertés* n°183.
[74] « Les ONG et la révolution numérique » (2016), Conférence internationale des ONG du 12 au 14 décembre 2016
[75] Google, Apple, Facebook, Amazon, Microsoft
[76] Baidu, Alibaba, Tencent, Xiaomi
[77] https://www.amnesty.fr/actualites/facebook-et-google-les-geants-de-la-surveillance

de paie se trouvent aujourd'hui digitalisés et stockés dans des coffres-forts électroniques non accessible sans accès à un ordinateur.

Le RGPD augmente, notamment, les exigences dans les relations des entreprises à leurs fournisseurs ; les entreprises attendent désormais que les fournisseurs soient en mesure de prouver leur conformité aux règlementations en vigueur, et inversement. Dans le même temps, la numérisation de certaines plateformes d'achats tend à supprimer les contacts physiques entre entreprises et fournisseurs.

Le numérique offre des possibilités grandissantes dans les relations de l'entreprise avec ses clients. Si ces possibilités apparaissent surtout positives pour l'entreprise – via la mise en place de publicités ciblées par exemple –, elles comportent, néanmoins, des risques relatifs au respect de la vie privée et à l'exigence de proposer des choix éclairés aux consommateurs, et doivent donc faire l'objet d'une vigilance accrue de la part des directions concernées.

Les autorités de contrôle sont aujourd'hui des actrices clés de la mise en conformité, obligatoire et nécessaire, des entreprises. À ce titre, la CNIL propose aux entreprises de mener une réflexion avec les entreprises le souhaitant sur les étapes menant à leur conformité au RGPD.

Par ailleurs, la CNIL recommande aux entreprises et organisations de conserver les données personnelles dans un délai maximum de trois ans si la personne prospectée ne réagit pas. Néanmoins, les particularismes des données sont à prendre en considération ; la durée doit en outre être proportionnée à la finalité du traitement des données. Ainsi la conservation des données personnelles par un concessionnaire automobile pendant trois ans semble justifiée, une telle durée pour une entreprise vendant des produits pour nourrissons ne se justifie pas de la même manière[78].

Les menaces pesant sur les entreprises

Les entreprises se voient soumises à des menaces multiples et protéiformes provenant de sources distinctes.

La CNIL[79] identifie trois sources majeures :

- Les sources humaines internes qui contribuent au fonctionnement de l'entreprise et qui peuvent faire l'objet de dérive de toutes sortes, c'est-à-dire, les salariés quelles que soient leur fonction et expertise ;
- Les sources humaines externes avec lesquelles les entreprises sont en contact quotidien tels que les prestataires, les parties prenantes, les destinataires des données à caractère personnel, les clients, les syndicats et les ONG. Ces sources de risques peuvent également être des organisations criminelles, des pirates informatiques ou même des concurrents et des journalistes ;

[78] Audition de Mme Sophie Nerbonne, directrice de la corégulation économique de la CNIL
[79] Idem

- Les sources non humaines prenant la forme de codes malveillants d'origine inconnue, d'eau, de matières inflammables ou encore d'épidémies.

Plusieurs menaces peuvent ainsi être citées : le détournement de l'utilisation des données, les cyberattaques affaiblissant les systèmes d'information – bloquant ainsi tout le fonctionnement de l'entreprise –, la non-conformité aux règlements, la nullité des contrats et des actifs, la concurrence déloyale ou encore les coûts financiers générés par la réparation de telles menaces.

La préoccupation de l'éthique

Le numérique introduit des changements de paradigme au sein des entreprises et les modèles d'affaires, les modes de management, les relations avec les salariés et les parties prenantes s'en voient transformés. Cette transformation engendre de nouvelles opportunités, mais également de nouvelles problématiques éthiques[80] : protection des données, respect de la vie privée, droit à l'oubli, droit à la portabilité, neutralité, transparence des algorithmes.

Le rapport d'activité 2019 de la CNIL[81] considère que la portabilité des données personnelles offre de *« nouvelles perspectives pour les utilisateurs, mais aussi pour les entreprises souhaitant créer des services innovants. »* La portabilité ne concerne pas l'ensemble des données personnelles détenues par une entreprise, elle concerne uniquement des données dont le traitement repose *« soit sur le contrat, soit sur le consentement »* et les données déclarées activement et consciemment par la personne concernée. Ce principe, développé dans l'article 20 du RGPD, donne davantage de contrôle aux individus sur leurs données ; la CNIL recommande ainsi aux acteurs de s'accorder sur des « formats interopérables » qui permettront la portabilité. Elle rappelle, néanmoins, que des progrès restent à faire dans la mise en œuvre du droit à la portabilité afin que ce nouveau paradigme offre des *« opportunités pour tous les acteurs qui sauront s'en saisir, sous le contrôle des individus concernés. »*

La CFDT rappelle dans ses ambitions pour la transition numérique[82] que la maitrise des données et leur traitement doivent concourir au progrès et, pour cela, la société dans son ensemble doit déterminer « les traitements qui vont dans le bon sens et ceux que nous ne pouvons accepter ». Dans cette perspective, doivent également être renforcés les droits des usagers sur leurs données, l'ouverture des plateformes et leur interopérabilité, le respect des principes d'égalité ou encore la régulation des situations concurrentielles.

Le Cigref et Syntec Numérique expliquent qu'il est nécessaire de distinguer l'éthique et la conformité. La conformité répond au respect de normes et de lois extérieures tandis que l'éthique répond à une réflexion personnelle ou collective qui vise à se donner soi-

[80] Syntec numérique (2018), CIGREF, *Ethique et numérique, un référentiel pratique pour les acteurs du numérique*
[81] CNIL (2020), Rapport d'activité « Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles »
[82] CFDT (2016), *Transition numérique, Analyse et propositions de la CFDT*

même ses lignes de conduite. L'éthique correspond donc à un acte de « responsabilisation, d'engagement et d'intégrité » qui incombe à l'entreprise. À ce propos, le rapport IA for Humanity porté par Cédric Villani, rappelle que « Dans ces cas où la norme est inexistante, muette ou insuffisante, la responsabilité morale du développeur est accrue. »

Quid des *open data de* l'administration publique ?

Anonymisation et *open data*

Le RGPD n'impose pas aux administrations d'anonymiser les données présentes dans les documents qu'elles possèdent ; cette pratique demeure une solution pour pouvoir exploiter les données personnelles dans le respect des droits et libertés des personnes. Néanmoins, si une administration souhaite diffuser les documents ou les données qu'elle possède, l'anonymisation est une obligation légale s'imposant par principe en application de l'article L. 312-1-2 du Code des Relations entre le public et l'administration (CRPA). Ainsi, les documents administratifs comportant des données personnelles ne peuvent être rendus publics qu'après avoir fait l'objet d'un traitement rendant impossible l'identification des individus.

Le processus d'anonymisation, en éliminant la possibilité d'une ré-identification, implique une perte de la qualité des données.

À cet effet, la CNIL[83] conseille de :
- Supprimer les éléments d'identification directe et les valeurs rares qui pourraient permettre une réidentification aisée des personnes ;
- Distinguer les informations importantes et celles qui sont secondaires ;
- Définir la finesse idéale et acceptable pour chaque information conservée ;
- Définir les priorités.

Les techniques d'anonymisation peuvent être regroupées en deux familles :
- La randomisation : modifier les attributs dans un jeu de données afin qu'elles soient moins précises (exemple : échanger la date de naissance des individus) ;
- La généralisation : modifier l'échelle ou l'ordre de grandeur des attributs du jeu de données afin de s'assurer qu'ils soient communs à un ensemble de personnes (exemple : remplacer la date de naissance par l'année de naissance).

Le Conseil européen de la protection des données[84] a publié, en avril 2014, un avis sur les principales techniques d'anonymisation et leur mise en œuvre. L'avis propose trois critères pour appréhender l'anonymisation :
- L'individualisation : isoler un individu ;
- La corrélation : relier entre elles des données distinctes concernant un même individu
- L'inférence : déduction d'une information sur un individu ;
- Un jeu de données pour lesquelles il n'est pas possible d'individualiser, de corréler ou d'inférer peut être considéré comme anonyme.

[83] https://www.cnil.fr/fr/lanonymisation-des-donnees-un-traitement-cle-pour-lopen-data
[84] https://www.cnil.fr/sites/default/files/atoms/files/wp216_fr.pdf

Santé
Quels enjeux des données détenues par les centres de santé ?

Les mutations technologiques induisant la massification des données de santé conduisent à s'interroger sur les enjeux éthiques liés à la collecte, le traitement et l'exploitation de ces données.

Les données de santé ne se limitent pas aux données recueillies dans un cadre médical (données cliniques, caractéristiques génomiques, mesures biologiques) ; le croisement entre plusieurs sources de données peut dévoiler l'état de santé d'une personne.

Dans un rapport rendu public en 2019, le Comité consultatif national d'éthique (CCNE) rappelle que *« la relation de soin se fonde sur une relation humaine directe, basée sur la confiance et un ensemble de décisions véritablement partagées entre le médecin et le patient, même si l'informatisation des systèmes de soin est maintenant généralisée. »* Ainsi, le rapport met en garde sur la fragilisation de principes éthiques par l'utilisation des données massives :

- le secret médical qui peut se voir fragilisé par la multiplication des informations partagées et échangées entre divers corps médicaux et autres organisations extérieures au domaine médical ;
- la responsabilité de la décision médicale soumise au risque d'automatisation sous l'effet de la multiplication des logiciels algorithmiques ;
- la relation personnelle entre le médecin et son patient s'appauvrissant à mesure que les innovations technologiques de traitement des données massives ramènent le patient à un ensemble de données à interpréter.

En ce sens, le CCNE considère que le numérique doit rester un outil d'aide à la décision médicale mis à profit d'un gain de temps d'écoute, d'échange et de prise en compte spécifique des besoins du patient.

Les données sont, par ailleurs, essentielles aux performances de la recherche médicale. Il faut donc qu'un équilibre se crée entre la « sous-exploitation des données limitant des recherches menées dans l'intérêt général » et le « partage des données trop large et insuffisamment contrôlé mettant en cause les droits fondamentaux de la personne. »

Le CCNE précise également que l'utilisation des avancées technologiques dans le domaine de la santé dans un cadre extérieur au parcours de soin – réseaux sociaux, applications, objets connectés, plateformes web – peut porter atteinte au travers d'informations déloyales, du non-respect du consentement à la diffusion, à l'hébergement et à la réutilisation des données de santé.[85]

Par ailleurs, la « grève du codage » observée dans de nombreux hôpitaux et Etablissement d'hébergement pour les personnes âgées dépendantes (EHPAD) au cours des derniers mois traduit la difficile liaison de la gestion des données dans le milieu hospitalier. En arrêtant la

[85] Comité Consultatif national d'Ethique (2019), *Données massives et santé : Une nouvelle approche des enjeux éthiques,* Saisine de la Ministre de la Santé en janvier 2017

transmission des données relatives aux patients via les logiciels adaptés, l'Assurance Maladie s'est retrouvée dans l'incapacité de facturer les actes réalisés.

Dénonçant l'inadéquation de la relation entre travail et collecte des données, ainsi que l'informatisation massive des établissements de santé, la « grève du code » considère que malgré des avantages concrets apportés par les outils numériques dans ce secteur – centralisation des informations, accélération et simplification des transmissions – la numérisation des données de santé, et plus particulièrement en milieu hospitalier, demeure complexe[86]. Les logiciels ne sont pas coordonnés sur tout le territoire mais peuvent être différents d'un établissement à l'autre et le temps dévolu à la saisie médicale reste encore trop long.

Depuis la Loi Informatique et Libertés, les données relatives à la santé des personnes se sont vues reconnaitre un caractère sensible ; leur utilisation est très encadrée. Ainsi, les données sur la santé des personnes peuvent être utilisées et communiquées dans des conditions spécifiques et seulement dans l'intérêt du patient[87] : suivi médical, diagnostics, soins, prévention, recherche médicale, statistiques de santé, évaluation des pratiques de santé.

Si la valorisation des données de santé peut contribuer à l'avancée de la recherche médicale, elle peut également s'apparenter à une forme de « marchandisation de la santé ».

Le Health Data Hub, dont la création a été entérinée par la loi du 24 juillet 2019 relative à l'organisation et à la transformation du système de santé et dont le déploiement a été accéléré par la crise sanitaire de la Covid-19, doit regrouper les données des hôpitaux publics, de la médecine libérale, de l'Assurance Maladie ou encore des pharmacies. Cette initiative, en permettant une ouverture des données de santé profitable au bien commun (en accès ouvert aux acteurs publics et privés), doit être encadrée afin d'éviter les dérives connues par le Royaume-Uni dans l'affaire de la NHS[88].

La CNIL s'inquiète des transferts des données en dehors de l'Union européenne[89]. Le 21 avril 2020, le gouvernement français a publié un arrêté autorisant le Health Data Hub et la Caisse nationale de l'assurance-maladie à collecter de nombreuses données « aux seules fins de faciliter l'utilisation des données de santé pour les besoins de la gestion de l'urgence sanitaire et de l'amélioration des connaissances sur le virus Covid-19 »[90]. À ce titre, seraient récoltées les données relatives au Système National des Données de Santé (SNDS) qui regroupe « les données de pharmacie », les « données de prise en charge en ville telles que les diagnostics ou des données déclaratives de symptômes issues d'applications mobiles de

[86] Zielinska A. et Pegny M. (2020), « L'épineuse question des données numériques de santé, The Conversation
[87] CNIL « Données sur la santé des personnes, des données sensibles ? »
[88] L'affaire de la NHS renvoie à la vente des données de santé de millions de patients de la NHS à des entreprises pharmaceutiques américaines ; Amazon ayant un accès aux données de la NHS https://www.theguardian.com/commentisfree/2019/dec/09/nhs-data-goldmine-value-private-companies
[89] Hourdeaux J. (2020), « La CNIL s'inquiète d'un possible transferts de nos données de santé aux Etats-Unis », Mediapart
[90] Arrêté du 21 avril 2020 complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de covid-19 dans le cadre de l'état d'urgence sanitaire - Article 1

santé et d'outils de télésuivi, télésurveillance ou télémédecine », les données des laboratoires, les données des services d'urgence, les données issues du système de suivi des victimes lors de catastrophes sanitaires (SI-VIC) ou encore les données issues des programmes de médicalisation des systèmes d'information qui comptabilisent les actes médicaux facturés dans les hôpitaux.

A ce propos, de multiples acteurs, dont la CNCDH, ont exprimé leurs inquiétudes concernant les systèmes d'information mis en place. Le 9 juin 2020, une quinzaine de personnalités et d'organisations ont ainsi déposé un référé-liberté contre le déploiement, accéléré suite à la situation d'état d'urgence sanitaire, de la plateforme dont l'hébergement a été confié à Microsoft[91].

Le 19 juin a été adopté par le Conseil d'Etat, l'ordonnance n°440916. Ce texte ordonne que la Plateforme des données de santé fournisse à la CNIL tout éléments relatifs aux procédés de « pseudonymisation » utilisés afin d'en analyser le niveau de protection avant de les fournir au secrétariat du contentieux du Conseil d'Etat pour justifier les mesures prises en conséquence.

Assurance
Les données au cœur du secteur assurantiel

Le secteur de l'assurance accompagne toute personne tout au long de sa vie afin de lui permettre de faire face aux aléas. Les données sont au cœur des activités de ce secteur, et la protection de la vie privée doit être une priorité. Florence Picard, présidente de la Commission scientifique de l'Institut des actuaires, confirme ainsi que les données constituent « la matière première des assureurs, et ont toujours été utilisées pour l'évaluation du risque. »[92]

La collecte et l'exploitation des données doit donc se faire de manière responsable et dans le cadre des exigences règlementaires en vigueur. Les données collectées par les assurances sont utilisées afin d'obtenir une relation contractuelle pérenne avec les assurés. Le RGPD a provoqué des changements profonds dans le secteur[93] :

- Les compagnies d'assurance sont désormais amenées à sécuriser les données stockées dans le cadre de leurs activités. Par exemple, tant que les contrats assurantiels demeurent actifs, les compagnies doivent s'engager à protéger les données leurs clients ;
- La conservation des données personnelles se voit limitée dans le temps en effaçant les données de leurs « prospects », si ceux-ci n'ont pas souscrit à un contrat, dans un délai de 3 ans. Le délai est allongé à 10 ans pour les clients après la fin d'une relation contractuelle. Par ailleurs, prospects et clients peuvent demander – comme dans tous les secteurs – la suppression totale des données les concernant ou bien leur modification ;

[91] Mediapart (2020), « Le Health Data Hub attaqué devant le Conseil d'Etat »
[92] Ligue des Droits de l'Homme (2017), « Big Data, Algorithmes et risques de discriminations, l'exemple de l'assurance »
[93] *L'impact du RGPD dans le secteur de l'assurance*, Données et RGPD, décembre 2019

- Les traitements ayant lieu sur les données des prospects et des clients doivent être consignés dans un registre des traitements automatisés.

Slimane Laoufi[94], chef du pôle emploi, biens et services privés au Défenseur des droits, estime que l'enjeu central pour les assurances demeure la lutte contre les discriminations. Les algorithmes servant à profiler les individus, les assurances doivent redoubler de vigilance dans l'utilisation faite des données récoltées afin de lutter contre les discriminations et les refus de demande d'assurance ou encore l'octroi de produits sous conditions.

2. L'échange des données

L'économie de la donnée s'impose dans l'économie française et internationale, et est au cœur du développement économique des entreprises. Ainsi, la transformation numérique de l'économie devient une réalité du marché pour les entreprises[95]. L'explosion de la donnée via la multiplication des sources et des formats, l'évolution de leur nature et la capacité des entreprises à les collecter, les analyser et les exploiter constituent des éléments concurrentiels majeurs. En 2018, le marché du *big data* européen s'élevait à 250 milliards d'euros. Le potentiel du *big data* a été perçu tout d'abord par le secteur de la finance puis par le secteur de la santé, le domaine public, et aujourd'hui la grande majorité des secteurs économiques.

Dans une optique de performance, l'échange de données se révèle être une pratique au haut potentiel, permettant de donner un avantage concurrentiel certain aux entreprises.

Par ailleurs, la numérisation croissante des entreprises participe à la construction d'un « horizon numérique collectif »[96]. Dans une logique de performance économique et d'intérêt collectif, les données gagnent à être partagées entre différents secteurs d'activités et entre différents acteurs d'un même secteur et d'un même territoire ou de plusieurs territoires.

Dawex[97] – une plateforme d'échange de données – considère que, pour les entreprises, la première étape pour recueillir, analyser et mettre les données au cœur de nouveaux usages est d'établir un inventaire de toutes les données générées, de les catégoriser et de définir une stratégie adaptée à chaque typologie de donnée. L'échange de données se fait à 71 % entre entreprises issues de différents secteurs ; la libre circulation des données et la fluidité des échanges favorisent l'innovation. Par ailleurs, le partage des données et les relations entre divers secteurs ne signifient pas la perte de contrôle et de propriétés des données détenues par les entreprises. Dawex conseille, en ce sens, que les modalités d'échanges de données soient discutées en amont et fassent l'objet d'un

[94] Ligue des Droits de l'Homme (2017), « Big data, Algorithmes et risques de discriminations, l'exemple de l'assurance »
[95] « Transformation numérique : comment l'économie de la donnée impacte les architectures informatiques », Evernote
[96] Idem
[97] L'Usine Digitale (2019), *« Développer une stratégie d'échange de données, un enjeu d'avis pour les entreprises françaises »*

contrat de licence afin de garantir la responsabilité de chacune des parties. La mise en place d'une telle stratégie constitue une étape fondamentale dans le maintien de la gouvernance des données par l'entreprise.

Le « rapport Villani » paru en 2018[98] rappelle que les données constituent majoritairement le point de départ des stratégies en IA. Pourtant, les données bénéficient surtout à quelques grands acteurs plutôt qu'à la majorité de l'économie. Afin de rééquilibrer les rapports de force, il semble nécessaire que l'accès aux données soit généralisé, que leur circulation soit meilleure afin d'en faire bénéficier les pouvoirs publics, les acteurs économiques plus petits et la recherche publique.

Cédric Villani recommande, en ce sens, que la puissance publique amorce de nouveaux modes de production, de collaboration et de gouvernance sur les données par la création de « communs de données », c'est-à-dire des ressources dont l'usage et la gouvernance sont définis par une communauté précise. L'Etat pourrait ainsi jouer le rôle de tiers de confiance afin d'inciter les entreprises au partage et à la mutualisation de leurs données.

A titre d'exemple l'Echange de Données Informatisées (EDI) permet de faire communiquer, de manière automatisée, les systèmes informatiques de plusieurs partenaires commerciaux. Ce procédé qui a débuté au travers des bons de commande et des factures s'est étendu massivement dans les entreprises afin que celles-ci puissent communiquer de manière pérenne avec leurs parties prenantes.

La connexion des systèmes contribue à améliorer les relations entre producteurs et distributeurs et a aussi des effets positifs pour une majorité des départements de l'entreprise. Ainsi, au niveau commercial, l'échange de données informatisé permet d'améliorer la relation entre les clients et les fournisseurs et d'obtenir une fiabilisation des échanges et un gain de temps sur les étapes entourant les cycles de vente. Au niveau de la production, les tâches administratives diminuent, la communication est plus efficace et les cycles de production sont améliorés. Et, au niveau de la logistique, l'EDI permet la diminution des délais de traitement et une baisse du niveau des réclamations clients. Pour de nombreuses organisations, l'EDI facilite les relations avec les Commissaires aux Comptes.

L'association Newmeric considère que la « véritable promesse des données est de générer à la fois de la performance économique et du bien-être sociétal » [99] ; s'opère ainsi un changement de paradigme ou l'enjeu n'est plus de posséder toujours plus de données mais de « réunir les conditions de leur circulation pour en faire une richesse individuelle et collective. » Pour y parvenir, de nouveaux modèles de mise en circulation des données privées deviennent nécessaires, fondés sur la souveraineté, la réciprocité et le partage de la valeur créée par les données. L'association développe ainsi le concept d'« économie circulaire de la donnée ». L'économie circulaire de la donnée est

[98] Villani C. (2018), *Donner un sens à l'intelligence artificielle, pour une stratégie nationale et européenne*, rapport au Premier ministre (lien)
[99] L'économie circulaire de la donnée, Newmeric https://newmeric.eu/innover

un modèle de mise en réseau des données de l'entreprise au sein d'un écosystème étendu à l'environnement territorial, sectoriel ou sociétal, dans l'objectif de créer des *« boucles de valeur réciproque qui associent performance économique et contribution à des intérêts collectifs ».*

Les données qui créent cette valeur réciproque entre l'entreprise et les réutilisateurs de ses données, sont dites des données circulaires. La valeur des « données circulaires » s'appuie sur trois facettes : la valeur partagée à l'origine d'une performance collective ; la valeur responsable grâce à laquelle l'entreprise peut faire valoir le sens de ses objectifs et démontrer la performance de sa mission ; et la valeur co-construite qui fait fructifier les ressources informationnelles communes et les régénère.

Newmeric développe en partenariat avec l'Institut Mines-Télécom et son équipe d'experts, la méthode C.I.R.C.U.L.A.R dont la vocation est de faciliter et accélérer les processus de constitution de réseaux de données à valeur ajoutée. La méthode est construite autour de trois phases :

- Une phase de cadrage permettant d'identifier les enjeux de l'entreprise au croisement de sa stratégie relative aux données et de sa raison d'être, et de rechercher les cas d'usage de partage des données en matière d'opportunités de valorisation ;
- Une phase de design permettant de réunir les conditions nécessaires au partage des données : conditions règlementaires, bonnes pratiques, gouvernance, interopérabilité, etc. ;
- Une phase d'évaluation de la valeur économique et sociale visant à développer un modèle d'affaires côté « Offre » qui soit adapté au modèle économique de la « Demande ».

Le partage des données agricoles

Le secteur agricole demeure l'un des secteurs les plus impactés par la transition numérique au travers du volume de données dont il dispose[100] : données issues des outils utilisés par les agriculteurs et les coopératives agricoles (provenant de satellite, de capteurs au sol, d'outils mécaniques) et données issues des opérations de distribution (provenant des informations du marché). Ainsi, en raison de sa compétitivité intrinsèque, les enjeux économiques autour de l'utilisation des données sont importants.

Les premiers systèmes d'Internet des Objets (IdO) ont été consacrés à la récolte de données météorologiques, qui sont rapidement devenues indispensables aux prévisions agricoles. Par la suite, les tracteurs et véhicules spécialisés ont fait partie des premiers véhicules soumis à l'IA et à l'autonomisation. Aujourd'hui, les exploitants agricoles sont nombreux à utiliser des drones afin de surveiller leurs cultures et l'agriculture de précision utilise l'imagerie satellite pour optimiser la production.

Néanmoins, ce secteur est confronté à différents enjeux. D'une part, les données proviennent de sources diverses et prennent de multiples formes, leur connexion doit permettre à tous les acteurs d'en faire un usage égal et raisonné. D'autre part, il semble nécessaire de réunir les acteurs du secteur autour d'un modèle économique satisfaisant pour toutes les parties prenantes. À titre d'exemple, un supermarché sera intéressé par la qualité des produits issus des abattoirs, tandis qu'un éleveur sera intéressé par les prévisions de vente des qualités de viande pour ajuster leur prix. Ces deux acteurs doivent ainsi pouvoir se retrouver autour d'un modèle économique égalitaire.

Le ministère de l'Agriculture et de l'Alimentation[101] estime majeur le partage des données agricoles. Les transformations numériques permettront aux agriculteurs de consacrer davantage de temps à la compréhension de leurs exploitations et à la prise de décisions stratégiques. Les outils numériques tendent à faciliter le travail agricole et l'utilisation des données collectées donnent une connaissance grandissante de la production. Ces données doivent, toutefois, être utilisées dans l'intérêt des agriculteurs et non contre leur gré, au profit d'un monopole numérique duquel ils déprendraient.

Ainsi, le partage de données pour les entreprises, de secteurs similaires ou différents, peut constituer une source d'innovation non négligeable et d'une meilleure performance. Par ailleurs, la mise en commun de jeux de données dans une perspective d'intérêt général entraîne la responsabilisation accrue des acteurs économiques qui s'insèrent dans des logiques de réciprocité et de confiance.

[100] Blog de l'Institut Mines-Telecom (2019), « Le partage des données : un enjeu du secteur agricole »
[101] https://agriculture.gouv.fr/le-partage-des-donnees-un-enjeu-majeur

3. Quelle souveraineté sur les données ?

En octobre 2019, le Sénat a publié un rapport, porté par Gérard Longuet, sur le devoir de souveraineté numérique[102]. Appelant à ne pas se résigner et à ne pas tomber dans la naïveté, ce rapport établit les constats suivants :

- Les citoyens ne sont pas une somme de données à exploiter ;
- Le cyberespace est devenu un lieu d'affrontement mondial, où s'exercent luttes d'influence, conflits d'intérêts et logiques sociale et économiques divergentes ;
- La révolution numérique et la maîtrise des données ont fait émerger des acteurs économiques capables de rivaliser avec les États.

À ce titre, le rapport préconise de répondre à une « quadruple remise en cause pour conserver notre souveraineté numérique » au travers de la Défense, de l'ordre juridique, de l'ordre économique et des systèmes fiscaux et monétaires.

Le rapport met ainsi en évidence que les moyens dédiés à la cyberdéfense et à la lutte informatique défensive doivent être renforcés. Il expose que la souveraineté de l'État se voit remise en cause par la révolution des données et l'activité des géants du numérique – majoritairement établis à l'étranger – qui collectent et exploitent massivement les données personnelles des Français et des européens, et échappent aux contraintes juridiques en vigueur dans ces espaces. Considérant le poids économique des Gafam, dont la capitalisation boursière est deux fois plus élevée que celle du CAC40, le Sénat appelle à la vigilance des autorités françaises et européennes. Par ailleurs, l'économie numérique favorise la constitution de monopoles d'entreprises conduisant à des abus de concurrence. Les systèmes fiscaux et monétaires s'en trouvent également impactés.

La commission d'enquête sénatoriale a établi cinq recommandations majeures : définir une stratégie nationale numérique, inscrire l'effort pour la souveraineté numérique dans le temps, protéger les données personnelles et les données économiques stratégiques, adapter la réglementation aux nouveaux défis numériques et utiliser les leviers de l'innovation et du multilatéralisme.

La massification des données détenues par les entreprises et l'internationalisation croissante de leurs activités rend la souveraineté sur les données complexe aussi bien au niveau étatique qu'au niveau des entreprises.

Ainsi, la question de la souveraineté des données des entreprises constitue un enjeu essentiel. En 2013, Fleur Pellerin, alors ministre déléguée chargée des PME, de l'innovation et de l'économie numérique, déclarait à l'Assemblée Nationale[103] : « Nous prenons aujourd'hui conscience, peut-être un peu tard, de la nécessité d'être moins dépendants des infrastructures, des plateformes ou des points d'accès à internet autres qu'européen. La nécessité d'avoir un *cloud* souverain se pose avec une grande acuité. »

[102] Longuet G. (2019), Rapport n°7 (2019-2020) de M. Gérard Longuet, fait au nom de la commission d'enquête sur la souveraineté numérique, déposé le 1er octobre 2019 au Sénat
[103] Arnulf S. (2013), « Avec l'affaire Prism, la nécessité d'avoir un cloud souverain se pose, selon Fleur Pellerin », *L'Usine Digitale*

La souveraineté sur les données signifie que les données sont soumises aux lois du pays où elles sont stockées et utlisées. Ainsi, en France, l'utilisation et la gestion des données relatives au respect de la vie privée sont régies par le droit national en vigueur et le droit européen sous le prisme du RGPD.

La question des entreprises multinationales se pose. Leur surveillance par des instances policières et judiciaires soulève des interrogations. L'entreprise a intérêt à être mondiale pour ses clients, mais nationale pour les organisations à qui elle rend des comptes.

Pour l'État français favoriser l'émergence d'un *cloud* souverain, c'est-à-dire un service indépendant, de droit français, avec une localisation des données en France, est un enjeu clef, pour soutenir la compétitivité des entreprises françaises.

Selon des données communiquées à *L'Usine nouvelle* par le cabinet Pierre Audoin Consultants[104], les plus gros acteurs du marché du *cloud computing* français sont (données de 2016) :

- Atos avec un chiffre d'affaires de 950 millions d'euros ;
- Orange avec un chiffre d'affaires de 330 millions d'euros ;
- Capgemini avec un chiffre d'affaires de 225 millions d'euros ;
- OVH avec un chiffre d'affaires de 165 millions d'euros.

L'échec du « Projet Andromède » : le *cloud* de Numergy et Cloudwatt

Deux plateformes de *cloud computing* françaises, Numergy porté par SFR et Bull (filiale de Atos), et Cloudwatt, porté par Thalès et Orange, ont fait leur entrée dans le marché français de *cloud computing* en 2012, dans le but de créer un « *cloud* souverain » français.

Dans cette filière riche de 400 acteurs selon l'Afnic, l'office d'enregistrement des noms de domaines désigné par l'État, cette entrée sur le marché a été considérée comme de la concurrence déloyale, du fait de la participation de l'État dans ces deux nouvelles sociétés par le truchement de la Caisse des dépôts et consignations, via les investissements d'avenir.

L'investissement initial est de 225 millions d'euros dans chacune des plateformes, dont 75 millions d'euros de l'État, ce qui peut paraître peu face aux milliards investis par les géants américains[105].

Le projet est un échec, principalement pour des raisons financières. Orange a débranché son service Cloudwatt en février 2019[106], après avoir racheté la totalité de ses parts à l'État et à Thalès en 2015. SFR avait également racheté la totalité des parts à l'État et à Bull en 2016, à la suite d'une procédure de sauvegarde.

[104] *L'Usine Nouvelle* « Orange à la manœuvre pour relancer son Cloud souverain Cloudwatt » (20/02/2018)
[105] Ibid.
[106] Dèbes F. (2019), « Une page se tourne pour le cloud souverain français », *Les Échos*

Le but de ces plateformes était de créer un *cloud* souverain grâce à des *data centers* localisés en France, afin de mettre à l'abri des données sensibles en France, à l'abri d'intrusions de gouvernements étrangers.[107]

Stratégie nationale pour la sécurité du numérique

Présentée par le Premier ministre le 16 octobre 2015, la Stratégie nationale pour la sécurité du numérique est destinée à accompagner la transition numérique de la société française. Il s'agit de trouver un bon équilibre entre prise en compte de la sécurité et dynamisme économique, afin de faire face aux menaces protéiformes liées au détournement du numérique par des individus malveillants et des organisations criminelles ou terroristes.

Cette stratégie est divisée en cinq objectifs stratégiques :

1. Intérêts fondamentaux, défense et sécurité des systèmes d'information de l'État et des infrastructures critiques, crise informatique majeure ;
2. Confiance numérique, vie privée, données personnelles, cybermalveillance ;
3. Sensibilisation, formations initiales, formations continues ;
4. Environnement des entreprises du numérique, politique industrielle, export et internationalisation ;
5. Europe, souveraineté numérique, stabilité du cyberespace.

« *Cloud* de confiance » français

A la suite de l'échec du « *cloud* souverain » représenté par le Projet Andromède, Bruno Le Maire, ministre de l'Économie, a annoncé vouloir bâtir un « c*loud* de confiance » tricolore à partir de 2020.[108]

Courant 2019, le ministre a donc sollicité Dassault Systèmes, maison mère d'Outscale, et OVH afin de travailler sur un *cloud* permettant de mettre à l'abri les données les plus sensibles de l'État et des entreprises face à l'extraterritorialité des lois américaines. [109]

Les Echos rapportent que « Organisés en comité stratégique de filière (CSF), les acteurs français du *cloud* et de la cybersécurité participent depuis plusieurs mois aux débats avec les autorités afin de définir les impératifs techniques et juridiques du *cloud* de confiance. Début octobre, le ministre a signalé avoir demandé aux Français OVH et Outscale (Dassault Systèmes) de lui remettre leurs propositions en décembre. »[110]

La direction interministérielle des systèmes d'information de l'Etat (Dinsic) a défini trois niveaux de protection en fonction de la sensibilité des données, ce qui correspondra à différents types d'appels au marché. Pour les informations sensibles, les hébergeurs

[107] https://www.usinenouvelle.com/article/le-cloud-de-numergy-et-cloudwatt-c-est-de-la-concurrence-deloyale.N181536
[108] Dèbes F. (2019), « La France cherche son cloud de confiance », Les Echos
[109] Filippone D. (2019), « OVH-Outscale : le cloud souverain vraiment ressucité ? », LeMondeInformatique
[110] *Op.cit.*

devront répondre aux exigences du label SecNumCloud de l'ANSSI (cf. ci-dessous) et pour les informations les plus sensibles, l'Etat construira sa propre infrastructure.

Référentiel SecNumCloud de l'ANSSI, agence française de cyberdéfense

En 2016, l'Agence nationale pour la sécurité des systèmes d'informations (ANSSI) a lancé deux référentiels, correspondant à un « Visa de Sécurité » ANSSI, en vue de permettre la qualification de prestataires de services *cloud*. Sont concernés les prestataires d'informatique en nuage offrant des services de type SaaS (*Software as a service*), PaaS (Platform as a service) et IaaS (Infrastructure as a service) et souhaitant obtenir un visa de sécurité ANSSI.

Le référentiel SecNumCloud conjugue ainsi des exigences relatives au prestataire de service informatique *cloud*, à ses salariés et à la localisation des données des clients au sein de l'Union européenne.[111]

À la suite de l'entrée en vigueur du RGPD, SecNumCloud inclut des exigences relatives à la protection des données répondant aux attentes des besoins des entreprises, des administrations et des collectivités.

Le premier acteur *cloud* à décrocher ce référentiel est Oodrive, spécialiste français des services de travail collaboratif et du partage de fichiers. Le premier fournisseur de service *cloud* Infrastructure-as-a-Service à être labellisé est 3DS Outscale, filiale de Dassault Systèmes.

Un label franco-allemand a été lancé en 2016, « European Secure Cloud », en coopération avec l'homologue allemand de l'ANSSI, la BSI. Il est basé sur 15 règles « *techniques et organisationnelles* » communes entre SecNumCloud et le catalogue C5 allemand. [112] Malheureusement, cette action n'a pas été suivie des effets attendus : en 4 ans, l'ANSSI n'a certifié que trois acteurs locaux de petites tailles. Tous les acteurs concernés déplorent cette lenteur qui entrave les actions si utiles de certifications, en particulier en matière d'exportation.

La France et l'Allemagne proposent de créer une infrastructure commune de données sécurisées

Les ministres de l'Économie allemand et français ont conjointement annoncé le 29 octobre 2019, lors du Sommet du numérique allemand, que les deux pays allaient travailler à mettre en place une infrastructure commune de données sécurisées.[113]

Ce projet s'inscrit dans la continuité du traité d'Aix-la-Chapelle du 22 janvier 2019. La France et l'Allemagne entendent ainsi intensifier leur coopération dans les secteurs de la recherche et de la transformation numérique, notamment autour de l'intelligence

[111] https://www.ssi.gouv.fr/actualite/secnumcloud-evolue-et-passe-a-lheure-du-rgpd/
[112] https://www.ssi.gouv.fr/actualite/escloud-un-label-franco-allemand-pour-les-services-informatique-en-nuage-de-confiance/
[113] Mann N. (2019), « La France et l'Allemagne veulent créer une infrastructure de données sécurisée », L'Usine Nouvelle

artificielle et des innovations de rupture (visant à rendre accessible des processus paraissant hors de portée).

Des groupes de travail et un groupe d'entreprises ont initié le processus de création d'une solution alternative en matière de solutions de stockage, gestion et partage de données. Les résultats ont été présentés le 4 juin 2020 par les ministres de l'économie allemands et français.[114]

Bruno Le Maire a indiqué vouloir « établir une infrastructure de données européennes sûre et souveraine, incluant entrepôts de données et pools de données et développer une interopérabilité sur les données », ce qui fait écho à l'appel d'Angela Merkel « l'Europe a besoin de son propre *cloud* ».[115]

Ainsi, l'un des objectifs de projet est de briser les silos de données et de renforcer leur interopérabilité. Un autre objectif est de mettre en commun des infrastructures afin de permettre l'accès pour les industriels à des supercalculateurs partagés. Dans ce cadre, le projet a notamment pour objectif « la mise en réseau de services d'infrastructure décentralisés, en particulier d'instances en nuage et en périphérie de réseau pour former un système homogène et convivial ».

« Projet Gaia-X »

Présenté comme « l'Airbus de l'Intelligence artificielle », l'objectif du projet GAIA-X est de créer une infrastructure de données sécurisées et en réseau en Europe. Il s'agit de renforcer l'indépendance et la souveraineté du *cloud* européen contre les acteurs américains et chinois. Le projet devrait être lancé au printemps 2020, par une présentation de son contexte technique et organisationnel.[116]

Selon la feuille de route du projet, « GAIA-X renforce la souveraineté des données des milieux économiques et scientifiques, de l'État et de la société en matière de stockage, d'échanges et d'utilisation des données et des services. L'infrastructure de données en réseau met les données et les services à la disposition des applications de l'intelligence artificielle tout en protégeant les droits, les intérêts et la propriété intellectuelle en rapport avec les données et le savoir-faire associé. L'infrastructure est neutre vis-à-vis des fournisseurs et tient compte des intérêts des producteurs, des fournisseurs et des utilisateurs de données. L'écosystème élargit le savoir des acteurs européens dans leurs domaines, renforce les échanges tant à l'intérieur des domaines qu'entre ceux-ci et permet l'élaboration de modèles commerciaux innovants sur le marché unique du numérique. »[117]

Force est ainsi de constater que les exemples cités ci-dessus s'apparentent à des tentatives, plutôt qu'à des réalités. L'effectivité d'une souveraineté numérique française

[114] Portail de l'économie, des finances, de l'action et des comptes publics (2020), Concrétisation du projet « Gaia-X », une infrastructure européenne de données https://www.economie.gouv.fr/concretisation-projet-gaia-x-infrastructure-europeenne-donnees#
[115] Forbes « Le cloud souverain est mort, vive l'internet de l'Intelligence » (28/11/19)
[116] https://www.euractiv.com/section/digital/news/european-cloud-network-to-start-in-late-2020/
[117] Ministère fédéral allemand de l'Economie et de l'Energie (2019), Le Projet Gaia-X, une infrastructure de données en forme de réseau, berceau d'un écosystème européen vital (lien)

et européenne fait l'objet de débats et de dispositifs/projets multiples. Leurs échecs et la temporalité dans laquelle ils s'inscrivent démontrent la complexité d'une économie de la donnée en constante croissance.

Une Europe numérique

Le Conseil de l'Union européenne[118]

En décembre 2018, l'UE a établi un programme de financement « Europe numérique » – couvrant la période 2021 - 2027 – afin d'accompagner la transformation numérique des sociétés et des économies européennes. L'objectif de ce programme financier est de contribuer à ce que l'ensemble des particuliers et des entreprises puissent profiter des avantages de la transformation numérique. Ce programme passera par le financement de projets issus de cinq domaines : le calcul à haute performance, l'intelligence artificielle, la cybersécurité, les compétences numériques avancées et la large utilisation des technologies numériques.

Pendant la présidence roumaine du Conseil de l'Union européenne du 1er janvier au 30 juin 2019, Alexandru Petrescu, ministre des communications et de la société de l'information de la Roumanie, a affirmé que « *Le programme pour une Europe numérique aidera les entreprises européennes, en particulier celles de petite taille, à tirer parti des vastes possibilités qu'offre la transformation numérique, ainsi qu'à se développer et à gagner en compétitivité.* »

La Commission européenne[119]

En décembre 2019, le collège de Commissaires de la nouvelle Commission européenne présidée par Ursula von der Leyen est entré en fonction.

Les données, et plus largement l'avenir du numérique de l'Europe, constituent l'une des cinq priorités énoncées dans le programme de la Présidente. Considérant les données comme le cœur de la transformation de l'économie et de la société, la Commission européenne entend créer un espace européen unique des données où les données à caractère personnel et non personnel – telles que les données industrielles sensibles – soient en sécurité. Ce marché unique des données permettrait aux entreprises d'avoir un accès facilité à une grande quantité de données industrielles afin de stimuler la croissance tout en réduisant l'empreinte carbone et environnementale humaine.

Dans un premier temps, la Commission souhaite mettre en place un cadre législatif pour la gouvernance des espaces européens communs des données. Ensuite, elle s'efforcera d'ouvrir davantage de données issues du secteur public en vue de leur réutilisation – notamment par les PME. Enfin, la Commission entamera une réflexion législative sur l'incitation des acteurs d'une même économie à partager leurs données[120]. Par ailleurs, la transformation verte et la transformation numérique « constituent deux défis indissociables »[121].

[118] https://www.consilium.europa.eu/fr/press/press-releases/2018/12/04/digital-europe-programme-council-agrees-its-position/
[119] https://ec.europa.eu/commission/presscorner/detail/fr/FS_20_283
[120] https://www.flexsi.fr/2020/02/21/strategie-europenne-donnees/
[121] Communication de la Commission au Parlement européen, au Conseil, au Comité économique et social européen et au comité des régions – Façonner l'avenir de l'Europe, février 2020

4. Intelligence artificielle et usage des données

L'intelligence artificielle s'est imposée comme une « technologie stratégique »[122] offrant de nombreux avantages aux entreprises, aux citoyens et à la société dans son ensemble. Selon le Livre Blanc de la Commission européenne sur l'IA, elle doit être éthique, durable, axée sur le facteur humain et respectueuse des valeurs et droits fondamentaux. En augmentant les capacités productives des entreprises, elle permet de renforcer la compétitivité des entreprises et d'améliorer le bien-être des citoyens et de favoriser la croissance de nombreux secteurs d'activités[123] ; elle met ainsi en exergue la responsabilité des entreprises.

Dans le domaine de l'agroalimentaire, les applications d'analyse de données en temps réel permettent aux producteurs d'optimiser leurs rendements et leurs profits.

Dans le secteur de la santé, l'INSERM affirme que l'IA permet d'améliorer la qualité des soins et permet à la médecine de se perfectionner – opérations assistées, suivi des patients à distance, traitement personnalisé.

Le rapport Villani a montré que l'IA peut être un outil d'opportunités environnementales grâce à l'optimisation des ressources énergétiques – via la gestion des consommations des *data centers* – ou à la protection à la biodiversité via la reforestation par les drones.

Dans le secteur financier, l'IA révolutionne la collecte des informations et des relations entre les conseillers et les clients.

Le secteur des transports se voit également renforcé par l'IA – métros, VTC, navires, drones de livraisons, etc. – ; des transformations majeures sont à venir au travers, notamment, des véhicules autonomes.

L'usage des données dans le temps

Les données sont soumises à différents types d'usages[124] et leur utilisation plus ou moins intrusive nécessite des réponses différenciées :

- Usage statistique anonyme : cas classique d'utilisation des données utilisé depuis la fin du 18e siècle ;
- Usage à des fins de publicité ciblée : usage reposant sur des informations parcellaires fournies par les utilisateurs à partir d'informations s'inscrivant dans un but marchand ;
- Usage à des fins de fixation de prix individualisé : pratiques existant notamment dans les plateformes de transport et de logement – aucune réglementation n'existe aujourd'hui ;
- Vente de fichiers d'informations personnelles : pratique qui n'est pas interdite, l'entreprise doit simplement notifier qu'elle y a recours ;

[122] Commission européenne (2020), *Livre blanc. Intelligence artificielle, une approche européenne axée sur l'excellence et la confiance*
[123] *Les trois avantages de l'intelligence artificielle*, isatech, janvier 2019
[124] Audition de Mme Valérie Charolles

- Intrusions ou actes malveillants : enjeu pour toutes les entreprises, notamment les entreprises traitant de sujets sensibles.

Les jumeaux numériques[125]

Le concept de jumeaux numériques désigne la réplique d'un objet, d'un système, d'une implantation ou d'un processus sous une forme numérique.

Il existe deux grands d'approche des jumeaux numériques :
- Une approche « *bottom-up* » dans laquelle on part d'un actif équipé de capteurs qui récupèrent les données qui en sont issues. Grace aux techniques d'IA – *machine learning, deep learning* – cette approche permet de construire des modèles de prédiction.
- Une approche « *top down* » où les équations issues de la physique sont nourries de mesures et résolues numériquement afin de prédire des comportements.

Les jumeaux numériques ont révolutionné le secteur industriel en modifiant la phase de développement d'un produit ou l'utilisation d'un équipement. Auparavant l'entreprise créait physiquement un objet afin de lui faire subir des tests et y apporter des modifications ; aujourd'hui les données recueillies sur l'évolution de l'objet permettent d'anticiper les risques et d'optimiser les performances.

Le secteur de la santé s'est également vu amélioré par l'émergence des jumeaux numériques, au travers de différentes méthodes : test de traitements sur des patients virtuels, simulation d'opérations complexes, amélioration de dispositifs médicaux tels que les prothèses, etc.

L'accroissement de l'intelligence artificielle

L'intelligence artificielle occupe une place grandissante dans nos modes de vie et dans les processus de fonctionnement des entreprises. Une étude réalisée par l'International Data Corporation en 2017[126] analysait la montée progressive de l'IA au travers de trois variables : les dépenses, les cas d'usage et les raisons poussant les entreprises à investir.

L'IDC prévoit une multiplication par six des dépenses relatives à l'IA d'ici cinq années – de 2017 à 2021 – grâce à la montée en compétences des secteurs des télécommunications (+61,5 % d'augmentation des dépenses), de la santé (+58,3 % d'augmentation des dépenses) et du commerce de détails (+57,8 % d'augmentation des dépenses).

Par ailleurs, l'étude estime que les cas d'usage de l'IA vont fortement se multiplier et ce, notamment, dans les recommandations et conseils de vente en magasin, dans les opérations de merchandising pour les opérations omnicanales, dans les systèmes de diagnostic et de traitement des problèmes ou encore dans la gestion des flottes et des actifs. Ainsi, les raisons majeures poussant les entreprises à investir dans l'IA se

[125] *Journal du Net (2019), « Jumeau numérique : l'IoT au service de la simulation »*
[126] https://idc.fr/infographies/index/lia_en_france_tendances_et_chiffres_cles

retrouvent dans la réduction des coûts au profit d'une amélioration de la productivité et de l'efficacité, dans l'accroissement de la qualité des produits et des services, dans l'amélioration des supports et relations clients ainsi que dans l'amélioration des systèmes IT et des opérations marketing.

En 2018, une étude menée par PwC[127] identifiait huit impacts majeurs de l'intelligence artificielle sur les entreprises et sociétés, à court terme :

- l'intelligence artificielle aura un impact sur les employeurs avant que cela n'affecte l'emploi ;
- les cas d'usage à plus forte valeur ajoutée vont rapidement se préciser et se généraliser ;
- beaucoup d'entreprises ne savent pas encore comment valoriser leurs données et l'IA va pouvoir les aider à relever ce défi ;
- les spécialistes fonctionnels, et non les techniciens, décideront de la course aux talents de l'IA ;
- les cyberattaques seront plus puissantes à cause de l'IA, mais la cyberdéfense le sera aussi grâce à l'IA ;
- ouvrir la « boite noire » de l'IA deviendra une priorité ;
- les nations se disputeront l'IA ;
- la pression pour une IA responsable ne concernera pas uniquement les entreprises de technologie.

Utilisée depuis la fin des années 1950[128], l'IA reste soumise à l'appréciation encore mitigée des entreprises. Même si de nombreuses entreprises utilisent l'IA ou envisagent de l'intégrer dans leur modèle, et malgré une montée en puissance de la *data* dans les modèles organisationnels et professionnels des entreprises, des freins restent encore très présents.

Aujourd'hui, plus d'une entreprise sur deux collecte des données et plus de deux entreprises sur trois hébergent leurs données dans le *cloud*. Les entreprises interrogées par PwC admettent l'utilité de l'IA pour améliorer la connaissance et l'expérience client, augmenter leur efficacité opérationnelle, renforcer la détection des fraudes, la mise en conformité aux cadres législatifs existants ou encore gestion des risques. À ce titre, plus de 40 % des grandes entreprises s'appuient sur des techniques de l'IA pour pallier aux risques de cyberattaques.

Néanmoins, 65 % des répondants estiment que les entreprises ne sont pas ou peu matures en matière d'exploitation des données et 47 % d'entre eux estiment que leur entreprise n'est pas ou peu mature en la matière.

Le premier facteur qui freine le déploiement de l'IA est humain : les directions et les équipes manquent de connaissances (64 %) et ne sont pas formées à l'utilisation de tels procédés (57 %), et la gouvernance qui ne s'y prête pas. Dans le même temps, près

[127] http://images.content.pwc.com/Web/PwCGlobal/%7Bcc8d47f3-006e-4bf5-993a-ca17640b7dcc%7D_PwC_Etude_AI_Big_Data_2018_Web.pdf
[128] McCorduck 2004, pp. 111–136, Crevier 1993, pp. 49–51 and Russell & Norvig 2003, p. 17

d'une grande entreprise sur trois avoue souffrir d'un manque de confiance envers les algorithmes.

L'IA doit aujourd'hui reposer sur deux fondamentaux nécessaires à une utilisation Le 19 février 2020, la Commission européenne a publié un Livre Blanc sur la régulation de l'intelligence artificielle[129]. Au vu de la vague économique générée par la donnée, la Commission entend positionner l'Union européenne comme leader mondial de l'IA. Le Livre blanc dessine les contours d'un cadre règlementaire adapté autour de deux piliers principaux : la création d'un « écosystème d'excellence » tout au long de la chaîne de valeur et la création d'un « écosystème de confiance » qui garantisse le respect des règles de l'UE en matière de droits fondamentaux et de droits des consommateurs.

La Commission européenne souligne que l'IA peut comporter des nuisances et des biais – discriminations, risques pour la sécurité des utilisateurs, opacité des programmes, atteinte à la liberté d'expression – sur lesquels elle estime nécessaire d'agir.

Le Livre blanc propose que la législation évolue pour[130] :

- assurer l'application et la mise en œuvre efficace de la législation communautaire et nationale en vigueur ;
- encadrer la limitation de la législation communautaire ;
- prendre en considération l'évolution des fonctionnalités des systèmes d'IA ;
- clarifier la répartition des responsabilités entre les différents opérateurs économiques dans la chaine de distribution ;
- faire évoluer la notion de sécurité.

Néanmoins, la Commission ne souhaite pas déployer une règlementation trop lourde pour les TPE et PME. Elle recommande, en ce sens, d'appliquer un cadre à l'IA définie comme « à haut risque » si le secteur et l'utilisation de l'IA comportent des risques relatifs à la sécurité, aux droits des consommateurs et aux droits fondamentaux.

La liste d'obligations à suivre par les opérateurs pour l'IA à haut risque porte sur[131] :

- les données d'entrainement doivent être soumises à des exigences afin de garantir le respect des valeurs de l'UE, et en particulier des droits des citoyens ;
- la conservation des données et des dossiers doit être soumise à une exigence particulière afin pouvoir reconstituer l'historique des actions ou décisions potentiellement problématiques prises par les systèmes d'IA et de les vérifier ;
- afin de promouvoir une utilisation responsable de l'IA et renforcer la confiance des citoyens et des organisations à son encontre, il est important de fournir les informations adéquates sur l'utilisation des systèmes d'IA à haut risque – jeux de données, choix réalisés, techniques, méthodologies d'entrainement, etc. ;

129 https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf
130 *Analyse du livre blanc de la Commission européenne sur la régulation de l'IA*, Florian Renault, DPO chez Axionable, Village de la Justice, février 2020
131 Commission européenne, *Livre blanc. Intelligence artificielle, une approche européenne axée sur l'excellence et la confiance*, février 2020

- une analyse des risques susceptibles d'être générés par les systèmes d'IA précise doit être produite pour contribuer à garantir la fiabilité des systèmes d'IA ;
- le contrôle humain doit être systématique afin de contribuer à éviter qu'un système d'IA mette en péril l'autonomie humaine ou ne provoque d'autres effets néfastes ;
- l'identification biométrique à distance doit faire l'objet d'exigences spécifiques car elle comporte des risques particuliers.

IA et éthique

Les algorithmes ne doivent pas être déconnectés de l'utilisation humaine et de son impact constant sur ces processus, en effet, ce n'est pas la technologie en tant que telle qui entraine des problèmes éthiques, mais bien l'utilisation qui en est faite.

Elise Bruillon, Risk Manager chez Orange et administratrice de l'Observatoire des Réseaux Sociaux d'entreprise[132], explique que, pour les entreprises, miser sur l'intelligence artificielle constitue un moyen de surpasser les difficultés et montre une forme de « résilience à un moment où l'entreprise est en quête de sens dans sa façon de gérer son potentiel humain ». Elle considère que concilier intelligence artificielle et RSE répond donc à la volonté de l'entreprise de cadrer les usages qui en sont fait, d'identifier les risques et d'accompagner les salariés dans ces nouveaux processus.

En octobre 2018, Syntec Numérique et le Cigref ont publié un référentiel pratique pour les acteurs du numérique relatif à la relation entre éthique et numérique[133].

Le référentiel part du constat que l'IA pose des problématiques éthiques spécifiques dus au manque de transparence et d'outils de traçabilité permettant d'expliciter les résultats des algorithmes. Il précise plusieurs niveaux à prendre en considération afin de rendre les algorithmes plus éthiques :

- La sélection des jeux de données. Les jeux de données servent de base d'apprentissage aux algorithmes et peuvent ainsi véhiculer des biais cognitifs – genre, couleur de peau, handicap. Il est donc fondamental de pouvoir expliciter le contenu des données sélectionnées et utilisées par les algorithmes apprenants afin de s'assurer de leur neutralité.
- Le suivi de l'apprentissage. L'apprentissage automatique (*machine learning*) n'est pas exempt de risques de reproduction des injustices ou de discrimination. En ce sens, la supervision de cet apprentissage est fondamentale, et les phases de test avant le déploiement des algorithmes doivent devenir systématiques.
- L'acceptabilité sociale. L'impact social de certains algorithmes n'est pas négligeable, notamment lorsque ceux-ci permettent d'influencer massivement des comportements politiques par les « bulles de filtres ».

Le CCNE[134] a montré que le principe fondamental du consentement libre et éclairé est

[132] « Comment concilier Responsabilité sociale d'entreprise et intelligence artificielle ? Elise Buillon – Orange », Observatoire des Réseaux Sociaux d'Entreprise, juin 2018
[133] idem
[134] Rapport du CCNE : https://www.ccne-ethique.fr/sites/default/files/publications/avis_130.pdf

menacé par l'utilisation d'outils technologiques relatifs au *big data*. Le comité propose de responsabiliser les acteurs. À cet effet, les organisations qui manipulent des données doivent être claires sur leurs intentions et les usages faits des données qu'elles récoltent ; elles doivent également faire preuve de transparence dans les processus de collecte et d'utilisation des données personnelles et être soumises au contrôle d'acteurs tiers. Le Comité propose qu'une garantie humaine soit assurée dans les différentes étapes du processus de l'analyse des données sous le prisme de :

- la qualité et l'adéquation des données sélectionnées afin d'entrainer les algorithmes ;
- l'adéquation du choix des traitements algorithmiques à la question posée ;
- la vérification sur un jeu de données indépendantes de la robustesse et de l'exactitude du résultat donné par l'algorithme.

Le rapport Villani[135] met en exergue que les considérations éthiques soulevées par l'IA tiennent à l'opacité des technologies et à leur manque de transparence. La production des modèles algorithmiques doit être explicable, la production des interfaces plus intelligible, et la compréhension des mécanismes cognitifs doit être satisfaisante.

Les considérations éthiques doivent irriguer le développement des algorithmes. L'émergence de technologies d'IA conformes aux valeurs et normes sociales en vigueur doit se faire en mobilisant la communauté scientifique, les pouvoirs publics, les industriels, les entrepreneurs et les organisations de la société civile.

Gouverner, est-ce mesurer ?

Cette question, que les professionnels de la RSE connaissent bien, se pose pour l'utilisation des données, de manière cruciale, à l'État et aux entreprises. De nouveaux acteurs de la gouvernance de la santé mondiale apparaissent, aux côtés des organisations internationales, comme l'OMS, qui monopolisait jusqu'alors les nomenclatures et la normalisation des collectes de données dans le monde. La Bill and Melinda Gates Foundation ou le Fonds mondial de lutte contre le sida, la tuberculose et le paludisme ont créé leurs propres modes de collecte de données et d'indicateurs de performance basés sur la culture d'audit du secteur privé – dont sont précisément issus leurs principaux bailleurs de fonds. Ces organisations dépensent chacune plus de trois milliards de dollars par an (2,7 milliards d'euros), faisant d'elles des opérateurs incontournables de la lutte contre les maladies dans le monde. Elles ont ainsi créé une forme de « redevabilité épidémiologique » (*epidemiological accountability*), susceptible d'orienter les politiques nationales et multilatérales de santé publique au nom d'une « culture du résultat ».[136]

[135] Cédric Villani, *Donner un sens à l'intelligence artificielle, pour une stratégie nationale et européenne*, rapport au premier ministre, mars 2018

[136] Travaux de Grégoire Lurton, chercheur à l'Institute for Health Metrics and Evaluation (IHME) de l'université de Washington, Cité par Reverchon

Numérique et Covid-19

Durant la rédaction de ce rapport, le développement du numérique a explosé dans le cadre de la crise sanitaire provoquée par la pandémie de Covid-19. Les usages numériques se voient modifiés, de la généralisation du télétravail au déploiement du *tracing.*

La Plateforme RSE a jugé intéressant de formuler quelques observations sur le respect des mesures RSE dans l'utilisation du numérique et de l'intelligence artificielle en situation d'exception.

Elle a fait le choix de lister différents sujets qui pourront faire l'objet d'un traitement ultérieur.

Le respect de la sécurité des données en télétravail

Le site gouvernemental dédié à la cybermalveillance[137] rappelle que « les cybercriminels cherchent à tirer profit de la précipitation et de la baisse de vigilance des personnes directement ou indirectement concernées pour les abuser » ; force est de constater que ces risques se voient amplifiés par l'accroissement de l'usage numérique lié aux mesures de confinement.

Remarquant que « cette situation inédite et qui va s'inscrire dans la durée, n'avait pas été anticipée », le site gouvernemental a établi une liste de recommandations à l'attention des collaborateurs et des employeurs afin de limiter les risques de sécurité informatique liés aux conditions de télétravail. Les entreprises, associations, administrations ou collectivités qui en avaient la possibilité ont dû mettre en place des mesures de travail à distance pour préserver les activités essentielles que ce mode de fonctionnement peut permettre. Le Gouvernement note aussi que même les organisations qui avaient déjà mis en place des dispositifs de télétravail, n'étaient pas prêtes à y recourir de manière aussi massive et sur un temps aussi long.

Pour de nombreuses entreprises et organisations, la mise en place du télétravail a dû se faire dans l'urgence, et beaucoup ont dû s'initier à ces pratiques à distance avec des collaborateurs confinés et sans réelle maîtrise des mesures de sécurité pour protéger de manière satisfaisante les systèmes informatiques.

Il existe plusieurs risques et menaces liés au télétravail[138] :

– L'hameçonnage (*phishing*) *:* messages (email, SMS, chat, etc.) visant à dérober des informations confidentielles (mots de passe, informations personnelles ou bancaires) en usurpant l'identité d'un tiers de confiance ;

– Les rançongiciels (*ransomware*) : attaque consistant à chiffrer ou empêcher l'accès aux données de l'entreprise et à généralement réclamer une rançon pour les libérer. Ce type d'attaque s'accompagne de plus en plus souvent d'un vol de données et d'une destruction

[137] https://www.cybermalveillance.gouv.fr/
[138] Voir Recommandations de sécurité informatique pour le télétravail en situation de crise sur le site cybermalveiilance.gouv.fr

préalable des sauvegardes (intrusion sur le réseau de l'entreprise, soit par ses accès à distance, soit par la compromission de l'équipement d'un collaborateur.) ;

– Le vol de données : attaque consistant à s'introduire sur le réseau de l'entreprise, ou sur ses hébergements externes (*cloud*) pour lui dérober des données afin de les revendre, de les diffuser pour nuire ou d'établir toute forme de chantage ;

– Les faux ordres de virement (FOVI/BEC) : ordres erronés intervenant suite au piratage d'un compte de messagerie, par message ou par téléphone ;

L'irruption du télétravail dans la RSE, phénomène conjoncturel ou pérenne ?

Selon Novethic, depuis le début de la crise, les entreprises ayant les meilleures notations environnementales, sociales et de gouvernance (ESG) ont montré une plus forte résistance au choc économique et financier actuel. L'habitude du télétravail fait partie de ces éléments de bonne notation – étude en date du 25 mars, de la Bank of America Merrill Lynch, et de Morgan Stanley – au même titre que la protection sanitaire et sociale des salariés, la politique de congés et de garde d'enfants.

Par ailleurs, plusieurs entreprises prennent position en faveur du télétravail. En France, PSA souhaite désormais que ses salariés ne viennent qu'une fois par semaine sur leur lieu de travail lorsque ceux-ci travaillent dans le domaine tertiaire, commercial ou de R&D[139]. Aux États-Unis, des entreprises des Gafam ont proposé à leurs salariés de télétravailler jusqu'en 2021, et Twitter estime que si les employés peuvent travailler chez eux, cette situation peut devenir indéfinie. Néanmoins, une attention particulière est à donner à l'expérience d'IBM et Yahoo qui, en avance sur le télétravail, ont constaté un manque de créativité des salariés et une atteinte à la cohérence de la culture d'entreprise.[140]

La formation au numérique pour tous les salariés est en passe de devenir un atout pour le développement responsable des entreprises. Si les multinationales y ont déjà recours, les PME subissent, du fait de la crise, une « formation accélérée » en termes de travail à distance. Toute la question est de savoir si cette tendance perdurera à l'issue de l'état d'urgence sanitaire. Cela dépendra des conséquences de cette forme d'autonomisation des salariés pour les entreprises, et de leurs souhaits de maintenir ce mode de travail.

La question des inégalités

La crise de la Covid-19 a rendu plus visibles et les mesures prises pour lutter contre la pandémie, notamment le confinement - ont aggravé les inégalités sociales et porté atteinte aux droits fondamentaux. Les personnes les plus vulnérables et précaires ont vu leur situation empirer, certaines ne pouvant plus subvenir à leurs besoins primaires. (conditions de logement dégradées, accès à l'éducation très compliqué voire impossible, baisse de revenus…).

[139] « Le télétravail : nouvelle norme pour les entreprises ? », Novethic, mai 2020
[140] Idem

Si le numérique constitue une voie de réduction des inégalités car elle peut rendre plus facile et accessible certaines procédures et démarches, l'usage extensif qui en est fait a généré une « fracture numérique », les plus vulnérables étant encore plus précarisés. La Fondation Internet Nouvelle Génération (Fing) fait état de difficultés induites par une utilisation des outils numériques différenciée selon la taille du logement, le temps de régulation de l'espace et du temps privé, la nécessité ou pas d'assurer une continuité pédagogique, selon l'âge des enfants, ou les diverses situations professionnelles (chômage partiel, arrêt de travail, télétravail, précarité, maladie)[141].

Dans une interview accordée à *La Tribune*[142], Jacques-François Marchandise, délégué général de la Fing, considère que « *Le confinement agit aussi comme un révélateur des inégalités d'accès au numérique. Outre le développement du télétravail, Internet est devenu un outil à privilégier pour quantité de démarches quotidiennes. Les Français sont poussés à téléconsulter au lieu d'aller voir leur médecin, à se faire livrer leurs courses plutôt que d'aller au supermarché. Quand les collégiens et lycéens, eux, sont priés de suivre leurs cours en ligne. Le problème, c'est que tout le monde n'a pas accès, ou ne maîtrise pas, ces usages.* ».

Afin de pallier cette situation la plateforme Solidarité Numérique[143] a été lancée par le Secrétaire d'État chargé du numérique, regroupant des acteurs de la médiation numérique et permettant, sur un simple appel téléphonique, de bénéficier de l'aide d'un médiateur pour les démarches en ligne essentielles.

Le débat sur la santé et les utilisations de l'IA

Dès l'annonce du confinement, l'État a encouragé les téléconsultations médicales avec des mesures spécifiques pour les salariés. Ainsi, afin de permettre aux professionnels de santé d'assurer la prise en charge des patients dont le diagnostic d'infection à la Covid-19 a été posé cliniquement ou biologiquement, les pouvoirs publics ont mis en place des mesures dérogatoires aux règles habituelles régissant l'exercice de certaines professions et la prise en charge des actes par l'assurance maladie :

- Le médecin peut recourir à la téléconsultation sans connaître préalablement le patient et en dérogeant aux règles du parcours de soins pour les patients infectés par la Covid-19 ou susceptibles de l'être[144] ;
- Les téléconsultations peuvent être réalisées en utilisant n'importe quel moyen technologique actuellement disponible pour réaliser une vidéotransmission ;
- Des mesures facilitant le suivi des patients par les infirmiers sont mises en place ;
- Les circuits des pièces justificatives à la facturation sont simplifiées ;

[141] Jacques-François Marchandise observe, par exemple, que des individus officiellement en télétravail, prêtent leur seul ordinateur aux enfants par souci de continuité pédagogique, et donc travaillent la nuit.
[142] « Dans l'épreuve que nous traversons, le besoin de médiation numérique est énorme », interview de Jacques-François Marchandise, La Tribune, mars 2020
[143] https://solidarite-numerique.fr/
[144] Fiche médecins - Covid-19 : recours à la téléconsultation (PDF), Fiche médecins - Covid-19 : la téléconsultation simplifiée – Facturation en métropole (PDF), Fiche médecins - Covid-19 : la téléconsultation simplifiée – Facturation dans les DROM (PDF).

- La validité des ordonnances médicales se voient prolongées, notamment pour l'accès des femmes à la pilule contraceptive ;
- La simplification des arrêts de travail des personnes considérées comme vulnérables (femmes enceintes, personnes présentant des fragilités de santé) est portée par un téléservice.[145]

Terra Nova a posé les avantages et inconvénients soulevés par le numérique en temps de crise, l'institut distingue ainsi :
- Les dispositifs d'analyse qui visent à suivre et modéliser l'avancée de l'épidémie ;
- Les dispositifs de « counseling » destinés aux individus, à l'auto-évaluation de la maladie et à l'isolement volontaire. Ces dispositifs sont divers, du simple questionnaire en ligne pour orienter le malade au dispositif de « backtracing » permettant de retracer ses interactions et de s'isoler en cas de contacts à risques ;
- Les dispositifs de contrôle qui visent à permettre un suivi individualisé de l'épidémie et à automatiser les contrôles jusqu'alors assurés manuellement par les autorités sanitaires. À côté du recours massif aux données personnelles, très développé en Chine par exemple, d'autres modèles de contrôle de la quarantaine moins invasifs sont mis en place.

Terra Nova, dont la note prend position de manière forte pour une démultiplication du numérique dans la sphère publique et privée, concède cependant qu'un débat existe. Il recommande d'adjoindre au RGPD une autorité administrative indépendante supplémentaire, afin de ne pas tomber sur une « gouvernementabilité algorithmique » qui serait en charge d'encadrer et contrôler les dispositifs algorithmiques utilisés pour la sortie de crise, et ultérieurement pour tous ceux utilisés par l'État. Terra Nova explique, à ce titre, qu'il faut « *faire une mise en balance entre liberté individuelle et sécurité collective, entre respect de la vie privée et contraintes de santé publique. Cette discussion n'est pas nouvelle. La science et les circonstances historiques nous ont obligés régulièrement à reconsidérer des équilibres que nous pensions indépassables. La première dette de l'État envers ses concitoyens est la sécurité : s'il n'assume pas cette clause du contrat social, sa justification risque dès lors d'être remise en cause. Nous pensons que, dans le cadre de l'épidémie de Covid- 19, compte tenu des risques encourus par la population, l'État doit maintenir l'équilibre entre libertés publiques et contraintes de santé publique pour assurer la sécurité sanitaire des citoyens*. »

Egalement, en avril 2020, Mounir Mahjoubi, député LREM et ex-Secrétaire d'Etat au numérique a publié une note parlementaire sur la mise en place du « *contact tracing* » - à savoir le suivi des contacts (ou des interactions sociales des personnes). Il y exemplifie les finalités du traçage des données mobiles dans la lutte contre la pandémie de Covid-19 :
- L'observation des pratiques collectives de mobilité et de confinement afin d'obtenir une vision nationale, régionale et affinée à l'échelle d'un quartier ;
- L'identification des sujets « contact » afin de retracer les parcours récents des personnes testées positives, d'information la population des zones à risques, de relever les contacts récents entre individus testés positifs et personnes tierces ;
- Le contrôle des confinements individuels afin de veiller au respect des quarantaines et des confinements et de développer un permis de circuler.

[145] Le Haut Conseil de la santé publique a établi une liste précise des pathologies concernées.

Par ailleurs, la CNIL a été saisie d'une demande d'avis par le Secrétaire d'Etat chargé du numérique, Cédric O, afin d'évaluer le respect des règles relatives à la protection des données par l'application « Stop Covid » - application de suivi de contacts dont le téléchargement et l'utilisation reposeraient sur une démarche volontaire qui a été lancée le 2 juin 2020. L'application permet aux individus d'être alertés lorsqu'ils se trouvent à proximité d'une personne diagnostiquée positive à la Covid-19 et disposant de la même application. Reposant sur le « *contact tracking* », l'application pose des questions relatives à l'éthique du numérique.

Il est à noter que Google et Apple ne prendront pas part à l'application. Cédric O a estimé que les solutions proposées par les deux géants posaient « un certain nombre de problèmes en termes de protection de la vie privée et d'interconnexion avec le système de santé ».

La CNIL a jugé le dispositif conforme au RGPD seulement si certaines conditions sont respectées :
- L'usage de l'application doit rester volontaire et ne pas impliquer de conséquences négatives en cas de non utilisation ;
- La protection des données dès la conception est respectée car l'application utilise des pseudonymes ne permettant pas de remonter la liste des personnes contaminées ;
- L'utilité d'une telle application pour la gestion de la crise doit être avérée ; son utilisation doit ainsi être temporaire et les données conservées pendant une durée limitée. À ce titre, la CNIL recommande que l'impact du dispositif sur la situation sanitaire soit régulièrement évalué afin de juger de sa pertinence ;
- La confiance du public constitue un facteur déterminant du succès d'une telle application, ainsi, l'architecture et la sécurisation du dispositif doivent être assurées.

Le Conseil National du Numérique a également répondu à une saisine du Secrétaire d'Etat chargé du Numérique afin d'étudier les conditions de déploiement de l'application[146]. S'il est favorable au principe de *l'application « en tant que brique d'une stratégie plus globale »*, le CNnum pose lui aussi des conditions pour garantir l'intérêt général de l'État de droit, dont la création d'un comité de contrôle, avec des parlementaires, des chercheurs et des citoyens-experts, disposant d'un pouvoir d'arrêt de l'application » ; la limitation dans le temps d'une telle application qui doit rester exceptionnelle, il appelle à ce que le dispositif soit transparent et inclusif.

En revanche, la Quadrature du Net[147] dénonce des « libertés inutilement sacrifiées » en termes de :
- Discriminations : consentement non libre à l'application, facilitation possible de l'accès aux tests sérologiques pour les personnes ayant l'application ;
- Surveillance : obligation d'utilisation de l'application, contradiction avec la notion juridique d'anonymat ;

[146] StopCovid, Avis du Conseil Nationale du Numérique, 24 avril 2020, https://cnnumerique.fr/files/uploads/2020/2020.04.23_COVID19_CNNUM.pdf
[147] Nos arguments pour rejeter StopCovid, La Quadrature du Net, avril 2020

- Acclimatation sécuritaire : le déploiement de l'application n'est pas soumis à une durée précise, ajouts possibles de fonctions coercitives, surveillance constante des corps, renforcement des solutions technologiques.

Dans un avis adopté en avril 2020, la Commission nationale consultative des droits de l'homme (CNCDH) s'est autosaisie afin d'alerter les pouvoirs publics des dangers présentés par une application de suivi sur les droits fondamentaux[148]. Le rapport dénonce le « caractère transversal des atteintes potentielles aux droits de l'homme pouvant résulter de telles mesures de suivi » et rappelle que la seule conformité au RGPD ne constitue pas un respect des droits et libertés fondamentaux. La CNCDH considère ainsi que « l'intérêt et l'efficacité d'un tel suivi pour endiguer la propagation du virus sont trop incertains en comparaison de la menace disproportionnée qu'ils font peser sur les droits et les libertés fondamentaux. » La Commission a réitéré ses inquiétudes après que la CNIL a donné son feu vert[149].

En mai 2020[150], la CNCDH a aussi émis des réserves les systèmes d'information Si-DEP et Contact Covid, « *la nature des données, l'ampleur de la collecte et le nombre encore important des personnes y ayant accès appellent une particulière vigilance*. » La CNCDH s'inquiétait en particulier de la levée du secret médical impliqué par le recours à ces systèmes d'information.

Valérie Charolles, Pierre-Antoine Chardel et Eric Guichard[151] mettent en garde contre une application relevant d'une « solution techniciste de court terme » qui pourrait entrainer la défiance des citoyens envers les pouvoirs publics, ou un excès de confiance dans le numérique au détriment de « projets technologiques soucieux de l'éthique ». Les chercheurs soulignent, notamment, les discriminations induites par une telle application – exclusion de 20 % des Français qui ne possèdent pas de smartphone – et dénoncent l'illusion que les solutions numériques sont à même de venir à bout d'une pandémie mondiale. Ils posent également la question de la légitimité démocratique d'un tel recours et appellent à la vigilance quant au contenu de tels protocoles et à la qualité de la décision démocratique conduisant à la mise en œuvre du dispositif. Enfin, ils estiment que « les moments d'exception comme ceux que nous vivons ne doivent pas conduire à mettre de côté ce contrat social mais au contraire à le réaffirmer, en rappelant qu'il est fondé sur la confiance dans autrui et non sur la défiance et la désocialisation, où l'autre est vu comme une menace, et non comme un partenaire. »

La mise en pratique d'une telle application demeure encore incertaine, de nombreuses questions techniques restent à résoudre, comme le stockage et la sécurisation des données. Pour cela, le Gouvernement a confié le pilotage du projet à l'Institut National de Recherche en Informatique et en Automatique (Inria)[152], en collaboration avec des partenaires tels que

[148] Avis sur le suivi numérique des personnes, Commission nationale consultative des droits de l'homme, 28 avril 2020
[149] https://www.cncdh.fr/fr/publications/la-cncdh-souligne-les-dangers-de-lapplication-stopcovid
[150] Avis « Prorogation de l'état d'urgence sanitaire et libertés », CNCDH, mai 2020
[151] Pierre-Antoine Chardel, Valérie Charolles, Eric Guichard, « StopCovid : une application problématique sur le plan éthique et politique », Revue Politique et Parlementaire, mai 2020
[152] « Le gouvernement s'embourbe dans son projet d'application StopCovid », Mediapart, avril 2020

le projet européen PEPP-PT. Le *Pan European Privacy Preserving Proximity Tracing*[153] est un projet européen fondé sur des technologies numériques privacy by design, regroupant plusieurs organisations scientifiques de premier plan (Fraunhofer, EPFL, ETHZ) et plus de 130 scientifiques en provenance de 8 pays dans la lutte contre la Covid-19. La Plateforme PEPP-PT a pour ambition de proposer des technologies et des standards pour une approche de suivi numérique des contacts de proximité fondée sur le consentement, l'anonymat et le respect de la vie privée, en conformité avec le RGPD.

En avril, deux protocoles informatiques entraient en compétition[154] :
- Un protocole centralisé : le *ROBust and privacy-presERving proximity Tracing* dans lequel les identifiants générés par les téléphones sont stockés dans un serveur qui se charge, en cas de contamination, de retrouver les contacts de l'utilisateur et de leur envoyer une alerte ;
- Un protocole décentralisé : le *Decentralized Privacy-Preserving Proximity Tracing* dans lequel les identifiants sont stockés dans les smartphones des utilisateurs qui décident d'envoyer un message d'alerte en cas de contamination.

Un arrêté gouvernemental encadrant les mesures d'organisation et de fonctionnement du système de santé afin de faire face à l'épidémie de Covid-19 a été publié le 21 avril 2020. Le texte précise les données auxquelles peuvent accéder la Plateforme des données de santé de l'Etat et de la Caisse nationale de l'assurance maladie. La CNIL, saisie sur le sujet, tient à rappeler que « au vu de l'urgence, quel que soit le contexte, des garanties suffisantes au regard du respect des principes fondamentaux du droit à la protection des données à caractère personnel doivent être mis en œuvre »[155] ; pour cela, des mesures juridiques et techniques devront être prévues pour assurer un niveau de protection acceptable.

Saisi, le Conseil Constitutionnel a validé, lundi 11 mai 2020, la loi prorogeant l'état d'urgence sanitaire adoptée par le Parlement le 9 mai 2020. Les juges constitutionnels ont censuré les modalités de mise en quarantaine ou en isolement des personnes entrant sur le territoire national ou arrivant en Corse et dans une collectivité d'outre-mer sans intervention d'un juge judiciaire ; ces mesures ont été jugées « privatives de liberté ». L'article 6 de la loi, créant un système d'information aux fins de lutter contre l'épidémie, a été jugé conforme, car même s'il y a bien *« atteinte au droit au respect de la vie privée »* – ces données pouvant être collectées sans consentement –, « *le législateur a entendu renforcer les moyens de la lutte contre l'épidémie du Covid-19, par l'identification des chaînes de contamination. Il a ainsi poursuivi l'objectif de valeur constitutionnelle de protection de la santé.* ». Le Conseil Constitutionnel a, cependant, formulé plusieurs réserves d'interprétation[156].

[153] https://www.inria.fr/fr/initiative-pepp-pt
[154] « Le gouvernement s'embourbe dans son projet d'application StopCovid », Mediapart, avril 2020
[155] Délibération n° 2020-044 du 20 avril 2020 portant avis sur un projet d'arrêté complétant l'arrêté du 23 mars 2020 prescrivant les mesures d'organisation et de fonctionnement du système de santé nécessaires pour faire face à l'épidémie de Covid-19 dans le cadre de l'état d'urgence sanitaire, CNIL, 20 avril 2020
[156] Décision n°2020-800 DC du 11 mai 2020, à retrouver ici : https://www.conseil-constitutionnel.fr/decision/2020/2020800DC.htm

La possession et la gestion des données par les entreprises constituent des enjeux fondamentaux dans une société en évolution constante. Le numérique a entrainé une révolution totale des modes de fonctionnement privés et publics. Les engagements des entreprises se voient ainsi renforcés au profit de valeurs nouvelles : protection de la vie privée, protection contre les cyberattaques ou encore respect des normes juridiques et règlementaires en vigueur.

Ce sont aujourd'hui les relations clients qui se voient majoritairement impactées par les avancées technologiques ; les possibilités des entreprises se multiplient et elles peuvent désormais proposer des services adaptés aux besoins et habitudes de consommation de leurs clients. Dans le même temps, les activités s'accélèrent et les liens avec les parties prenantes sont renforcés.

Néanmoins, de tels bouleversements appellent une vigilance accrue. Les entreprises, quelle que soit leur taille, doivent désormais faire preuve d'un devoir de responsabilité majeur. En maniant des données toujours plus nombreuses, et confrontées aux problématiques de stockage et d'utilisation de ces données mais également à leur utilité privée et publique, les entreprises développent des stratégies nouvelles.

Car il touche au plus près les droits humains et les libertés fondamentales, le numérique s'inscrit pleinement dans la responsabilité sociétale des entreprises. Loin d'être une activité propre au business, la détention et le traitement de données des entreprises est, aujourd'hui, un sujet sociétal à part entière.

II. QUELLE ORGANISATION DES ENTREPRISES SUR LE NUMÉRIQUE ?

La maîtrise des données par les entreprises constitue aujourd'hui un moteur de croissance et d'innovation, ainsi les entreprises ont aujourd'hui intérêt à placer les données au centre de leur stratégie. Néanmoins, même si les entreprises tireraient profit de l'ensemble des données, de nombreuses données ne sont pas exploitables ou exploitées, faute d'une architecture capable de gérer, en bonne gouvernance, la diversité des données et les solutions technologiques adéquates[157].

1. La gouvernance des données au sein de l'entreprise

La gouvernance des données rend la transformation numérique possible. Le contrôle de la gestion des activités dans différents domaines a toujours nécessité la collecte de données par les entreprises. Cependant, le volume actuel de données générées rend impossible à la fois leur intégration à l'aide de méthodes de réplication classiques et leur stockage en un seul endroit comme cela se faisait il y a quelques années.

Aujourd'hui, la difficulté d'intégrer les données au sein des entreprises est encore plus grande. Il est d'autant plus complexe de procéder à une bonne gouvernance des données qui soit efficace et unifiée à mesure que l'environnement numérique compte une variété de plus en plus grande de volumes et de formats de données. Les questions de management et de gouvernance s'avèrent fondamentales à la transformation numérique pérenne des entreprises.

L'impact de cette évolution est résumé par Sara Fert, directrice Client Groupe Axa, pour qui « la transformation digitale génère davantage de transversalité et de coordination

[157] « Transformation numérique : comment l'économie de la donnée impacte les architectures informatiques », Evernote

entre les différentes équipes en remettant le client (*data* et parcours clients) au centre des préoccupations de l'entreprise. »[158] L'enjeu de la *data* porte donc le plus souvent sur la connaissance client, mais est aussi un enjeu de différenciation fort face à la concurrence.

Dans les entreprises dont le modèle d'affaires est guidé par les données (*data driven*), l'importance de la gouvernance des données est d'autant plus grande qu'elle est prise en compte dans la définition de la stratégie. Ainsi, selon Mme Jeanne Bossi Malafosse, Responsable du département Données Personnelles de DELSOL Avocats, « la donnée personnelle et le capital informationnel d'un organisme ont indéniablement acquis une valeur économique qu'ils n'avaient pas auparavant. » Par ailleurs, le traitement des données peut permettre aux entreprises de créer de la valeur et de s'inscrire dans de nouvelles perspectives commerciales et de renforcer leurs liens avec les clients et les parties prenantes.[159]

En d'autres termes, la transition numérique permet d'avoir une meilleure connaissance client et de, à terme, monétiser les données. De nouvelles relations s'instaurent avec les clients grâce aux possibilités offertes par le numérique (publicités ciblées, personnalisation de l'offre existante, collectes de données avec les cookies…). L'entreprise peut acquérir de nouveaux clients et fidéliser ses anciens clients ou encore apparaitre comme un acteur de confiance au sein de l'écosystème dans lequel elle évolue. De nouveaux outils sont développés afin d'en exploiter les potentialités offertes par les données : *data analytics*, la *data visualisation* ou encore l'IA[160].

Auparavant, les données étaient considérées comme des produits dérivés issus de l'activité principale, et non comme un actif en tant que tel. La responsabilité de leur gestion a longtemps été déléguée à la DSI. Pourtant, dans les entreprises dont le modèle d'affaires est guidé par les données comme dans les autres, la gouvernance des données interroge la répartition des rôles entre les différentes fonctions de l'entreprise : *data protection officer*, direction des services d'information, direction RSE, direction des opérations, comité exécutif. Dans un contexte où les données participent de plus en plus directement à la création de valeur, elle interroge également la prise en compte de cet enjeu au niveau de la gouvernance stratégique de l'entreprise.

Selon Xavier Brucker, expert en projets digitaux et IA dans l'industrie, il existe six principes clés pour déployer une gouvernance des données :[161]

1. la qualité des données : sur la base de critères prédéfinis, la qualité des données est régulièrement vérifiée, les éventuels problèmes sont gérés et corrigés ;
2. la standardisation et l'harmonisation : les sources de données sont définies et cohérentes ; elles partagent un dictionnaire commun et sont standardisées ;

[158] EY et EBG (2019), « La transformation digitale au sein des organisations Lien
[159] ADEL (2018), « Vade-Mecum sur le traitement des données numériques » Lien
[160] Audition de M. Rémi Dusaud
[161] Brucker X. (2019), « La gouvernance des données : un investissement critique pour l'avenir » Lien

3. l'intégrité : les données sont vérifiables et fiables ; elles permettent à tout moment de prendre des décisions opérationnelles. Cette intégrité doit être accompagnée de metadata décrivant le contexte dans lequel chaque donnée a été créée ;
4. l'accessibilité : les droits d'accès sont gérés et permettent aux utilisateurs l'accès aux données nécessaires à leur mission ; le partage de données est encouragé pour faciliter la collaboration ;
5. la responsabilité : des "*data owners*" sont identifiés et en charge de vérifier la bonne gestion des données dans leur cycle de vie. Les équipes métiers sont responsables de leurs données ;
6. la stratégie de l'entreprise.

1.1. Le rôle des directions des systèmes d'information (DSI)

Le rôle de la Direction des Systèmes d'Informations (DSI)

Dans le passé, le rôle de la DSI se situait plus dans l'opérationnel, dans le « time to market ». La gouvernance des données appelle aujourd'hui les DSI à se rapprocher des fonctions stratégiques de l'entreprise. Leur rôle dans la gouvernance des données est permanent. Un programme de gouvernance des données est une succession de cycles répétés, et non pas un projet défini dans le temps.

Selon la définition de l'APEC, « le directeur des systèmes d'information a pour mission de définir et mettre en œuvre la politique informatique en accord avec la stratégie générale de l'entreprise et ses objectifs de performance. Il doit garantir la continuité du service informatique fourni aux utilisateurs et anticiper les changements et leurs impacts métiers sur le système d'information. »[162], « Le rôle du DSI est d'appliquer les technologies pertinentes afin de fournir les bonnes données aux bonnes personnes et leur permettre de répondre aux questions afférentes. Pour fournir ces données, il est nécessaire d'intégrer les applications et connecter les référentiels de données, établir des politiques de gouvernance des données, mettre en place des dictionnaires de données et identifier les enregistrements de référence unique pour chaque type de données utilisé dans l'entreprise, afin qu'elles soient cohérentes et fiables. »[163]

Le rôle du DSI est donc aujourd'hui en pleine évolution. Pour jouer un rôle pertinent dans la transformation numérique de son organisation, il doit passer du statut de preneur de commandes à celui d'innovateur et de stratège.

Les DSI se voient également soumises, via l'article 32 du RGPD, à une "obligation générale de sécurité", qui repose sur plusieurs principes :

- la pseudonymisation et le chiffrement des données ;
- l'intégrité, la disponibilité, la résilience et la confidentialité,
- des phases de test, d'analyse et d'évaluation du SI ;
- la mise en place de moyens pour rétablir l'accès et la disponibilité des données.

[162] APEC, Lien
[163] Oudot P. (2019), « Transformation numérique : la gouvernance des données et agilité au secours des DS Lien

DSI et RSE

1. *La contribution des DSI à la RSE* d'une entreprise

Il y a encore quelques années, il était assez rare de citer l'implication dans la mise en œuvre de démarche RSE de la DSI, qui est une fonction opérationnelle.

L'intégration des préoccupations sociales, environnementales et économiques à l'activité des DSI inclue la réduction des impacts environnementaux des technologies employées, le *Green IT*.

Les DSI, en permettant la mise en place de la *digital workplace* (espace de travail numérique) au sein des entreprises, en fournissant des outils collaboratifs (salles de réunions virtuelles, écrans interactifs, télétravail), contribue indéniablement à la mise en œuvre de la stratégie RSE d'une entreprise. Grâce à ces technologies, l'intelligence collective, le dialogue social et le faire ensemble d'une entreprise se trouvent grandement augmentés. Toujours d'un point de vue RSE, les contributions de la DSI améliorent les conditions de vie au travail et facilitent les relations interpersonnelles en rendant habituel l'échange et le partage d'informations. Elles facilitent donc l'agilité organisationnelle permettant de mettre en œuvre une démarche de développement durable.[164] Cette *digital workplace* construite par la DSI permet également une réduction concrète des impacts environnementaux. Sous l'impulsion de cette dernière, la transformation des espaces de travail préconise les pratiques du développement durable avec, par exemple l'éco-conception numérique, l'utilisation d'énergies renouvelables, les éco-gestes, la diminution du *commuting,* l'économie du papier.[165] De plus, les moyens mis en œuvre par les DSI facilitent la mesure de l'impact environnemental des entreprises, et dans certain cas, l'impact des projets numériques.

Le numérique pourrait faire partie des moyens permettant de mettre en œuvre les objectifs de transparence et promouvoir une gouvernance plus démocratique, en recourant à l'intelligence collective, ou au dialogue social interne.[166] En effet, en promouvant les TIC au sein de leur entreprise, les DSI facilitent le dialogue avec les parties-prenantes, par exemple avec l'interopérabilité entre les PGI (voir partie « EDI : *electronic data interchange* »), ou avec les innovations de la *digital workplace* décrites ci-dessus. La logique collective des TIC mise en place par les DSI favorise l'ouverture aux parties prenantes. Le numérique est donc un levier transverse, qui permet de fédérer un écosystème d'acteurs.[167]

2. *Enjeux déontologiques de la DSI*

Alors que la mise en œuvre de solutions numériques par les DSI est en plein essor, la question se pose de la déontologie des concepteurs : la prise en compte par exemple de la *Privacy by Design* ou de la protection des données pose une pression accrue sur la déontologie des Directions des Systèmes d'Information. Dans ce contexte, avec les

[164] Filippone D. (2020), « Les DSI peinent à jouer un rôle dans la RSE de l'entreprise » Lien
[165] Creche M. (2018), « RSE : quelle adéquation avec le digital workplace ? » Lien
[166] Audition d'Axelle Lemaire
[167] Audition de Cécile Wendling

fonctions qu'elles assurent au sein d'une organisation, les DSI doivent faire preuve d'engagement et d'intégrité. L'éthique du numérique peut être appliquée par la DSI. Par exemple, l'*éthique by design* s'intéresse à la phase de conception des outils numériques : les concepteurs ont une responsabilité éthique dès la conception des algorithmes. Les données et algorithmes peuvent faire apparaitre des biais humains et de nouvelles discriminations. Les concepteurs étant à l'origine de la supervision de l'apprentissage automatique, ils doivent être impartiaux, formés aux problématiques de discriminations, et prendre en considération ces enjeux en amont.[168]

Par ailleurs, un autre axe fort de la RSE concerne les fonctions techniques du numérique : l'égalité entre les femmes et les hommes. Car ces postes sont encore majoritairement occupés par des hommes. On ne retrouve ainsi que 15 % de femmes dans ces métiers[169]. Le numérique et sa gouvernance au sein des entreprises doivent inclure les femmes et tenir compte des enjeux fondamentaux de parité.

Le Cabinet McKinsey estime qu'atteindre la parité engendrerait une augmentation de 10 % du PIB d'ici 2025. Le secteur du numérique est en évolution et croissance constantes et peine à recruter. Engager une politique favorable à l'évolution professionnelle des femmes, notamment au sein des DSI, doit s'imposer comme un objectif fondamental pour les entreprises ; la diversité des profils est essentielle à la santé du secteur numérique au moyen et long terme.

La Participation de la DSI à la gouvernance RSE

Godefroy de Bentzmann, président du Syntec Numérique, interroge le rôle du DSI, qui devrait aller au-delà des questions budgétaires ou techniques. La DSI doit s'assurer de l'accessibilité et de l'acceptation des projets par l'ensemble des parties prenantes. Selon lui, le DSI doit travailler en alertant, en éduquant et en analysant les impacts potentiels : ainsi, il serait indispensable que les DSI fassent partie des comités exécutifs.[170]

Or, selon Véronique Torner, administratrice de Syntec Numérique en charge du programme numérique responsable, les DSI restent, à ce jour, mises à l'écart et ne sont pas encore intégrées aux démarches RSE. Elle explique que « *Les DSI doivent intégrer dans leurs équipes des personnes qui peuvent la représenter dans la gouvernance de la RSE* ». Des sujets tels que la collecte des données, l'IA et l'Open Source pour lesquels les DSI ont une expertise certaine doivent être inclus dans l'élaboration de la stratégie RSE intégrant un volet numérique. Par l'expertise qu'elles sont sur ces thématiques, les DSI peuvent contribuer à la gouvernance RSE. Cela permettrait aux entreprises de développer une responsabilité numérique, et de rapprocher les mondes de la RSE et de la DSI. On constate encore un manque de postes faisant la jonction entre DSI et RSE.

À ce titre, le DSI de Saint-Maclou estime que le numérique doit « être au centre des prises de décisions faites par l'entreprise et en l'occurrence au sein des politiques

[168] Syntec et Cigref (2018), « Ethique et Numérique : un référentiel » Lien
[169] Goulmot I. (2019), « Les femmes dans le secteur digital en 2019 : quelles avancées ? » Lien
[170] Hirsch N. (2019), « Compte-rendu partiel de l'Assemblée Générale du Cigref » Lien

RSE. » L'aspect transversal du numérique et la création de valeur grandissant qu'il engendre s'accompagne d'enjeux sociaux, sociétaux et environnementaux.[171]

L'avis de Isabelle Juppé, directrice de la responsabilité sociétale du groupe Lagardère abonde en ce sens : « Le numérique est devenu transversal, c'est-à-dire qu'il s'applique à tout type de structure et domaine, ce qui amplifie son impact. Il doit donc être au centre des prises de décisions faites par l'entreprise et en l'occurrence au sein des politiques RSE. »

1.2. Le rôle des délégués à la protection des données (DPD)

1.2.1. Un métier récent et en pleine évolution

Le délégué à la protection des données (DPD, aussi appelé, dans certaines entreprises « *data protection officer* ») est reconnu comme un acteur clé de la gouvernance des données par le RGPD. L'article 37, paragraphe 5 du RGPD, dispose que le DPD « est désigné sur la base de ses qualités professionnelles et, en particulier, de ses connaissances spécialisées du droit et des pratiques en matière de protection des données ».

Sa désignation est obligatoire pour :

- Les autorités et 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 infractions.

Toutefois, la désignation d'un délégué est toujours encouragée par les autorités de protection des données en ce qu'elle facilite l'identification et la mise en œuvre des actions de conformité au sein d'une structure.

L'article 37, paragraphe 7, du RGPD dispose que le responsable du traitement ou le sous-traitant publie les coordonnées du DPD et communique ses coordonnées à l'autorité de contrôle compétente. À titre de bonne pratique, le G29 recommande également que tout organisme communique le nom et les coordonnées du DPD à ses employés. Le DPD est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions.[172]

Le nombre de DPD/DPO ne cesse d'augmenter. Selon The International Association of Privacy Professionals, en mai 2019, environ 500 000 organisations ont enregistré des DPD dans toute l'Europe dans le cadre du RGPD[173]. En France, la CNIL a comptabilisé 65 000 déclarations de DPO, soit une augmentation de 31 % par rapport à l'année 2018[174]. Pour la majorité des entreprises, la fonction de DPD a été créée il y a moins de

[171] Filippone D. (2020), « Les DSI peinent à jouer un rôle dans la RSE de l'entreprise » Lien
[172]
[173] IAPP (2019), " Study : an estimated 500k organisations have registered DPO across Europe" Lien
[174] CNIL (2020), Rapport d'activité « Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles »

3 ans, et est donc consécutive à l'entrée en vigueur du RGPD, ce qui atteste de la mobilisation récente des entreprises autour des enjeux du numérique.

L'article 37 du RGPD autorise un groupe d'entreprises à désigner un seul DPD à condition qu'il soit « facilement joignable à partir de chaque lieu d'établissement ». Pour favoriser sa disponibilité, le Conseil européen de la protection des données (ex-G29) recommande qu'il soit basé dans l'Union européenne. Puisque les organisations sont autorisées à faire appel à des DPD externes qui, à leur tour, peuvent servir plusieurs organisations, le nombre de DPD est inférieur au nombre total d'organisations. En France, l'effet de mutualisation est important. Alors que près de 52 000 organisations sont enregistrées, le nombre de DPD est à peine inférieur à 18 000.

Selon une étude PwC[175], les difficultés à intégrer l'IA dans les process de l'entreprise conduisent les entreprises à professionnaliser leurs équipes et créer de nouveaux métiers. PwC affirme que depuis deux ans, en renfort du *chief data officer*, de nouveaux emplois très spécialisés sont mis en place : *chief analytics officer*, *chief data scientist*, *data engineer* ou encore *data protection officer*.

Les DPD ne sont pas personnellement responsables en cas de non-respect du RGPD, l'article 24 du RGPD établit clairement que c'est le responsable de traitement qui est responsable.

Les missions, fonctions et objectifs des DPD

Dans les textes

L'article 39, paragraphe 1, du RGPD, énumère les missions du DPD, qui ne constitue cependant qu'un seuil acceptable. Le DPD peut se voir confier d'autres missions :

- « Informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du RGPD ».[176]
- « Aider le responsable du traitement ou le sous-traitant à vérifier le respect, au niveau interne, du présent règlement »[177]
- « Dispenser des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifier l'exécution de celle-ci en vertu de l'article 35 ».[178]
- « Coopérer avec l'autorité de contrôle » et « faire office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mener des consultations, le cas échéant, sur tout autre sujet »[179].

[175] PwC (2018), « Du Big Data à l'intelligence artificielle : le défi des entreprises françaises » Lien
[176] Article 39, paragraphe 1, point a) du RGPD
[177] Article 39, paragraphe 1, point b) du RGPD
[178] Article 39, paragraphe 1, point c) du RGPD
[179] Article 39, paragraphe 1, points d) et e) du RGPD

- « Tenir dûment compte [...] du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement ».[180]
- « C'est le responsable du traitement ou le sous-traitant, et non le DPD, qui doit tenir « un registre des activités de traitement effectuées sous [sa] responsabilité » ou « un registre de toutes les catégories d'activités de traitement effectuées pour le compte du responsable du traitement »[181]. Le Conseil européen de la protection des données précise, néanmoins, que dans la pratique, les DPD dressent des inventaires et tiennent un registre des opérations de traitement sur la base d'informations fournies par différents services. Par ailleurs, « cette pratique a été inscrite dans de nombreuses législations nationales ainsi que dans les règles en matière de protection des données applicables aux institutions et organes de l'Union européenne ».[182]

Les lignes directrices du G29 (aujourd'hui : Conseil européen de la protection des données) recommandent que le DPD soit associé dès le stade le plus précoce possible à toutes les questions relatives à la protection des données. Les recommandations suivantes sont formulées, et elles vont dans le sens d'une association la plus poussée possible des DPD à la définition et l'exécution d'une stratégie de gouvernance des données. Il est recommandé qu'une organisation veille à ce que :

- *Le DPD soit invité à participer régulièrement aux réunions de l'encadrement supérieur et intermédiaire;*
- *Sa présence soit recommandée lorsque des décisions ayant des implications en matière de protection des données sont prises. Toutes les informations pertinentes doivent être transmises au DPD en temps utile afin de lui permettre de fournir un avis adéquat;*
- *L'avis du DPD soit toujours dûment pris en considération. En cas de désaccord, le G29 recommande, à titre de bonne pratique, de consigner les raisons pour lesquelles l'avis du DPD n'a pas été suivi;*
- *Le DPD soit immédiatement consulté lorsqu'une violation de données ou un autre incident se produit.*

En pratique : retours d'expérience

Dans la pratique, selon l'étude *Chief data officer : de l'inspiration à l'action* conduite par l'entreprise EBG, les DPD identifient cinq objectifs prioritaires pour leur profession, qui se positionnent dans cet ordre :

1. Mise en place d'une gouvernance *data* (54 % des répondants) ;
2. Abattre les silos entre les différents métiers (38 %) ;
3. Diffuser la culture *data* (35 %) ;

[180] Article 39, paragraphe 2 du RGPD
[181] 'article 30, paragraphes 1 et 2 du RGPD
[182] Article 24, paragraphe 1, point d), du règlement (CE) nº 45/2001.

4. Se conformer à la réglementation (36 %) ;
5. Travailler sur l'omnicanalité (33 %).

Les DPD, interrogés dans le cadre du rapport *Data Protection and Privacy Officer Priorities 2020* de *CPO Magazine*, qui étudie les priorités des responsables de la protection des données, déclarent :

- mettre en œuvre de programmes – 24 % ;
- définir les priorités du programme de protection des données – 22 % ;
- déterminer la stratégie de ce programme – 22 % ;
- évaluer la performance du programme – 20 % ;
- gérer les budgets du programme – 10 %. [183]

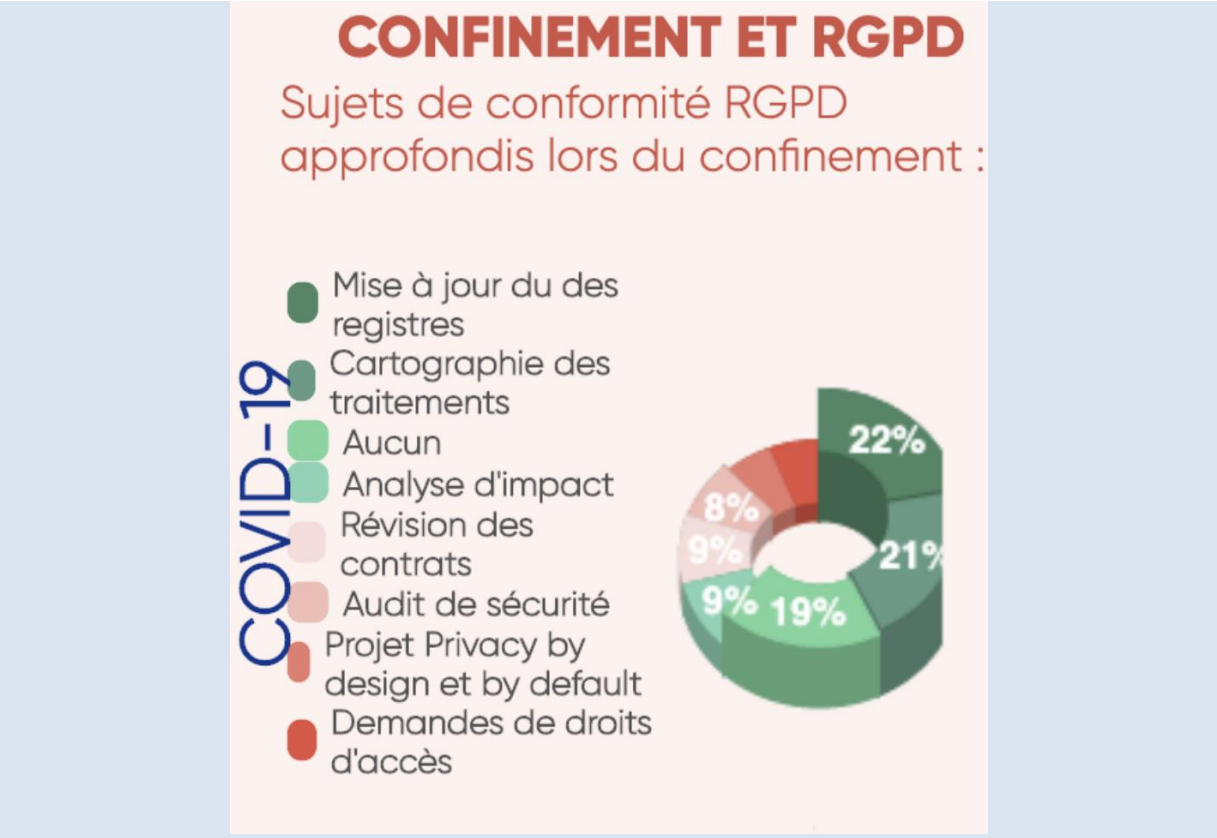
En gardant tout le recul nécessaire, ces chiffres semblent montrer que, contrairement aux lignes directrices du Conseil européen de la protection des données, les DPD ne participent que peu à la définition de la stratégie de protection des données. Ils semblent plus être les exécutants, pilotes, et évaluateurs de ces programmes que les stratèges.

Pourtant, 81 % des répondants à l'étude de CPO Magazine sont au moins cadres, dont 41 % sont des directeurs ou administrateurs de l'entreprise. Une telle réponse pourrait avoir deux justifications : la formulation de la politique de gouvernance des données est une décision collégiale, et pas l'œuvre d'une seule personne dans la plupart des organisations, ou les DPD ne disposent pas d'une autonomie et de ressources suffisantes pour s'acquitter efficacement de leurs missions.

L'impact du confinement déclaré durant la crise sanitaire de la Covid-19 sur les missions des DPD

L'étude menée par Data Legal Drive, Dalloz auprès de 216 répondants du 16 avril au 22 mai 2020, DPO et juristes, montre que la mise en conformité au RPGD a accéléré avec le confinement184. Selon cette enquête, « 40 % des DPO et juristes interrogés ont mis à profit le confinement pour traiter les sujets de fond de la mise en conformité RGPD de leur entreprise, et en particulier, pour près de la moitié des répondants, la mise à jour du registre des traitements. »

[183] CPO Magazine (2020), "Data Protection and Privacy Officer Priorities Report" Lien
[184] Data Legal Drive et Dalloz (2020), "Data Privacy et COVID19" Lien



1.2.2. Des ressources insuffisantes menant à une participation amoindrie à la gouvernance

Les contraintes et les limites auxquelles font face le DPD

Le RGPD exige que l'organisme aide son DPD « en fournissant les ressources nécessaires pour exercer [ses] missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées ».[185]

En pratique cependant, cette disposition ne semble pas encore assez appliquée dans les entreprises : le *Data Protection and Privacy Officer Priorities 2020* de *CPO Magazine* nous renseigne sur les contraintes auxquelles doivent faire face le DPD.[186] **27 %** ont désigné l'obtention du budget et des ressources disponibles comme le défi numéro 1 de l'organisation. **49 %** ont fait de la gouvernance du traitement des données et de la formation d'une culture de la protection de la vie privée une priorité absolue. **20 %** font de la mise en œuvre de nouvelles technologies de protection de la vie privée une priorité uniquement lorsque les programmes de protection de la vie privée sont arrivés à maturité. **57 %** des organisations disposent d'un budget annuel de 250 000 dollars maximum pour la protection des données et de la vie privée. **76 %** des organisations

[185] Article 38, paragraphe 2 du RGPD

comptent moins de 10 employés dans des rôles axés sur la protection des données et de la vie privée.

Les trois plus grands défis à relever par le DPD dans leur organisation, selon le *Data Protection and Privacy Officer Priorities 2020*, sont la conduite du changement (54 % des répondants), la gouvernance (51 %) et le manque de ressources humaines (32 %).

La place accordée au DPD dans la gouvernance de l'entreprise

Le paragraphe précèdent suggère donc un déficit de ressources accordé aux DPD dans le cadre de leur mission, ainsi qu'un manque d'assurance quant à la prise en compte de leur avis pour élaborer la gouvernance des données.

Pourtant, le responsable du traitement et le sous-traitant doivent veiller à ce que le DPD « soit associé, d'une manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel ». Les DPD, « qu'ils soient ou non des employés du responsable du traitement, devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance ». [187]

Il est donc primordial, pour s'assurer de la bonne application des principes de gestion des données, qu'ils soient soutenus par le reste de l'entreprise, et surtout qu'ils trouvent un sponsor au plus haut niveau. À cet égard le RGPD dispose que le DPD « fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant ».[188] Dans ce sens, les lignes directrices du G29 recommandent un « soutien actif de la fonction du DPD par l'encadrement supérieur (par exemple, au niveau du conseil d'administration) ». Une telle reddition de compte directe permet d'assurer que l'encadrement supérieur soit instruit des avis et recommandations du DPD, et prennent en compte l'avis de ce dernier.[189]

Le respect de la protection des données relève de la responsabilité sociale du responsable du traitement des données, et non du DPD. En cas de dissensus entre la direction et le DPD, il devrait avoir la possibilité de faire connaitre clairement son avis divergent au niveau le plus élevé des décideurs. La responsabilité juridique du respect de la législation reste dévolue au responsable de traitement, qui doit être en mesure de le démontrer.

Dès lors, les choix stratégiques des organes de direction, notamment la place qu'ils accordent aux DPD au sein de ces organes, ou le niveau de responsabilité et d'autorité hiérarchique qui leur est dévoué, jouent donc aussi un rôle dans la qualité de la gouvernance des données mise en place.

[187] Article 38 du RGPD
[188] Article 38, paragraphe 3 du RGPD

1.3. Le rôle des organes de direction de l'entreprise

1.3.1. Le rôle des organes de direction

Le Conseil d'administration et le Comité de Direction partagent collégialement l'orientation stratégique et les décisions de gestion.

Alors que le Décret d'application de la loi Pacte est récemment entré en vigueur, les instances dirigeantes des entreprises ayant recours aux données pour créer de la valeur (*data driven*) doivent prendre en compte les enjeux liés aux données dans la définition de leur Raison d'être, et plus généralement de leur stratégie.

Le Conseil d'Administration et le Comité de Direction se retrouvent au centre de l'équation de l'équilibre à trouver entre le profit de l'actionnaire et l'intérêt général lié à la bonne gestion des données.

Selon la Note de Synthèse de la Commission Déontologie de l'Institut Français des Administrateurs[190], la détermination des composantes éthiques d'une organisation est une mission qui incombe à la direction générale sous la supervision du Conseil d'administration. Selon cette Note, le rôle du Conseil d'administration est triple :

- Faire preuve d'engagement et d'exemplarité, par exemple avec la mise en place d'un code et d'un comité éthique, ou la prise en compte de critère éthiques dans les décisions stratégiques ;
- Superviser et contrôler la démarche éthique, par exemple les risques liés aux comportements non-éthiques ;
- Démontrer une culture d'entreprise forte basée sur des valeurs communes.

La gouvernance et la protection des données sont un enjeu d'éthique qui devraient relever de ces rôles. Elles ne semblent cependant pas encore figurer parmi les priorités des organes de direction, comme en atteste le déficit relatif de reporting sur le rôle des organes de direction dans la gestion des données.

41 % des répondants à l'enquête *Data Protection and Privacy Officer Priorities 2020* de *CPO Magazine*[191], occupaient un poste de directeur ou de cadre supérieur/vice-président, ce qui atteste d'une certaine présence des responsables des données au sein des organes de direction.

On observe toutefois une implication croissante des organes de direction, qui viennent accompagner et soutenir les projets des personnels en charge des données, comme en attestent les exemples ci-dessous (purement déclaratifs issus de l'annexe 5) :

- **Orange** : le programme RGDP a été présenté au Comité des risques du Groupe et le sujet de la protection des données a été présenté au moins une fois au cours de l'année 2018 aux CEO des entités en Europe et au Comité exécutif du Groupe.

[190] Commission Déontologie de l'Institut Français des Administrateurs (2013), « Note de synthèse » Lien

- **Société Générale** : la politique de sécurisation des données personnelles est intégrée à la stratégie du Groupe en matière de sécurité.
- **Schneider** : l'exécution de la « *global data privacy policy* » est contrôlée périodiquement par la direction de l'entreprise, ce qui montre qu'elle peut aussi avoir un rôle de contrôle de la gouvernance des données.[192]

1.3.2. La distribution des rôles dans les organes de direction : la nécessité d'administrateurs conscients des enjeux de gouvernance des données

Force est de constater que les problématiques liées à la gestion des données personnelles ne sont pas prises en considération par les directions RSE et soutenabilités des entreprises, mais par les directions juridiques sous l'angle de la conformité et des obligations relatives au RGPD.

Par ailleurs, les entreprises ont tendance à faire sous-traiter la question des données et de la conformité à des cabinets d'avocats, ne disposant pas de compétences en matière de RSE. Même si la RSE a tendance à se rapprocher des organes stratégiques de l'entreprise, le numérique en reste éloigné. Il serait ainsi intéressant que les directrices et directeurs stratégie aient en charge la RSE, le numérique et l'innovation afin de se donner les moyens d'une politique d'entreprise ambitieuse.[193]

Le rattachement du DPO à la direction Juridique, DSI ou autre est un choix de gouvernance fait par l'entreprise. Dans certaines entreprises, la direction en charge de la protection des données, la DSI ou encore direction RSE, peuvent ne pas faire partie des organes de direction, ce qui est un frein à la prise en compte de ces enjeux dans la stratégie.

Cependant, il faut veiller à éviter un conflit d'intérêt si d'autres fonctions sont assignées au DPD. Le RGPD autorise les DPD à « exécuter d'autres missions et tâches ». Il exige toutefois que l'organisme veille à ce que « ces missions et tâches n'entraînent pas de conflit d'intérêts ».[194]

Les lignes directrices du Conseil européen de la protection des données concernant les DPD précise que les fonctions de directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique sont susceptibles de donner lieu à un conflit d'intérêt, ainsi que les cas où son rôle suppose la détermination des finalités et des moyens du traitement. Il peut également y avoir conflit d'intérêts, par exemple, si un DPD externe est appelé à représenter le responsable du traitement ou le sous-traitant devant les tribunaux dans des affaires ayant trait à des questions liées à la protection des données.

[193] Audition d'Axelle Lemaire
[194] Article 38, paragraphe 6 du RGPD

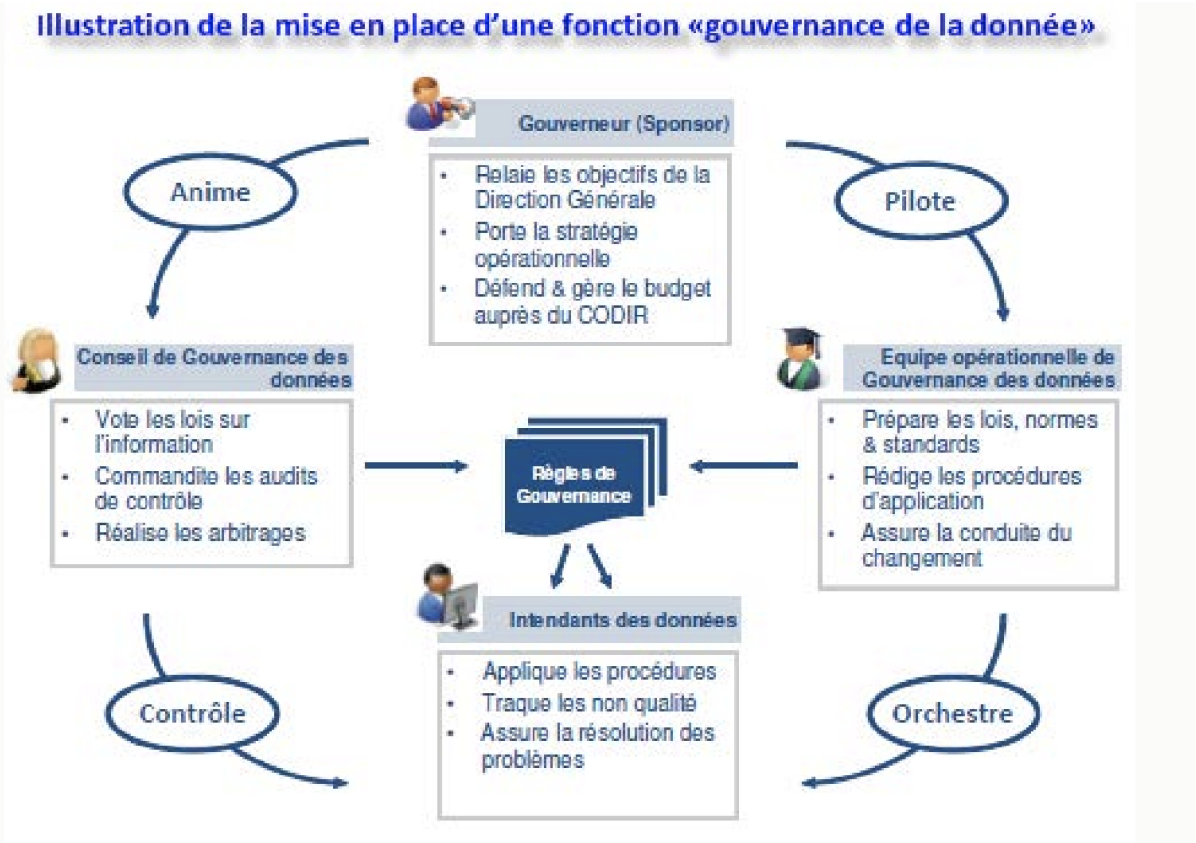
Cependant, il est important de noter que dans leurs déclarations réglementaires, certaines entreprises du CAC 40 intègrent les directeurs responsables de la gouvernance des données au sein de leur organe de direction[195] :

- **Air Liquide** : la Direction de la Sureté Numérique est rattachée à la direction du contrôle général.
- **Hermès** : les dispositifs de protection des données personnelles sont sous la responsabilité du directeur général gouvernance et développement des organisations, membre du Comité exécutif du groupe.
- **Valéo** : le programme de conformité sur la protection des données est dirigé par la Direction de l'Éthique et de la Conformité, qui est membre du Comité Exécutif du Groupe. De plus, le Directeur de la Sécurité de l'Information du Groupe est rattaché au Directeur Financier, également membre du Comité Exécutif.
- **Vivendi** : il existe un comité « *data protection* » au niveau du groupe, en présence du Secrétaire général, des représentants de la Direction des programmes, des *data protection officers* et des représentants des directions concernées par la mise en œuvre du RGPD (juridique, technique, sécurité, etc.). Il a pour objectif d'assurer un suivi centralisé des plans d'actions et des projets de chacune des entités, d'arbitrer les priorités ainsi que d'encadrer les travaux transverses (harmonisation des pratiques liées à la gestion du consentement, dispositifs d'alertes, contrats sous-traitants, etc.).[196]
- **Suez** : le DPO Groupe rapporte hiérarchiquement au Directeur Juridique Groupe, au sein du Secrétariat Général.
- **Veolia** : la direction de la Stratégie intègre le développement durable et les enjeux propres à l'innovation et au numérique.

L'illustration suivante, du cabinet de conseil Solucom, depuis devenu Wavestone, vise à schématiser le rôle des différentes parties-prenantes dans la mise en place d'une gouvernance des données. Bien que datant de 2011, elle rend compte des relations hiérarchique et du rôle des métiers de l'entreprise dans la gouvernance des données décrites jusqu'à présent. Le terme d'intendant des données correspond au rôle actuel de DPD. [197]

[195] Propos issus d'une étude du Groupe de travail sur les documents de référence des entreprises du CAC 40 publiés en 2019 (données 2018)

[197] Wavestone – Solucom (2011), "Data governance : how to bring data under control for the long term ?" Lien



Fonctions de la Gouvernance de la donnée - Une gouvernance de donnée passe par la création d'un conseil de gouvernance et de postes de data steward (ou intendants des données) dans les directions métiers. Ceux-ci exercent différents rôles dont celui d'appliquer les processus définis par le conseil. (Source : Solucom)

1.4. Intégrer en pratique la responsabilité numérique au cœur de la stratégie

1.4.1. La mise en place de comités de protection des données

Rôle

Les organisations sont confrontées à un défi difficile lorsqu'il s'agit de collecter, de partager et d'utiliser des données dans le respect de l'éthique. Il existe une demande croissante pour l'intégration de considérations éthiques dans les produits et services impliquant les données. En dehors de la simple conformité légale, il existe peu d'indications sur la manière d'intégrer ces considérations éthiques. Pour combler cette lacune, les entreprises ont la possibilité de mettre en place des comités de protection des données et intégrer certains enjeux d'éthique dans leur gouvernance des données.

L'éthique et la conformité doivent être distinguées. La conformité répond au respect de normes et de lois extérieures tandis que l'éthique répond à une réflexion collective qui correspond à se donner soi-même ses lignes de conduite. L'éthique correspond donc à un acte de responsabilisation, d'engagement et d'intégrité, qui incombe à l'entreprise. À ce propos, le rapport *IA for Humanity* porté par Cédric Villani, rappelle que *« Dans ces*

cas où la norme est inexistante, muette ou insuffisante, la responsabilité morale du développeur est accrue. »

Même lorsque les entreprises se dotent de codes de conduite, leur traduction en pratiques organisationnelles, en prise de décision et en produits et services n'a pu être que partielle. Le respect de la réglementation est la responsabilité minimale des organisations, et elle ne sera pas suffisante pour maintenir la confiance, répondre aux attentes du public en matière de responsabilité sociale, gérer les risques ou répondre aux attentes des parties prenantes.[198]

La mise en place d'un Comité de protection des données est un dispositif de gouvernance interne, qui permet une gouvernance des données forte, coordonnée, et impliquant de multiples parties prenantes. Il permet une gestion des risques unifiée, et d'accroître la maturité organisationnelle en ce qui concerne l'impact de l'utilisation des données sur les parties prenantes.

Missions

Le reporting des entreprises du CAC 40 mentionne avoir confié les missions suivantes aux comités ou groupes de travail spécialisés :

- assurer le bon déploiement de la démarche de conformité et de sécurité ;
- alerter en cas d'activité suspecte ;
- s'adapter à l'évolution de la règlementation ;
- mutualiser et diffuser les bonnes pratiques ;
- analyser les typologies de plainte ;
- revoir les procédures internes ;
- poser les bases d'une gouvernance des données ;
- supporter les métiers.

En résumé, on peut les synthétiser en 4 missions clés :

1. Rassembler des personnes possédant la gamme d'expertise nécessaire pour analyser, évaluer et répondre efficacement à des problèmes complexes.
2. Être réactif aux progrès rapides des capacités technologiques et aux nouvelles applications.
3. Développer les normes, les cas, les jurisprudences et les ressources à utiliser dans les processus décisionnels.
4. Constituer un organe de gouvernance capable d'apprendre, de s'adapter et d'être un référentiel de connaissances institutionnelles.

Qui y participe ?

Les comités de protection des données peuvent être formels ou informels. Une entreprise peut faire travailler plusieurs directions de concert en mode projet sans pour autant officiellement former un comité de protection des données. Par ailleurs, la

[198] Accenture (2019), "Building Data and AI ethics commitees" Lien

démarche de protection des données peut être confié à une seule Direction, souvent la direction juridique ou de la conformité, ou la DSI.

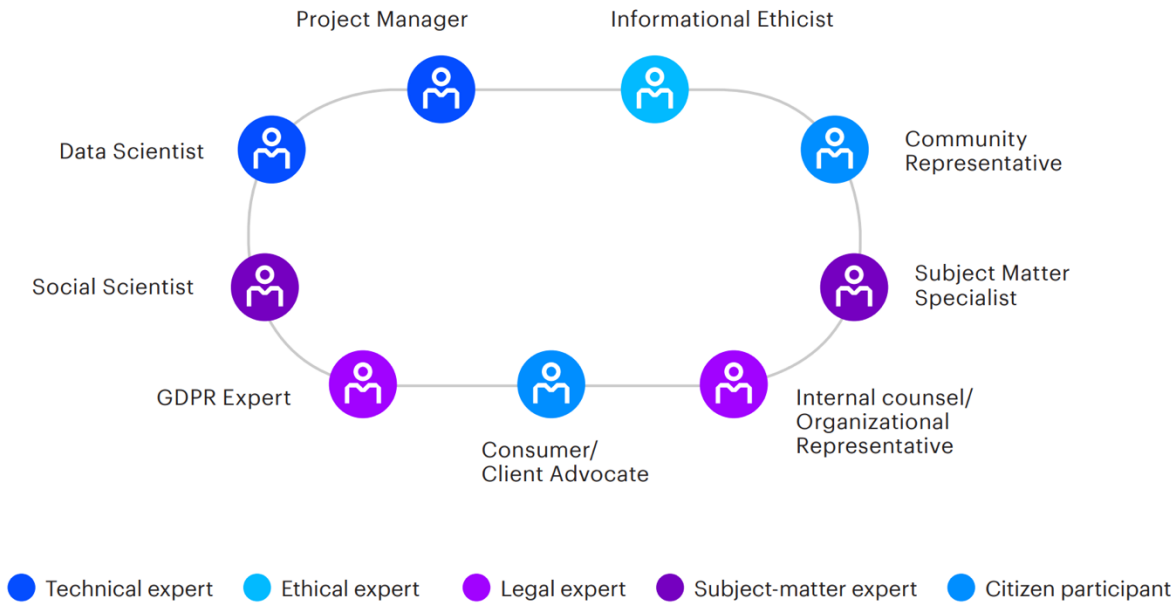
Dans le cas où une entreprise ne crée pas un comité spécialisé, de nouveaux objectifs liés aux données peuvent être confiés à d'autres comités déjà existants, par exemple le Comité de sécurité, le comité d'audit ou le comité des risques.

Il est souhaitable de faire participer à la fois des fonctions techniques ou non-techniques, et des responsables fonctionnels et opérationnels, qui peuvent apporter différents points de vue. Dans les cas où une entreprise créé un comité, les acteurs suivants ont été cités dans les reporting du CAC 40 comme en faisant partie : le ou les DPD, responsable de la sécurité des systèmes d'informations, responsable du marketing digital, le responsable RH, la Direction Éthique.

Dans les grands groupes comprenant plusieurs entités, comprenant chacune des DPD, ce comité peut aussi être composé exclusivement du réseau de DPD du groupe, ou par les référents des différents métiers ou pays en charge de la protection des données.

Dans les deux entreprises comptant un comité spécialisé sur l'éthique de la donnée, ceux-ci sont composés d'un panel plus large de parties prenantes : le *Data ethics panel* d'Axa est composé d'experts universitaires, de membres de think tank ou d'anciens membres d'organismes de réglementation ; celui d'Orange est une structure mixte composée d'acteurs externes, des représentants des clients et des collaborateurs.

Accenture, dans son rapport *Building Data and AI Ethics Committee*[199], propose hypothétiquement la composition souhaitable d'un Comité d'Éthique des données.



[199] idem

Les pratiques des entreprises telles que déclarées dans leur reporting[200]

Accor, Bouygues, Danone, Essilor, L'Oréal, Kering, Orange, Publicis, Sodexo, Véolia, Vinci et Vivendi ont mis en place un Comité ou un groupe de travail spécialisé soit sur le RGPD, sur la protection des données ou sur la cyber sécurité.

L'Oréal a, par ailleurs, mis en place une organisation reposant sur un Comité de Gouvernance Groupe, un Comité de Pilotage mondial, ainsi que sur un réseau de référents Métiers, Zones, Pays en charge de la protection des données personnelles, qui animent l'ensemble des acteurs opérationnels impliqués.

Kering, en plus d'avoir mis en place un comité informel chargé de la conformité avec le RGPD, a créé un centre de Sécurité Opérationnelle afin d'identifier et résoudre les menaces d'actes malveillants et incidents.

Orange et Axa ont mis en place comité d'éthique sur l'usage de la *data*.

Au sein d'**AXA**, le *Data protection and ethics panel*[201], dédié à la responsabilité d'AXA sur les données est indépendant, et conseille l'entreprise sur les décisions à prendre en matière de protection des données et d'utilisation de l'IA. Le comité consultatif réunit des experts en matière de données sur la vie privée, notamment des universitaires, des membres de groupes de réflexion ou d'anciens membres d'organismes de réglementation. Trois thèmes principaux sont abordés :

- Politiques publiques, législation et éthique
- Concept de "*privacy-by-design*" et progrès technologique
- Technologie de l'information, marketing et aspects opérationnels

Parmi les questions abordées figurent la confiance dans un monde d'interaction numérique, l'utilisation des données dans le secteur des assurances, les échanges internationaux de données dans un contexte de cadres réglementaires nationaux différents, la construction d'un marché unique numérique et son impact pour AXA et ses clients.

Ce panel a permis de prendre des décisions de responsabilité numérique de l'entreprise allant au-delà du droit, par exemple ne pas revendre les données personnelles des clients même en ayant le droit.[202]

[200] Partie établie grâce à l'analyse des documents de référence des entreprises du CAC40 réalisée par le groupe de travail.
[201] https://www.axa.com/en/about-us/data-privacy
[202] Audition de Cécile Wendling

L'échec du comité d'éthique des données de Google

En mars 2019, Google a créé un Advanced Technology External Advisory Council (ATEAC) qui aurait eu pour fonction d'apporter des perspectives sur certains des défis qui découlent de l'éthique de l'IA, comme la reconnaissance faciale et l'équité dans le *machine learning*.[203]

Mais moins d'une semaine après son lancement, Google a été forcé de le dissoudre. Constitué de huit membres, ATEAC a fait face à une levée de boucliers : par le biais dans une pétition[204], 2256 employés de Google, ainsi que des personnalités du monde académique, et de l'industrie se sont insurgés contre ce comité d'éthique de l'IA, exigeant notamment la démission de l'un des membres, connue pour ses opinions homophobes, climatosceptiques et racistes.[205]

Cet échec n'interdit pas de continuer les actions privilégiant l'éthique. Il illustre, par ailleurs, la difficulté que peuvent avoir les multinationales du numérique à être en phase avec les implications sociales des technologies qu'ils mettent en œuvre.

1.4.2. Évaluation des risques, audit et mise en conformité

1.4.2.1. Une pratique nécessaire, avantageuse, mais encore peu mise en pratique

Le risque prend une place importante dans le RGPD : les termes de risques et d'analyse d'impact y apparaissent plus de 100 fois. Plusieurs aspects du Chapitre IV du Règlement visent à améliorer l'évaluation des risques par les organisations. Mais il ne contient pas de définition de la notion de « risques », ni d'instructions pour mettre en place une procédure d'évaluation des risques.

La gestion des risques en interne et donc la responsabilisation de l'organisation face à ceux-ci deviennent donc des enjeux majeurs dans le renforcement de la protection des données personnelles. Cette gestion consiste en une collection de bonnes pratiques qui renforcent ses défenses et protègent ses activités, qui vise à une mise en conformité qui implique plusieurs acteurs.

Dans un contexte d'évolution technologique, les risques liés au numérique auxquels font face les entreprises sont en mutation constante, rendant plus critique que jamais leur évaluation et leur audit régulier par les entreprises. Il existe aussi un enjeu sur ce sujet lors du choix entre le recours à un *data center* interne ou au *cloud* : selon un rapport de CapGemini, les dirigeants interrogés identifient les plateformes c*loud* comme technologie la plus utilisée pour évaluer les risques liés à la protection des données.

[203] Walker K. (2019), "An external advisory council to help advance the responsible development of AI" Lien
[204] Googlers against transphobia (2019) Lien
[205] Piper K. (2019), "Google cancels AI ethics board in response to outcry" *Lien*

Le même rapport formule la recommandation d'« industrialiser l'évaluation des risques ». Il recommande de mettre en place des *Security Operations Center* (Centres d'opérations de Sécurité) qui surveilleraient les menaces et les vulnérabilités externes et internes pour améliorer la capacité de l'organisation à surveiller et à prévenir les violations de données.

Les entreprises appliquant le RGPD et se mettant en conformité avec les principes de protection des données constatent des effets positifs dont l'augmentation de la confiance des consommateurs et des salariés et l'augmentation des pratiques de cyber-sécurité.

Les sollicitations qu'elles reçoivent soulignent l'importance de cette conformité : presque toutes les organisations (90 %) ont reçu de la part des personnes concernées des questions relatives au RGPD et 13 % ont reçu plus de 5 000 questions au cours de l'année écoulée.

Les entreprises ont encore du chemin à parcourir pour atteindre la conformité : un an après la mise en application du RGPD, en mai 2019, seulement 28 % des entreprises disent être conformes au RGPD, et 30 % "proches de la conformité".[206]

1.4.2.2. L'évaluation des risques effectuée par les entreprises

L'évaluation des risques est une démarche qui s'appuie sur les bases suivantes :

- Évaluer précisément le propre profil de risque
- Prendre les mesures adéquates pour réduire les risques de sécurité identifiés
- Répéter très régulièrement les processus d'évaluation et de réduction des risques : le RGPD exige que l'évaluation des risques soit un processus continu.[207]

Pratiques des entreprises

Parmi les entreprises du CAC 40, 32 sur 40 identifient dans l'évaluation des risques de leur Déclaration de performance extra-financière (DPEF) des risques liés à l'utilisation et la protection des données.

Les risques les plus souvent mentionnés sont les cyberattaques, sous la forme de compromission ou de vol des données, ainsi que la perpétuelle mutation et innovation des menaces cyber (Ransowmare, DDOS, Hameçonnage). Le risque juridique de conformité aux différentes réglementations, et les risque de sanction et d'impact réputationnel afférents, sont également mentionnés. Les renforcements et possibles évolutions à venir de ces réglementations sont également affichées comme un risque par certaines entreprises. Enfin, un plus faible nombre d'entreprise mentionne le risque lié à la complexité de gérer une grande quantité de données, ou encore évoque les nouveaux défis liés aux technologies émergentes (Internet des Objets, véhicules connectés).

[206] CapGemini (2019), "Championing Data Protection and Privacy" Lien
[207] Lussan P. (2018), « Comment bien démarrer avec l'évaluation des risques exigée par le RGPD ? » Lien

Classification des différents types de risque

Risques d'image et risques business

Une étude IBM/Ponemon Institute a permis de démontrer que sur 350 entreprises réparties sur 11 pays différents, une violation de données représente un coût total consolidé de 3,62 millions de dollars en 2017, qui le rend supérieur de 20 % par rapport à 2013.[208]

Ainsi, une violation de données, qui ne seraient pas assez sécurisées, peut amoindrir la confiance des clients et heurter l'image de l'entreprise. L'entreprise s'expose donc à la perte de clients et à une baisse de son chiffre d'affaire.[209]

Un exemple d'entreprise ayant reçu un avertissement public de la CNIL du fait d'une conservation de données bancaires non sécurisées est Fnac direct, l'éditeur du site Fnac.com, ce qui a porté atteinte à l'image de l'entreprise.[210]

Risques juridiques

1. Pour le responsable de traitement

La CNIL peut dénoncer au Procureur de la république les infractions à la loi. Cependant, les condamnations restent rares malgré leur pouvoir dissuasif, qui reste à nuancer pour des entreprises telles que les GAFA, pour qui de telles sanctions ne représentent en général qu'une faible partie de leur chiffre d'affaires.

2. Pour le sous-traitant

Le RGPD renforce les responsabilités du sous-traitant, tel que détaillé dans la partie 3.3.1. Celles-ci sont contractualisées dans le contrat le liant au prestataire de service.

Le règlement prévoit que le sous-traitant sera considéré comme responsable de traitement et par conséquent du dommage, en cas de non-respect de ses obligations ou s'il agit en dehors des instructions du responsable de traitement.

Risque opérationnel

Depuis le dispositif Bale II, le risque opérationnel est défini comme le « risque de perte résultant de procédures internes, de membres du personnel ou de systèmes inadéquats ou défaillants, ou d'évènements extérieurs. »[211]

Le RGPD nécessite d'entreprendre une approche par les risques opérationnels pour permettre une meilleure gouvernance des données. La mise en conformité doit donc passer par une analyse sur l'organisation des systèmes d'information, et du pilotage.

Risque financier

[208] Ponemon Institue, 2017 Cost of Data Breach Study : Global Overview
[209] Audition de Rémi Dusaud
[210] Ercolani E. (2012), « Conservation des données : la FNAC avertie par la CNIL » Lien
[211] Banques des Réglements Internationaux (2003), « Saines pratiques pour la gestion et la serveillance du risque opérationnel » Lien

Le risque financier est d'abord constitué par les peines très lourdes qui peuvent être infligés par la CNIL. Mais il présente une deuxième dimension : étant lié à tous les autres risques, l'entreprise doit prévoir un budget conséquent pour faire face à ceux-ci.

Risque extraterritorial

La partie 1.5 « Les outils d'encadrement global des transferts des données » détaille les modalités des obligations en ce qui concerne les transferts de données extraterritoriaux. Le responsable de traitement doit offrir les outils permettant d'encadrer ces transferts.

Risque d'efficacité

Le risque d'efficacité et de performance est le risque lié à l'impact sur la productivité des processus et sur l'efficience opérationnelle, de tous les autres risques. Il relève aussi de la capacité de l'entreprise à mobiliser des ressources pour construire sa responsabilité numérique.

1.4.2.3 L'audit de conformité RGPD : plus qu'un outil de mise en conformité

Une entreprise qui souhaiterait vérifier dans quelle mesure le règlement européen est respecté peut demander à un auditeur externe de réaliser un audit de conformité RGPD. Celui-ci permet de vérifier sa conformité vis-à-vis de la loi, et de mettre en place les actions nécessaires, afin de se prémunir contre d'éventuelles sanctions.

Il s'agit d'une procédure recommandée par la CNIL, mais elle constitue aussi un facteur de compétitivité en renforçant la confiance des parties-prenantes. L'audit ne peut être conduite que par des auditeurs reconnus et labellisés par la CNIL.

L'audit de conformité des données personnelles de l'entreprise tend à dépasser les exigences règlementaires en matière de sécurité. L'auditeur, en établissant son programme d'audit et ses axes d'investigation, joue un rôle dans le respect des données « privacy by design » puisque la démarche d'audit va permettre de déceler les éventuels dysfonctionnements, d'en identifier les causes et les impacts et d'établir des recommandations. Ainsi, l'auditeur a pour rôle d'analyser les mécanismes permettant de s'assurer que l'information est obtenue légalement, de vérifier la qualité de la conservation des données, de la documentation en vigueur, de la conformité aux droits à la vie privée et à la législation.[212]

Lors du contrat entre responsable de traitement et sous-traitant, des clauses d'audibilité peuvent être intégrés au contrat.

1.4.2.4 Les contrôles et audits interne à l'aune du RGPD : les principes du Privacy Impact Risk Assessment

L'« analyse d'impact relative à la protection des données » (AIPD) est plus souvent identifiée sous son nom anglophone, le « *privacy impact assessment* » (PIA). Le RGPD

[212] « L'audit de la protection des données personnelles à l'aune du Règlement Général sur la Protection des Données », Nadège Rispoli, sous la direction de M. Jacques Vera, 2017

utilise le terme de « *data protection impact assessment* » (DPIA). Ces termes sont tous synonymes.

L'article 35 du RGPD dispose que « lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés de personnes physiques, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, **le responsable de traitement effectue, avant le traitement une analyse de l'impact des opérations de traitement envisagées sur la protection des données** à caractère personnel ».

En d'autres termes, l'AIPD présente l'avantage d'offrir une gestion des risques flexibles, puisque le responsable de traitement évalue lui-même les risques. Cette flexibilité doit cependant toujours rester dans le principe de responsabilité (*accountabily*) et doit être capable de rendre des comptes. Un AIPD est un processus qui vise à apporter la preuve de la conformité aux règles existantes.

Qu'est-ce que l'AIPD ?

L'AIPD se décompose en trois parties :

1. Une description détaillée du traitement mis en œuvre, comprenant tant les aspects techniques qu'opérationnels
2. L'évaluation, de nature plus juridique, de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux (finalité, données et durées de conservation, information et droits des personnes, etc.) non négociables, qui sont fixés par la loi et doivent être respectés, quels que soient les risques ;
3. L'étude, de nature plus technique, des risques sur la sécurité des données (confidentialité, intégrité et disponibilité) ainsi que leurs impacts potentiels sur la vie privée, qui permet de déterminer les mesures techniques et organisationnelles nécessaires pour protéger les données.[213]

Une analyse d'impact relative à la protection des données est requise dans les cas cités dans la liste d'opérations de types de traitement de la CNIL, disponible en note de bas de page[214], ou encore dans le cas où le traitement remplit au moins deux des neuf critères issus des lignes directrices du G29[215]. La CNIL publie également une liste des types d'opérations de traitement pour lesquelles une analyse d'impact relative à la protection des données n'est pas requise.[216]

Comment la réaliser ?

Le logiciel open source d'évaluation de l'impact sur la vie privée (PIA) fourni par la CNIL facilite la conduite et la formalisation d'analyses d'impact relatives à la protection des

[213] https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-lanalyse-dimpact-relative-la-protection-des-donnees-aipd
[214] https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-requise.pdf
[215] G29 (2017), « Lignes directrices concernant l'AIPD » Lien
[216] https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-non-requise.pdf

données (AIPD).[217] Notons que cela est une aide précieuse, un accompagnement, pour les PME qui n'ont pas forcément des équipes expertes de cette démarche.

Ce guide décrit la méthode suivante :

1. délimiter et décrire le contexte du (des) traitement(s) considéré(s) ;
2. analyser les mesures garantissant le respect des principes fondamentaux : la proportionnalité et la nécessité du traitement, et la protection des droits des personnes concernées ;
3. apprécier les risques sur la vie privée liés à la sécurité des données et vérifier qu'ils sont convenablement traités ;
4. formaliser la validation du PIA au regard des éléments précédents ou bien décider de réviser les étapes précédentes.

Le G29, aujourd'hui devenu le Conseil européen de protection des données, a édité des « Lignes directrices concernant l'analyse d'impact relative à la protection des données (AIPD) et la manière de déterminer si le traitement est susceptible d'engendrer un risque élevé », qui s'emploie à clarifier les dispositions pertinentes du RGPD afin de faciliter le respect de la législation par les responsables du traitement et de procurer une sécurité juridique aux responsables du traitement tenus d'effectuer une AIPD.[218]

Qui est impliqué dans la réalisation de l'Analyse d'Impact relative à la Protection des Données ?

La CNIL précise que « *Si le responsable de traitement a désigné un délégué à la protection des données, il lui demande conseil et le charge de vérifier l'exécution de l'AIPD. Si un sous-traitant intervient dans le traitement, il doit fournir son aide et les informations nécessaires à la réalisation de l'AIPD. Les métiers (RSSI, maîtrise d'ouvrage, maîtrise d'œuvre) peuvent aider à la réalisation d'AIPD en fournissant les éléments adéquats Le responsable de traitement devrait également demander l'avis des personnes concernées (par le biais d'une enquête, d'un sondage, d'une question formelle aux représentants du personnel), ou le justifier sinon.* »[219]

1.5 Les outils d'encadrement global des transferts des données

L'innovation fondée sur les activités à forte intensité de données, y compris l'apprentissage automatique et l'intelligence artificielle (IA), bénéficient de l'ouverture et de l'interconnexion des systèmes et réseaux, qui favorisent la circulation efficace, fluide et peu coûteuse des données parmi une population d'acteurs virtuellement illimitée. L'amélioration de l'accès aux données peut maximiser l'utilité sociale et économique des données, à condition que tous les acteurs concernés respectent les différents mécanismes prévus pour l'encadrement du transfert des données.

L'article 25.1 de la directive européenne 95/46/CE relative aux données à caractère personnel n'autorise « le transfert vers un pays tiers de données à caractère personnel

[217] https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

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

faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert [...] que si [...] le pays tiers en question assure un niveau de protection adéquat ».

Le Règlement général sur la protection des données (RGPD) prévoit qu'un transfert de données à caractère personnel vers un pays tiers peut être réalisé si le responsable du traitement ou le sous-traitant a prévu des garanties appropriées (article 46 du RGPD).

Actuellement, les deux mécanismes les plus appropriés pour ce type de transfert de données personnelles sont les BCR (règles d'entreprise contraignantes), les clauses contractuelles types (également appelées SCC (clauses contractuelles types), et les auto-certifications.

1.5.1 Règles d'entreprises contraignantes (Binding Corporate Rules - BCR)

Les règles d'entreprise contraignantes (communément appelées BCR) permettent à des groupes d'entreprises d'encadrer juridiquement leurs transferts de données hors de l'Union européenne (UE) tout en leur offrant la possibilité d'engager une démarche de mise en conformité globale à l'échelle de tout le groupe. Cela permet d'unifier les règles concernant le traitement des données personnelles par leurs filiales.

Elles sont définies dans l'article 4 du RGPD : « règles internes relatives à la protection des données à caractère personnel qu'applique un responsable du traitement ou un sous-traitant établi sur le territoire d'un État membre pour des transferts ou pour un ensemble de transferts de données à caractère personnel à un responsable du traitement ou à un sous-traitant établi dans un ou plusieurs pays tiers au sein d'un groupe d'entreprises, ou d'un groupe d'entreprises engagées dans une activité économique conjointe. »

Les BCR représentent une « garantie appropriée » au sens du RGPD pour assurer la base juridique des transferts (article 46.2(b)). Elles sont conçues par les groupes comme un moyen de *data management*, c'est-à-dire une preuve de la mise en conformité dans une optique de formalisation de leurs politiques en matière de protection des données.

Un groupe d'entreprises peut soumettre à l'approbation d'une autorité de contrôle compétente un projet de BCR à condition que ces règles :

- soient juridiquement contraignantes ;
- soient mises en application par toutes les entités concernées du groupe d'entreprises ;
- confèrent expressément aux personnes concernées des droits sur le traitement de leurs données personnelles ;
- répondent aux exigences prévues par l'article 47 du RGPD.

En mettant en place des BCR, la société met en place une convention interne basée sur des référentiels. Ceux-ci ont été étoffés et mis à jour suite au RGPD. La CNIL est en charge du contrôle de ces conventions et de ces référentiels.

La CNIL estime ainsi que les BCR sont des outils à destination des grands groupes dont les dimensions sont telles qu'elles ont des conséquences sur les transferts internationaux. Dans le même temps, la mise en place de BCR nécessite la création d'une structure de gouvernance « unique, complète et harmonisée » au sein du groupe. L'implantation grandissante des BCR les conduit à s'imposer comme la « traduction de leur politique globale en matière de protection des données personnelles. »

A ce titre, entre 2007 et le 25 mai 2018, 151 BCR ont été approuvées par l'ensemble des autorités de protection européennes. La CNIL fait également le constat que depuis l'adoption du RGPD, la demande d'approbation de BCR est en croissance constante, aussi bien en France qu'à l'étranger.[220]

Référentiels du BCR

Les référentiels du BCR définissent un contenu minimal imposé. Ainsi, les demandeurs doivent respecter les engagements du RGPD et expliciter dans les BCR la manière dont ils mettent en œuvre :

- un régime de responsabilité pesant sur le siège européen ou sur la filiale européenne responsable par délégation de la protection des données (ou autre régime de responsabilité, sur justification) ;
- une procédure de formation du personnel quant aux règles posées par les BCR ;
- une procédure d'audit pour veiller au contrôle du respect des BCR ;
- une procédure interne de gestion des plaintes ;
- un réseau de délégués à la protection des données ou d'employés qualifiés pour la gestion des plaintes, la surveillance et le contrôle du respect des règles internes ;
- une procédure permettant de déterminer l'opportunité de conduire une analyse d'impact sur la vie privée (AIPD) ;
- pour les BCR « sous-traitant », les obligations du sous-traitant envers le responsable de traitement ;
- des mesures techniques et organisationnelles appropriées permettant de respecter les principes de la protection des données.[221]

Suite à la mise en application du RGPD, les exigences minimales ont été étendues pour inclure des détails supplémentaires tels que les coordonnées de chaque membre du groupe, la description des principes de *privacy by design* et *privacy by default* (protection de la vie privée dès la conception) les droits des personnes concernées, les obligations d'information et les coordonnées des personnes chargées de maintenir les procédures de formation et de conformité.

La procédure d'approbation

La procédure d'approbation du BCR prend 12 à 16 mois, et comporte plusieurs étapes détaillées dans l'annexe 5. En premier lieu, l'organisme candidat désigne une autorité compétente qui notifie les autres autorités européennes. Ensuite, des échanges ont lieu

[220] https://www.cnil.fr/fr/ce-quil-faut-savoir-sur-les-regles-dentreprise-contraignantes-bcr
[221] https://www.cnil.fr/fr/comment-preparer-un-dossier-de-bcr

entre l'autorité compétente et l'entreprise jusqu'à satisfaction de l'instruction du dossier. Enfin, après saisine du Comité européen de protection des données, la délibération est éventuellement adoptée par la CNIL qui notifie l'entreprise et publie l'avis du Conseil européen de protection des données (CEPD).

Pratiques des entreprises du CAC 40

AXA : AXA est le premier groupe d'assurance à avoir adopté les Binding Corporate Rules (BCR). Ils ont été approuvés par la CNIL en France et par 15 autres autorités européennes de protection des données. Aujourd'hui, 315 entités d'AXA ont adhéré à la BCR.

Bouygues : une certification est en cours auprès de la CNIL. Cependant, en 2018, la CNIL a prononcé une sanction pécuniaire d'un montant de 250 000 euros, considérant que la société avait manqué à son obligation d'assurer la sécurité des données personnelles des utilisateurs de son site, conformément à l'article 34 de la loi Informatique et Libertés.

Capgemini : Les Binding Corporate Rules ont été approuvés par la CNIL en Mars 2016. L'entreprise interprète sa BCR comme un cadre complet de protection des données personnelles définissant une approche en matière de responsabilité dans le traitement des données à caractère personnel.

Ces BCR s'appliquent à toutes les données à caractère personnel traitées au sein de Capgemini, que ce soit en tant que responsable du traitement ou en tant que sous-traitant.

Hermès : Hermès perçoit ces BCR comme un outil essentiel pour promouvoir efficacement une culture de la protection des données. Elles favoriseront également le respect de la protection des données et faciliteront la gestion des données à caractère personnel au sein de l'ensemble du groupe. Hermès a mis en place une structure de gouvernance efficace pour gérer ces obligations en matière de protection des données.

Schneider Electric : Les BCR de cette en entreprise, adoptées en 2012, sont reprises dans une publication externe de sa *global data privacy policy*. L'exécution de ce plan d'action est contrôlée périodiquement par la direction de l'entreprise assistée par le délégué à la protection des données groupe. Ce règlement est une opportunité pour Schneider Electric de renforcer son dispositif global de gouvernance de la protection des données personnelles.

Sodexo a déposé des BCR auprès de la CNIL qui restent en cours d'instruction.

Il ressort des documents de référence des entreprises du CAC40 que les BCR sont un cadre de responsabilité qui s'intègre dans une stratégie plus large de la protection des données. Les BCR constituent un outil essentiel de gouvernance des données, et permettent de mettre en place des bonnes pratiques contraignantes contrôlées par une autorité publique.

Un BCR approuvé et effectivement mis en œuvre garantit l'application d'un plan de gouvernance de la protection des données adapté et de processus uniformes dans toute l'organisation. Cela améliore la qualité et la maturité de la sécurité des données et de la gestion des données dans l'ensemble du groupe.

Les BCR offrent de multiples avantages aux groupes d'entreprises. C'est un moyen d'officialiser et de faire connaître le programme de gestion de la protection des données du groupe. Cela offre la possibilité de démontrer à ses parties-prenantes (particulièrement régulateurs, employés, clients et partenaires commerciaux) que l'organisation assume la responsabilité de la sécurité des informations personnelles et permet la transparence en divulguant la façon dont elle traite les données au sein du groupe. Outre la conformité, les BCR contribuent à promouvoir une culture d'utilisation sûre et responsable des données dans l'ensemble du groupe.

En ce sens, les BCR sont un levier de la RSE en ce qu'elles permettent de contrôler et uniformiser les pratiques de gestion des données entre les groupes d'entreprise, dans toutes leurs filiales. Ce levier permet donc, en allant au-delà du minimum légal, de limiter l'impact négatif de l'entreprises sur ses parties prenantes, dans le cadre des transferts de données.

1.5.2 Clauses Contractuelles Types

La CNIL détaille que « Les clauses contractuelles permettent d'encadrer les transferts de données personnelles hors de l'Union européenne. Elles ont pour but de faciliter la tâche des responsables de traitement dans la mise en œuvre de contrats de transfert. »

Elles sont instituées par la décision de la Commission européenne du 5 février 2010[222] relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen.

Elles constituent une alternative aux *Binding Corporate Rules*.

« On distingue les transferts de responsable de traitement à un responsable de traitement et les transferts de responsable de traitement à un sous-traitant. Il existe donc deux types de clauses afin d'encadrer chacun de ces transferts.

Clauses contractuelles encadrant les transferts de données personnelles d'un responsable de traitement à un autre responsable de traitement.

Afin d'encadrer les transferts de données entre deux responsables de traitement, il existe deux ensembles de clauses contractuelles applicables aux transferts.

Le premier ensemble résulte de la décision de la Commission du 15 juin 2001 (2001/497/CE) et le second de la décision de la Commission du 24 décembre 2004 (2004/915/CE) modifiant la décision 2001/497/CE. »

[222] Journal Officiel de l'Union européenne (2010), « Décision de la Commission du 5 février 2010 » Lien

Clauses contractuelles encadrant les transferts de données personnelles d'un responsable de traitement à un sous-traitant

Les Clauses Contractuelles Types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers résultent de la décision de la Commission du 5 février 2010 (2010/87/UE). Ce jeu de clauses remplace, depuis le 15 mai 2010, les Clauses contractuelles antérieures de 2001 (décision 2002/16/CE). »[223]

1.5.3 Privacy Shield

« Le Bouclier de Protection des Données, mieux connu sous le nom de « Privacy Shield » , est un mécanisme d'auto-certification pour les entreprises établies aux États-Unis qui a été reconnu par la Commission européenne comme offrant un niveau de protection adéquat aux données à caractère personnel transférées par une entité européenne vers des entreprises établies aux États-Unis. Ce mécanisme est par conséquent considéré comme offrant des garanties juridiques pour de tels transferts de données.

Le Bouclier de Protection des Données s'applique à tout type de données à caractère personnel transférées par une entité depuis l'UE aux États-Unis, notamment des données commerciales, de santé ou de ressources humaines à condition que la société destinataire au États-Unis ait adhéré au dispositif. »[224]

[223] CNIL, « Les clauses contractuelles types de la Commission européenne » Lien
[224] https://www.cnil.fr/fr/le-privacy-shield

Accord Safe Harbor[225]

Il s'agit d'un programme conclu entre le *Department of Commerce* américain et Commission européenne adopté en juillet 2000. La décision 2000/520 est un programme d'autorégulation déclaratif par lequel les organisations qui y adhèrent doivent se déclarer auprès de la Commission européenne, et s'engager à assurer aux données européennes une protection équivalente à celle accordée au sein de l'Union européenne. Cela constitue ainsi une exception à l'interdiction de principe d'exportation des données à caractère personnel européennes, hors de l'Union européenne.

Suite au recours d'un étudiant autrichien ayant saisi les juridictions irlandaises, pays d'établissement de Facebook, la Cour de Justice de l'Union européenne a été saisie dans le cadre d'une question préjudicielle sur la légalité de Safe Harbour. Dans le contexte des révélations d'Edward Snowden sur la surveillance généralisée du programme PRISM, qui permettent aux autorités US d'accéder à des données stockées aux USA, la CJUE l'invalide le 6 octobre 2015.

En remplacement du Safe Harbour, le EU-US Privacy Shield (bouclier de protection des données) est, officiellement, entré en vigueur en août 2016. Cet accord, conclu grâce à la signature du Judicial Redress Act226 par l'ancien président américain Barack Obama en février 2016, doit garantir le respect des normes européennes en matière de protection des données personnelles pour les transferts vers les États-Unis – notamment au travers de l'utilisation massive et quotidienne des réseaux sociaux. Ainsi, les services en ligne comme Facebook, Amazon ou Google seront légalement autorisés à collecter les données personnelles de leurs utilisateurs et à transmettre les paquets de données aux États-Unis ; pour cela, le gouvernement américain garantit le respect de certaines normes afin d'atteindre le niveau des standards européens en la matière.

Dans le cadre du Privacy Shield, les États-Unis se sont également engagés à créer un médiateur au sein du Ministère des Affaires Étrangères auprès duquel les citoyens de l'Union européenne pourront s'adresser pour déposer quelconque plainte et qui indiquera si la législation a été respectée.

Une fois par an, le fonctionnement de l'Accord est évalué et la Commission européenne réalise un rapport en coopération avec le Département du commerce américain.

Il est à noter que les autorités américaines peuvent continuer de collecter, légalement, des données à des fins de surveillance. L'accord limite le recours à la surveillance de masse à six objectifs spécifiques : la lutte contre le terrorisme, la détection et l'opposition à certaines activités de puissances étrangères, la lutte contre la prolifération des armes de destruction massive, la cybersécurité, la détection de menaces pour les Etats-Unis ou les forces alliées et la lutte contre les menaces et les crimes transnationaux.

[225] Iteanu O. (2016), « Safe Harbour et Privacy Shield pour les nuls » Lien
[226] Loi sur la réparation judiciaire signée par Barack Obama le 25 février 2016 et permettant aux citoyens de l'Espace économique européen d'intenter une action aux Etats-Unis lors d'une violation du droit de la protection des données personnelles

Le Privacy Shield a mené à de fortes réserves en 2019. Le Comité européen de la protection des données, dont fait partie la CNIL, estime que certains domaines requièrent une attention particulière tels que la bonne application des exigences du Privacy Shield au regard des transferts ultérieurs des données, le cas des sous-traitants ou encore le processus de recertification des entreprises liées au dispositif.

1.6 Former et éduquer au numérique

Si aujourd'hui les français sont relativement bien équipés et ont accès à Internet (dont l'accès s'est démocratisé avec le smartphone), l'enjeu demeure la diffusion des bonnes pratiques et l'émergence d'une culture numérique.

Les plus jeunes (de la « Génération Z », nés entre 1998 et 2016), bien que nés dans l'ère des nouvelles technologies, ne possèdent pas toujours une pratique étendue des outils numériques. Si les usages récréatifs sont maîtrisés, l'usage des outils et des applications à vocation scolaire ou professionnelle ne l'est pas toujours[227].

En parallèle, les outils numériques sont de plus en plus mobilisés pour favoriser l'apprentissage. Les tableaux numériques, les tablettes ou des plates-formes d'échanges entre le corps enseignant et les familles ont investi les établissements scolaires. Les familles familiarisées avec ces outils accompagnent leurs enfants dans leur scolarité. En revanche, pour celles qui ne parviennent pas à s'en saisir pleinement, le numérique représente un facteur d'exclusion supplémentaire. Dès lors, l'école ne parvient plus à compenser les écarts initiaux de capital culturel et matériel. Loin de réduire les inégalités d'apprentissage, ces outils peuvent creuser les inégalités sociales, mettant à mal notre pacte républicain, annihilant tout espoir d'ascension sociale.

Pour les administrés, la dématérialisation des procédures administratives peut représenter un véritable parcours d'obstacles. Une étude du CREDOC estime qu'une personne sur quatre se dit inquiète à l'idée de réaliser toutes ses démarches en ligne (déclaration d'impôt, demande de carte d'identité, etc.). Ces difficultés d'usage sont d'autant plus exacerbées pour les plus démunis, qui dépendent de prestations sociales dont ils doivent faire les demandes (et le suivi) en ligne. Il en est de même pour bénéficier d'un accompagnement et des indemnités versés par Pôle emploi, les prestations de la CAF, l'obtention d'un titre de résidence, etc. Dès lors, l'outil numérique remet en cause l'accès aux droits des populations les plus précaires. Si de nombreuses collectivités mettent en place des actions palliatives et ouvrent des lieux de sensibilisation ou de formation au numérique, cette initiative relève d'une politique de proximité, et pose la question de l'égalité d'accès des citoyens à leurs droits. Cet enjeu a été souligné par le Défenseur des Droits, Jacques Toubon, qui recommande d'introduire dans la loi une clause de protection des usagers. Cette clause prévoirait l'obligation d'offrir une voie alternative au service numérique lors de la dématérialisation d'un service public ou d'une procédure administrative.

[227] Mission Société Numérique – Agence Nationale de la cohésion des territoires, « 13 millions de français en difficulté avec le numérique »,

Au-delà d'interroger l'accès aux droits des plus démunis, le développement des services publics sous forme numérique, et son corollaire, la disparition des interfaces physiques (guichet, réunions, etc.) se traduit par le passage d'un échange physique, de « vive voix », à celui d'une relation virtuelle, déshumanisée (mail, chatbox, interface du compte personnel, etc.)

Par ailleurs, en janvier 2020, Pôle Emploi[228] comptabilisait 775 577 salariés dans le secteur numérique dont 58 % dans l'informatique, 19 % dans les télécommunications, 9 % dans l'édition des logiciels ou encore 7 % dans le commerce et l'industrie. Les activités dont les recrutements se font le plus nombreux sont les études et le développement informatique et la maintenance informatique et bureautique.

Le numérique s'impose ainsi comme un secteur de recrutement en expansion et dont le taux d'embauche est 2,4 fois plus élevé que dans les autres secteurs. Dans les prochaines années, Pôle Emploi estime que ce sont 191 000 postes qui seront à pourvoir d'ici 2022. Les métiers les plus recherchés en 2018 sont ceux de « développeur web », « développeur mobile » et « chef de projet digital ». Une étude menée par la plateforme de recherche d'emploi Indeed a montré que la demande de spécialiste des données a augmenté de 344 % depuis 2013[229]. Par ailleurs, le guide des métiers de la science des données de l'école Télécom Paris identifiait en février 2019[230] vingt métiers dédiés à la *data science* – ingénieur en apprentissage machine, ingénieur IA, etc. -

Néanmoins, malgré la massification des études dédiées aux processus d'intelligence artificielle, ces considérations demeurent quasi-absentes des enseignements dispensés au sein des cursus des écoles d'ingénieurs ou des parcours informatiques des universités. Par ailleurs, le volume et la complexité des problématiques éthiques auxquelles vont être confrontés les futurs développeurs rend nécessaire leur formation pour lutter contre les biais discriminants.

Les spécialistes des données doivent, ainsi, faire preuve d'un niveau de connaissance sur les limites mathématiques et éthiques des modèles qu'ils utilisent. À ce titre, Jean-Davis Benassouli, associé responsable de l'activité *data analytics* et intelligence artificielle PwC France[231] affirme que « les entreprises considèrent l'IA comme une réelle source de valeur et son prêtes à l'intégrer à leurs activités. Dans un contexte où le facteur humain reste le principal frein au développement de l'IA, l'accompagnement, le recrutement et la formation sont cruciaux au sein des entreprises. »

Le rapport Villani[232] affirme qu'il est nécessaire que l'éthique des algorithmes soit pensée dès leur conception. À ce titre, la formation des développeurs aux enjeux éthiques liés au développement des technologies numériques s'avère majeure.

[228] « Les métiers du numérique : quelles opportunités d'emploi ? », Pôle Emploi, janvier 2020
[229] « Demand for data scientists is booming and will only increase », SearchBusinessAnalytics, kanvier 2019
[230] "Data Scientists ! Les métiers qui façonnent les transitions vers demain", TelcomParis, février 2019
[231] http://images.content.pwc.com/Web/PwCGlobal/%7Bcc8d47f3-006e-4bf5-993a-ca17640b7dcc%7D_PwC_Etude_AI_Big_Data_2018_Web.pdf
[232] Cédric Villani, *Donner un sens à l'intelligence artificielle, pour une stratégie nationale et européenne*, rapport au premier ministre, mars 2018

Il apparait que les codes algorithmiques des entreprises ne sont pas le résultat d'une réflexion collective, les individus évoluant dans les espaces numériques ne choisissent pas leurs droits ou les conditions d'utilisation qu'ils signent. Les règles qui régissent nos vies virtuelles sont, ainsi, confiées aux codeurs et développeurs.[233]

A ce titre, l'étude des *Digital Humanities* anglo-saxonnes est intéressante. Chercheurs, universitaires et professionnels du numérique voient dans l'étude des technologies numériques en lien avec les humanités contemporaines, un élément fondamental de la formation des futurs professionnels du secteur numérique.

En septembre 2015, l'OCDE[234] démontrait que la France était l'un des pays les plus compétents en matière de formation au numérique.

La Grande Ecole du Numérique répond à cette logique ; lancée par le gouvernement français en 2015, elle s'inscrit dans un objectif de formation aux technologies et de réduction des écarts de compétences. En regroupant un réseau de plus de 750 formations aux métiers du numérique, elle favorise, notamment, l'inclusion et forme les individus pour répondre aux besoins grandissants des recruteurs. L'enjeu est de lier les institutions pédagogiques et numériques dans le développement de programmes de formation, labellisés, destinés à des publics en décrochage scolaire ou éloignés des outils numériques[235].

Ces dernières années, plusieurs initiatives de formation au numérique ont vu le jour grâce au concours de la société civile.

En 2016, la Commission européenne, en coopération avec les Etats membres, les entreprises, les partenaires sociaux, les ONG et les acteurs de l'enseignement lancent la Coalition française en faveur des compétences numériques (*Digital Skills and Job Coalition*). La coalition a pour objectif de répondre à la demande grandissante de compétences numériques en Europe – aujourd'hui indispensables sur le marché du travail et dans la société. La Commission européenne incite ainsi les Etats membres à créer des coalitions nationales ; la coalition française est coordonnée et animée par le Medef. Les acteurs économiques et sociaux regroupés au sein de la coalition identifient et promeuvent des bonnes pratiques en France et à l'international.

Les « petits débrouillards », mouvement associatif d'éducation populaire à la culture scientifique et technique, propose également des formations aux pratiques du numérique. Considérant que le numérique constitue un enjeu d'éducation du XXIème siècle, l'association forme des enfants et adolescents aux techniques du code et de l'information, à la fabrication numérique et électroniques, aux objectifs connectés ou encore à l'esprit critique et à la prévention des risques liés à l'utilisation des réseaux sociaux et nouveaux outils technologiques.

[233] Informations détenues lors de l'audition de MM. Guillaume Buffet et Etienne Drouard le 4 février 2020
[234] Students, Computers and Learning – Making the Connection, OCDE, septembre 2015
[235] « Grande école du numérique, une nécessité pour les acteurs de l'éducation », The Conversation, octobre 2015

Dans le même temps, le CNRS[236] a initié un plan d'action afin de mettre l'accent sur la formation, la sensibilisation, l'utilisation des outils de développement et de favoriser une utilisation plus efficiente des logiciels. L'institution a établi des livrables de bonnes pratiques à l'attention des concepteurs et développeurs (chercheurs, ingénieurs et techniciens) afin de leur indiquer leurs droits et obligations ainsi que les pratiques de développement et de diffusion.

Le rapport d'activité 2019 de la CNIL[237] affirme qu' *« au travers de l'analyse des pratiques numériques et des rapports quotidiens à la vie privée, il est nécessaire de « proposer un accompagnement à la protection des données personnelles adapté à l'ensemble des personnes. »* En ce sens, le rapport rappelle que les usages du numérique varient selon le contexte et les caractéristiques sociales des individus ; les débats sur la souveraineté numérique et la collecte massive des données personnelles ont encore un « écho limité » au sein des classes populaires.

Algorithmes et discriminations

En mai 2020, le Défenseur des droits et la CNIL ont réuni chercheurs, juristes et développeurs afin d'analyser l'impact des systèmes algorithmiques sur les droits fondamentaux. En résulte un rapport et une liste de recommandations[238] pour que le sujet, défini par Jacques Toubon comme *« un angle mort du débat public »* devienne un angle de réflexion concret. Le rapport réaffirme les propos du Conseil d'Etat quant à au tournant inédit pris par l'utilisation intensive des algorithmes grâce à la puissance de calcul des ordinateurs et à l'exploitation massive des données. Le Défenseur des droits et la CNIL mettent ainsi en garde contre les risques induits par les systèmes algorithmiques sur les droits fondamentaux et les discriminations qu'il peut faire peser sur les individus dans toutes les sphères de leurs vies : accès aux prestations sociales, police, justice, fonctionnement des hôpitaux, accès aux services publics, procédures d'embauche, etc.

Les deux institutions affirment ainsi que des biais peuvent être intégrés à *« toutes les étapes de l'élaboration et du déploiement des systèmes : dès l'intention qui préside à l'élaboration de l'algorithme en amont, pendant la réalisation du code informatique, celle du code exécutable, celle de l'exécution, celle du contexte d'exécution et celle de la maintenance ».* Elles explicitent ainsi que les algorithmes peuvent être discriminatoires en raison de :
- L'existence de données biaisées et non représentative : à l'image de la forte prédominance des visages masculins blancs dans les stocks de données des systèmes de reconnaissance faciale ou des données d'emploi représentant les femmes dans certaines filières de métiers et à des postes et rémunérations moindres ;
- Leur fausse neutralité : la prise en compte de critères neutres, en apparence, peut discriminer certaines catégories de population. Par exemple, dans la décision du Défenseur des droits sur Parcoursup, était établi que le critère de l'établissement d'origine pouvait

[236] Lila Ammour, Olivier Cappé, Thierry Chaventre, Karin Dassas, Marc Dexet, et al.. Je code : Les bonnes pratiques de développement logiciel. 2019. hal-02083801
[237] CNIL (2020), Rapport d'activité « Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles »
[238] « Algorithmes : prévenir l'automatisation des discriminations », Le Défenseur des droits, en partenariat avec la CNIL, mai 2020

conduire à discriminer les jeunes d'origine immigrée en raison de la ségrégation résidentielle et scolaire s'opérant dans de nombreuses régions[239].

Le rapport alerte également que si les effets discriminatoires des algorithmes sont mesurables par les chercheurs à l'échelle des groupes, ils demeurent invisibles à l'échelle individuelle des victimes. Les algorithmes faisant état de mouvements de groupe, peuvent renforcer les discriminations en leur donnant une apparence d'objectivité ; ces risques s'avèrent d'autant plus grands pour les groupes sociaux faisant déjà l'objet de discriminations tels que les femmes, les personnes en situation de handicap ou encore les personnes issues de l'immigration.

Malgré les alertes du Rapport Villani et plusieurs initiatives[240], la prise de conscience *« tarde à émerger »* et *« les concepteurs d'algorithmes, comme les organisations achetant et utilisant ce type de systèmes, n'affichent pas la vigilance nécessaire pour éviter une forme d'automatisation invisible des discriminations. »* Le Défenseur des droits et la CNIL émettent donc des orientations afin d'engager et de structurer une réflexion collective. Elaborées autour de 4 axes, ces orientations appellent à : former et sensibiliser les professionnels, soutenir la recherche afin de développer des études de mesure et des méthodologies de prévention des biais, renforcer les obligations en matière d'information, de transparence et d'explicabilité des algorithmes et réaliser des études d'impact afin d'anticiper les effets discriminatoires des algorithmes.

IA et biais genrés

Conscients des biais multiples induits par les algorithmes, le groupe de travail a pris le parti de focaliser son attention sur les biais genrés, sources de rapports multiples.

Syntec numérique[241] estime que les femmes ne représentent que 27 % des employés du secteur numérique, et seulement 11 % des employés dans la cybersécurité. Au sein de Google, les femmes parmi les salariés travaillant sur les sujets relatifs à l'IA ne sont que 10 %, elles ne représentent que 15 % de ces effectifs dans le laboratoire spécialisé de Facebook[242]. Pourtant, il est important de rappeler que la première personne à avoir inventé la programmation informatique – le codage – est une femme, Ada Lovelace. Et que, nombre de consœurs après elle ont façonné l'histoire du numérique à l'image de Grace Hopper qui a inventé le langage informatique Cobol devenu une référence pour les militaires et les entreprises ou encore Margaret Hamilton dont les compétences en codage informatique ont permis le succès de la mission Apollo 13 en 1970.

[239] Décision 2019-021 du 18 janvier 2019 relative au fonctionnement de la plateforme nationale de préinscription en première année de l'enseignement supérieur, Le Défenseur des droits, janvier 2018
[240] Telecom Paris Tech, Algorithmes : biais, discrimination et équité, février 2019 ; Aude Bernheim, Flora Vincent, L'intelligence artificielle,pas sans elles !, Laboratoire de l'égalité, éditions Belin, 2019 ; Institut Montaigne, Rapport Algorithmes : contrôle des biais SVP, mars 2020 ; Rapport collectif sur commande de la mission Etalab, Ethique et responsabilité des algorithmes publics, ENA, Promotion 2018-2019 « Molière », Juin 2019.
[241] https://syntec-numerique.fr/syndicat-professionnel-numerique/programme/femmes-numerique
[242] https://www.wired.com/story/artificial-intelligence-researchers-gender-imbalance/

Aude Bernheim et Flora Vincent, autrices de l'ouvrage *L'intelligence artificielle, pas sans elles !* estiment que les produits de l'IA reproduisent les stéréotypes de genre à l'œuvre dans la société. Elles constatent, à ce titre, que les logiciels de traduction vont donner à des mots tels que « *doctor* » ou « *nurse* » une traduction française genrée. Par ailleurs, une étude ciblée sur les publicités de Google, a montré qu'à profils équivalents, les offres envoyées aux femmes proposaient des salaires plus bas que celles envoyées aux hommes. Les deux chercheuses militent pour que les écoles d'informatique mettent en place des modules afin d'apprendre à coder l'égalité. Partant du constant que les modes d'écriture des algorithmes ont un rôle majeur dans la perpétuation des biais genrés, elles estiment qu'il est crucial de sensibiliser les développeurs à ces problématiques. Ainsi, considérant que les créations algorithmiques répondent à des choix subjectifs intégrés dans le produit final comme étant objectifs, la manière dont les développeurs perçoivent le monde à un impact sur l'algorithme.

Les algorithmes fonctionnent grâce aux données issues d'un monde inégalitaire. En octobre 2018, Amazon a cessé d'utiliser une intelligence artificielle pour trier automatiquement les CV ; l'IA, nourrie par des données récoltées sur une dizaine d'années, affublait de mauvaises évaluations aux femmes lorsque celles-ci postulaient pour les métiers techniques en raison de l'embauche systématique d'hommes sur ces postes durant la période. L'IA reproduisait les habitudes d'embauche et ainsi, les discriminations sexistes[243].

Les fondements de tels biais résident, notamment, dans les jeux de données utilisés pour entrainer un algorithme. À titre d'exemple, la chercheuse américaine du MIT Joy Buolamwini[244] a observé que les logiciels de reconnaissance faciale ne l'identifiaient pas correctement ; cette défaillance venait du fait que c'est une femme jeune et noire et que les algorithmes avaient été entrainés sur un jeu d'images comprenant essentiellement des hommes blancs âgés de 30 à 50 ans. Ainsi, le taux d'erreur du Logiciel Rekognition d'Amazon était de 1 % pour les hommes de peaux claires, de 7 % pour les femmes de peaux claires, de 12 % pour les hommes de couleur et de 35 % pour les femmes de couleur[245].

L'intelligence artificielle dispose d'un pouvoir considérable sur la société et son implémentation peut changer la réalité en intégrant de l'éthique dans ses processus de création et de décision.

En France, la startup Social Builder[246] travaille à l'insertion des femmes dans le secteur numérique. En s'inscrivant dans les Objectifs de Développement Durable (ODD) des Nations Unis 5 (Egalité entre les sexes), 8 (Travail décent et croissance économique) et 10 (Inégalités réduites), Social Builder concrétise les parcours professionnels des femmes dans le numérique au travers d'actions d'orientation, de formation et d'insertion professionnelle. Depuis sa création en 2010, ce sont 28 000 femmes qui ont été accompagnées et formées.

[243] https://www.forbes.fr/femmes-at-forbes/quand-lintelligence-artificielle-reproduit-les-biais-sexistes/?cn-reloaded=1&cn-reloaded=1
[244] Garreau M. (2019), « "Les biais sexistes de l'IA peuvent être corrigés", selon les chercheuses Aude Bernheim et Flora Vincent » Lien
[245] Larry Hardesty, "Study Finds Gender and Skin-Type Bias in Commercial Artificial Intelligence Systems", MIT News, 11 février 2018
[246] https://socialbuilder.org/

2. Les pratiques de protection des données

Les entreprises ont recours à diverses pratiques novatrices en ce qui concerne la gestion et l'utilisation des données, qui sont détaillées dans la partie « Modalité de gestion des données par les entreprises ». Ces pratiques innovantes appellent des pratiques de cybersécurité nouvelles et en constant développement. Les menaces se multiplient depuis quelques années avec la généralisation des attaques DDOS, ainsi que les Rançongiciels (*Ransomware)*. En général, les entreprises sont de plus en plus exposées aux violations de données.

Face à ses risques, la Responsabilité numérique des entreprises va au-delà de la simple conformité à la réglementation. Au-delà des formalités préalables à accomplir auprès de la CNIL, cette responsabilité exige de s'inquiéter dès la conception des produits et des processus de la façon d'assurer le respect des principes de protection des données, et de fournir des systèmes de sauvegarde et de protection en cas d'attaques.

Face à cette crise de confiance, de fiabilité, et d'efficacité autour des Systèmes d'Informations, la responsabilité des entreprises se trouvent accru en ce qui concerne leur impact sur la société que constituent la protection des données personnelles.

2.1 L'augmentation des « violations de données » : un enjeu de gestion du risque pour les entreprises

Qu'est-ce qu'une violation de données ?

« Une violation de la sécurité se caractérise par la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

Il s'agit de tout incident de sécurité, d'origine malveillante ou non et se produisant de manière intentionnelle ou non, ayant comme conséquence de compromettre l'intégrité, la confidentialité ou la disponibilité de données personnelles. »[247]

La prise de conscience publique de cet enjeu eut lieu lors de l'attaque *WannaCry*, en 2017 qui toucha plus de 300 000 ordinateurs dans 150 pays à travers à travers plus de 45.000 attaques. Il avait alors été mis en évidence les niveaux insuffisants et inadaptés de protection et de gestion des données dans les secteurs public et privé de nombreux pays. L'état de la menace Rançongiciel pour les entreprises et les institutions est évaluée régulièrement par l'ANSSI.[248]

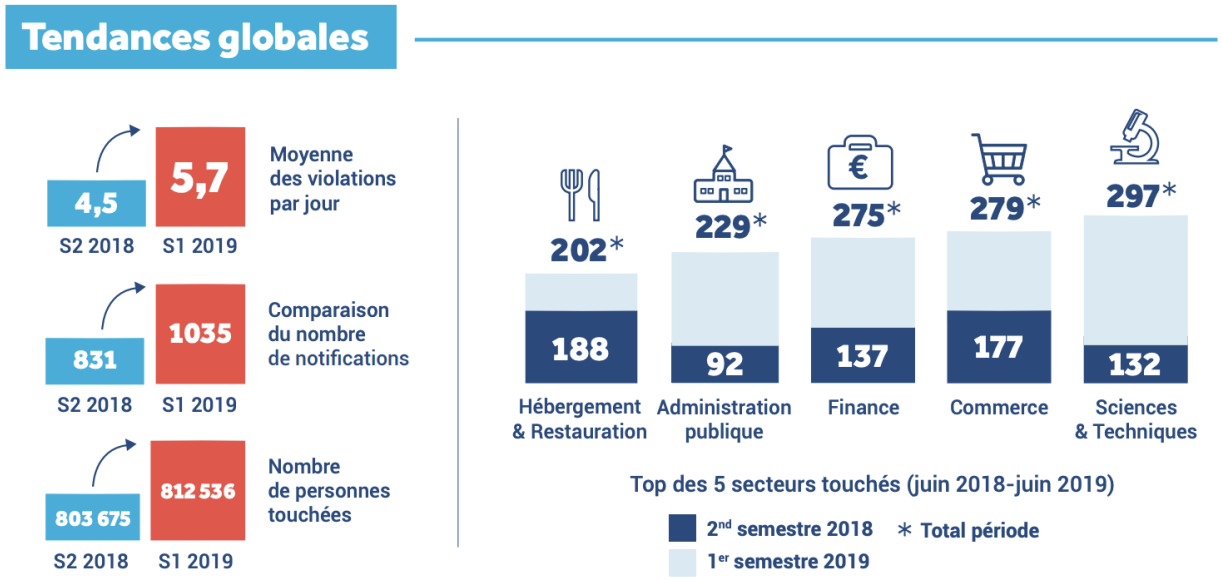
Un autre exemple de révélateurs de la crise de confiance à l'égard de la protection des données fut la controverse autour de la sécurité des données lors de la mise en œuvre des compteurs Linky.

[247] Article 4.12 du RGPD
[248] ANSSI (2020), « État de la menace rançongiciel » Lien

Une entreprise responsable de traitement ne notifiant pas à la CNIL d'une violation de donnée s'expose une amende s'élevant jusqu'à 10 millions d'euros, ou 2 % du chiffre d'affaires de l'entreprise.

Une tendance en augmentation, touchant tous les secteurs

Le *Baromètre data breach* publié par PwC et Bessé en 2020[249] rappelle la nette progression de l'ampleur et de la personnalisation des attaques. Pour la période allant de juin 2018 à juin 2019, on estime à 54 % le nombre des violations de données d'origine malveillante. Les tendances sont résumées dans le graphique suivant :



Quel impact d'une violation de données sur l'entreprise ?

Une violation de données peut avoir trois types d'impact sur les données d'une entreprise :

1. Atteinte à **l'intégrité** des données (altération)
2. Atteinte à la **disponibilité** des données (données rendues inaccessibles)
3. Atteinte à la **confidentialité** des données (des données privées sont exposées)

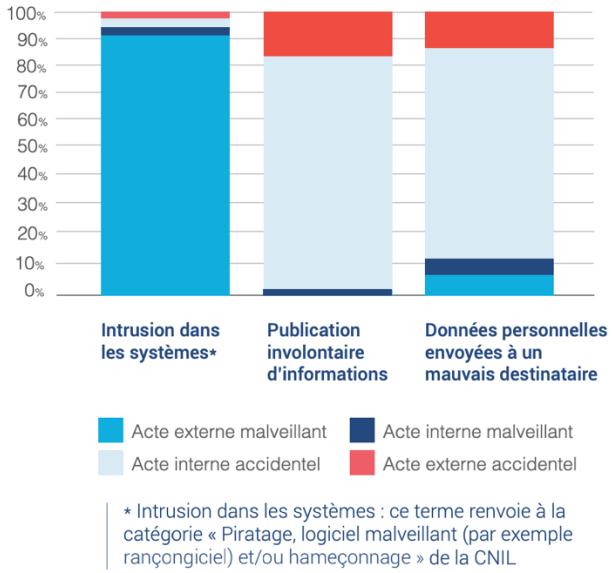
Le *Baromètre data breach* fait état de la répartition des atteintes auxquelles les entreprises ont dû faire face entre le 01/06/18 et 30/06/19 :

Intégrité	178
Disponibilité	305
Confidentialité	2027

Par ailleurs, pendant la même période, **10,4 %** des données affectées par une violation étaient considérées comme « sensible » (cf. Définitions).

[249] FIC, Bessé, PwC (2020), « Baromètre Data Breach » Lien

L’origine des incidents de violations de données



Quelle est la responsabilité de l’entreprise en cas de violation des données ?

Pour respecter la conformité au RGPD, les organismes traitant des données personnelles doivent anticiper et mettre en place des processus : détection d’une violation, capacité à l’endiguer, à appréhender les risques engendrés, et déterminer qui notifier de cette violation.

Les entreprises doivent mettre en place un registre de violation des données, qui peut être contrôlé par la CNIL si besoin. Il doit contenir les éléments suivants :

- La nature de la violation ;
- Les catégories et le nombre approximatif des personnes concernées ;
- Les catégories et le nombre approximatif de fichiers concernés ;
- Les conséquences probables de la violation ;
- Les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation ;
- Le cas échéant, la justification de l’absence de notification auprès de la CNIL ou d’information aux personnes concernées.

Les mesures à mettre en œuvre sont variables en fonction de la criticité de la violation. Le tableau suivant synthétise les obligations en fonction de la violation.

POUR LES PERSONNES CONCERNÉES, LA VIOLATION ENGENDRE :	AUCUN RISQUE	UN RISQUE	UN RISQUE ÉLEVÉ
Documentation interne, dans le « registre des violations »	X	X	X
Notification à la CNIL, dans un délai maximal de 72h	-	X	X
Information des personnes concernées dans les meilleurs délais, hors cas particuliers	-	-	X

250

Pour se conformer à ces obligations, les entreprises doivent faire preuve de responsabilité et de vigilance. Certaines mettent en place un système interne d'alerte. Ces centres de supervision peuvent être chargé de la surveillance d'évènements, d'alerter, et de remédier aux incidents.

Ainsi, les entreprises Orange, Safran, Valéo, Véolia, LVMH, Sanofi, Schneider Electric, Atos, Dassault Systemes, Peugeot et AXA déclarent dans leurs rapports intégrés avoir mis en place de tels systèmes d'alerte.

2.2 Les enjeux de protection des données dans un contexte d'externalisation de la gestion des données

En externalisant la gestion de base de données, les organisations s'exposent à de nouveaux risques : l'entreprise cliente perd une partie du contrôle sur la sécurité de ses données. Il y a également des enjeux de confidentialité des données, puisqu'elles sont partagées à une tierce-partie en dehors des locaux de l'entreprise.

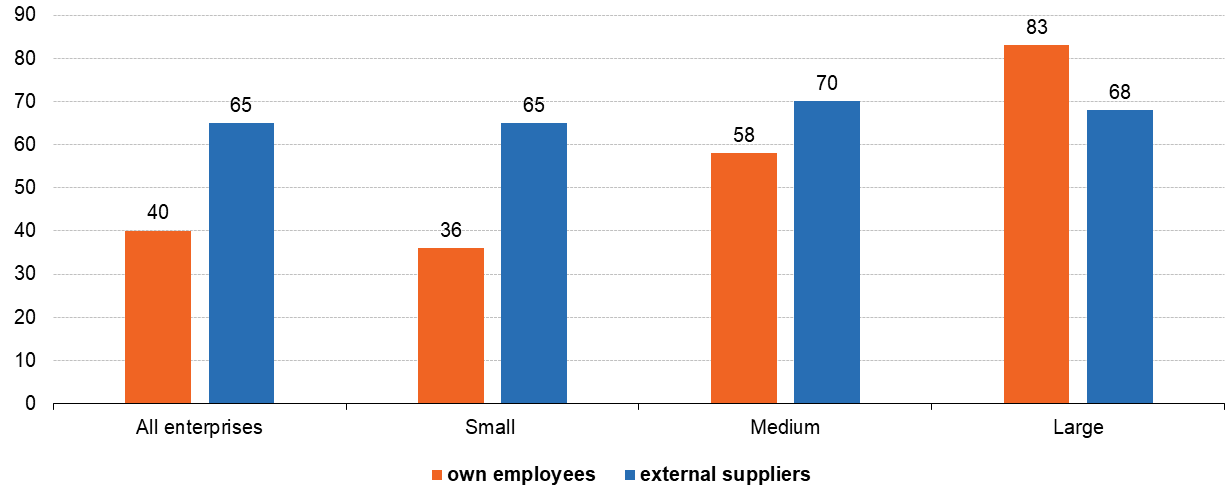
Cependant, l'utilisation d'un tel service peut aussi présenter un meilleur profil de protection des données puisque le fournisseur de services est spécialisé. Les caractéristiques de sécurité des données peuvent inclure le chiffrement de bout en bout (*encryption end-to-end*), la microsegmentation (technique de sécurité des réseaux qui permet aux architectes de la sécurité de diviser logiquement le centre de données en

250 https://www.cnil.fr/fr/les-violations-de-donnees-personnelles

segments de sécurité distincts) ou encore la mise en place d'un réseau privé virtuel (VPN - *Virtual Private Network*).

En 2019, la majorité des entreprises de l'UE (65 %) ont déclaré que les activités liées à la sécurité des TIC étaient réalisées par des fournisseurs externes, tandis que 40 % des entreprises ont déclaré que les activités liées à la sécurité des TIC étaient réalisées par leurs propres salariés. Comme le montre le graphique suivant, le schéma selon lequel les activités liées à la sécurité des TIC reposent principalement sur des fournisseurs externes est valable pour les petites et moyennes entreprises. En revanche, la grande majorité des grandes entreprises (83 %) ont déclaré que les activités liées à la sécurité des TIC étaient effectuées par leurs propres salariés. [251]

ICT security related activities performed in enterprises by own employees and external suppliers, by size, EU-27, 2019
(% enterprises)



Source: Eurostat (online data code: isoc_cisce_ra)

eurostat

À mesure que les entreprises adoptent les nouvelles technologies, il est important pour les DSI de construire ou de co-construire des infrastructures informatiques sécurisées capables de faire face aux attaques.

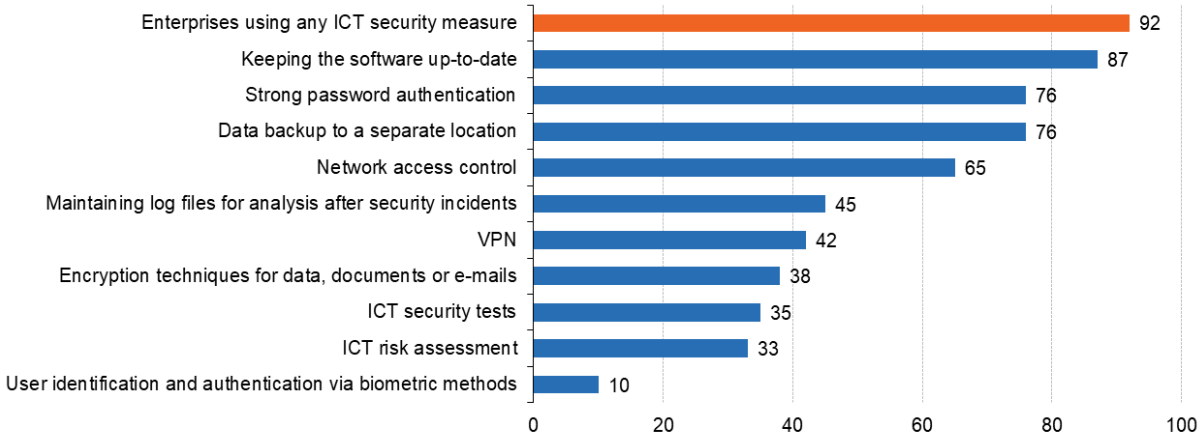
2.3 Des technologies de protection insuffisantes face aux risques émergents

Comme le montre le graphique suivant, 92 % des entreprises de l'UE ont utilisé en 2019 une mesure de sécurité des Technologies de l'Information et de la Communication (TIC). La mesure la plus couramment utilisée était la mise à jour des logiciels ou des systèmes d'exploitation (87 % des entreprises de l'UE), suivie de l'authentification par mot de passe fort (76 %), de la sauvegarde des données dans un lieu ou un nuage séparé (76 %) et du contrôle d'accès au réseau (65 %). Moins de la moitié des entreprises ont

[251] Eurostat (2020), « ICT Security in Entrerprises » Lien

déclaré conserver des fichiers journaux pour analyse après un incident de sécurité (45 %) et utiliser un réseau privé virtuel (VPN) (42 %). Les entreprises ont moins souvent utilisé des techniques de cryptage pour les données, les documents ou les courriers électroniques (38 %), des tests de sécurité des TIC (35 %), l'évaluation des risques liés aux TIC (33 %) et l'identification et l'authentification des utilisateurs par des méthodes biométriques (10 %).[252]

ICT security measures used by enterprises, EU-27, 2019
(% enterprises)



Source: Eurostat (online data code: isoc_cisce_ra)

Les outils numériques sont en constante évolution. Néanmoins, force est de constater que malgré les solutions de protection des données et de cybersécurité apportées par les entreprises, celles-ci restent soumises à des risques émergents.

À ce titre, une étude menée par Dell, *Data Protection in a Multi-Cloud World*[253], fait état des technologies émergentes en matière de protection des données. Regroupant les réponses de plus de 250 décideurs informatiques issus d'organisations privées du monde entier et publiques comptant plus de 250 employés, l'étude démontre que la plupart des organisations déploient ou prévoient de déployer des charges de travail conséquentes comme les Progiciels de Gestion Intégrée – outil central des systèmes d'informations des entreprises permettant de gérer l'ensemble des processus opérationnels des entreprises en intégrant diverses fonctions de gestion –, les applications de productivité, les systèmes de business intelligent ou encore des outils de gestion des relations clients. Ces outils seront intégrés dans les *clouds* publics et privés.

Par ailleurs, de nombreuses organisations estiment que leurs technologies actuelles de protection des données ne seront pas capables de protéger les technologies émergentes dans lesquelles elles investissent. Considérant que 98 % des répondants investissent dans des technologies émergentes de gestion des données, et que 52 % d'entre eux rapportent un manque de solution de protection des données, le risque s'avère conséquent. Les répondants jugent faible la protection des données de leur organisation

[252] idem
[253] DELL (2019), "Data Protection in a multi-cloud world" Lien

au travers de l'IA (64 %), des applications natives au *cloud* (60 %) ou des applications *Software as a Service* (SaaS).

Evoluant dans un environnement *multi-cloud*, la plupart des organisations s'appuient sur des solutions de protection des données issues de plusieurs fournisseurs, la tendance tend ainsi à s'accentuer. À ce titre, 60 % d'entre elles ont fait appel à différents fournisseurs en 2016, 76 % en 2018 et 80 % en 2019. Néanmoins, la dispersion des technologies n'est pas sans risque. Les entreprises qui font appel à plusieurs fournisseurs de protection des données risquent de connaitre 5 fois plus de coûts engendrés par des pertes de données, 2 fois plus de coûts engendrés par des temps d'immobilisation de leurs données et elles sont 1,7 fois plus susceptibles d'avoir des difficultés à récupérer leurs données après une cyberattaque que celles qui utilisent un seul fournisseur.

2.4 Mettre en œuvre une protection efficace au long des différentes étapes du cycle de vie de la donnée

2.4.1 Le cycle de vie de la donnée

Comme indiqué en première partie de ce rapport, on identifie plusieurs phases dans le cycle de vie de donnée. Au nombre de six, ces phases concernent l'acquisition et la production ; le traitement ; l'analyse, l'informatique décisionnelle et l'IA ; l'accès, la sécurisation, l'intégrité et la confidentialité, la conservation, l'archivage et/ou l'effacement ; la réutilisation, la libération et les processus d'*open data*[254].

Les données peuvent être produites de manières *ex-nihilo* ou *ex-post*[255]. Les données *ex-nihilo* émanent de la captation de signaux bruts issus de différents phénomènes naturels et humains – astronomie, transports, vidéo surveillance, santé. Les données *ex-post,* sont quant à elles produites par des processus de calculs ou de traitement additionnels à partir de données préexistantes mais non structurées. Ces processus de traitement permettent ainsi de les rendre exploitables par les entreprises pour leurs activités : progiciels de gestion intégrés, études de marché, marketing, etc.

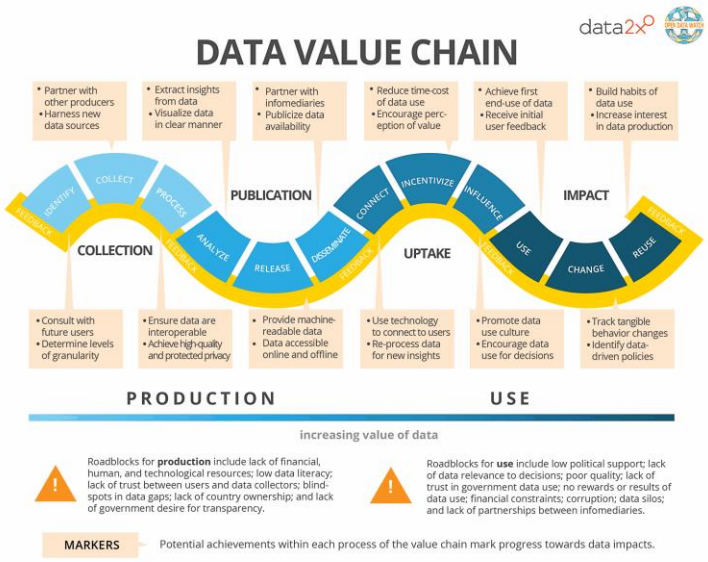
Les données passent ainsi par des processus divers dus à leur origine ou leur utilisation future. À ce titre, une grande partie des données des entreprises sont liées à d'autres données pour justifier de nouveaux calculs.

Par ailleurs, le cabinet Veritas[256] estime qu'il existe trois catégories de données mégadonnées – ou *big data* –, les données « propres », les données « obscures » et les données « inutiles ». Ces données sont définies ainsi en fonction de leur contribution à la prise de décision. Les données propres donnent ainsi lieu à une exploitation utile dans la prise de décision, ce caractère-là doit entrainer leur protection et leur sécurisation. Les

[254] « Étude sur le cycle de la donnée dans la conception et la mise en œuvre des services et usages numériques des collectivités territoriales », FNCCR, mars 2019 http://www.fnccr.asso.fr/wp-content/uploads/2019/04/FNCCR-R%C3%A9sum%C3%A9-Etude-cycle-de-la-donn%C3%A9e_20190318.pdf
[255] « L'économie numérique est une industrie lourde », The Conversation, novembre 2015
[256] Etude Databerg 2015, Veritas Technologies LLC

données obscures peuvent éventuellement donner lieu à une exploitation pertinente à terme, mais leur accessibilité reste difficilement évaluable. Les données inutiles désignent des données jugées redondantes, obsolètes ou inexploitables, elles peuvent être supprimées sans dommage pour l'entreprise. L'étude Databerg 2015 estime ainsi que moins d'un quart des données stockées par les entreprises sont inutiles ; ainsi les sommes dépensées pour leur stockage et leur gestion s'avère obsolète.

A ce titre, il est important pour les entreprises de caractériser, identifier et catégoriser les données qu'elles détiennent et d'analyser les risques auxquels elles sont confrontées dans toutes les étapes de leur production.



257

2.4.2 PSSI : Politique de Sécurité des Systèmes d'Information

Alors que les systèmes d'information sont de plus en plus ouverts, la politique de sécurité des systèmes d'information s'érige comme un élément fondamental de la gestion des données détenues par une entreprise.

En 2004, l'ANSSI a publié un guide d'élaboration pour une PSSI efficace, qui conserve aujourd'hui sa pertinence[258]. Cette politique constitue le principal document de référence en matière de sécurité des systèmes d'information d'une organisation ou entreprise. Partant d'une analyse des risques de sécurité des SI, la politique doit être validée par les acteurs de la sécurité de l'information avant d'être diffusée à l'ensemble des acteurs de l'entreprise (utilisateurs, exploitants, sous-traitants, prestataires, etc.).

Le guide de l'ANSSI estime que les patrimoines matériels, immatériels et les informations relatives aux personnes physiques et morales doivent être protégés par la PSSI. Ainsi, différentes bases de légitimité fondent les règles d'une politique efficace :

[257] Open Data Watch, "The Data Value Chain, Moving from Production to Impact" Lien
[258] Bureau de la DCSSI (2004), « Guide pour l'élaboration d'une politique de sécurité de systèmes d'information PSSI »,

- les lois, règlementations, normes et recommandations issues d'instances européennes, nationales et internationales ; mais également des instances professionnelles idoines ;
- les règles éthiques relatives aux principes internationaux et aux codes éthiques de certains secteurs ;
- les principes de protection des intérêts de l'Etat relatifs au secret de défense notamment ;
- les principes de préservation des intérêts de l'organisation ou de l'entreprise vis-à-vis de ses parties prenantes.

Le rôle de Responsable de la sécurité des systèmes d'information (RSSI) s'avère stratégique pour les entreprises et organisations. Ce rôle permet de prendre en charge et d'assurer la sécurité des réseaux, des systèmes, des télécommunications, des applications ou encore des stratégies de sauvegarde des données. Rattaché à la direction de systèmes d'information ou à la direction générale, le RSSI est tenu à une déontologie professionnelle stricte.

Charles Gengembre, responsable de la Business Unit réseaux et sécurité chez SCC[259] estime que de nombreuses entreprises disposent d'une PSSI, néanmoins celles-ci demeurent perfectibles. Au sein des PME, le manque de moyens et de compétences en interne rend complexe la mise en place de politiques efficientes. Dans le même temps, les grands groupes cloisonnent la sécurité des systèmes d'information aux spécialistes, alors que ces politiques ont intérêt à s'élever à tous les niveaux de l'entreprise. Il s'avère donc essentiel d'impliquer un maximum de collaborateurs et collaboratrices dans ces choix politiques et sécuritaires.

2.4.3 L'anonymisation des données personnelles

Dans un contexte où la collecte et le traitement des données personnelles par les entreprises devient un enjeu économique incontournable, l'anonymisation constitue un enjeu à prendre en considération.

L'anonymisation, en permettant d'empêcher l'identification suite à l'analyse de données personnelles, doit d'abord se faire de manière irréversible. Sans ce fondement, l'anonymisation relève davantage de la pseudonymisation qui réduit simplement la corrélation entre les données et l'identité d'une personne.

L'anonymisation offre une double garantie[260] : la sécurisation de l'exploitation des données à caractère personnel et le respect des droits fondamentaux des individus dont les données sont traitées.

La loi « informatique et libertés » estime que l'anonymisation doit être utilisées à deux stades différents[261] :

[259] Le Monde Informatique, « Quelle gouvernance de sécurité mettre en place face à la transformation numérique ? »
[260] Galichet C. (2017), « Données personnelles : anonymisation ou pseudonymisation ? »
[261] Idem

- l'anonymisation à bref délai qui suit de manière immédiate la collecte des données. La CNIL doit apprécier l'efficacité du procédé d'anonymisation envisagé afin de garantir la sécurité des personnes ;
- l'anonymisation ultérieure qui agit comme un second traitement des données. L'anonymisation a lieu après la collecte, et impose ainsi à l'entreprise de respecter les exigences légales et réglementaires en matière de données personnelles, jusqu'à leur anonymisation.

Il existe plusieurs techniques d'anonymisation : la randomisation et la généralisation :

La randomisation consiste à altérer la véracité des données personnelles collectées. Ainsi, les attributs sont modifiés pour l'ensemble des données afin de le rendre moins précis. À cela, peut être ajoutée la suppression d'attributs évidents et identifiant la personne.

La généralisation consiste à généraliser les attributs des individus concernés en modifiant l'échelle ou l'ordre de grandeur des données – à titre d'exemple, mentionner la région plutôt que la ville ou un mois plutôt qu'une semaine. Cette technique est efficace jusqu'à un certain degré et doit donc être combinée avec d'autres techniques.

Afin d'apprécier l'anonymisation concrète de données personnelles, le Conseil européen de la Protection des Données [262] estime que les entreprises et les organisations doivent se fonder sur trois critères essentiels :

- l'individualisation qui permet d'isoler une partie ou la totalité des données d'un individu dans un ensemble de données ;
- la corrélation qui permet de relier entre eux au moins deux données se rapportant à la même personne ;
- l'inférence qui permet de déduire la valeur d'un attribut à partir des valeurs d'un ensemble d'autres attributs.

Néanmoins, force est de constater que cette technique reste difficile. Les volumes de données augmentent considérablement et les risques de réidentification par recoupement de données demeurent importants. À ce titre, le G29 – regroupement des Commission Nationales de l'Informatique et des Libertés des pays membres de l'Union européenne – recommande aux responsables des traitements de données « d'effectuer une veille régulière pour préserver dans le temps le caractère anonyme des données produites ».

Un premier point de vigilance doit être souligné. Les données anonymisées ne sont plus considérées comme des données personnelles et ne font plus partie des domaines de surveillance du RGPD. Ainsi, leur échange ne requiert plus le consentement des usagers. À ce titre, en 2013, SFR a remporté le prix de l'innovation *big data* en annonçant la commercialisation des données géolocalisées détenues. Les données

[262] « Avis 05/2014 sur les techniques d'anonymisation », adopté le 10 avril 2014, Groupe de Travail « article 29 » sur la protection des données, G29

collectées par SFR pourront, après anonymisation, renseigner les entreprises du Groupe sur la fréquentation d'un lieu[263].

Un second point de vigilance doit être souligné. Si les données collectées sont souvent anonymisées par les organismes qui les collectent, un article publié dans la revue Nature Communications[264] montre qu'il est loin d'être acquis que les données anonymisées le reste. Le modèle mathématique développé par les auteurs permet une réidentification certaine à 99,98 % à partir de seulement 15 attributs par individu. 15 attributs est une valeur faible, dans un contexte où les *data brokers* peuvent posséder jusqu'à 5000 attributs par individu.[265]

Ces résultats suggèrent que même des ensembles de données anonymes fortement échantillonnées ont peu de chances de satisfaire aux normes modernes d'anonymisation établies par le RGPD et remettent sérieusement en question l'adéquation technique et juridique du modèle de dé-identification utilisé jusqu'à présent.

Les solutions de « cyberassurance »

Les risques dits « cyber » sont aujourd'hui identifiés comme une menace majeure pour les entreprises. Certaines sont ainsi tentées de s'assurer.

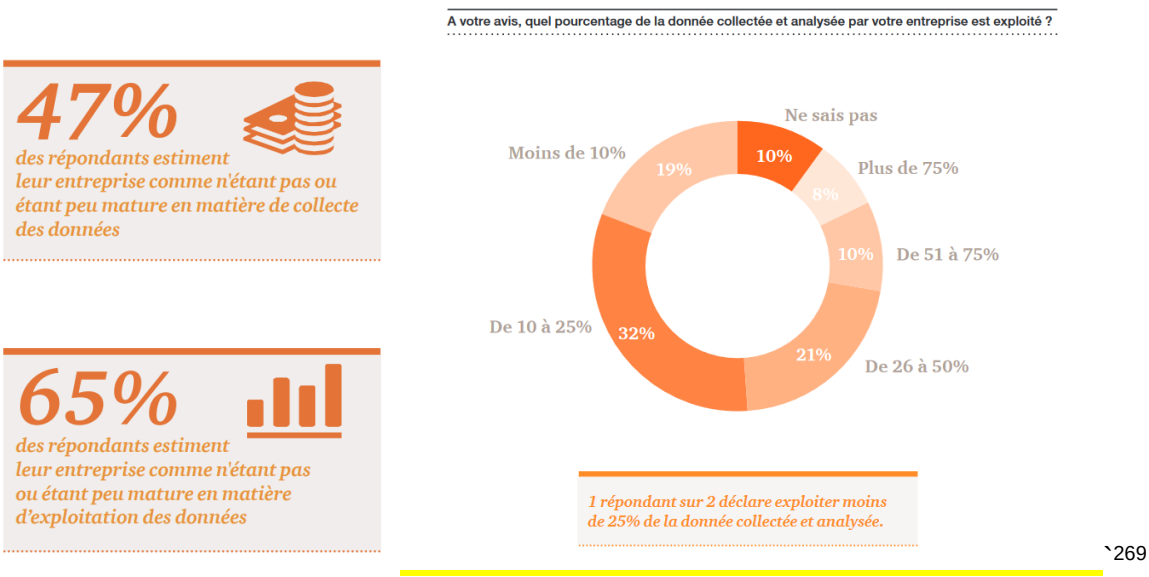
La Fédération Française des Assurances déplore le fait que les statistiques sur la sinistralité ou le montant des indemnisations liés aux cyberattaques ne soient pas encore officielles et consolidées[266]. Dans le même temps, la probabilité de survenance des risques est également un facteur à prendre en considération. En 2018, l'ANSSI recensait, à ce titre, 1869 signalements et 391 incidents hors opérateurs d'importance vitale et 16 incidents majeurs.

Afin d'augmenter leur résilience aux cyberattaques, 80 % des entreprises du CAC40 ont souscrit à une cyberassurance[267]. Christophe Delcamp, directeur adjoint en charge de la détention des assurances de dommages et responsabilités de la FFA, estime que les bénéfices d'une telle assurance sont nombreux et permettent d'obtenir une évaluation de la qualité des protections mises en place par l'entreprise. Il note également, qu'avec le RGPD, la cyberassurance constitue un élément complémentaire et non négligeable pour contracter avec certains donneurs d'ordre se devant d'apprécier le niveau de protection liés aux cyberattaques de leurs sous-traitants.

En 2019, 21 % des entreprises de l'UE ont déclaré avoir une assurance contre les incidents de sécurité des TIC. Le pourcentage d'entreprises ayant déclaré être assurées contre les incidents de sécurité des TIC varie en fonction de la taille de l'entreprise.[268] Si 35 % des grandes entreprises déclarent en avoir une, seulement 28 % des moyennes et 20 % des petites déclarent avoir souscrit à une telle assurance.

[263] Le Monde Datablog (2016), « Big Data, vos données en vente »
[264] Rocher L., Hendrickx J., de Montjoye Y. (2019), "Estimating the success of re-identifications in incomplete datasets using generative models" Lien
[265] Acxiom (2019), Document publicitaire Lien
[266] Daf Mag (2020), « Une cyberassurance, pour quoi faire ? »
[267] Idem
[268] Lien

3. Les modes de gestion des données par les entreprises



`269

3.1 Progiciel de gestion intégrée

Un progiciel de gestion intégrée ou PGI (en anglais : *Enterprise Resource Planning* ou ERP) est un progiciel qui permet « de gérer l'ensemble des processus d'une entreprise en intégrant l'ensemble de ses fonctions, dont la gestion des ressources humaines, la gestion comptable et financière, l'aide à la décision, mais aussi la vente, la distribution, l'approvisionnement et le commerce électronique ».[270]

Il peut s'agir d'une solution mise en œuvre sur des serveurs distants (*cloud*) ou sur des serveurs propres à l'entreprise.

« Pour le pilotage d'un service ou d'une structure dans son ensemble, le PGI s'impose comme une solution capable de répondre à des besoins disparates, notamment en matière de logiciel pour la gestion de base de données.

Le PGI se révèle polyvalent et, par conséquent, s'inscrit dans une stratégie entrepreneuriale globale. Il se constitue de modules et d'outils pour réaliser différentes tâches. Afin de rendre son exploitation pertinente et cohérente par rapport aux objectifs présentés, il assure l'uniformité des informations à travers une gestion de base de données performantes, pérennes et adaptables à toute forme de structure. Pour résumer, le PGI possède plusieurs modules ou logiciels indépendants qui sont reconnus et utilisés à partir d'une base de données commune. Il permet d'améliorer l'organisation de l'entreprise et de minimiser les coûts liés à son usage. »[271]

269 Lien
270 Office québécois de la langue française, « Progiciel de Gestion Intégré » Lien
271 Journal du Net (2019), « ERP ou PGI : Définition, rôle, caractéristique » Lien

« La principale caractéristique d'un PGI c'est l'unicité de sa base de données. Cette base permet la mise à jour en temps réel des données, leur unicité ainsi que leur mise à disposition de tous les modules du PGI.

Cette unicité assure une véritable cohérence des informations et permet une meilleure collaboration au sein de l'entreprise. Cet PGI est donc un référentiel commun qui est partagé par toutes les parties prenantes. »[272]

Entreprises proposant des solutions PGI : Sage, CEGID, Microsoft, SAP, Abas ERP

Le PGI est utile dans plusieurs domaines :

- comptabilité et finance : facturation, trésorerie ;
- logistique, transport et gestion des stocks ;
- gestion des ventes et des achats ;
- planification de la production ;
- ressources humaines et paie ;
- management de projets ;
- sous-traitance, maintenance et suivi qualité ;
- gestion commerciale et fournisseur : suivi, fidélisation…

Utilité dans le cadre du RGPD

La RGPD précise que les entreprises sont tenues d'obtenir le consentement explicite des individus si elles veulent les contacter à des fins de vente et de marketing. Comme les systèmes PGI centralisent les données, les entreprises seront en mesure de localiser facilement la trace de la communication si elles ont besoin de preuves qu'un client a consenti à être contacté à des fins de vente et de marketing.

Les entreprises sont tenues de supprimer les données des clients dans le cadre du droit à l'oubli garanti par le RGPD. Les systèmes PGI facilitent cette opération, car toutes les données se trouvent au même endroit. Si les entreprises doivent parcourir des documents papier, des feuilles de calcul et différents systèmes dans plusieurs appartements pour supprimer tous les enregistrements d'un client, elles risquent davantage de manquer quelque chose et d'enfreindre la réglementation.

EDI (Echange de Données Informatisées) qui permettent aux entreprises de synchroniser leurs Progiciels de gestion intégrée

Les parties-prenantes font face à une hétérogénéité des Systèmes d'Informations et des solutions technologiques. Les discussions entre acteurs économiques ne permettent pas de trouver des outils communs. En bref, on constate un manque d'harmonisation et d'interopérabilité des solutions technologiques.[273]

[272] CELGE (2020), « Qu'est-ce qu'un ERP ? » Lien
[273] Audition de Mme Françoise Durand-Rivoire, Directrice Corporate Social Responsibility & Digital Transformation chez Novasep

L'échange de données informatisées (EDI), ou en anglais *electronic data interchange* est la communication interentreprises de documents commerciaux dans un format standardisé.[274]

Aujourd'hui, les entreprises utilisent l'intégration EDI pour partager toute une série de types de documents - des bons de commande aux factures, en passant par les demandes de devis et les demandes de prêt, entre autres. Dans la plupart des cas, ces organisations sont des partenaires commerciaux qui échangent fréquemment des biens et des services dans le cadre de leurs chaînes d'approvisionnement et de leurs réseaux interentreprises (B2B).

Tous les progiciels de gestion ne sont pas conçus pour intégrer l'EDI. D'autres sont nativement paramétrés pour intégrer cette fonction. Une fois que l'EDI est intégré au PGI, deux entreprises différentes peuvent consulter les mêmes données synchronisées entre leurs PGI.

Les principaux avantages des EDI sont l'économie de coûts, la vitesse, la fiabilité des données, la traçabilité, l'augmentation de la productivité, et la provision d'un langage communs aux entreprises pour échanger.

Cependant, les systèmes EDI sont extrêmement coûteux, ce qui rend leur mise en œuvre difficile pour les petites entreprises. De nombreuses grandes organisations ne travaillent qu'avec d'autres qui utilisent l'EDI. Cela peut limiter les opportunités de partenariat commercial des petites entreprises.

Si ces outils permettent de nouveaux modes de collaboration, il est néanmoins nécessaire de considérer la propriété des données partagées ainsi que le conditions précises qui lient les parties prenantes et leur permettent d'utiliser les données de partenaires.

3.2 *Cloud computing :* les enjeux de responsabilité sociale des nouvelles pratiques de gestion, exploitation et valorisation des données

3.2.1 Le *cloud computing* permet aux entreprises d'exploiter de de valoriser leurs données

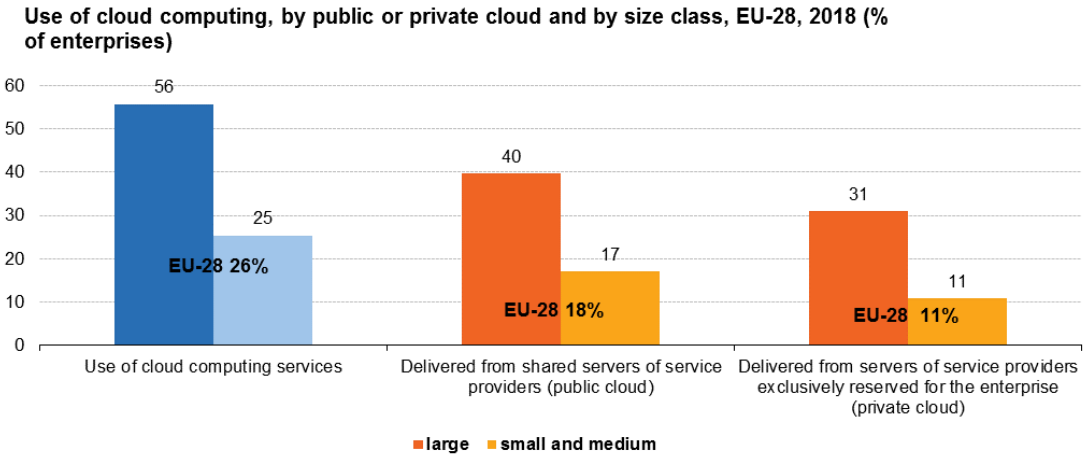
Le *cloud computing* (informatique en nuage) est un modèle qui permet un accès réseau omniprésent, pratique et à la demande à un ensemble partagé de ressources informatiques configurables (par exemple, réseaux, serveurs, stockage, applications et services) qui peuvent être rapidement mobilisées avec un minimum d'efforts de gestion ou d'interaction avec les fournisseurs de services. [275]

Le *cloud computing* s'est développé rapidement et est devenu crucial dans le développement l'économie des données. Grâce au règlement sur la libre circulation des données à caractère non personnel[276], les entreprises peuvent désormais stocker et

[274] IBM, « Electronic Data Interchange » Lien
[275] National Institute of Standards and Technology
[276] Règlement 2018/1807 du Parlement européen et du Conseil Lien

traiter leurs données dans un *cloud* n'importe où. Le *cloud computing* ouvre l'accès aux technologies futures et émergentes, telles que l'intelligence artificielle, le calcul haute performance, les algorithmes appliqués au marketing, des Systèmes d'informations plus performants, ou encore l'Internet des Objets et la blockchain.

Les fournisseurs de services de *cloud computing* peuvent fournir des services liés aux TIC à partir de serveurs partagés (*cloud* public) ou d'une infrastructure en nuage fournie à l'usage exclusif d'une entreprise particulière (*cloud* privé), ou à partir d'une combinaison des deux (*cloud* hybride).



Source: Eurostat (online data code: isoc_cicce_use)

eurostat

Les différents modèles de *cloud computing*

Infrastructure as a service (IaaS) : « Offre de *cloud computing* dans laquelle un fournisseur offre aux utilisateurs l'accès à des ressources informatiques comme des serveurs du stockage et de l'équipement de réseau. Les entreprises utilisent leurs propres plateformes et applications dans l'infrastructure du fournisseur. »

Plateform as a service (PaaS) : « Offre de *cloud computing* qui fournit aux utilisateurs un environnement *cloud* dans lequel ils peuvent développer, gérer et mettre à disposition des applications. Outre le stockage et les autres ressources informatiques, les utilisateurs peuvent utiliser une suite d'outils disponibles pour développer, personnaliser et tester leurs applications. »

Software as a Service (Saas) : « Offre de *cloud computing* qui donne aux utilisateurs l'accès aux logiciels en *cloud* d'un fournisseur. Les utilisateurs n'installent pas les applications sur leur terminal. Elles résident sur un réseau *cloud* distant auquel ils accèdent par le web ou par une interface de programme (API - Application Programming

Interface). Avec les applications, les utilisateurs peuvent stocker et analyser des données et collaborer sur des projets. »[277]

Une solution avantageuse pour exploiter et gérer les données

L'externalisation des Systèmes d'information et de la gestion des données en mode « as a Service » requiert au préalable une gouvernance des données efficaces. Lorsque c'est le cas, le *cloud computing* permet garantir la maîtrise de la disponibilité, de la cohérence et de l'exactitude des données.[278]

Le modèle de *cloud computing* fournit aux utilisateurs une forme d'accès à une base de données sans qu'il soit nécessaire de configurer le matériel physique, d'installer des logiciels ou de configurer les performances. Toutes les tâches administratives et la maintenance sont prises en charge par le prestataire de services, de sorte que l'utilisateur ou le propriétaire de l'application n'a plus qu'à utiliser la base de données. D'énormes ressources de calcul peuvent être mises à la disposition en quelques minutes, permettant une grande flexibilité de la planification de la capacité.

Ainsi, les entreprises ont de plus en plus recours à un tiers pour la gestion de leurs services d'informations et bases de données. Ce passage dans le *cloud* s'avère bénéfique en termes de sécurité et de coût puisque l'entreprise paie seulement ce qu'elle consomme ; cela évite le stockage inutile au sein de l'entreprise qui engendre des coûts prévisionnels et de ressources humaines[279]. Il permet des économies d'échelle en réduisant les coûts d'exploitation, car l'entreprise paie uniquement pour les services qu'elle utilise.

Cependant, l'émergence du paradigme du *cloud computing* soulève deux enjeux majeurs[280] : la perte de contrôle sur les données (cf. Partie 3.2 « Quelle souveraineté pour les données ») et une perte de contrôle sur la sécurité des données (cf. partie 2 « Les pratiques de protection des données »). Ainsi, la migration vers le *cloud computing* relève de décision stratégique qui doivent se baser sur une gouvernance des données solide et coordonnée.

Le *cloud computing* pour valoriser les données

1. *Les caractéristiques du* cloud computing *comme outil de création de valeur*

Comme mentionné précédemment, le traitement des données numériques grâce aux solutions de *cloud computing* est en mesure de constituer pour les entreprises un vaste champ de développement et de création de valeur.

[277] IBM, « Modèle de service cloud » Lien
[278] Lien

[279] Audition de Rémi Dusaud
[280] Ben Arfa Rabai (2013), "A cybersecurity model in cloud computing environments" Lien

Selon une étude Eurostat ayant porté sur 158 000 entreprises des 1.6 millions d'entreprises européennes[281], les services de *cloud computing* fournis par les serveurs des fournisseurs de services devrait présenter les caractéristiques suivantes :

- *On-demand self-service* : les utilisateurs peuvent demander des ressources informatiques sans interaction humaine avec le fournisseur de services ;
- *Élasticité de la prestation* : les capacités doivent pouvoir facilement modulées, de sorte que les entreprises puissent répondre aux pics de demande sans avoir à investir dans des infrastructures qui, autrement, resteraient sous-utilisées ;
- *Des services pay-per-user, pay-per-use or pre-paid*

Selon la brochure sur le *cloud computing* de l'UE, le *cloud computing* apporte certaines opportunités aux entreprises :

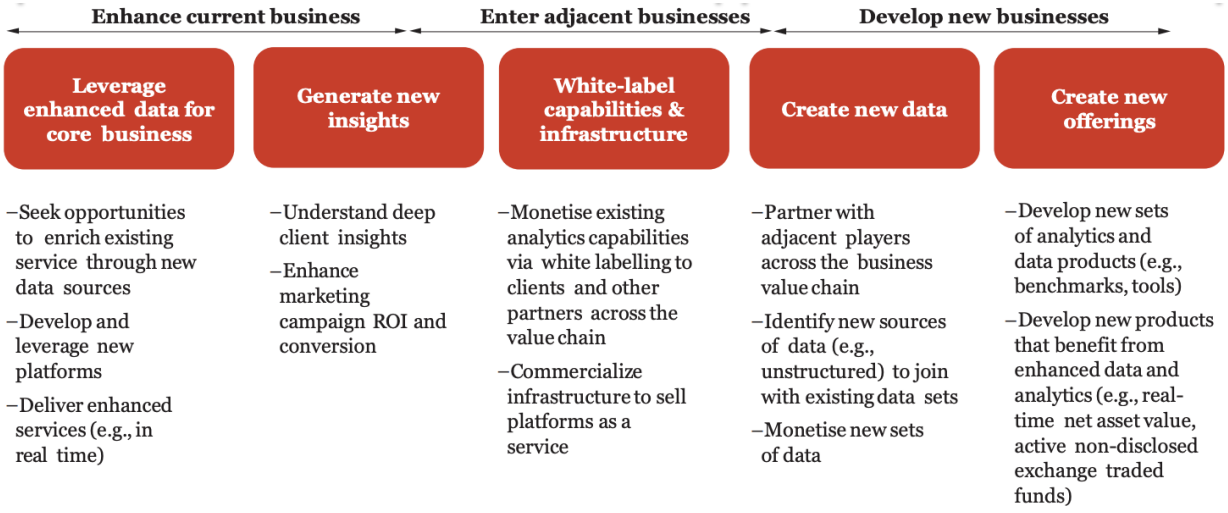
- Des capacités de stockage informatique sur lesquelles tous les types de services peuvent fonctionner, pour tous les secteurs de l'économie
- Un achat des ressources informatiques nécessaires à la demande, sans courir le risque d'un manque de retour sur investissement matériel
  Permet aux start-ups et les PME utilisant des moyens informatiques simples pour acquérir de nouveaux modèles commerciaux et s'épanouir en conséquence[282]

2. *Le* cloud computing *: différentes façons de créer de la valeur*

Le *cloud computing* donne donc aux entreprises la capacité de développer des solutions de PaaS, d'Iaas, et de SaaS, qui permettent de mettre en œuvre des technologies émergentes telles que l'intelligence artificielle, l'Internet des Objets, la blockchain et le *big data analytics*, qu'elles ne pourraient pas développer seules. Ces solutions permettent trois choses aux entreprises :

- améliorer sa compétitivité et son activité actuelles ;
- conquérir des marchés adjacents ;
- développer de nouveaux marchés.

[281] Eurostat (2018), "Cloud Computing – statistics on the use by enterprise" Lien
[282] Commission européenne (2019), « Cloud computing : Brochure » Lien

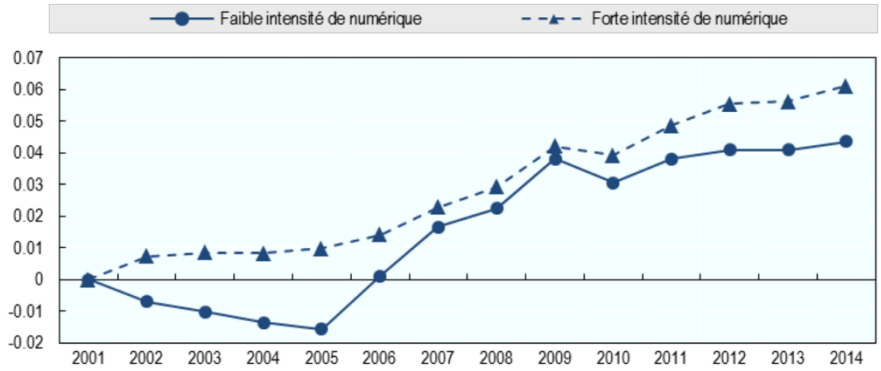


Options to create value from data

283

Ces différents leviers de la monétisation de la donnée semblent effectivement favoriser la croissance des entreprises qui y recourent[284] :

Graphique 2. Comparaison de l'évolution de la croissance du facteur de marge (2001-2014), dans les secteurs à forte et à faible intensité de numérique



Note : Un secteur est considéré à forte ou à faible intensité de numérique selon qu'il se situe au-dessus ou en-deçà du secteur médian en termes d'intensité de numérique, calculé à l'aide de l'ensemble des indicateurs de la transformation numérique exposés dans Calvino et al. (à paraître), *Business dynamics and digitalisation: A progress report*. Ce graphique prend pour point de départ le classement des secteurs tel qu'établi pour la période initiale (2001-03) et fait uniquement apparaître les facteurs de marge estimés en faisant l'hypothèse d'une fonction de production Cobb-Douglas.

3. *L'amélioration des solutions commerciales et la personnalisation de l'expérience client*

L'article « Welcome to the Experience Economy » paru dans la Harvard Business Review en 1998 a développé le concept de l' « Experience thinking », qui renvoie au fait

283 PwC (2019), "Creating Value from Data" Lien
284 Calligaris, S., C. Criscuolo et L. Marcolin (2018), Mark-ups in the digital era, Lien

que la valeur économique dérive de plus en plus de la création d'une expérience client personnalisée, par opposition à la fabrication de biens ou la fourniture de services. [285]

La solidification de ce courant de pensée a conduit à l'émergence du marketing expérientiel[286], puis du marketing participatif, qui suppose la participation du client à la création de valeur de l'entreprise. Ce sont les directions Marketing des entreprises qui les premières se sont emparées de l'exploitation des données que les individus et les objets connectés produisent, avec la finalité de mieux connaître les clients et les consommateurs. De fait, les entreprises soucieuses de valoriser les masses de données accumulées ont développé des usages marketing du *big data*.[287]

Pour ce faire, les entreprises ont recours aux solutions de *big data analytics*, ou la science de tirer des conclusions à partir de l'analyse d'informations brutes, grâce à l'automatisation des algorithmes. Ces solutions demandant des puissances de calculs élevés sont fournies par des prestataires de service externe. Ils peuvent révéler des tendances et des mesures qui, autrement, seraient perdues dans la masse d'informations. Une entreprise peut également utiliser le *big data analytics* pour prendre de meilleures décisions commerciales et aider à analyser les tendances et la satisfaction des clients, ce qui peut conduire à des produits et services nouveaux et améliorés.

À titre d'exemple, les plateformes numériques aussi variées que les GAFAs, ou Le Bon Coin pour la France, utilisent des données issues des actions des utilisateurs afin de personnaliser la navigation et améliorer l'expérience client. L'entreprise Le Bon Coin en particulier déclare que le numérique responsable est le socle de sa politique RSE, la donnée est mobilisée de la façon la plus responsable possible (pas de vente des données à de tierces-parties). Alors que la question de l'utilisation des données surgit de manière plus fréquente dans le débat public, cela constitue un avantage comparatif et de différenciation.[288]

État des lieux de l'utilisation du *cloud computing* par les entreprises européennes : des enjeux RSE naissants, sur lesquels l'UE est mobilisée

1. *Un recours encore au* cloud computing *par les entreprises européennes encore limité*

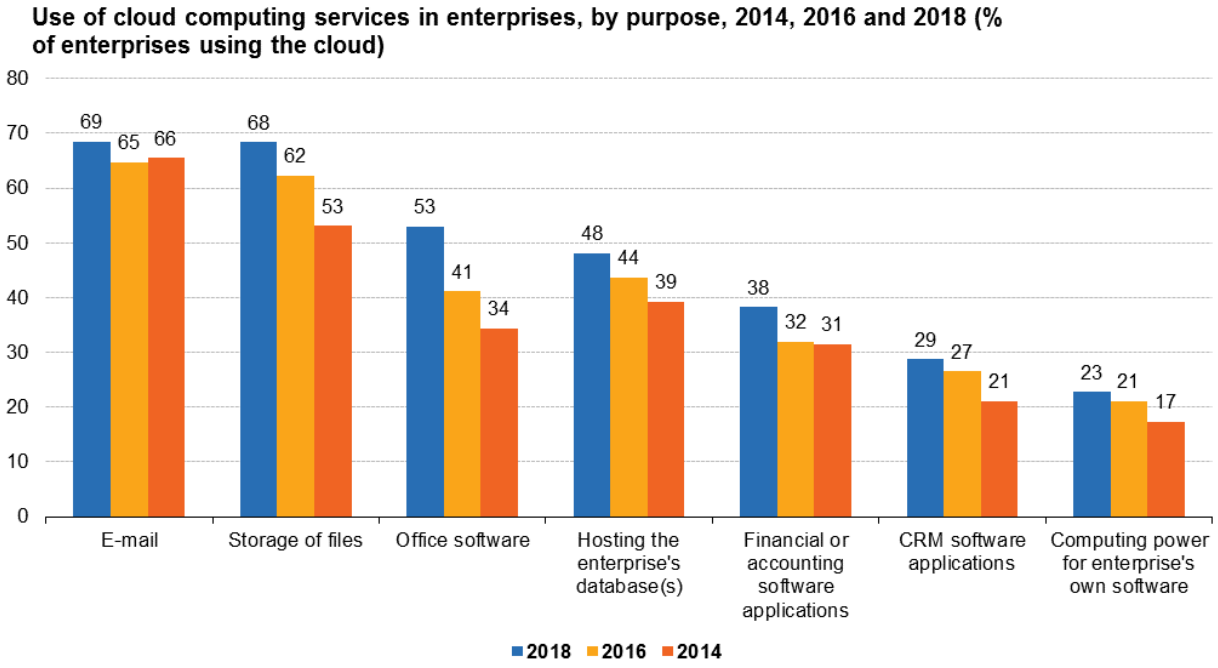
On peut connaître le niveau d'utilisation des solutions de *cloud computing* par entreprises européennes grâce à l'étude d'Eurostat, évoquée précédemment[289], ayant porté sur 158 000 entreprises des 1.6 millions d'entreprises européennes. Cette étude, qui date de Décembre 2018, devrait être mise à jour en 2020. Aujourd'hui, dans l'Union européenne, **seules 26 % des entreprises et une PME sur cinq utilisent le *cloud***

[285] Pine J. et Gimore H. (1998), « Welcome to the experience economy" Lien
[286] W. Batat & I. Frochot(2014), « Marketing Expérientiel, comment concevoir et stimuler l'expérience client ? »
[287] Frimousse S. et Peretti J. (2019), « « Expérience collaborateur » et « Expérience client » : comment l'entreprise peut-elle utiliser l'intelligence artificielle pour progresser ? » Lien
[288] Audition de Arnaud Jacques
[289] Eurostat (2018), "Cloud Computing – statistics on the use by enterprise" Lien

computing. Il apparaît que les entreprises étaient beaucoup plus nombreuses à utiliser des *clouds* publics (**18 %**) plutôt que des *cloud*s privés (**11 %**).

L'utilisation a augmenté en particulier dans les grandes entreprises où plus d'une sur deux (**56 %**) l'a utilisé en 2018, soit une augmentation de 21 points par rapport à 2014. L'augmentation pour les petites et moyennes entreprises au cours de cette période a été trois fois moindre (de **18 % à 25 %**).

Le *cloud computing* répond à plusieurs besoins des entreprises en matière de TIC : **68 %** de celles recourant au *cloud* l'ont utilisé pour stocker des fichiers sous forme électronique. 48 % l'utilisent pour héberger leur base de données, tandis que **53 %** déclarent l'utiliser pour des logiciels de bureautique. **38 %** l'utilisent pour la gestion de la comptabilité, et **29 %** pour le CRM. Enfin, **23 %** déclarent y avoir recours pour gérer leurs propres applications logicielles.



Source: Eurostat (online data code: isoc_cicce_use)

eurostat

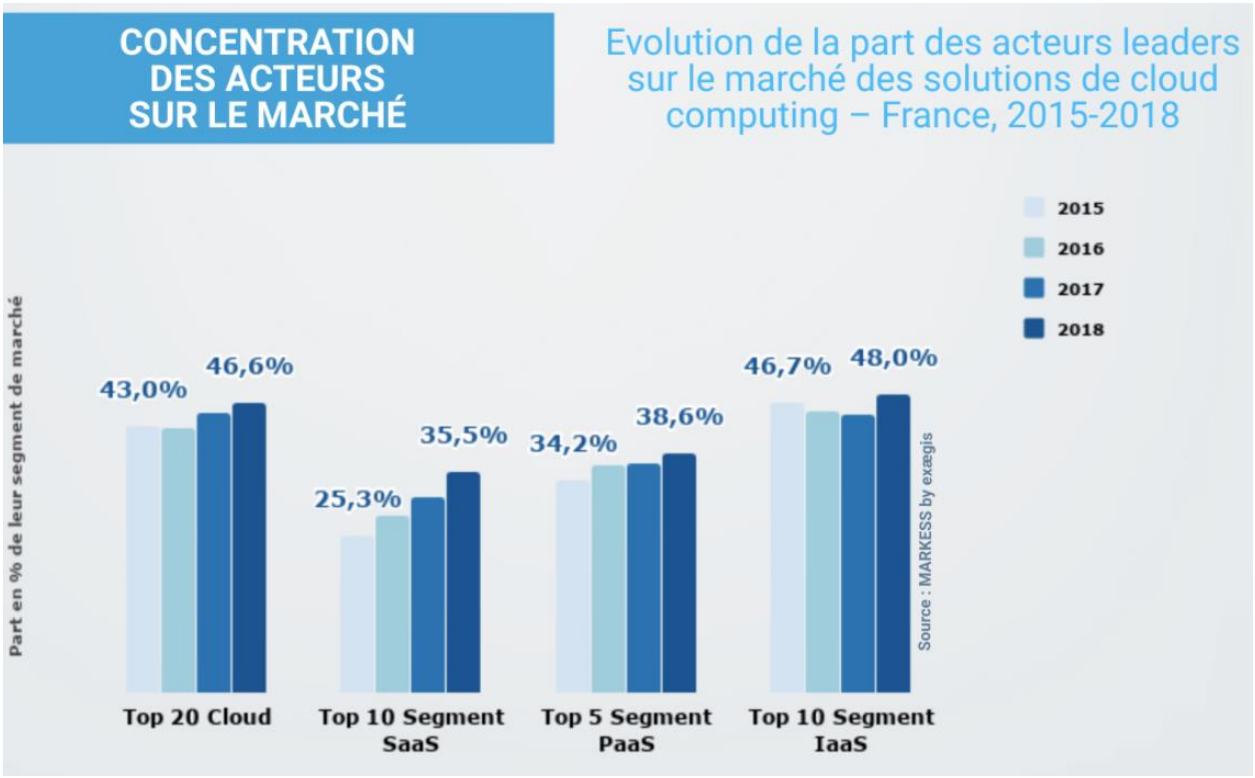
Les secteurs d'activité ayant le plus recours au *cloud computing* sont, sans surprise, le secteur de l'Information et de la Communication (**64 %**), suivi par le secteur scientifique et technique (**44 %**) Dans les autres secteurs économiques, le pourcentage varie **entre 20 % et 33 %.**

2. *Un encadrement protéiforme au niveau de l'UE pour faire face à un marché concentré dominé par quelques acteurs*

Le marché du *cloud computing* français se concentre progressivement entre les mains de quelques acteurs. On peut dire que ce marché est fortement consolidé, et que cette tendance s'accélère. Cela a été rendu possible les économies d'échelle, ayant conduit à

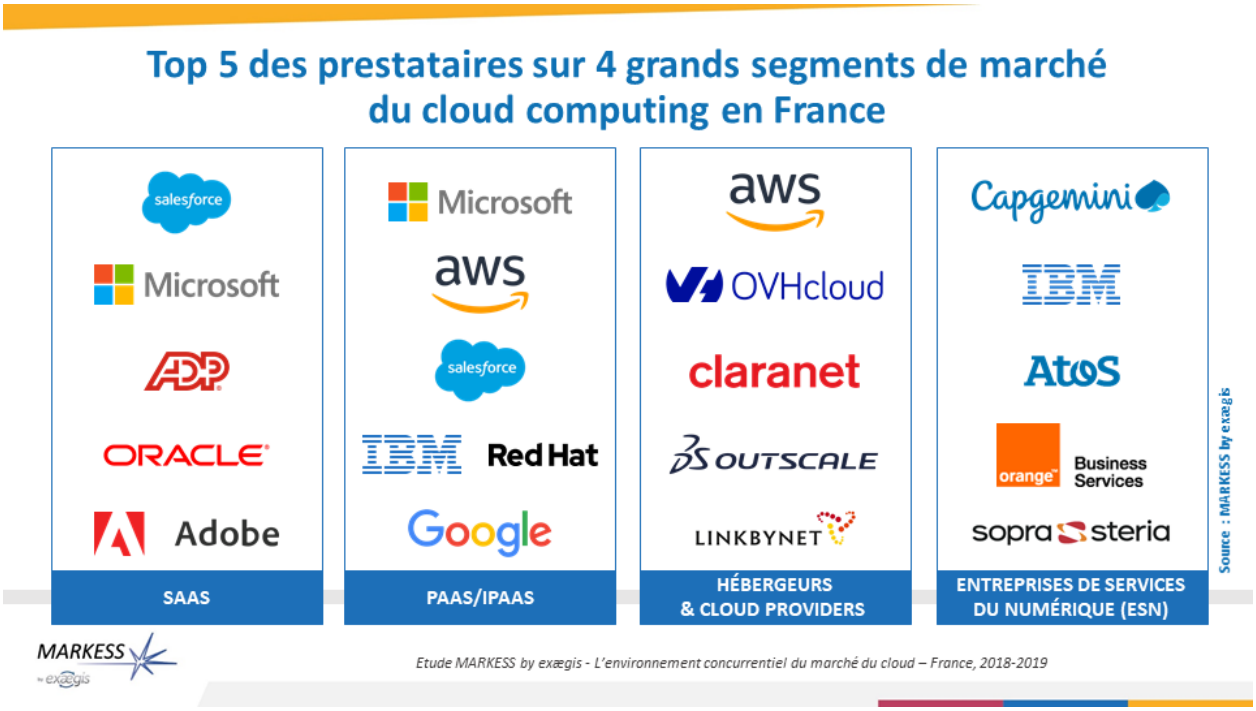
un accroissement des parts de marché. Cette dynamique est soutenue par une innovation toujours plus pointue (R&D) et une accélération du nombre de fusions-acquisitions.

Dans ce sens, Ariel Ezrachi de l'Université d'Oxford, qui a publié un livre appelé « Virtual Competition » avec Maurice Stucke de l'Université du Tennessee[290], avancent l'argument qu'avec leurs données et leurs algorithmes, les géants d'Internet peuvent détecter les menaces concurrentielles et racheter les start-ups qui peuvent devenir leurs rivales. Ils peuvent également manipuler les marchés qu'ils hébergent, par exemple en faisant réagir rapidement leurs algorithmes afin que les concurrents n'aient aucune chance de gagner des clients.



291

[290] Ezrachi A. et Stucke M. (2016), « Virtual Competition » Lien
[291] Benyalef N. (2020), « 5 tendances stratégiques à 2021 sur le marché du cloud en France » Lien



292

[292] Benyalef N. (2020), « Concentration des acteurs sur le marché du cloud en France » Lien

Alors qu'une partie considérable des entreprises européennes (**14 %**) était classifiée par Eurostat comme dépendant fortement du *cloud* pour son activité, celles-ci sont mal équipées pour faire face à la puissance monopolistique des fournisseurs de solutions de *cloud computing*. Si **72 %** des PME interrogées déclarent avoir l'intention d'en changer, **57 %** déclarent avoir des difficultés à la faire. Cet effet de *lock-in* est lié à un manque de portabilité des données et de transférabilité, et heurte la capacité des organisations à choisir librement leur prestataire de service.

Pour faire face à ses défis, l'Union européenne cherche à développer et à encadrer le marché européen du *cloud computing*. Pour l'UE, il est important que le marché européen du cloud reste compétitif, fiable, abordable, et sécurisé. Le *cloud computing* est la pierre angulaire du Digital Single Market (cf. Partie X). La Règlement UE/2018/1807 relatif au libre flux des données à caractère non personnel, détaillé dans le Cadre Normatif. Il vise à de créer un marché unique numérique et les conditions d'une concurrence plus forte entre fournisseurs de services informatiques, particulièrement du *cloud*. Il aurait permis d'augmenter de 4 % le PIB de l'UE entre 2019 et 2020.[293]

À cette *hard law* s'ajoute la *soft law* : la Commission européenne travaille à un certain nombre d'initiatives d'autorégulation[294] sur les thèmes suivants :

- des dispositions contractuelles équitables et équilibrées, notamment en normalisant les Service Level Agreement, ou « entente de niveau de service » ;
- portabilité des données et transférabilité entre les prestataires de service *cloud* : un code de conduite a été mis en place ;
- un système de certification européen de la cybersécurité du *cloud* ;
- un code de conduite sur l'efficience énergétique des *data centers* ;
- des codes de conduites sur la protection des données du *cloud computing.*

L'UE pilote par ailleurs le marché du *cloud computing* avec des investissements directs. Entre 2014 et 2020, dans le cadre de projet de financement Horizon 2020, l'UE a investi environ 300 millions d'euros dans des projets ayant trait au *cloud computing*. Ces investissements ont donné lieux à quelques succès, tel que Sunfish, une plateforme pour la fédération des *clouds* du secteur public, utilisant la blockchain pour les données sensibles. Ce projet pionnier a suscité un grand intérêt parmi les administrations publiques : 6 États membres ont collaboré étroitement en partageant en toute sécurité des informations sensibles telles que les casiers judiciaires, les coordonnées des contribuables et les données relatives aux soins de santé.[295]

3.2.2 Hybridation du *cloud*

Les transformations numériques actuelles tendent à rendre les données de plus en plus fragmentées et décentralisées. Les entreprises peuvent choisir de les disperser dans différents lieux au sein-même de l'entreprise, ou bien à l'extérieur dans le *cloud* ou chez de tierces-parties. Le cabinet de conseil IDC Technologies estime, à ce titre, que 90 %

[293] Commission européenne (2019), « Free flow of non-personal data » Lien
[294] Lien
[295] http://www.sunfishproject.eu/

des organisations prévoient d'utiliser le *cloud* pour la protection de leurs données dans les 12 mois à venir.[296]

En pratique, on observe une hybridation du *cloud* au travers du recours à des clouds privés et publics. La combinaison de ces deux types de *cloud* répond à l'ambition d'obtenir les meilleurs avantages. En 2018, une étude de Nutanix révélait que 91 % des responsables IT d'entreprises considèrent que le modèle le plus adapté est celui du *cloud* hybride[297].

Le *cloud* privé est un système où les serveurs – sur site ou hors site – sont dédiés à une seule entreprise. Au contraire, le *cloud* public est un système où les serveurs sont partagés entre plusieurs clients d'un seul et même fournisseur. À ce titre, les serveurs des *clouds* publics sont hors-site, dans les *data centers* dudit fournisseur.

Le National Institute of Standards and Technology[298] définit ainsi le *cloud* hybride comme « une infrastructure *cloud* composée de deux infrastructures *cloud* distinctes, ou plus, pouvant être privées ou publiques et qui restent des entités uniques, mais sont connectées par une technologie standard ou propriétaires permettant la portabilité des données et des applications. » ; c'est ainsi une forme croisée entre le *cloud* privé et le *cloud* public, une partie des applications et données se trouvent dans les serveurs d'un prestataire externe et l'autre partie se trouve dans les locaux de l'entreprise.

Le *cloud* hybride fonctionne selon un mécanisme conjoint entre les *clouds*, qui doivent travailler de pairs. Ce processus comporte des avantages et des inconvénients pour les entreprises. Dans un premier temps, l'alliance du *cloud* privé sur lequel l'entreprise garde la main et du *cloud* public adapté seulement aux besoins permet de conserver les données critiques sur site et de réduire les charges de l'entreprise en payant seulement ce dont elle a besoin. Néanmoins, le *cloud* hybride[299] n'est pas adapté à toutes les situations. Les coûts engendrés par l'installation et la gestion de serveurs privés peuvent s'avérer trop hauts pour les PME et PMI, qui s'en tiennent au *cloud* public moins onéreux et plus adapté.

3.2.3 Data lakes

Jusqu'à ce jour, les organisations collectaient et rassemblaient les données « en silo », ce qui engendrait un certain manque d'accessibilité, de traçabilité et d'interopérabilité. Il s'agit d'une masse de données brutes, d'informations et d'idées potentielles.

Pour convertir cette masse en lac de données, il faut le classer, y attacher des métadonnées pertinentes et tout classer dans les segments de stockage appropriés.

« Un *data lake* est un référentiel de données permettant de stocker une très large quantité de données brutes dans le format natif pour une durée indéterminée. Cette méthode de stockage permet de faciliter la cohabitation entre les différents schémas et

[296] Ho. A (2019), "Data Protection for multicloud environments" Lien
[297] Le Big Data (2018), « Cloud Hybride : qu'est ce que c'est et à quoi ça sert ? »
[298] « The NITS Definition of Cloud Computing », septembre 2011
[299] « Cloud Hybride : qu'est ce que c'est et à quoi ça sert ? », Le Big Data, novembre 2018

formes structurelles de données, généralement d'objets ou de fichiers (Blob – Binary Large Objects).

Au sein d'un seul *data lake*, toutes les données de l'entreprise sont stockées. Les données brutes, y compris les copies des données système source, côtoient les données transformées. Ces données sont ensuite utilisées pour établir des rapports, pour visualiser les données, pour l'analyse de données ou pour le *machine learning*.

Ce composant technique vient parfois en complément ou substitut du fameux *data warehouse* et autre *datamart.* À cela une bonne raison, le Data Lake capte les données en temps réel et donne directement accès aux applications métiers qui peuvent interagir avec ce lac de données à des fins diverses. »[300]

Une pratique qui peut renforcer la responsabilité des organisations face à leurs données, en les rendant plus accessibles, traçables, et interopérables. À la condition d'une gouvernance efficace : le désordre peut s'installer rapidement, à moins de hiérarchiser et catégoriser les données.

Les différences entre un *data warehouse* et un *data lake* :

« Au sein d'une *data warehouse*, on trouve uniquement des données traitées et structurées. Dans un *data lake*, elles peuvent être structurées, semi-structurées, non-structurées ou brutes. Avant de charger une donnée dans une *data warehouse*, il est nécessaire de lui donner une forme et une structure, par exemple un modèle. Au sein d'un *data lake*, il est possible de charger des données brutes, et de leur conférer une forme et une structure uniquement quand le moment est venu d'utiliser ces données.

Le stockage dans une *data warehouse* est très cher pour les grands volumes de données, tandis qu'un *data lake* comme Hadoop est conçu pour un stockage low-cost. Deux raisons à cela. Tout d'abord, Hadoop est un logiciel open source. De fait, la licence et le support communautaire sont gratuits. De plus, Hadoop est conçu pour être installé sur du hardware bon marché.

La Warehouse est moins agile, sa configuration est figée. Il est possible de modifier sa structure, mais cela nécessite du temps. De son côté, le Lake est très agile et peut être configuré ou reconfiguré à volonté. Les modèles, les requêtes, et les applications peuvent être aisément modifiées par les développeurs et les *data scientists*. En revanche, la *data warehouse* est plus mature en termes de sécurité, grâce à des décennies d'existence. Malgré tout, de nombreux efforts sont déployés par l'industrie du *big data* pour sécuriser les *data lakes*, et le retard devrait être rapidement rattrapé. Enfin, les principaux utilisateurs du *data lake* sont des *data scientists*, tandis que la *data warehouse* est ouverte à tous les membres de l'entreprise. »[301]

[300] Lien
[301] Bastien L. (2017), « Data lakes : définition » Lien

Les bonnes pratiques de la gestion d'un *data lake*[302] :

- embarquer et ingérer rapidement les données avec très peu d'amélioration ;
- contrôler qui charge quoi, quand et comment dans le *data lake* ;
- conserver des données dans leur état brut afin de préserver les détails originaux et les schémas ;
- améliorer le temps de lecture des données pendant que le *data lake* est accessible et en cours de traitement ;
- capturer les *big data* et autres nouvelles sources de données dans le *data lake* ;
- intégrer les données provenant de différentes sources, structures et crus ;
- étendre et améliorer les architectures de données de l'entreprise ;
- faire que chaque *data lake* serve à des objectifs techniques et architecturaux multiples ;
- activer les nouvelles meilleures pratiques axées sur le libre-service *data driven*
- sélectionnez les plates-formes de gestion des données qui satisfont aux exigences du *data lake.*

3.3 Gestion et exploitation des données : les spécificités des PME

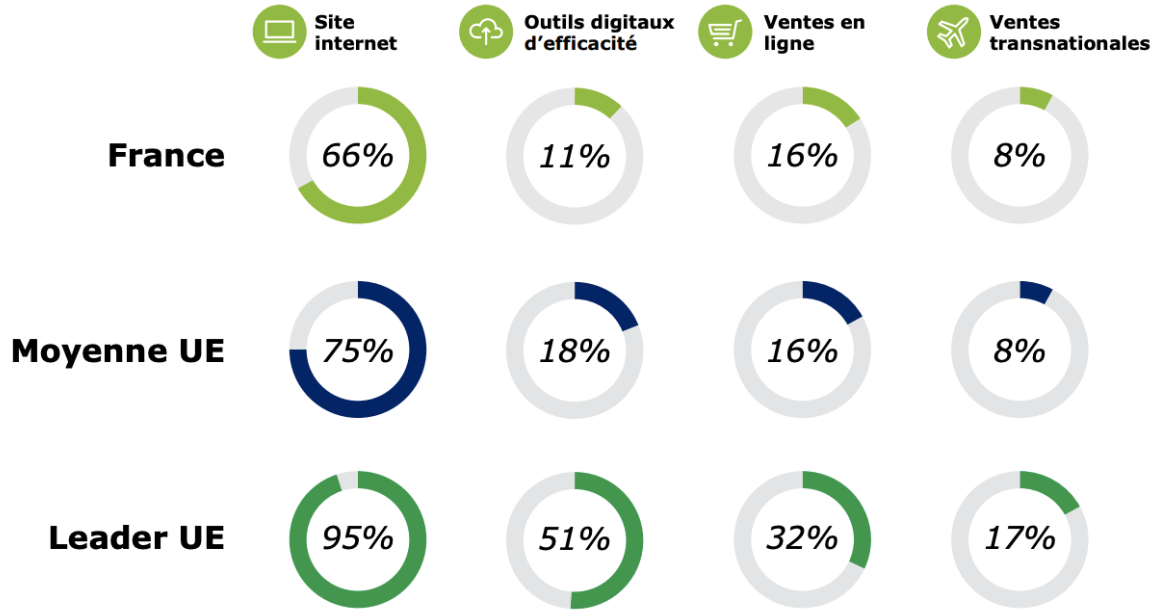
La France en retard

Alors que l'innovation au sein des PME a des retombées positives sur leur performance dans la mesure où elle est accompagnée par des investissements en technologies, ou bien par un usage plus poussé des technologies déjà présentes dans l'entreprise[303], un rapport de la CPME[304] nous indique que moins d'une TPE sur trois a déployé ou est en train de déployer sa transformation digitale.

Selon un rapport de Deloitte[305], en 2016, tandis que l'exploitation des outils digitaux et des plateformes représentaient un levier de croissance important pour les PME, la France accuse toujours un retard par rapport au reste de l'Union européenne, au regard de différents indicateurs de maturité digitale.

[302] Grandmontagne Y. (2018), « Top 10 des meilleures pratiques du data lake » Lien
[303] Deltour F. et Lethiais V. (2014), « L'innovation en PME et son accompagnement par les TIC : quels effets sur la performance ? » Lien
[304] CPME (2019), « Transformation digitale des TPE : entre prise de conscience et attentisme » Lien
[305] Deloitte (2016), « Economie numérique : le digital, une opportunité pour les PME françaises » Lien

Figure 2 - L'adoption de nouvelles technologies en France, par rapport au reste de l'UE



Source : Eurostat, entreprises de moins de 10 employés exclues. Le cloud computing est utilisé comme référence pour les outils digitaux d'efficacité. Les pays leaders de l'UE sont, de gauche à droite, la Finlande, la Finlande, l'Irlande et l'Irlande.

306

Un nombre encore plus faible de PME profitent du e-commerce. Alorsqu'en France 7 consommateurs sur 10 achètent et paient en ligne, en 2015, seulement une PME sur huit recevait des commandes en ligne pour un chiffre d'affaires global de près de 60 milliards d'euros, soit près de 3 % du chiffre d'affaires total des PME françaises. À titre de comparaison, la proportion des PME réalisant des ventes en ligne en Allemagne à la même période était deux fois plus importante.[307]

Selon le rapport de Deloitte, les PME les plus petites subissent le retard le plus important : elles réalisent quatre fois moins de ventes en ligne que les grandes entreprises, et sont trois fois moins susceptibles de déployer des outils technologiques de productivité.

La digitalisation peut pourtant être un levier de croissance, car elle permet d'accéder aux marchés globalisés : les PME françaises ayant initié ou réalisé leur transformation digitale sont trois fois et demi plus susceptibles d'exporter que la moyenne des PME françaises.

Le rapport Villani met en lumière que la France compte 80 ETI et PME et plus de 270 start-ups spécialisées dans l'IA.

306 idem
307 Eurostat (2019), « E-commerce statistics » Lien

Des barrières persistantes

Ainsi, le rapport de la CPME, identifie les freins qui s'opposent encore à la transformation digitale des PME :

- le manque de compétences techniques digitales ;
- la méconnaissance des bénéfices potentiels de la transformation en termes de coûts ;
- le manque de familiarisation des employés aux outils digitaux disponibles.

Selon l'étude de la CPME, 7 TPE sur 10 rencontrent de nombreuses difficultés dans leur en œuvre de leur transformation digitale. Les principales difficultés auxquelles elles font face sont :

- l'adaptation des équipes et des process (43 %) ;
- le manque de compétences techniques (41 %) ;
- le financement des investissements (40 %).

Sur le plan de la cybersécurité, 48 % des TPE ne se sentent pas concernées par les cyberattaques.

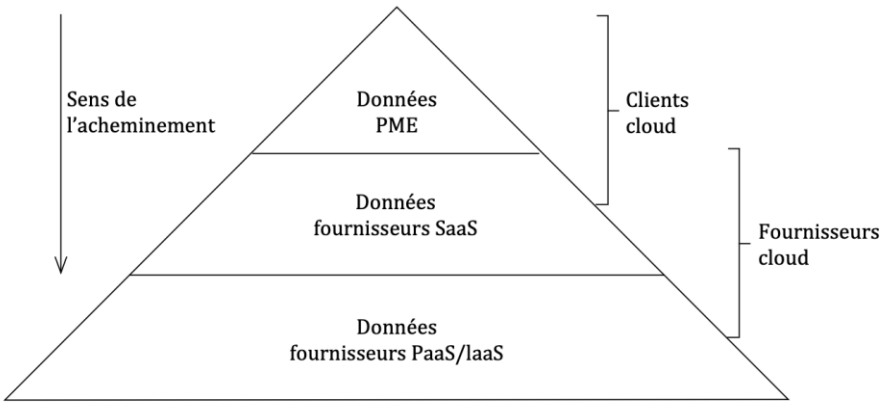
Pourtant, pour les PME, les exigences de sécurité peuvent être tellement fortes qu'il peut être difficile de trouver des prestataires de service de stockage des données apportant des garanties suffisantes. Il est important pour elles de choisir un environnement informatique accrédité qui a fait ses preuves. [308]

Les PME face au *cloud computing*

1. *L'acheminement des données des PME vers leur fournisseur* cloud

La concrétisation d'un service *cloud* au sein d'une PME dépend à la fois du modèle de déploiement utilisé (Public, Privé, Hybride) et du modèle de service (Saas, PaaS, Iaas). Dans tous les cas, la migration des données vers le prestataire informatique entraine un transfert de pouvoirs, d'applications, et de processus vers une tierce-partie.

Figure 2 - Modélisation de l'acheminement des données



[308] Audition de Mme Françoise Durand-Rivoire, Directrice Corporate Social Responsibility & Digital Transformation chez Novasep

Pour les fournisseurs de services qui détiennent les données hétérogènes de différentes PME, le croisement de celles-ci peut créer un avantage concurrentiel. Dans le même temps, les entreprises clientes sont exposées à une perte de contrôle.

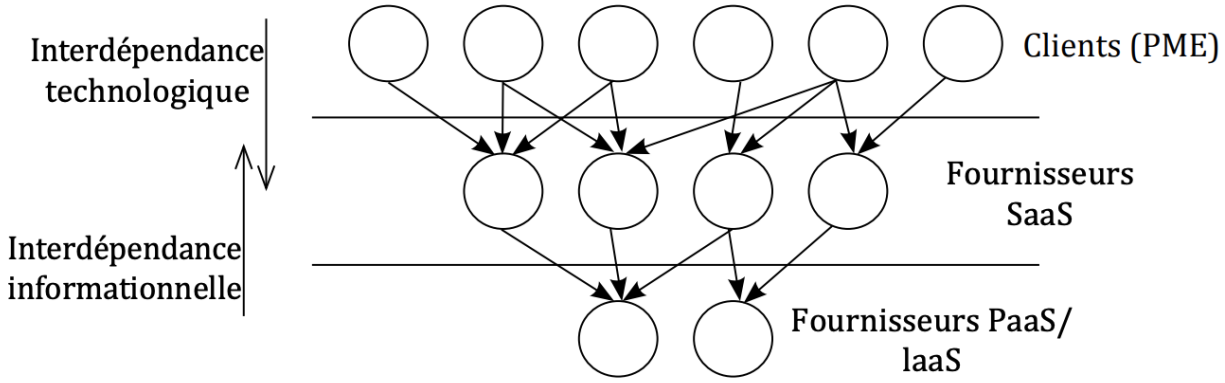
2. *Le mécanisme de domination des opérateurs* cloud

Il existe des inégalités entre les grandes et petites entreprises en ce qui concerne l'externalisation des SI. Elle est éloignée des typologies homogènes des grandes entreprises. L'orientation technologique du marché de l'externalisation des SI des PME peut être compris au travers de trois tendances majeures[309] :

- L'incompréhension des enjeux et défis du SI par le dirigeant lui-même
- Le choix pragmatique de s'orienter vers le système le plus simple à piloter, à financer et à faire évoluer à court terme
- L'orientation stratégique de la puissance publique vis-à-vis du *cloud* souverain

La contractualisation entre les PME et les opérateurs du *cloud computing* permet d'obtenir des garanties opérationnelles et de sécurité, dans le cadre d'un processus de migration de leurs données que les PME peuvent ne pas maitriser suffisamment. En effet, l'asymétrie des positions des acteurs de ce marché donne aux PME un faible pouvoir de négociation. La décision de recourir au *cloud* n'est ni facilement réversible ni clairement neutre. Elle résulte d'une obligation opérationnelle de minimisation des coûts.

Figure 1 - Les interdépendances d'un réseau Cloud Computing



Pour une PME, la migration des SI vers le *cloud* nécessite donc une préparation importante et un accompagnement direct de la part des dirigeants : ce passage touche en profondeur la stratégie et le business model de la PME.

[309] Bouaynaya W et Bidan M. (2017), « Une exploration du rôle des opérateurs du cloud computing dans l'acheminement des données des PME » Lien

Un nécessaire accompagnement

1. *BPI France*

Il ressort que les TPE attendent un accompagnement dans le choix et l'équipement en solutions digitales, pour les aider dans l'élaboration de la stratégie de transformation digitale, et pour les former aux outils digitaux.

Ainsi, il semble qu'un accompagnement des TPE et PME françaises dans leur transformation digitale serait souhaitable.

La BPI est le chef de file des solutions d'accompagnement de la digitalisation des entreprises. Elle met à disposition des experts et des offres d'accompagnement.[310] Elle a également réalisé un « Digitalomètre »[311] qui permet à une entreprise d'évaluer sa maturité digitale. Il s'agit d'un autodiagnostic qui permet d'identifier les phases de progression pour guider vers l'action.

La BPI France a également développé un Digital Guide, une application mobile qui contient des étapes concrètes permettant d'activer des actions digitales[312], un guide de sensibilisation aux bonnes pratiques RGPD à destination des TPE et des PME[313], ainsi qu'un e-learning pour aider les TPE / PME à intégrer la transformation digitale dans leur stratégie.[314]

2. *La Plateforme France Num*

« France Num est l'initiative gouvernementale pour la transformation numérique des TPE/PME pilotée par la Direction Générale des Entreprises. France Num fédère des ressources pratiques, des aides financières et un réseau de conseillers (« les activateurs ») qui sont actifs sur tout le territoire. Le programme d'actions a été construit en partenariat avec Régions de France, l'ensemble des Régions et les organisations professionnelles, il s'appuie sur les recommandations du Conseil national du numérique. »[315]

France Num a notamment lancé une campagne de communication radio et Internet ciblant les TPE PME, visant à faire connaître la marque France Num auprès du tissu économique sur les territoires et de mettre en relation les entreprises avec des activateurs France Num, experts du numérique, proches de chez eux.

Il semble, ainsi, souhaitable d'adopter des politiques favorisant la digitalisation des TPE/PME : pédagogie, accompagnement, mise à disposition d'outils.

310 Lien
311 Lien
312 Lien
313 Lien
314 Lien
315 Lien

3.4 Quelle délégation de responsabilité entre une entreprise et son prestataire de services numériques ?

Alors que les entreprises ont de plus en plus recours à des prestataires externes pour la gestion de leurs données ou à des outils de transferts de données entre organisations. Pour mettre en œuvre cette sous-traitance, elles en du plus en plus recourt à des outils de transfert de données vers de tierces-parties, dans le cadre d'un contrat comportant des obligations vis-à-vis des données. La question se pose donc de la délégation de responsabilité, spécifiquement RSE, qui s'applique entre une entreprise et son sous-traitant prestataire de services numériques.

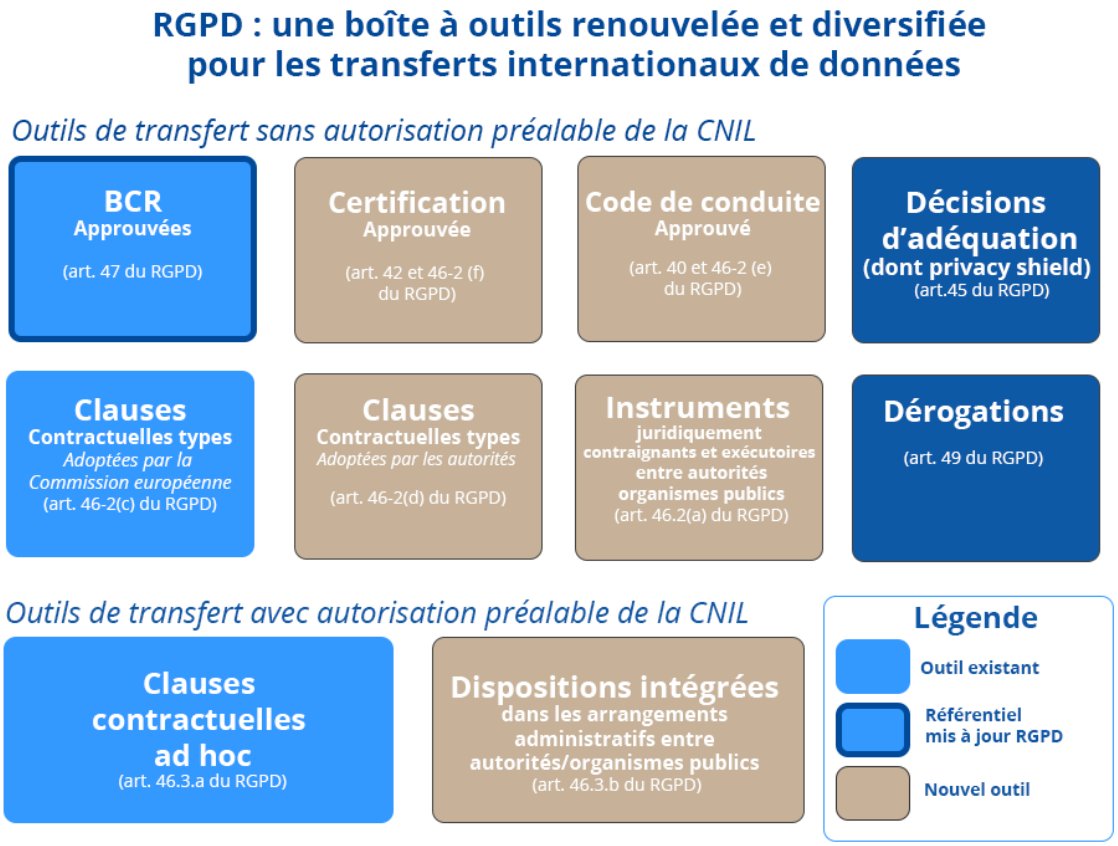
Spécifiquement dans un contexte de sous-traitance, il convient de se demander quel contrat lie l'entreprise au prestataire, et se demander si le choix du prestataire est dicté par la technique, la responsabilité, où la règlementation applicable.

Dans ce contexte, il convient d'étudier quelle application de la vigilance est demandée.

Dans le cadre d'un contrat entrainant un transfert de données, on distingue[316] :

- Le «responsable du traitement» est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre;
- Le «sous-traitant» est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données personnelles pour le compte d'un autre organisme, dans le cadre d'un service ou d'une prestation. Sont notamment concernés :
  - Les prestataires de services informatiques (hébergement, maintenance, etc.),
  - Les intégrateurs de logiciels ;
  - Les sociétés de sécurité informatique ;
  - Les entreprises de service du numérique ou anciennement sociétés de services et d'ingénierie en informatique (SSII) qui ont accès aux données ;
  - Les agences de marketing ou de communication qui traitent des données personnelles pour le compte de leurs clients.

[316] Article 4 du RGPD



317

3.4.1 Des obligations pour les sous-traitants de données

Les articles 28, 30.2 et 37 du RGPD apportent des précisions sur les obligations du sous-traitant dont la responsabilité sera susceptible d'être engagée en cas de manquement.

Lorsqu'un sous-traitant intervient dans la mise en œuvre d'un traitement de données personnelles, il doit offrir à son client « des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du présent règlement et garantisse la protection des droits de la personne concernée » (article 28 du RGPD).» [318]

Le guide du sous-traitant édité par la CNIL[319] détaille en pratique les obligations des sous-traitants :

Une obligation de transparence et de responsabilité, notamment pour toutes les informations nécessaires pour démontrer le respect des obligations et pour permettre la réalisation d'audits. Les sous-traitants devront tenir un registre des activités de traitement effectuées pour le compte de leurs clients.

317 Lien
318 CNIL (2017), « Guide pour accompagner les sous-traitants » Lien
319 Lien

La prise en compte des principes de protection des données dès la conception et de protection des données par défaut. Cela inclut par exemple la minimisation des données collectées (finalité), ou encore la purge des données après une durée définie.

Une obligation de garantir la sécurité des données traitées, notamment un système d'alerte et la mise en place d'un niveau de sécurité adapté.

Une obligation d'assistance, d'alerte et de conseil : Ils doivent les aider dans la mise en œuvre de certaines obligations du règlement (étude d'impact sur la vie privée, notification de violation de données, sécurité, contribution aux audits).

Le respect de ces obligations par les sous-traitants est effectivement contrôlé tout au long de la relation contractuelle par des audits par les responsables de traitement : selon un rapport de Capgemini[320], 82 % des organisations conformes au RGPD ont pris des mesures pour s'assurer que les fournisseurs de technologies sous-traitants (entreprises de produits technologiques, fournisseurs de "cloud", centres de données, matériel/infrastructure, etc.) sont conformes aux réglementations applicables en matière de confidentialité des données, contre 63 % des organisations non conformes. De plus, 61 % des entreprises conformes au RGPD ont également contrôlé la conformité de leurs sous-traitants à la réglementation sur la protection des données et la vie privée, contre 48 % pour les entreprises non conformes au RGPD.

3.4.2 Les modalités du contrat liant responsable de traitement et sous-traitant

La loi Informatique et Libertés spécifie qu'en cas de recours à un sous-traitant :

- Le contrat entre ce sous-traitant et le responsable du traitement doit indiquer les obligations incombant au sous-traitant pour protéger la sécurité et la confidentialité des données et prévoir qu'il ne peut agir que sur instruction du responsable du traitement ;
- Ce sous-traitant doit présenter des garanties suffisantes pour assurer la mise en œuvre des mesures de sécurité et de confidentialité prévues à l'article 34 de la loi Informatique et Libertés ;
- Cette exigence ne décharge pas le responsable du traitement de son obligation de veiller au respect de ces mesures.

L'acte 28 du RGPD stipule qu'un sous-traitant doit établir avec son client un contrat ou un autre acte juridique précisant les obligations de chaque partie et reprenant les dispositions de l'article 28 du règlement européen.

Dans ce contrat, il devra recenser par écrit les instructions de son client concernant les traitements de ses données afin de prouver qu'il agisse « sur instruction documentée du responsable de traitement ».

[320] Lien

Par ailleurs, dans le cadre de ce contrat, si le sous-traitant veut faire appel à un autre sous-traitant, il devra d'abord recueillir l'autorisation écrite du responsable de traitement.

La CNIL fournit aux entreprises des exemples de clauses de sous-traitance pour les aider dans cette démarche.[321]

3.4.3 Cas particulier : responsabilités spécifiques de l'entreprise et du sous-traitant lors d'un contrat dans le cadre du Privacy Shield :

L'article 10.a. du *Privacy Shield Framework*[322] stipule que :

i. « Lorsque des données à caractère personnel sont transférées de l'UE vers les États-Unis uniquement à des fins de traitement, **un contrat sera nécessaire,** indépendamment de la participation du sous-traitant au bouclier de protection de la vie privée. »
ii. « Les responsables du traitement des données dans l'Union européenne **sont toujours tenus de conclure un contrat lorsqu'un transfert est effectué** pour un simple traitement, que le traitement soit effectué à l'intérieur ou à l'extérieur de l'UE et que le sous-traitant participe ou non au bouclier de protection de la vie privée. »
iii. Étant donné que les participants au programme Privacy Shield assurent une protection adéquate, **les contrats conclus avec les participants au programme Privacy Shield pour le simple traitement ne nécessitent pas d'autorisation** préalable (ou cette autorisation sera accordée automatiquement par les États membres de l'UE)

Notons toutefois que lorsque des informations personnelles sont transférées entre deux contrôleurs au sein d'un groupe contrôlé de sociétés ou d'entités, un contrat n'est pas toujours nécessaire en vertu du « *Accountability for Onward Transfer Principle* ». Les responsables du traitement au sein d'un groupe contrôlé de sociétés ou d'entités peuvent fonder ces transferts sur d'autres instruments, tels que les règles d'entreprise contraignantes de l'UE ou d'autres instruments intra-groupe (par exemple, les programmes de conformité et de contrôle)

1. Les spécificités du contrat s'agissant des transferts vers une société établie aux Etats-Unis agissant en qualité de responsable de traitement

« Avant de transférer des données à caractère personnel auprès d'une entreprise établie aux États-Unis qui déclare être certifiée au Bouclier de Protection des Données, les entreprises européennes doivent s'assurer que la société américaine dispose d'une certification active (les certifications doivent être renouvelées tous les ans) et que la certification couvre les données en question (plus particulièrement : les données RH, les données non-RH respectivement).

[321] https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses
[322] https://www.privacyshield.gov/article?id=10-Obligatory-Contracts-for-Onward-Transfers

Afin de vérifier si une certification est active et applicable, les sociétés européennes doivent consulter la Liste du Bouclier de Protection de Données qui est publiée sur le site du Département du Commerce américain.[323]

Toutes les sociétés américaines ayant accompli avec succès le processus d'auto-certification sont répertoriées sur la Liste. La Liste du Bouclier de Protection des Données précise en outre le type de données à caractère personnel pour lequel une société américaine a procédé à l'auto-certification (données RH ou non-RH) et fournit également des informations sur les services qu'elle propose.

Avant de procéder au transfert de données à caractère personnel, les entreprises européennes agissant en qualité de responsable de traitement doivent veiller à ce que le transfert soit conforme au droit applicable en matière de protection de données à caractère personnel. En premier lieu, les entreprises européennes peuvent uniquement communiquer des données à caractère personnel à une société établie aux Etats-Unis si le transfert bénéficie d'une base légale (c'est-à-dire si le transfert est conforme aux dispositions de la loi nationale transposant les articles 7 et 8 de la Directive 95/45/CE). En outre, l'ensemble des autres obligations générales prévues par la législation européenne en matière de protection de données à caractère personnel, pour le(s) transfert(s) doivent être respectées (notamment, les principes de finalité, de proportionnalité, de qualité des données, les obligations d'information envers les personnes concernées). Si les données ont vocation à être transférées à une société établie aux Etats-Unis, l'entreprise européenne qui transfère les données doit également informer les personnes concernées de l'identité des destinataires de leurs données et du fait que les données bénéficient de la protection accordée par le Bouclier de Protection des Données.»

2. Les spécificités du contrat s'agissant des transferts vers une société établie aux Etats-Unis agissant en qualité de sous-traitant

« Lorsqu'une société établie en Europe agissant en qualité de responsable de traitement transfère des données à un sous-traitant établi aux États-Unis, agissant pour son compte, à des fins d'opérations de sous-traitance uniquement (stockage, maintenance informatique, helpdesk, etc.), conformément à l'article 17 de la Directive 95/46/CE, les deux sociétés sont tenues de conclure un contrat de sous-traitance de données, indépendamment du fait que le sous-traitant ait adhéré ou non au Bouclier de Protection des Données.

Il convient de noter qu'en vertu de la Directive européenne sur la protection des données à caractère personnel, la législation nationale en matière de protection des données à caractère personnel peut imposer des obligations additionnelles, comme par exemple exiger que les sociétés européennes incluent des dispositions supplémentaires dans leurs contrats de sous-traitance des données.

[323] *https://www.privacyshield.gov/welcome*

Il est par exemple recommandé que la société européenne indique si elle accepte que le sous-traitant américain sous-traite à son tour le traitement des données à caractère personnel auprès d'un sous-traitant tiers ainsi que les conditions applicables (en termes de transparence et de responsabilité). En outre, il pourrait également être utile pour les sociétés européennes d'obtenir une assurance sur la notification des failles de sécurité ainsi que sur les engagements relatifs à la suppression des données une fois le contrat de prestation de service est résilié. »[324]

3.4.4 La responsabilité sociétale des sous-traitants fournissant des prestations de services numériques

Un exemple de sous-traitance des données par un responsable de traitement est le recours à un éditeur de solutions informatiques intégrées, telles les Progiciels de Gestion intégrée. Le contrat d'intégration de ce logiciel dans le système informatique du client devra respecter toutes les obligations précédemment citées.

L'éditeur de solutions numériques peut toutefois aller plus loin que le seul respect de la réglementation dans le traitement des données : il convient dès lors de s'intéresser à la démarche de responsabilité sociétale de l'entreprise d'un éditeur de PGI.

Par ailleurs, c'est un système qui facilite la piste d'audit RSE des données, en fournissant une base de données uniques aux métadonnées standardisées.

Toutefois, la démarche RSE de l'éditeur de services numériques a aussi son importance, puisqu'elle fournit des garanties de meilleures pratiques au responsable de traitement faisant appel à un sous-traitant.

Par exemple, l'entreprise SAP (Systems, Applications and Products for data processing) a une politique RSE de protection des données qui montre quelques bonne pratiques [325] :

- Protéger les droits fondamentaux de toutes les personnes dont les données sont traitées par SAP, qu'il s'agisse de nos clients, prospects, employés ou partenaires.
- Respecter toutes les exigences légales applicables en matière de protection des données.
- Le cycle de développement de logiciels sécurisés est conforme à la norme ISO/IEC 27034 pour la sécurité des applications et est étroitement lié à notre cadre de processus certifié ISO 9001 pour le développement de logiciels standard.
- La stratégie d'opérations sécurisées se concentre sur les principes de sécurité de "confidentialité, intégrité et disponibilité" pour soutenir la protection globale de notre entreprise, ainsi que celle de nos clients.
- La plupart des solutions de cloud computing sont soumises aux audits de contrôle des organisations de services (SOC) ISAE3402, SSAE16 SOC I Type II, et

[324] https://www.cnil.fr/fr/le-privacy-shield
[325] https://www.sap.com/corporate/en/company/sustainability-csr.html

SSAE16 SOC II Type II. Les normes SOC sont harmonisées avec un certain nombre de certifications ISO, notamment ISO 9001, 27001 et 22301.

- SAP s'engage à assurer la conformité avec la loi européenne harmonisée sur la protection des données, le Règlement général sur la protection des données (RGPD). Nous avons mis en place un large éventail de mesures pour protéger les données contrôlées par SAP et ses clients contre tout accès et traitement non autorisé, ainsi que contre toute perte ou destruction accidentelle. Ces mesures comprennent, entre autres, la mise en œuvre de notre système de gestion de la protection des données (DPMS) dans des domaines essentiels à la protection des données. Ce système est certifié chaque année par le British Standards Institute.

III. LE NUMÉRIQUE À L'AUNE DES OUTILS DE LA RSE

Numérique et RSE, quand ils coïncident, peuvent enrichir les entreprises. Néanmoins, comme l'étude des pratiques des entreprises l'a montré, ces deux domaines sont rarement reliés au sein des entreprises. La stratégie de la RSE est donc rarement liée aux stratégies de protection des données de l'entreprise.

La Responsabilité numérique des entreprises engage la protection des données détenues par les acteurs économiques dans une perspective de respect des libertés, de la vie privée ou du bien-être des salariés, des consommateurs et des parties-prenantes tout en gardant l'individu au cœur de ces transformations.

Dans un contexte d'évolution numérique constant, la protection des données s'inscrit comme un critère fondamental d'une démarche responsable des entreprises. Les perspectives offertes par la RSE doivent constituer les vecteurs d'une responsabilisation accrue des entreprises dans leurs processus numériques.

1. Certifications, normes et labels d'application volontaire

1.1 Les certifications

La certification désigne une procédure selon laquelle un organisme d'évaluation externe (ou « tiers certificateur ») va assurer par écrit qu'une personne, un produit, un processus ou un service est en conformité avec les exigences données dans un référentiel[326]. Prévue aux articles 42 et 43 du RGPD, la certification est établie par un organisme tiers qui doit justifier de son indépendance et de son impartialité.

A ce titre l'activité de labellisation de la CNIL se transforme en certification.

[326] « La certification », CNIL

Ainsi, deux types de procédures peuvent être engagées[327] :

- L'obtention d'un agrément auprès de la CNIL après avoir démontré son indépendance et son expertise sur la base d'un référentiel ;
- L'obtention d'une accréditation, auprès du Comité Français d'Accréditation (COFRAC). L'impartialité et la compétence du tiers sont évaluées sur la base d'un référentiel d'accréditation (exigences de la norme ISO 17065 et de la CNIL).

Au regard du RGPD et de la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, deux catégories de référentiels sont prévues :

- Le référentiel d'agrément ou d'accréditation : utilisé par la CNIL et le COFRAC pour évaluer les organismes certificateurs ;
- Le référentiel de certification : utilisé par les quatre organismes certificateurs agrées par la CNIL – Afnor Certification, LCP, SGS, Bureau Veritas et Apave[328] – pour évaluer des produits, des procédés, des services ou des personnes.

Dans une perspective RSE, l'entreprise ou l'organisme qui a obtenu la certification d'un de ses produits ou de ses services peut l'utiliser afin de démontrer que ses opérations respectent le règlement.

Par ailleurs, pour permettre l'identification des compétences et savoir-faire du délégué à la protection des données (DPO). Sur une base volontaire, les personnes physiques peuvent justifier qu'elles répondent aux exigences de compétences et de savoir-faire propres aux DPO établies dans le RGPD. La certification des DPO par la CNIL constitue ainsi un vecteur de confiance pour l'organisme faisant éventuellement appel à ces personnes certifiées mais également pour les clients, les fournisseurs ou les salariés de l'entreprise.

Les critères[329] ont été inscrits dans la Délibération n° 2018-318 du 20 septembre 2018 portant adoption des critères du référentiel de certification des compétences du délégué à la protection des données (DPO)[330].

1.2 Les normes d'application volontaire

Une norme volontaire est un cadre de référence choisi par un acteur économique afin de fournir des lignes directrices, des prescriptions techniques et qualitatives relatives à des produits, des services ou des pratiques et ce, au service de l'intérêt général. Définie par Afnor Normalisation comme une « co-production consensuelle entre les professionnels et les utilisateurs qui se sont engagés dans son élaboration », la norme d'application volontaire entraine, de fait, une responsabilisation accrue des entreprises.

[327] Idem
[328] « Liste des organismes agréés par la CNIL », CNIL
[329] Les informations sont à retrouver ici : https://www.cnil.fr/fr/certification-des-competences-du-dpo-la-cnil-adopte-deux-referentiels
[330] Délibération à retrouver ici : https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000037485691&dateTexte=&categorieLien=id

Dans le secteur numérique, la mise en place de normes d'application volontaire au sein des entreprises constitue un gage de confiance. En obtenant le consensus entre les acteurs économiques, les consommateurs, les professionnels et les utilisateurs, une norme permet de clarifier et d'harmoniser les pratiques de gestion et de protection des données détenues par l'entreprise et d'élever le niveau de qualité et de sécurité.

A ce titre, la norme ISO 27001[331] définit les exigences pour la mise en place d'un système de management de la sécurité de l'information (SMSI). L'objectif est de protéger les fonctions et informations de toute perte, vol ou altération, et les systèmes informatiques de toute intrusion et sinistre informatique.

Elle définit une méthodologie pour identifier les cybermenaces, maîtriser les risques associés aux informations cruciales de l'organisation, mettre en place les mesures de protection appropriées afin d'assurer la confidentialité, la disponibilité et l'intégrité de l'information.

ATOS, Orange, certaines entités d'ENGIE et de Publicis sont ainsi certifiées. Legrand base aussi sa politique de management de la sécurité des systèmes d'information sur cette norme.

1.3 Les labels volontaires

La notion de label volontaire définit les dispositifs d'évaluation permettant la reconnaissance des pratiques et des politiques mises en œuvre par une entreprise.

Florissant dans le domaine de la RSE, les labels constituent un critère intéressant pour évaluer les stratégies des entreprises. Les labels relatifs aux enjeux numériques demeurent peu développés ; leur développement nécessitant des exigences techniques, sociales et économiques importantes.

Le Label Numérique Responsable

Le label Numérique Responsable est porté par plusieurs partenaires : WWF, ministère de la transition écologique et solidaire, ADEME, INR, GreenIt.fr, SGS, FING, LUCIE, France Digitale, France IT, IDDRI.

Partant du postulat que « *le numérique responsable est une démarche d'amélioration continue qui vise à réduire l'empreinte écologique, économique et sociale des technologies de l'information et de la communication* »[332], le label Numérique Responsable entend répondre à trois objectifs : accélérer la prise de conscience et le passage à l'acte d'un maximum d'organisations publiques et privées ; proposer une méthode opérationnelle accessible à toutes les organisations pour réduire l'impact du numérique ; reconnaitre et valoriser l'engagement des organisations pionnières dans ce domaine.

[331] https://www.iso.org/fr/isoiec-27001-information-security.html
[332] https://label-nr.fr/

Pour cela, il s'appuie sur cinq axes : stratégie et gouvernance ; formation ; démarches transversales ; usagers / utilisateurs ; organisation.

Le label a été conçu pour que tous les types d'organisations puissent s'en emparer : entreprises, associations, administrations, collectivités, peu importe leur taille ou leur secteur d'activités. Il a été co-construit par l'Institut du Numérique Responsable en partenariat avec le ministère de la Transition écologique et solidaire, l'ADEME et WWF.

La labellisation se déroule en 6 étapes :

- un engagement public de l'organisation candidate via la signature de la charte numérique responsable. Elle rejoint alors la Communauté LUCIE ;
- durant trois jours, l'organisation suit une formation avec un expert du Green IT ;
- à l'aide des outils fournis lors de la formation, l'organisation évalue son niveau sur la thématique du numérique responsable et se met en conformité avec les exigences du label ;
- la démarche numérique responsable de l'organisation est ensuite évaluée par SGS ou par Bureau Veritas. En s'appuyant sur le rapport d'évaluation, l'organisation prend des engagements pour réduire l'impact du numérique. Ces engagements devront être mis en œuvre durant le cycle de labellisation qui dure trois ans ;
- un comité de labellisation piloté par l'Institut du Numérique Responsable, composé d'acteurs privés, publics, institutionnels et associatifs, délivre ou non le label après avoir étudié l'évaluation et les engagements de l'organisation ;
- une fois le label attribué, SGS ou Bureau Veritas renouvèle l'évaluation au bout de 18 mois afin de faire un point sur la mise en œuvre des engagements en matière de Green IT.

Plusieurs organisations sont labellisées Numérique Responsable, telles que la cité scolaire de Surgères, les services GTS de la Société Générale, la DSI de Pôle Emploi, le service communication de La Rochelle ou encore l'Université de La Rochelle.

Le Label ADEL (Algorithm Data Ethics Label)

ADEL est une SAS fondée en 2017. Première plateforme d'évaluation éthique française à vocation mondiale et indépendante, elle est dirigée par Jérôme Béranger (fondateur et CSO) et Frédéric Kleindienst (CEO) et intègre un comité d'experts indépendants (à l'image de ses présidents d'honneur Cédric Villani et Gilles Babinet)[333].

Ce label se fonde sur un « audit automatisé (à la fois scientifique et transversal) qui évalue la valeur éthique d'un système numérique fondée sur cinq familles d'éthique et trente-cinq critères robustes » ; l'audit est réalisé sur les systèmes numériques, les bases de données, les plateformes informatiques ou encore les projets IA et la Blockchain. Le label permet ainsi d'obtenir un compte-rendu comprenant une cartographie détaillée de l'état de situation du demandeur pour le traitement des données numériques, un score final éthique, et des préconisations de bonnes pratiques.

[333] http://www.adel-label.com/en-savoir-plus/

Les objectifs de cette labellisation sont les suivants[334] :

- développer un cadre éthique aux systèmes d'information pour garantir sens, confiance, transparence et sécurité auprès de la société ;
- accompagner les évolutions des systèmes d'information et des traitements qui leur sont associés au plan éthique ;
- mettre à disposition des entreprises, des outils d'évaluation éthiques ;
- passe d'une exigence éthique universelle à une éthique pratique et concrète ;
- apporter des recommandations et des préconisations éthiques ;
- accompagner et anticiper la transformation numérique des sociétés grâce à une plateforme d'évaluation guidée par le concept d'*ethic by design*[335].

2. RSE et nouveaux modèles d'entreprise

La responsabilité numérique s'invite dans le *reporting* RSE

Bien qu'il n'existât dans le passé aucune d'obligation juridique, désormais, on observe que la gestion des données et de la vie privée est de plus en plus prise en compte dans le *reporting* RSE. Les mesures de RSE intègrent de plus en plus les notions du numérique.[336]

Pour valoriser le respect des règles de collecte et d'exploitation des données dans leur politique RSE, les organisations doivent rendre compte de cette collecte dans le rapport d'activité RSE. Elles peuvent aussi afficher une politique sur leur site internet. Par exemple, les banques et les assurances ont utilisé très tôt leur démarche RGPD comme un argument commercial auprès de leurs clients et prospects.

Le RGPD introduit la notion de responsabilité de l'organisation à démontrer sa conformité. Ainsi il est souhaitable qu'un corpus documentaire soit constitué de façon à démontrer sa conformité lors d'une sollicitation de la CNIL à distance ou sur site. Ce corpus documentaire, outil de *reporting* RSE et données à part entière, doit être partagé en interne et en externe

Certaines entreprises ont une dimension critique (qualité de l'air, détails des votes au conseil municipal, études d'impact, décisions de justice, qualité des services publics, données d'études cliniques présidant à l'autorisation sur le marché des produits de santé, etc.) : Les entreprises ont un rôle à jouer dans la transparence des données dont elles disposent. Certaines bases ont été posées par la Loi pour une République Numérique (Loi n°2016-1321 du 7 octobre 2016, article 17) en 2016, puisqu'elle impose l'ouverture des données des entreprises exerçant une délégation de service publique, et donc de données d'intérêt général.

Les bénéfices de la transparence sont multiples. Outre la mise en valeur de données pour l'intérêt général, cela permettrait de renforcer la confiance des clients, usagers ou

[334] Idem
[335] C'est-à-dire, dès la conception du produit
[336] Audition de Cécile Wendling

patients, de favoriser leur contribution en termes de facilitations et d'élargissement des données collectées et aurait une incidence positive sur l'efficacité de l'action publique. [337]

Analyse du *reporting* du CAC 40 vis-à-vis des données

La quasi-totalité des entreprises du CAC 40 mentionnent le RGPD dans leur rapport intégré. Les rapports intégrés des entreprises du CAC 40 s'entendent le plus souvent à identifier le numérique comme un risque. Le RGPD est abordé comme un enjeu de contrainte réglementaire, exigeant une mise en conformité. Certaines entreprises ont recours à des panels ou des comités d'experts sur la protection des données.

Lorsqu'elles ont recours à la grille de matérialité, les entreprises du CAC 40 placent systématiquement l'enjeu de « Protection des données » à un haut niveau d'importance à la fois sur l'axe de l'impact sur les Parties-prenantes et sur celui de l'impact sur l'activité.

Le dispositif d'alarme en cas de faille est un dispositif fréquemment cité, car imposé par le RGPD. (*data breach management*)

La protection de la vie privée est souvent présentée comme un programme global, intégrant plusieurs volets de RGPD ainsi qu'une réponse aux risques identifiés par chaque entreprise : les entreprises notifient souvent de la réorganisation des processus à laquelle ils ont procédé.

Le RGPD influence et détermine les initiatives des entreprises. Toutes les entreprises ne détaillent pas tous les processus mis en place, la référence aux différents volets du RGPD n'est que parcellaire.

Les déficits du *reporting* sur l'utilisation des données par les entreprises

Au vu de l'importance des enjeux liés à la création de valeur par l'exploitation des données présentés dans cet avis, il est regrettable que seul un faible nombre de rapports ne s'attardent sur ce sujet. Les seules à le faire sont les entreprises du numérique (Airbus Defense & Space, Safran, Atos, Orange)

Aucun rapport ne s'attarde non plus sur le recours aux solutions de Cloud Computing publics ou privés, ni sur les mesures prises vis-à-vis des *data center*. Aucune mention non plus dans les DPEF du CAC 40 de l'enjeu de souveraineté des données.

3. Outils d'autodiagnostic

Les entreprises gagnent à établir leur propre diagnostic numérique. L'autodiagnostic permet d'évoluer dans des perspectives de responsabilisation accrue face à l'utilisation des technologies numériques.

Concrètement, l'autodiagnostic permet aux entreprises d'analyser leurs avancées et leurs pratiques en matière numérique.

[337] Audition de Rémi Dusaud

Ainsi, doivent être analysés la présence sur les réseaux, le site internet, la commercialisation, les services numériques dédiés aux parties-prenantes, aux salariés et aux clients ou encore la stratégie marketing.

A ce titre, l'agence gouvernementale pour la transformation numérique des TPE et PME, France Num[338], fédère des ressources pratiques, des aides financières et un réseau de conseillers afin d'apporter des solutions aux entreprises pour leur transformation numérique : recommandations en ligne, recherche des financements disponibles, appui d'outils adaptés.

Pour les entreprises les plus avancées sur les processus numériques, des outils d'aide à la décision peuvent être mobilisés :

Le DEDA (Data Ethics Decision Aid)

Le DEDA[339] est une « boîte à outils » qui aide à cartographier les enjeux éthiques dans les projets embarquant des traitements de données.

Cet outil a été développé, en collaboration avec des « praticiens » de la donnée, par la Utrecht Data School et l'Université d'Utrecht et permet aux entreprises d'analyser les enjeux grandissant auxquels elles sont confrontées.

« TransAlgo », la plateforme scientifique pour le développement de la transparence et de la responsabilité des algorithmes et des données

Transalgo est un projet porté par l'INRIA[340] afin de développer des méthodes permettant de vérifier si une décision rendue par des algorithmes est éthique.

Le projet vise trois objectifs :

- Encourager la conception d'algorithmes de traitement de données « responsables et transparents par construction » (*responsible-by-design*) ;
- Aider à la vérification et au test de ces algorithmes afin d'analyser s'ils se comportent de manière légal et loyal ;
- Aider à la diffusion des savoir-faire et bonnes pratiques auprès des services de l'Etat, des industriels et des citoyens.

338 https://www.francenum.gouv.fr/france-num
339 http://www.dataschool.nl/deda/deda-workshop/?lang=en Source : Cigref, Syntec numérique.
340 https://www.economie.gouv.fr/files/files/PDF/Inria_Plateforme_TransAlgo2016-12vf.pdf

4. Chartes, réseaux d'entreprises engagées

4.1 Les chartes internes et externes

Les chartes sont des déclarations d'intention afin d'emmener le personnel à tenir des engagements et des obligations de l'entreprise en matière d'utilisation des systèmes d'information. Une charte permet ainsi de réglementer l'usage des systèmes d'information par le personnel interne de l'entreprise ; c'est l'affichage d'une culture d'entreprise.

La CNIL conseille, en ce sens, de sensibiliser les utilisateurs qui travaillent avec des données personnelles aux risques liés aux libertés et à la vie privée. Pour cela, la rédaction d'une charte informatique est fortement préconisée et doit comporter des éléments fondamentaux tels[341] :

- le rappel des règles de protection des données et les sanctions encourues en cas de non-respect ;
- le champ d'application de la charte incluant les modalités d'intervention des équipes chargées de la gestion des ressources informatiques, des moyens d'authentification ainsi que les règles de sécurité auxquelles les utilisateurs doivent se conformer ;
- les modalités des moyens informatiques et de télécommunications tels que le poste de travail, les équipements nomades de type Réseau Privé Virtuel (VPN), les réseaux locaux ou encore la messagerie électronique ;
- les conditions d'administration des systèmes d'information ;
- les responsabilités et les sanctions encourues en cas de non-respect de la charte.

L'analyse des rapports intégrés des entreprises du CAC40 met en lumière la mention par cinq entreprises d'une charte liée à l'utilisation des outils numériques : le Crédit Agricole, Orange, Valeo, Vinci et Vivendi. Lorsque les entreprises ne mettent pas de charte en place, il est récurrent de retrouver des référentiels d'évaluation interne à l'image d'Engie, de LVMH ou encore de BNP Paribas.

Une charte s'avère ainsi un bon moyen pour les entreprises de rappeler ses principaux engagements et de les promouvoir aussi bien en interne qu'en externe.

Les règles d'entreprise contraignantes (*Binding Corporate Rules*) évoquées dans la partie II.5.1.1, constituent également une forme de charte interne.

[341] « Sécurité : sensibiliser les utilisateurs », CNIL

4.1.1 Les chartes externes

Charte Ethique et big data

La Charte éthique et *big data* a été conçue à plusieurs voix, à l'initiative de l'Aproged, de l'Atala, de l'AFCP et de Cap Digital.[342] Cette charte met à disposition une description des données et permet de stocker les points essentiels à décrire lorsque l'on met des données à disposition ; le fournisseur des données les met ainsi à disposition et s'engage sur leur contenu.

Elle se structure autour de trois grands principes, que les adhérents s'engagent à respecter :

- le principe de traçabilité qui induit la fourniture des informations nécessaires et suffisantes pour que les données soient utilisées en tout confiance. Doivent être indiqués la description des données, leurs processus de fabrication, de transformation, de vérification et de diffusions ainsi que les personnes intervenues dans ces processus ou la propriété intellectuelle ;
- le principe de respect des droits de propriété intellectuelle qui implique la vérification que les droits de propriété intellectuelle liés à la fourniture ou à la transformation des données soient respectées et la précision de la nature de propriété intellectuelle sur les données fournies ou utilisées ;
- le principe de respect des cadres légaux génériques et particuliers visant à l'identification et au respect des règlements spécifiques à la nature des données traitées ou utilisées.

La Charte identifie plusieurs origines des données - primaires donc créées par le fournisseur, consolidées par différents fournisseurs et construites à partir de données tierces – et plusieurs natures de données – personnelles, personnelles sensibles et collectées dans un pays tiers à l'UE.

Pour les données consolidées et construites, la Charte[343] recommande de fournir les coordonnées de l'organisation dont elles sont issues ainsi que le contact permettant d'obtenir les informations afférentes.

La Charte recommande également de définir les auteurs et les processus de recrutement dans le cas de données primaires provenant de contributeurs humains. Dans le cas d'utilisation de *crowdsourcing*, les processus de sélection sont à mentionner (critères, plateformes utilisées, rémunération).

Si les données contiennent des informations liées au contributeur humain, doit être indiqué si un consentement a été demandé, la nature et la forme de l'information fournie pour obtenir le consentement. Également, les étapes de fabrication et de transformation des données doivent être mentionnées (transformation, enrichissement, travail manuel).

[342] http://wiki.ethique-big-data.org/chartes/CharteEthiqueBigDataLightTCOFPOS
[343] http://wiki.ethique-big-data.org/chartes/CharteEthiqueBigDatav2d.pdf

Dans le cas où les données sont personnelles, il est conseillé d'indiquer si le processus de transformation est compatible avec les modalités du consentement de la personne et si une anonymisation a été faite.

Charte numérique responsable

Faisant suite à la création du Label numérique responsable (cf. *supra*), une charte afférente a été mise en place. Des dizaines d'organisations en sont signataires telles que GreenIt.fr, La Poste, la SNCF, Enedis ou Decathlon.

Destinée aussi bien aux entreprises de toute taille, aux associations ou aux acteurs publics, la charte incite l'organisation à s'évaluer et à s'améliorer. Elle est développée autour de cinq points principaux :

- l'optimisation des outils numériques pour limiter leurs impacts sur l'environnement et leurs consommations ;
- le développement d'offres de services accessibles à toutes et tous, inclusives et durables ;
- le développement de pratiques numériques éthiques et responsables ;
- la promotion d'un numérique mesurable, transparent et lisible ;
- la mise en place de nouveaux comportements et valeurs.

4.1.2 Les chartes internes

Charte pour un monde numérique humain et éthique - Maif

Lancée par la Maif en 2017, cette charte entend donner de la cohérence aux initiatives numériques du groupe (Fonds d'investissement, portail Maif Social Club, assurance automobile communautaire, etc.). Considérant les risques induits par la révolution numériques en termes de libertés individuelles mais aussi de coûts sociaux, le groupe désire s'engager sur la « transparence complète en matière d'utilisation des données »[344].

Cette charte s'articule autour de trois principes décliner en onze points :

- Protéger les données personnelles en :
  - s'engageant à ne pas les vendre ;
  - étant transparent sur leur provenance, leur contenu et les usages qui en sont fait ;
  - sécurisant leur localisation dans des centres en France et au sein de l'Union européenne ;
  - promouvant le droit à l'oubli.
- Développer le partage des savoirs et des connaissances en :
  - formant les individus à la compréhension des enjeux numériques ;
  - intégrant des équipes pluridisciplinaires dans les démarches d'innovation ;

[344] « La Maif se dote d'une charte pour "un numérique humain et éthique », L'Usine Digitale, mai 2017

    - soutenant le recours aux technologies en source ouverte afin de permettre la diffusion et le partage des connaissances ;
    - aidant la recherche scientifique quand elle permet de détecter, comprendre et prévenir les risques numériques.
- Placer les technologies numériques au service de l'humain en :
    - utilisant les technologies au service de l'humain afin d'enrichir la qualité des relations avec les parties-prenantes et les salariés ;
    - garantissant que les technologies et les algorithmes sont placés sous le contrôle humain ;
    - promouvant une politique de la donnée visant à fournir aux individus le contrôle effectif et la maîtrise de l'usage des données qui les concernent.

Charte internationale pour une IA inclusive

En engageant les entreprises qui le souhaitent dans la lutte contre les stéréotypes, les discriminations et les biais dans l'IA, cette charte – lancée à l'initiative d'Orange et d'Arborus – est la première en son genre. Elle vise la promotion de la diversité ainsi que l'usage et le développement responsable des processus d'IA.

En signant cette charte, les entreprises s'engagent à favoriser la mixité et la diversité au sein des équipes, notamment les équipes spécialisées en IA, et à ce que leurs parties prenantes agissent de manière responsable.

La charte internationale pour une IA inclusive s'appuie donc sur sept engagements[345] :

- la promotion de la mixité et de la diversité dans les équipes qui travaillent sur des solutions IA ;
- l'évaluation des formes de discriminations qui pourraient résulter de données stéréotypées ;
- la garantie de systèmes plus équitables grâce à des données de qualité – unifiées, cohérentes, vérifiées, traçables et exploitables ;
- la formation aux stéréotypes et biais de tous les concepteurs, les développeurs et les acteurs impliqués dans la fabrique de l'IA ;
- la sensibilisation des prescripteurs de solutions à base d'IA aux risques de stéréotypes et biais et l'intégration des points de contrôle et d'évaluation itérative dans les cahiers des charges ;
- l'assurance que toute la chaîne de valeur de l'IA est non discriminatoire par un choix des fournisseurs réfléchi et leur évaluation de manière itérative ;
- le contrôle des solutions à base d'IA et l'adaptation des processus en continu.

Dans la continuité de cette charte, Orange et Arborus travaillent à la conception d'un label *Gender Equality European & International Standard on Artificial Intelligence* afin de mesurer les impacts des processus d'intelligence artificielle sur l'égalité entre les femmes et les hommes dans les entreprises[346].

[345] « Première charte internationale pour une IA inclusive : Orange s'engage », Orange, avril 2020
[346] Idem

4.2 Les réseaux d'entreprises

Comme le démontre l'Assemblée des chambres françaises de commerce et d'industrie[347], le recours à des réseaux d'entreprises pour traiter de sujets de manière collective permet de libérer « des ressources et de l'énergie sur le cœur de leur valeur ajoutée individuelle ». Véritable outil de mise en commun, les réseaux d'entreprises constituent une valeur non négligeable pour les entreprises.

L'association France Digitale

L'association France Digitale a été créée en 2012, elle compte 1400 membres, entrepreneurs et investisseurs du numérique et promeut l'économie numérique auprès des institutions publiques françaises, des grands acteurs économiques, des médias et de la Commission européenne.

Le Club Green IT

Le Club Green IT[348], aujourd'hui regroupé autour de l'Institution du Numérique Responsable, avait pour objectif d'aider les entreprises à renforcer ou amorcer leur réflexion sur le sujet du numérique responsable au travers de problématiques liées à l'identification des enjeux de transformation numérique et écologique, à l'analyse de l'empreinte environnementale de leurs systèmes d'information, à l'évaluation de la maturité des entreprises et au partage de bonnes pratiques numériques. Les entreprises faisant partie du Club ont désormais rejoint l'Institut du Numérique Responsable.

Les Designers Ethiques

Le collectif Designers Éthiques[349], fondé en 2016, regroupe professionnels du design, consultants, ingénieurs et chercheurs engagés dans une démarche de conception de services numériques respectueuse des utilisateurs.

Le collectif s'est formé autour de l'organisation des conférences « Ethics By Design » et travaille aujourd'hui autour de nombreux sujets – design de l'attention, éthique appliquée à l'UX design, design libre, conception éco-responsable, legal design – avec pour objectif principal de mettre la pratique professionnelle au centre de sa réflexion.

Le collectif analyse ainsi l'impact du design de service numérique sur ses utilisateurs et son environnement, et milite pour une pratique professionnelle responsable qui soit transparente et respectueuse.

[347] « Les réseaux d'entreprise : une valeur ajoutée pour les entreprises, une nécessité pour les territoires, une priorité pour les CCI », Assemblée des chambres françaises de commerce et d'industrie, novembre 2010
[348] https://www.wwf.fr/projets/numerique-responsable
[349] http://www.designersethiques.org/ Source : Cigref et Syntec numérique.

Le Serment Holberton-Turing

Le serment Holberton-Turing[350], initié par des scientifiques franco-américains, souhaite fédérer les professionnels de l'IA, au niveau mondial, autour de valeurs morales et éthiques communes, afin de les inviter à utiliser leurs compétences dans le respect de l'humain en évitant toute menace à la vie.

Le Serment d'Hippocrate pour data scientist*, Data For Good*

Proposé par une équipe de bénévoles rassemblés dans le cadre de l'association Data for Good, le serment d'Hippocrate pour *data scientist*[351] a impliqué plus d'une centaine de *data scientists* et d'experts qui collectent, stockent, traitent, modélisent, analysent des données et font de la prédiction dans le cadre de leur activité professionnelle. Ces *data scientists* travaillent dans des start-ups, des grandes entreprises, des cabinets de conseil, des PME, des administrations, ou sont indépendants ou chercheurs. La charte s'articule à la fois autour de principes éthiques fondamentaux et de bonnes pratiques d'utilisation des données.

Prévu comme un guide pratique accompagnant les praticiens des données dans les étapes de leur travail, le serment énonce une série de principes sur lesquels les signataires s'engagent.

Déclaration de Montréal pour un développement responsable de l'intelligence artificielle[352]

Initiative lancée en 2017 par l'Université de Montréal, la Déclaration de Montréal formule des principes et des recommandations afin de donner des orientations éthiques autour du développement de l'IA.

Sept valeurs structurent ces orientations éthiques : bien-être, autonomie, justice, vie privée, connaissance, démocratie et responsabilité.

Optic Technology

Optic Technology est un réseau de recherche et d'action, crée en 2012 à l'initiative de l'Ordre des Dominicains, qui place l'humain au cœur du développement des technologies. Regroupant chercheurs, philosophes et entrepreneurs, le réseau considèrent que les nouvelles technologies peuvent constituer des leviers pour « bâtir une société plus respectueuse de chacun », et appelle à l'appréhension des dimensions éthiques de ces outils.

Ainsi, les outils de la RSE servent à l'amélioration des pratiques numériques des entreprises. En alliant deux secteurs qui se croisent rarement, les entreprises génèrent de la valeur ajoutée à leurs activités : renforcement de l'image, transparence des relations avec les fournisseurs, mise en commun de connaissances, respect des règlementation, pertinence des algorithmes, etc. Véritables prérequis à la santé de long

[350] http://www.holbertonturingoath.org/ Source : Cigref et Syntec numérique.
[351] https://dataforgood.fr/projects/4_serment-hippocrate.html
[352] http://www.declarationmontreal-iaresponsable.com/ Source : Cigref et Syntec numérique.

terme des entreprises, numérique et RSE gagnent à être inclus de concert dans la stratégie globale des entreprises.

Impact AI

IMPACT AI est un think et do tank français qui étudie l'éthique de l'Intelligence artificielle. Il s'intéresse notamment à la neutralité des algorithmes, l'éthique dans la conception et le développement de l'IA, l'inclusion et la diversité, à la sensibilisation et à l'éducation au numérique.

IMPACT AI travaille avec l'écosystème numérique, les entreprises, les startups, les institutions, les organismes de recherche ou de formation et les acteurs de la société civile pour créer une approche de l'IA collective qui répond aux besoins et aux attentes des citoyens. Sa mission est de développer un cadre éthique des usages de l'intelligence artificielle répondant à des critères simples, lisibles et réplicables par le plus grand nombre.[353]

La liste de ses membres fondateurs compte notamment les entreprises Bouygues, AXA, Orange, le groupe Hervé, Schneider Electric, SNCF, Adecco, Capgemini, Accenture, Talan, Umanis, BCG, ainsi que des écoles. Par ailleurs, elle compte parmi ses membres adhérents Thalès, Maif, La Poste, PwC, Simplon, RATP, Deloitte, CGI, Enedis, Faurecia.

Il apporte un soutien technologique et financier à des projets innovants destinés à répondre aux grands enjeux sociétaux et à l'intérêt général.

Il promeut le développement et le partage d'outils favorisant et vérifiant l'usage responsable de l'IA. Notamment, le think tank met à disposition une boite à outil IA Responsable, composé d'outils techniques et de gouvernance, de formations, et de publications.[354]

Enfin, il publie un rapport annuel sur l'impact de l'IA en France en s'appuyant sur les retours d'expérience de ses membres ainsi qu'un baromètre sur la perception des Français face à l'IA.

Partnership on AI

Il s'agit d'une coalition à but non lucratif d'acteurs engagés dans l'utilisation responsable de l'intelligence artificielle. Elle effectue des recherches sur les meilleures pratiques en matière de systèmes d'intelligence artificielle et sensibilise le public à l'IA. Lancée le 28 septembre 2016, ses membres fondateurs sont Amazon, Facebook, Google, DeepMind, Microsoft, IBM et Apple. En 2019, elle comptait plus de 100 partenaires du monde universitaire, de la société civile, de l'industrie et des organisations à but non lucratif[355].

La coalition publie régulièrement des prises de position et des notes de recherche, par exemple sur le racisme systémique, et compte trois groupes de travail : « Safety-critical AI », « Fair, Transparent and Accountable AI » et « AI, Labor, and the Economy ».

[353] http://impact-ai.fr/qui-sommes-nous/
[354] http://impact-ai.fr/ia-responsable/
[355] https://www.partnershiponai.org/partners/

L'accord-cadre des partenaires sociaux européens sur la numérisation[356]

En vertu des articles 154 et 155 du Traité sur le Fonctionnement de l'Union européenne (TFUE), les accords-cadres réunissent les partenaires sociaux européens autour de décisions communes. Deux procédures existent aujourd'hui. Soit, les partenaires sociaux proposent à l'adoption du Conseil des Ministres une décision qui s'intègrent dans le droit communautaire ; soit les partenaires sociaux proposent des initiatives volontaires dont la mise en œuvre au niveau national, sectoriel et de l'entreprise est à la charge des partenaires sociaux eux-mêmes.

Les partenaires sociaux ont signé un accord-cadre sur la numérisation le 22 juin 2020. Considérant que la transformation numérique de l'économie comporte de multiples facettes et implique des modifications du marché du travail, du monde du travail et de la société, ce projet entend engager les partenaires sociaux européens intersectoriel autour de pratiques optimisant les avantager et les défis de la numérisation du monde du travail.

L'accord-cadre vise ainsi à :

- Sensibiliser et améliorer la compréhension des employeurs, travailleurs et représentants sur les opportunités et défis induits par les transformations numériques ;
- Encourager et guider les employeurs, travailleurs et représentants à concevoir des actions visant à tirer parti des possibilités numériques tout en prenant en considération les initiatives, les pratiques et les conventions collectives existantes ;
- Encourager une approche de partenariat entre les employeurs, travailleurs et représentants sur le numérique ;
- Soutenir le développement d'une approche humaine de l'intégration de la technologie numérique dans le monde du travail afin de soutenir les travailleurs et d'améliorer la productivité.

L'accord définit un processus circulaire dynamique commun tenant compte des rôles et responsabilités de chacun et chacune des acteurs économiques ; de manière adaptée aux situations nationales, sectorielles, d'entreprise, de systèmes de relations industrielles, d'emplois et d'outils numériques utilisés. Par ailleurs, l'accord cadre promouvra les approches, actions et mesures que les employeurs, travailleurs et représentants peuvent utiliser afin d'aborder des sujets relatifs aux compétences, l'organisation ou des conditions de travail.

[356] Draft european social partners framework agreement on digitalisation, à retrouver ici : http://pramprof.lt/images/dokumentai/draft_agreement-digitalization.pdf

5. Un enjeu essentiel : la Responsabilité numérique des entreprises

Les analyses menées dans cet avis mettent en évidence la nécessité de porter une définition claire et précise de ce que signifie, pour une entreprise, d'être numérique responsable.

La notion de Responsabilité numérique des entreprises (RNE) s'avère peu développée dans les organisations françaises. Inspiré du terme anglo-saxon de *corporate digital responsibility*[357], elle définit la prise en considération des impacts de l'usage du numérique sur l'environnement, les travailleurs et le modèle économique.

Selon Lobschat *et alii*. (2019)[358], la Responsabilité numérique des entreprises doit guider les entreprises dans le respect de quatre procédures fondamentales en matière numérique : la création de nouvelles technologies et la collecte des données, les processus de décisions, les analyses d'impact et les perfectionnements technologiques. La Responsabilité numérique des entreprises peut ainsi être définie comme une éthique d'entreprise envers l'utilisation des outils numériques et des technologies.

Accenture[359] identifie cinq principes nécessaires aux entreprises afin de s'inscrire dans les enjeux numériques actuels et de prendre part à la concurrence :

- Les entreprises doivent engager une gouvernance digitale ;
- Les entreprises doivent développer des stratégies afin de renforcer la transparence ;
- Les entreprises doivent utiliser les données pour augmenter le bien-être des consommateurs et/ou utilisateurs ; notamment en participant à la prise de décision consciente et éclairée en termes de santé, d'éducation ou encore d'économie ;
- Les entreprises doivent promouvoir une équité digitale ;
- Les entreprises doivent prendre en considération l'inclusion numérique.

CSR Europe[360] évoque trois dimensions à la Responsabilité numérique des entreprises :

- La digitalisation en vue d'assurer le bien-être et l'inclusion des salariés ;
- Le respect de la vie privée des employés et les engagements de l'entreprises ;
- L'intelligence artificielle et l'automatisation en gardant les individus au cœur des transformations de l'entreprise.

Les membres du Groupe de travail de la Plateforme RSE s'accorde ainsi pour définir la Responsabilité numérique des entreprises comme un déploiement nouveau et incontournable de la RSE, qui se fonde sur les mêmes principes de redevabilité,

[357] https://digitalmindfulness.net/corporate-digital-responsibility/
[358] https://www.sciencedirect.com/science/article/pii/S0148296319305946
[359] Cooper T., Siu J., Wei K., *Corporate Digital Responsibilty – Doing well by doing good*, rapport Accenture
[360] https://www.csreurope.org/sites/default/files/uploads/Corporate%20Digital%20Responsibility%20Factsheet.pdf

d'éthique et d'échanges avec les parties prenantes des entreprises. La transversalité du numérique et son omniprésence impliquent que la création de valeur qu'elle engendre soit comprise et partagée par tous, au regard de ses enjeux démocratiques, sociaux et sociétaux. Il s'agit d'un enjeu de confiance, d'une confiance à renouveler au regard des constantes évolutions des techniques.

La RNE s'exerce dans des champs nombreux liés à l'usage des moyens informatiques et digitaux dont disposent les entreprises. Une entreprise numériquement responsable devrait ainsi répondre à plusieurs enjeux majeurs – en lien avec les objectifs de développement durable :

- la responsabilité règlementaire liée à la protection des données et au respect du RGPD et des règlementations sectorielles ;
- la responsabilité éthique liée aux logiciels relatifs à l'intelligence artificielle ;
- la responsabilité sociétale relative à la gestion des données, à la transformation des modes de travail, au partage des données à l'inclusion de toutes et tous ;
- la responsabilité environnementale liée à l'utilisation des données dans la prise en considération des impacts environnementaux des activités des entreprises.

Après avoir étudié les enjeux de la Responsabilité numérique des entreprises au regard des données détenues par les entreprises, la Plateforme RSE mènera deux études conjointes sur la RNE appliquée aux transformations des modes de travail puis sur les impacts des activités numériques des entreprises sur l'environnement.

IV. RECOMMANDATIONS

La Plateforme RSE propose la définition suivante pour la Responsabilité numérique des entreprises (RNE) :

« La Responsabilité numérique des entreprises est un déploiement nouveau et incontournable de la RSE, qui se fonde sur les mêmes principes de confiance, de redevabilité, d'éthique et d'échanges avec les parties prenantes des entreprises. La transversalité du numérique et son omniprésence impliquent que la création de valeur qu'elle engendre soit comprise et partagée par tous, au regard de ses enjeux démocratiques, sociaux et sociétaux. Il s'agit d'un enjeu de confiance, d'une confiance à renouveler au regard des constantes évolutions des techniques.

La RNE s'exerce dans des champs nombreux liés à l'usage des moyens informatiques et digitaux dont disposent les entreprises. Une entreprise numériquement responsable devrait ainsi répondre à plusieurs enjeux majeurs – en lien avec les objectifs de développement durable :

- la responsabilité réglementaire, liée à la protection des données et au respect du RGPD et des règlementations sectorielles ;
- la responsabilité éthique, liée aux logiciels relatifs à l'intelligence artificielle ;
- la responsabilité sociétale, relative à la gestion des données, à la transformation des modes de travail, au partage des données et à l'inclusion de toutes et tous ;
- la responsabilité environnementale, liée à l'utilisation des données dans la prise en considération des impacts environnementaux des activités des entreprises. »

La Plateforme RSE s'engage à promouvoir cette définition auprès des pouvoirs publics et de toutes les parties prenantes de l'entreprise.

La Plateforme RSE recommande aux pouvoirs publics :

- **(1)** d'agir au niveau européen pour que les enjeux liés au numérique soient insérés dans les nouvelles directives sur l'impact extra-financier des entreprises et sur le devoir de vigilance, et de veiller à la prise en compte des risques et violations liés au recueil et au traitement des données dans la mise en œuvre du devoir de vigilance et dans les négociations internationales en cours sur l'entreprise et les droits de l'homme, notamment le traité international à l'ordre du jour des Nations unies ;

- **(2)** de s'assurer que les entreprises prennent des dispositions propres à contrôler les processus dits « d'intelligence artificielle » afin qu'ils aboutissent à des décisions conformes aux lois et réglementations en vigueur (non discriminatoires, respectueuses du droit du travail) ;

- **(3)** de renforcer et de promouvoir la formation au numérique dès le plus jeune âge et ce, tout au long de la vie, en insistant sur le droit à la protection de la vie privée et aux droits qui y sont liés, notamment les droits à la portabilité et à l'oubli, ainsi qu'à la cybersécurité et aux risques spécifiques liés à l'usage des nouvelles technologies tant sur la vie personnelle que professionnelle ;

- **(4)** de renforcer les mesures et les dispositifs d'accompagnement des TPE et PME dans leur transformation numérique responsable ;

- **(5)** d'intégrer dans les marchés publics un engagement à partager les données pouvant contribuer à l'intérêt général, collectées dans le cadre du marché ;

- **(6)** de définir les conditions dans lesquelles les entreprises pourraient partager les algorithmes en *open source* quand ceux-ci ont un impact sur l'intérêt général ;

- **(7)** de promouvoir la mutualisation des données sur les territoires (au niveau des groupements intercommunaux par exemple) afin d'augmenter l'efficacité du service public et d'engager une dynamique de développement de nouveaux services et activités bénéfiques à l'intérêt général ;

- **(8)** de mettre en œuvre une réflexion sur l'élargissement des recommandations de la loi du 7 octobre 2016 pour une République numérique lorsque les entreprises ont des participations de l'État afin de favoriser la diffusion de données d'intérêt

- **(9)** de promouvoir une certification européenne, ou *a minima* une déclaration de conformité, de fiabilité et de sécurité du *cloud*, sur la base d'une convergence et d'une reconnaissance mutuelle des certifications ;

- **(10)** de renforcer l'offre et la diffusion des guides pratiques indiquant la réglementation applicable en matière de gestion des données (personnelles et économiques), qui soient adaptés aux entreprises en fonction de leur taille et de leur secteur.

La Plateforme RSE formule les recommandations suivantes dont l'important est à moduler en fonction de l'objet social, de la taille et des enjeux générés par les activités de l'entreprises.

La Plateforme RSE recommande aux entreprises de faire converger les stratégies relatives à la RSE et au numérique en :

- **(11)** promouvant la coordination entre les équipes chargées d'élaborer et de mettre en œuvre la politique des données et celle chargée de la RSE ;
- **(12)** incluant, pour les entreprises concernées, dans leurs déclarations de performance extra-financière des indicateurs portant sur leurs politiques de protection des données ;
- **(13)** développant la négociation concernant la RNE à différents niveaux (IRP, accords-cadres internationaux, accords de branche) ;
- **(14)** incluant, pour les entreprises qui en sont dotées, dans le comité des parties prenantes au moins une personne spécialiste du numérique ;
- **(15)** adoptant des chartes éthiques relatives à la RNE au sein de l'entreprise et de ses filiales ;
- **(16)** veillant à ce que les enjeux relatifs aux données fassent l'objet de discussions dans les comités spécialisés des conseils d'administration, par exemple en nommant un administrateur référent sur l'utilisation des données ;
- **(17)** enrichissant les bases de données économiques et sociales (BDES) avec des informations pertinentes afin d'en faire un outil au service de la qualité du dialogue économique et social ;

La Plateforme RSE recommande aux entreprises de se former aux enjeux du numérique à tous les niveaux de l'entreprise en :

- **(18)** formant les membres situés au plus haut niveau hiérarchique de l'entreprise (comex) aux enjeux et principes de base relatifs à la gouvernance des données et en renforçant les équipes chargées de la RSE en compétences sur le cadre légal relatif à la protection des données ;
- **(19)** créant ou renforçant les dispositifs de formation continue, y compris à l'attention des dirigeants, aux enjeux numériques tout au long de la chaîne de valeur, notamment sur le droit au respect de la vie privée ;
- **(20)** s'assurant que les développeurs soient formés au repérage des biais discriminatoires des algorithmes et à la promotion de leur transparence ;
- **(21)** renforçant les équipes chargées de la RSE en compétences sur le cadre légal de la protection des données.

Dans l'optique de favoriser l'ouverture des données, lorsque cela est possible, la Plateforme RSE rappelle sa recommandation aux entreprises de :

- **(22)** publier sous un format exploitable par tous (*open data*) les données publiques de l'entreprise portant sur la RSE ;

La Plateforme RSE recommande aux entreprises de porter une attention particulière aux risques induits par le numérique en :

- **(23)** intégrant les risques liés à l'usage des données dans les politiques de diligence raisonnable en matière de droits humains ;
- **(24)** s'assurant, pour les entreprises soumises au plan de vigilance, que les impacts de leurs activités sur les droits humains soient clairement identifiés ;
- **(25)** s'assurant de la bonne compréhension et du respect des obligations du RGPD par les sous-traitants ;
- **(26)** accroissant leur vigilance sur les algorithmes et la prévention des risques de discrimination induits par leur développement et leur déploiemen,t en s'entourant de compétences et organismes appropriés ;
- **(27)** veillant à ce que la procédure d'alerte prévue par la loi Sapin 2 ou la loi sur le devoir de vigilance offre des garanties solides en matière de confidentialité de l'auteur de l'alerte, des faits ou des personnes visées ;
- **(28)** veillant à promouvoir les droits humains et les législations relatives à la protection de la vie privée.

La Plateforme RSE recommande aux syndicats de salariés :

- **(29)** de veiller à ce que les salariés soient davantage sensibilisés à l'utilisation des outils numériques et à la responsabilisation des processus informatiques.

La Plateforme RSE recommande aux investisseurs et aux acteurs de l'évaluation de la performance extra-financière des entreprises (agences de notation, certificateurs, labels, etc.) :

- **(30)** d'intégrer dans les référentiels d'évaluation des indicateurs permettant d'évaluer la Responsabilité numérique de l'entreprise.

La Plateforme RSE recommande aux acteurs de l'enseignement supérieur et de la recherche :

- **(31)** d'encourager la recherche sur la Responsabilité numérique des entreprises ;
- **(32)** d'intégrer la responsabilité numérique dans les formations des formateurs et des étudiants ;
- **(33)** d'intégrer la responsabilité numérique dans l'approche éthique de la recherche et de former les membres des Comités d'éthique de la recherche ;
- **(34)** de favoriser les échanges entre les incubateurs et les startups de la Tech avec les laboratoires de recherche.

ANNEXE 1
CADRE NORMATIF

Cadre normatif

Droit international

Nations Unies

Pacte international relatif aux droits civils et politiques, entré en vigueur le 23 mars 1976

Article 17

1. Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation.

2. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

Principes directeurs pour la règlementation des fichiers informatisés contenant des données à caractère personnel proclamés lors de la quarante-cinquième session de l'Assemblée générale des Nations Unies dans sa résolution 45/95 du 14 décembre 1990

Le 14 décembre 1990, les Nations Unies ont adopté des principes directeurs relatifs à la règlementation des fichiers informatisés contenant des données à caractère personnel. Les modalités d'application ont été laissées à la libre initiative des Etats sous réserve des orientations suivantes :

1. Le principe de licéité et de loyauté : les données personnelles doivent être obtenues et traitées via des procédés licites et loyaux ;

2. Le principe d'exactitude : les personnes responsables de l'établissement d'un fichier ou celles responsables de leur mise en œuvre doivent être tenues de vérifier l'exactitude et la pertinence des données enregistrées ;
3. Le principe de finalité : la finalité en vue de laquelle est créé un fichier et son utilisation en fonction de cette finalité doivent être spécifiées, justifiées et être portées à la connaissance de la personne concernée ;
4. Le principe de l'accès par les personnes concernées : toute personne justifiant son identité a le droit de savoir si des données la concernant font l'objet d'un traitement, d'en avoir communication sous une forme intelligible et d'obtenir les rectifications ou les destructions adéquates en cas d'enregistrements illicites, injustifiés ou inexactes et lorsqu'elles sont communiquées d'en connaitre les destinataires ;
5. Le principe de non-discrimination : sous réserve de cas dérogatoires, les données pouvant engendrer une discrimination illégitime ou arbitraire, notamment les informations sur l'origine raciale ou ethnique, la couleur, la vie sexuelle, les opinions politiques, les convictions religieuses, philosophiques ou autres, ainsi que l'appartenance à une association ou un syndicat, ne devraient pas être collectées ;
6. La faculté de dérogation : des dérogations aux principes 1 à 4 peuvent être autorisées si elles sont nécessaires pour protéger la sécurité nationale, l'ordre public, la santé ou la moralité publiques et les libertés d'autrui, des dérogations au principe 5 ne peuvent être autorisées que dans les limites prévues par la Charte internationale des droits de l'homme et autres instruments pertinents dans ce domaine ;
7. Le principe de sécurité : les fichiers doivent être protégés contre les risques naturels et humains ;
8. Le contrôle et les sanctions : les législations doivent désigner l'autorité en charge de contrôler le respect des principes précités ;
9. Les flux transfrontaliers des données : lors que la législation de deux ou plusieurs pays, concernés par un flux transfrontière de données, présente des garanties comparables au regard de la protection de la vie privée, les informations doivent pouvoir circuler aussi librement à l'intérieur de chacun des territoires concernés ;
10. Champ d'application : les principes précités doivent s'appliquer en premier lieu à tous les fichiers informatisés publics et privés, et aux fichiers traités manuellement.

Conseil de l'Europe

La Convention 108 du Conseil de l'Europe du 28 juillet 1981

La Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, dite Convention 108, du Conseil de l'Europe a été ratifiée le 28 janvier 1981 et est entrée en vigueur le 1er octobre 1985. À ce jour, elle a été ratifiée par les 47 États membres du Conseil de l'Europe, ainsi que l'Île Maurice, le Sénégal, l'Uruguay et la Tunisie. D'autres pays participent, à titre d'États observateurs, aux travaux du Comité de la Convention : le Canada, les États-Unis, l'Australie, la Corée, le Chili, le Ghana, le Japon, l'Indonésie, Israël et la Nouvelle-Zélande.

Elle constitue le premier instrument international contraignant visant à protéger les personnes contre l'usage abusif du traitement automatisé des données à caractère personnel. Elle a pour objectif de réglementer les flux transfrontaliers des données et

interdit le traitement des données ‘sensibles’ relatives à l’origine raciale, aux opinions politiques, à la santé, à la religion, à la vie sexuelle ou encore aux condamnations pénales.

Elle garantit le droit des personnes concernées de connaitre les informations stockées à leur sujet et d’exiger des rectifications. La seule restriction s’applique si les intérêts majeurs de l’État sont en jeu. Le texte assure des principes de base, que l’on retrouve aujourd’hui dans la réglementation européenne :

- Principes de loyauté et licéité du traitement des données ;
- L’obligation de sécurité lors du traitement des données ;
- La protection spécifique des données dites sensibles ;
- Les droits d’accès, de rectification et d’effacement reconnus aux personnes concernées.

En 2018, la Convention 108 a été amendée en vue de moderniser son application et de répondre aux nouveaux défis en matière de protection de la vie privée. Les modifications apportées permettent de reconnaitre de nouveaux principes : de transparence, de proportionnalité, de responsabilité, de limitation des données, de respect de la vie privée qui constituent aujourd’hui des éléments clés du mécanisme de protection.[361]

Résolution 428 du Conseil de l’Europe portant déclaration sur les moyens de communication de masse et les droits de l’homme, adoptée en janvier 1970

L’article 19 de la Résolution 428 du Conseil de l’Europe souligne l’importance du droit à la vie privée, et édicte que : « *Lorsque des banques régionales, nationales ou internationales de données informatiques sont instituées, l’individu ne doit pas être rendu totalement vulnérable par l’accumulation d’informations concernant sa vie privée. Ces centres doivent enregistrer uniquement le minimum de renseignements nécessaires aux questions, telles qu’impôts, systèmes de retraites, Sécurité sociale, etc.* »

Article 8 de la Convention européenne de sauvegarde des Droits de l’Homme et des Libertés fondamentales de 1950

Article 8 – Droit au respect de la vie privée et familiale

Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.

Il ne peut y avoir ingérence d’une autorité publique dans l’exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu’elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l’ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d’autrui.

Résolution 428 du Conseil de l’Europe portant déclaration sur les moyens de communication de masse et les droits de l’homme, adoptée en janvier 1970

[361] https://rm.coe.int/la-convention-108-modernisee-appercu-des-nouveautes-fr/16808b07e8

L'article 19 de la Résolution 428 du Conseil de l'Europe souligne l'importance du droit à la vie privée, et édicte que : « *Lorsque des banques régionales, nationales ou internationales de données informatiques sont instituées, l'individu ne doit pas être rendu totalement vulnérable par l'accumulation d'informations concernant sa vie privée. Ces centres doivent enregistrer uniquement le minimum de renseignements nécessaires aux questions, telles qu'impôts, systèmes de retraites, Sécurité sociale, etc.* »

Recommandation CM/Rec(2020)1 du Comité des Ministres aux Etats membres sur les impacts des systèmes algorithmiques sur les droits de l'homme, adoptée le 8 avril 2020

Considérant les évolutions technologiques majeures, leur ampleur dans la vie quotidienne, l'engagement des Etats membres à la garantie des droits et libertés, le Conseil de l'Europe recommande aux gouvernements des Etats membres :

- De revoir leurs cadres législatifs, leurs politiques et leurs pratiques en matière d'acquisition, de conception, de développement et de déploiement des systèmes algorithmiques ;
- De veiller à ce que cette recommandation soit traduite et largement diffusée auprès des autorités et des parties prenantes compétentes ;
- De s'assurer, par le biais de cadres législatifs, réglementaires et de contrôle appropriés relatifs aux systèmes algorithmiques, que les acteurs du secteur privé participant à la conception, au développement et au déploiement en cours de tels systèmes se conforment aux lois applicables et assument leurs responsabilités en matière de respect de droits de l'homme ;
- De doter les institutions nationales de surveillance, de contrôle et d'évaluation des risques et d'application compétentes des ressources et pouvoirs nécessaires pour enquêter, superviser et coordonner le respect de leur cadre législatif et réglementaire pertinent, conformément à la présente recommandation ;
- D'entreprise des consultations, une coopération et un dialogue réguliers, inclusifs et transparents avec toutes les parties prenantes concernées, en accordant une attention particulière aux besoins et aux voix des groupes vulnérables afin de veiller à ce que les impacts sur les droits de l'hommes engendrés par la conception, le développement et le déploiement en cours des systèmes algorithmiques fassent l'objet d'un suivi, d'un débat et d'une solution ;
- De privilégier le renforcement de l'expertise des établissements publics et privés participant à l'intégration des systèmes algorithmiques dans de multiples aspects de la société, en vue de protéger efficacement les droits de l'homme ;
- D'encourager et de promouvoir la mise en œuvre de programme d'éducation aux médias, à l'information et au numérique efficaces et adaptés, afin de permettre à toutes les personnes et à tous les groupes de comprendre, prendre des décisions éclairées, profiter des avantages et réduire l'exposition aux risques des systèmes de décisions automatisées ;
- De tenir compte de l'impact environnemental du développement des services numériques à grande échelle et de prendre les mesures nécessaires pour optimiser l'utilisation et la consommation des ressources naturelles et de l'énergie ;

- De réexaminer périodiquement, en concertation avec tous les acteurs concernés, les mesures prises pour mettre en œuvre la présente recommandation et ses lignes directrices et de faire un rapport à ce sujet au plan national et au sein du Comité des Ministres.

Organisation de Coopération et de Développement Economique (OCDE)

Recommandations de l'Organisation de Coopération et de Développement Économiques concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontaliers des données à caractère personnel du 23 septembre 1980

Le 23 septembre 1980, l'OCDE émettait des recommandations en vue de favoriser la libre circulation de l'information entre les pays membres et d'éviter la création d'obstacles injustifiés au développement des relations économiques et sociales entre les pays. Le texte énonce des principes fondamentaux applicables au plan national[362] :

- Principe de la limitation en matière de collecte des données, devant être obtenues par des moyens licites et loyaux et après en avoir informé la personne concernée ou avec son consentement ;
- Principe de la qualité des données, devant être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées. Les finalités doivent être définies au moment de la collecte des données ;
- Principe de la limitation de l'utilisation, déterminant que les données doivent être utilisées seulement dans les cadres définis en amont ;
- Principe des garanties de sécurité, contre la perte des données ou leur accès, destruction, utilisation ou divulgation non autorisés ;
- Principe de la participation individuelle, admettant que toute personne physique doit avoir le droit d'obtenir confirmation que le maitre d'un fichier détient ou non des données la concernant, de se faire communiquer ces données et de pouvoir les contester, les faire effacer, rectifier, compléter ou corriger ;
- Principe de la responsabilité, affirmant que tout maitre de fichier doit être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.

Dans le même temps, les recommandations s'intéressent au niveau international en appelant à la prise en considération des conséquences pour d'autres pays membres d'un traitement effectué sur leur propre territoire et de la réexportation des données à caractère personnel, de la sécurité des flux transfrontaliers et de l'absence d'obstacles à la circulation transfrontalière des données.

Recommandations de l'Organisation de Coopération et de Développement Économiques concernant les lignes directrices régissant la protection de la vie privée et les flux transfrontaliers des données à caractère personnel 11 juillet 2013

362 http://www.oecd.org/fr/sti/ieconomie/lignesdirectricesregissantlaprotectiondelaviepriveeetlesfluxtransfrontieresdedonneesdecaracterepersonnel.htm

Constituant une mise à jour des recommandations du 23 septembre 1980, ce rapport entend appuyer ses positions sur les pratiques de protection de la vie privée au travers d'une approche de management des risques et sur le besoin de donner une ampleur internationale à la protection via une interopérabilité améliorée.

Les experts de l'OCDE considèrent également que plusieurs thématiques devront être abordées dans le futur : les stratégies de protection nationales, les programmes de management des risques et des recommandations sur les violations de données.

Droit de l'Union européenne

Traités

Charte des droits fondamentaux de l'Union européenne

Article 8 - Protection des données à caractère personnel

1. Toute personne a droit à la protection des données à caractère personnel la concernant.

2. Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification.

3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante.

Directives

Directive 2002/58-CE du 12 juillet 2002 sur la protection de la vie privée dans le secteur des communications électroniques, dite e-privacy

La Directive 2002/58-CE vise à protéger de façon spécifique la vie privée sur internet en couvrant certains aspects mis de côté par la Directive 95/46/CE. Elle interdit le spam en instaurant le principe de l'opt-in voulant qu'un opérateur obtienne le consentement du destinataire avant de lui envoyer tout message à caractère commercial, ainsi que le principe de l'opt-out permettant de se retirer d'une liste d'envoi. Ces deux principes ont été transposés dans le droit français au travers de la loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique.

Directive sur la sécurité des réseaux et des systèmes d'information (Directive NIS) ((UE) 2016/1148)

Le Parlement européen et le Conseil de l'Union européenne ont adopté le 6 juillet 2016 la directive sur la sécurité des réseaux et des systèmes d'information, également appelée en anglais la directive NIS (Network and Information System Security).

La France a transposé cette directive par différents textes en 2018[363]. Celle-ci est structurée autour de quatre axes[364] :

- Le renforcement des capacités nationales de cybersécurité. Les Etat membres devront notamment se doter d'autorités nationales compétentes en matière de cybersécurité, d'équipes nationales de réponse aux incidents informatiques (CSIRT) et de stratégies nationales de cybersécurité. Respectivement en France, l'ANSSI, le CERT-FR et la stratégie nationale pour la sécurité du numérique ;
- L'établissement d'un cadre de coopération volontaire entre Etats membres de l'UE via la création d'un « groupe de coopération » des Etats membres sur les aspects politiques de la cybersécurité, ainsi que d'un « réseau européen des CSIRT » des Etats membres. Ce dernier visera notamment à faciliter le partage d'informations techniques sur les risques, vulnérabilités ;
- Le renforcement par chaque Etat de la cybersécurité d'« opérateurs de services essentiels » au fonctionnement de l'économie et de la société via la définition au niveau national de règles de cybersécurité auxquels ces derniers devront se conformer et par l'obligation pour les opérateurs de notifier les incidents ayant un impact sur la continuité de leurs services essentiels ;
- L'instauration de règles européennes communes en matière de cybersécurité des prestataires de services numériques dans les domaines de l'informatique en nuage, des moteurs de recherche et places de marché en ligne.

Règlements

Règlement n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000

Le règlement n°45/2001 du 18 décembre 2000 est relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données. Une de ses dispositions promulgue des mesures de conservation des données à une fin de police préventive. Elle introduit le nécessité de traiter les données à caractère personnel de manière loyale, licite, exacte, et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement.

Règlement n°2016/679 dit Règlement Général sur la Protection des Données (RGPD)

Le règlement n°2016/679 dit Règlement Général sur la Protection des Données (RGPD) est un règlement du Parlement européen et du Conseil constituant un texte de référence en matière de protection des données. Il fut adopté le 14 avril 2016, est entré en vigueur le 27 avril 2016 et ses dispositions sont obligatoirement et directement applicables dans l'ensemble des 28 États-membres de l'Union européenne depuis le 25 mai 2018.

[363] https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033122937
[364] https://www.ssi.gouv.fr/actualite/adoption-de-la-directive-network-and-information-security-nis-lanssi-pilote-de-la-transposition-en-france/

La conception du RGPD a été pensée autour de 3 objectifs :

- Le renforcement des droits des personnes physiques ;
- La responsabilisation des acteurs traitant des données ;
- La crédibilisation de la régulation grâce à la coopération renforcée entre les autorités de protection des données.

La CNIL[365] considère que le RGPD a apporté de nouveaux droits fondamentaux :

- Le droit à la portabilité des données (article 20) ;
- La limitation du traitement (article 18) ;
- La notification des violations de données personnelles – failles de sécurité (article 4, 33 et 34) ;
- Le droit de déposer une réclamation (articles 77 et 80) ;
- Des conditions particulières pour la protection des enfants (articles 8 et 17).

L'article 5 du RGDP définit plusieurs règles que les entreprises doivent respecter en matière de protection des données :

Article 5 - Principes relatifs au traitement des données à caractère personnel

Les données à caractère personnel doivent être :

a) traitées de manière licite, loyale et transparente au regard de la personne concernée (licéité, loyauté, transparence);

b) collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités; le traitement ultérieur à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques n'est pas considéré, conformément à l'article 89, paragraphe 1, comme incompatible avec les finalités initiales (limitation des finalités);

c) adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées (minimisation des données);

d) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour que les données à caractère personnel qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans tarder (exactitude);

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément à l'article 89, paragraphe 1, pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée (limitation de la conservation);

f) traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité);

[365] Sophie Nerbonne, audition du 26 novembre 2019

Le responsable du traitement est responsable du respect du paragraphe 1 et est en mesure de démontrer que celui-ci est respecté (responsabilité).

Dans le même temps, une entreprise détentrice de données doit pouvoir garantir le droit d'accès des personnes concernées. Ce droit sous-entend la transparence et la connaissance des données détenues sur soi.

Article 22 - Décision individuelle automatisée, y compris le profilage

La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire.

Le paragraphe 1 ne s'applique pas lorsque la décision:

a) est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et un responsable du traitement;

b) est autorisée par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis et qui prévoit également des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée; ou

c) est fondée sur le consentement explicite de la personne concernée.

Dans les cas visés au paragraphe 2, points a) et c), le responsable du traitement met en œuvre des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée, au moins du droit de la personne concernée d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision.

Les décisions visées au paragraphe 2 ne peuvent être fondées sur les catégories particulières de données à caractère personnel visées à l'article 9, paragraphe 1, à moins que l'article 9, paragraphe 2, point a) ou g), ne s'applique et que des mesures appropriées pour la sauvegarde des droits et libertés et des intérêts légitimes de la personne concernée ne soient en place.

Afin de guider les entreprises françaises dans leur mise en conformité avec les exigences européennes, la CNIL conseille six étapes[366] :

Étape 1 Désigner un délégué à la protection des données	« Pour piloter la gouvernance des données personnelles de votre structure, vous aurez besoin d'un véritable chef d'orchestre qui exercera une mission d'information, de conseil et de contrôle en interne : le délégué à la protection des données. En attendant 2018, vous pouvez d'ores et déjà désigner un « correspondant informatique et libertés », qui vous donnera un temps d'avance et vous permettra d'organiser les actions à mener. »
Étape 2 Cartographier les traitements de données personnelles	« Pour mesurer concrètement l'impact du règlement européen sur la protection des données que vous traitez, commencez par recenser de façon précise vos traitements de données personnelles. L'élaboration d'un registre des traitements vous permet de faire le point. »
Étape 3 Prioriser les actions à mener	« Sur la base de votre registre, identifiez les actions à mener pour vous conformer aux obligations actuelles et à venir. Priorisez ces actions au regard des risques que font peser vos traitements sur les droits et les libertés des personnes concernées. »
Étape 4 Gérer les risques	« Si vous avez identifié des traitements de données personnelles susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes concernées, vous devrez mener, pour chacun de ces traitements, une analyse d'impact relative à la protection des données (AIPD). »
Étape 5 Organiser les processus internes	« Pour assurer un haut niveau de protection des données personnelles en permanence, mettez en place des procédures internes qui garantissent la prise en compte de la protection des données à tout moment, en prenant en compte l'ensemble des événements qui peuvent survenir au cours de la vie d'un traitement (ex : faille de sécurité, gestion des demandes de rectification ou d'accès, modification des données collectées, changement de prestataire). »
Étape 6 Documenter la conformité	« Pour prouver votre conformité au règlement, vous devez constituer et regrouper la documentation nécessaire. Les actions et documents réalisés à chaque étape doivent être réexaminés et actualisés régulièrement pour assurer une protection des données en continu. »

Comparaison du RGPD et du California Consumer Privacy Act :

Le RGPD a inspiré de nouvelles législations dans d'autres pays. Ainsi, le *California Consumer Privacy Act* adopté le 28 juin 2019 et entré en application le 1er janvier 2020 s'inspire des acquis européens. Ce texte visant à renforcer la maîtrise et le contrôle des personnes sur leurs données constitue la première législation de ce type aux États-Unis. Il donne le droit aux californiens de demander aux entreprises quelles données sont collectées, comment elles sont utilisées, avec quelles tierce-parties elles sont partagées, qu'elles soient supprimées mais aussi de refuser que leurs données soient utilisées à des fin commerciales. Pour les enfants de 13 à 16 ans, les données ne peuvent être vendues sans leur accord explicite préalable et pour les enfants de moins de 13 ans, l'accord d'un adulte est nécessaire.

[366] https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

La législation californienne contient des différences notables avec le RGPD :

Règlement Général sur la Protection des Données	California Consumer Privacy Act
« Toute information se rapportant à une personne physique identifiée ou identifiable » (article 4)	« Informations qui identifient, se rapportent à, décrivent, sont susceptibles d'être associées à, ou pourraient raisonnablement être liées, directement ou indirectement, à un consommateur ou un ménage particulier »
Distinction entre les données classiques et les données dites sensibles	Pas de distinction entre les données Les données des salariés ne sont pas considérées comme des données à caractère personnel
Le RGPD contraint les entreprises à demander l'autorisation aux internautes avant de collecter leurs données	Les entreprises ne sont pas obligées de demander l'autorisation aux internautes avant de collecter leurs données
La protection s'applique sans distinction à tout organisme privé ou public disposant de données à caractère personnel. Il dispose d'un caractère extraterritorial puisqu'il ne s'applique pas seulement aux personnes présentes sur le territoire de l'Union européenne.	Exclusion des informations contenues dans un fichier tenu par un organisme public fédéral, étatique ou local et qui seraient rendues publiques La protection ne bénéficie qu'aux résidents de l'État de Californie et elle ne s'applique pas aux traitements de données liés à des activités commerciales réalisées intégralement hors de Californie. Le California Consumer Pivacy Act s'applique aux entreprises qui génèrent un chiffre d'affaires supérieur à 25 millions de $ sur le sol californien, achètent, reçoivent ou vendent les données de 50 000 consommateurs
	Autorise le responsable de traitement à créer des programmes d'incitation, notamment financières, au bénéfice de la personne qui accepte la collecte ou la revente de ses données personnelles
N'ouvre pas la possibilité d'engager des poursuites au civil	Ouvre la possibilité aux individus d'engager des poursuites au civil

Règlement du Parlement européen et du Conseil du 10 janvier 2017 concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques »)[367]

[367] https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52017PC0010&from=FR

La Commission européenne a publié une proposition de règlement du Parlement européen et du Conseil de l'Union européenne le 10 janvier 2017 afin d'élargir le champ d'application de la Directive 2002/58-CE et aligner ses dispositions avec le RGPD.

Néanmoins, les États-membres peinent à s'accorder et deux dispositions font débat :

- La notion de consentement préalable, qui permettrait à chaque internaute de décider, dès sa première connexion, du niveau de protection dont il a besoin pour l'ensemble de sa session et non par site
- La géolocalisation de leur clientèle par les entreprises, qui sans autorisation préalable, peuvent analyser les déplacements de leurs clients lorsque ceux-ci se trouvent dans des lieux surveillés par l'entreprise. Les entreprises doivent afficher l'information de surveillance à l'entrée du lieu.

En mai 2017, les éditeurs de presse ont adressé une lettre ouverte[368] à l'Union européenne afin d'alerter les pouvoirs publics sur la notion de consentement préalable qui avantagerait les entreprises qui contrôlent 90 % de l'accès à Internet sur le territoire européen – Google, Apple, Microsoft et Mozilla – et renforcerait l'asymétrie entre les éditeurs de presse et les portails numériques mondiaux.

La nouvelle présidence croate du Conseil de l'Union européenne relancera les débats avec la proposition d'un nouveau compromis.

Règlement 2018/1807 du Parlement européen et du Conseil du 14 novembre 2018 établissant un cadre applicable au libre flux des données à caractère non personnel dans l'Union européenne

Le règlement 2018/1807 vise à assurer le libre flux des données autres que les données à caractère personnel au sein de l'Union européenne. Pour cela, il établit des règles concernant les exigences de localisation des données, leur disponibilité pour les autorités compétences et le portage des données pour les utilisateurs professionnels.

Il s'applique au traitement des données électroniques fourni en tant que service aux utilisateurs résidant ou disposant d'un établissement dans l'UE, par un fournisseur de services établi ou non dans l'UE ou par une personne physique ou morale résidant ou disposant d'un établissement dans l'UE pour ses propres besoins.

Jurisprudences

Arrêt de la CJUE, grande chambre, 8 avril 2014, relatif à la directive 2006/24/CE du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications

Rendant décision dans le cadre d'un procès entre Digital Rights Ireland Ltd, cet arrêté du 8 avril 2014 condamne « *Une ingérence dans les droits fondamentaux de la quasi-totalité de la population européenne* », d'une si *« vaste ampleur »* qu'elle *« doit être*

[368] https://www.lapresse.be/wp-content/uploads/2018/03/Definitive-Open-letter-ePR-v05032018-VF_2PAGES.pdf

considérée comme particulièrement grave ». En effet, *« la conservation des données et l'utilisation ultérieure de celles-ci sont effectuées sans que l'abonné ou l'utilisateur inscrit en soit informé »,* ce qui génère *« le sentiment que* [sa] *vie privée fait l'objet d'une surveillance constante ».*

Droit français

Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, dite loi informatique et libertés, est une loi française règlementant la liberté de traitement des données personnelles.

Elle prévoit des obligations à la charge des détenteurs de données à caractère personnel sur plusieurs niveaux.

Collecte des données à caractère personnel	Le consentement de la personne doit être recueilli et les informations traitées doivent être exactes, complètes et tenues à jour. Il est interdit de collecter des données sensibles concernant les origines raciales ou ethniques, les opinions religieuses, politiques ou philosophique, l'orientation sexuelle, l'appartenance syndicale ou l'état de santé.	La collecte des données à caractère personnel par un moyen frauduleux, déloyal, illicite est punie de 5 ans d'emprisonnement et 300 000 euros d'amende (article 226-18 du Code pénal)
Finalité des traitements	la collecte de données doit se faire avec un objectif précis.	Tout détournement de finalité est sanctionné de 5 ans d'emprisonnement et 300 000 euros d'amende (article 226-21 du Code pénal)
Durée de conservation	La loi impose que la durée de conservation des données soit fixée par le responsable dans une limite « raisonnable » en fonction de l'objectif du fichier.	Une durée de conservation supérieure à celle déclarée par le responsable est sanctionnée de 5 ans d'emprisonnement et 300 000 euros d'amende (article 226-7 du Code pénal)
Mesures de sécurité	Les responsables de traitement de données à caractère personnel sont tenus d'adopter des mesures de sécurité fans la gestion des fichiers et le risque du traitement.	Tout manquement à l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et 300 000 euros d'amende (article 226-17 du Code pénal)
Confidentialité	Les données doivent être confidentielles, seuls les destinataires explicitement désignés et les tiers autorisés peuvent accéder aux données contenues dans un fichier.	La communication de données à un tiers non autorisé est sanctionnée de 5 ans d'emprisonnement et 300 000 euros d'amende. Si la divulgation fait suite à de la négligence ou de l'imprudence, la sanction est de 3 ans d'emprisonnement et 100 000 euros d'amende (article 226-22 du Code pénal)

La loi rappelle que les personnes ont des droits sur leurs données. Le responsable des données à caractère personnel permet aux individus d'exercer leurs droits et doit leur donner la possibilité d'obtenir les informations sur leur identité, la finalité de traitement de leurs données, le caractère obligatoire ou facultatif des réponses, l'existence de leurs droits et les transmissions envisagées.

La loi institue enfin la Commission Nationale de l'Informatique et des Libertés (CNIL). Elle constitue l'autorité indépendante garante de la protection des données à caractère personnel. Ainsi, certains traitements de données doivent être déclarés auprès de la CNIL ou être autorisés par celle-ci.

Les décrets n°2018-687 du 1er août 2018 et n°2019-536 du 29 mai 2019 ont permis de renforcer la loi n°78-17 et de l'adapter aux obligations du RGPD.

La loi du 7 octobre 2016 pour une République numérique

La loi n°2016-1321 prépare la France aux enjeux de la transition numérique en créant de nouveaux droits afin de permettre aux individus de mieux maitriser leurs données personnelles. Elle renforce également les pouvoirs de la CNIL et entend promouvoir une meilleure ouverture des données publiques.

Les dispositions prévues anticipaient le RGPD, ainsi la loi façonne de nouveaux droits pour les personnes[369] :

Maîtrise des données par l'individu	Droit à l'autodétermination informationnelle
Droit à l'oubli pour les mineurs	Droit à l'oubli spécifique et procédure accélérée pour l'effacement des données jugées problématiques
Organiser le sort de ses données après la mort	Possibilité de donner des directives concernant la conservation, l'effacement et la communication de ses données après son décès
Exercice de droits par voie électronique	Possibilité donnée, lorsque cela est possible, à toute personne d'exercer ses droits d'accès, de rectification ou d'opposition par voie électronique
Information sur la durée de conservation des données	Devoir d'information des responsables de traitement de données sur la durée de conservation des données traitées ou, en cas d'impossibilité, des critères déterminant la durée

La loi renforce les compétences de la CNIL, notamment en rendant sa consultation systématique pour tout projet de loi, décret ou disposition relatifs à la protection des données personnelles ou à leur traitement.

Loi du 20 juin 2018 relative à la protection des données personnelles

La loi n°2018-493 reprend les dispositions du RGPD. Certains articles du règlement renvoient aux législations nationales afin qu'elles soient en mesure d'adapter et de

[369] https://www.cnil.fr/fr/ce-que-change-la-loi-pour-une-republique-numerique-pour-la-protection-des-donnees-personnelles

clarifier certaines dispositions au regard de leurs spécificités, cette loi apporte des précisions complémentaires aux règles européennes.

Elle renforce ainsi le domaine de compétences de la CNIL qui est désormais un organe certificateur en mesure de certifier des personnes, produits, systèmes de données ou des procédures afin de reconnaitre leur conformité au RGPD.

La majorité numérique est également fixée à 15 ans, c'est-à-dire l'âge à partir duquel un adolescent a la faculté de consentir seul, sans autorisation parentale, au traitement de ses données.

ANNEXE 2
COMPOSITION DU GROUPE DE TRAVAIL

Les membres de la Plateforme RSE dont les noms suivent ont pris part aux travaux du présent avis :

Pôle des entreprises et du monde économique

- CPME (Sandrine BOURGOGNE, Sarah RACHI)
- EDH (Charlotte MICHON, Yves NISSIM)
- FIR
- France Chimie (Aurore FRIES)
- Medef (Maxence DEMERLE, Jean-Paul ALIBERT)
- Orée (Caroline ALAZARD)
- Orse (Géraldine FORT, Lydie RECORBET)

Pôle des organisations syndicales de salariés

- CFDT (Frédérique LELLOUCHE)
- CFE-CGC (François MOREUX)
- CFTC (Geoffroy DE VIENNE), co-rapporteur
- CGT (Pierre-Yves CHANU, Didier LASSAUZAY)

Pôle des organisations de la société civile

- Amnesty International France (Sabine GAGNIER)
- ATD Quart-Monde (Nicolas THOMAS)
- CCFD-Terres Solidaires (Swann BOMMIER)
- Sherpa (Lucie CHATELAIN, Sandra COSSART)
- 4D / Les Petits Débrouillards (Ghislaine HIERSO), co-rapporteure
- FNE (Bela LOTO)

Pôle des chercheurs et développeurs de la RSE

- Comité 21 (Bettina LAVILLE), animatrice
- Consult'in France (Agnès RAMBAUD-PAQUIN)
- CPU (Beatrice BELLINI, Fleur LARONZE, Kathia MARTIN-CHENUT)
- FACE (Camille PHE)

Pôle des institutions publiques

- AFNOR normalisation (Nicole GOINEAU)
- CNCDH (Céline BRANAA-ROCHE)

ANNEXE 3
LISTE DES PERSONNES RENCONTREES

Le groupe de travail a mené 18 auditions, de novembre 2019 à juin 2020. Il a rencontré des experts, académiques et praticiens, des avocats, des représentants d'institutions et d'associations ainsi que des professionnels des données, qu'il remercie pour leur disponibilité et leur contribution à ses travaux.

De plus, le secrétariat permanent de la Plateforme RSE remercie celles et ceux qui ont accepté de partager leurs analyses et leurs expériences dans le cadre de la préparation de ces travaux, notamment M. Arnaud Jacques (Le Bon Coin)

Audition du 26 novembre 2019

- Mme Sophie NERBONNE, directrice chargée de la co-régulation économique, Commission nationale informatique et libertés (CNIL)

Auditions du 17 décembre 2019

- Mme Valérie CHAROLLES, chercheure en philosophie à l'Institut Mines-Télécom Business School, membre de la Chaire « Valeurs et Politiques des Informations Personnelles »
- M. Jacques-François MARCHANDISE, délégué général de la Fing
- Mme Françoise SOULIÉ, conseillère scientifique, Hub France IA

Auditions du 8 janvier 2020

- M. Alain BENSOUSSAN, avocat spécialiste du numérique
- Mme Florence GAULLIER, avocate spécialiste du numérique

Auditions du 4 février 2020

- M. Guillaume BUFFET, Vice-président de Renaissance Numérique et Président de l'entreprise U Change

- M. Etienne DROUARD, Administrateur de Renaissance Numérique et Avocat associé chez K&L Gates

Audition du 25 février 2020

- Mme Salwa TOKO, présidente du Conseil National du Numérique
- M. Gilles BABINET, Digital Champion auprès de la Commission européenne

Audition du 10 mars 2020

- Mme Axelle LEMAIRE, ancienne Secrétaire d'État chargée du numérique
- Mme Caroline ALAZARD, Présidente de Newmeric

Audition du 20 avril 2020

- M. Rémi DUSAUD, Directeur Data & Analytics – Data Privacy chez PwC
- Mme Cécile WENDLING, Head of Security Strategy, Threat Anticipation and Research chez Groupe Axa

Audition du 25 mai

- Mme Sandrine FOUILLE, Directrice RSE France chez Capgemini
- Mme Florence BIGOT, General Counsel, Ethics and Compliance France et Maroc chez Capgemini
- Mme Françoise DURAND, Directrice de la RSE et de la transformation digitale chez Novasep Groupe

Audition du 8 juin

- M. Emmanuel BACRY, Chief Scientific Officer chez Health Data Hub

ANNEXE 4
BIBLIOGRAPHIE

Rapports publics

CNCDH (2018), *Protection de la vie privée à l'ère numérique*, avis

CNNum (2013), *Citoyens d'une société numérique : pour une nouvelle politique d'inclusion* (lien)

CNNum (2016), *Transformation Numérique des PME* (lien)

Conseil d'Etat (2014), *Le numérique et les droits fondamentaux*, rapport annuel 2014

Déclaration de Montreux (2005), *Dans un monde globalisé, un droit universel à la protection des données personnelles et à la vie privée dans le respect des diversités*

Commission européenne (2020), *Livre blanc. Intelligence artificielle, une approche européenne axée sur l'excellence et la confiance*

Défenseur des droits, *Discriminations : accessibilité des logiciels utilisés par les agents publics, des administrations encore en défaut*, étude (lien)

France Stratégie (2018), *Intelligence artificielle et travail*, rapport à la ministre du travail et au secrétaire d'Etat auprès du Premier ministre, chargé du numérique (lien)

INHESJ, *Big data. Entre risque et opportunité*, travaux des auditeurs 2015-2016 (lien)

Syndicat de la presse sociale (2019), *Livre Blanc contre l'illectronisme*, rapport, (lien)

Thieulin B. (2019), *Pour une politique de souveraineté européenne du numérique*, avis du CESE

Villani C. (2018), *Donner un sens à l'intelligence artificielle, pour une stratégie nationale et européenne*, rapport au Premier ministre (lien)

Terra Nova (2020), *Quelle réponse numérique à la crise du Covid-19 ?* (lien)

Mahjoubi M. (2019) *Traçage des données mobiles dans la lutte contre le Covid-19*, note parlementaire (lien)

Fing (2020) *Quel numérique voulons-nous pour demain ?,* Questions numériques, Cahier d'enjeux et de prospective (lien)

FNCCR (2019) *Etude sur le cycle de la donnée dans la conception et la mise en œuvre des services et usages numériques des collectivités territoriales* (lien)

France Stratégie (2018), *Les bénéfices d'une meilleure autonomie numérique,* Antoine Baena et Chakir Rachiq (lien)

France Stratégie (2017), *Mutations digitales et dialogue social*, Cécile Jolly et Antoine Naboulet (lien)

France Stratégie (2018), *Les enjeux des blockchains*, rapport du groupe de travail présidé par Joëlle Toledano (lien)

Kotlicki M. (2015), *Les nouveaux rapports industrie/services à l'ère du numérique*, avis du CESE

Peres E. (2015), *Les données numériques : un enjeu d'éducation et de citoyenneté*, avis du CESE

OCDE, Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel (lien)

Comité Consultatif national d'Ethique (2019), *Données massives et santé : Une nouvelle approche des enjeux éthiques,* Saisine de la Ministre de la Santé en janvier 2017

Longuet G. (2019), Rapport n°7 (2019-2020) de M. Gérard Longuet, fait au nom de la commission d'enquête sur la souveraineté numérique, déposé le 1er octobre 2019 au Sénat

Medef (2019), Approche d'une vision éthique de l'intelligence artificielle par et pour les entreprises – Commission Mutations technologiques et impacts sociétaux

CNIL (2020), Rapport d'activité « Protéger les données personnelles, accompagner l'innovation, préserver les libertés individuelles »

Ministère fédéral allemand de l'Economie et de l'Energie (2019), Le Projet Gaia-X, une infrastructure de données en forme de réseau, berceau d'un écosystème européen vital (lien)

Ouvrages et publications académiques

Ben Youssef, A. (2004). Les quatre dimensions de la fracture numérique. *Réseaux*, 127-128

Chalchat C. (2018), « La technologie, menace ou levier de la conduite du changement ? », *Enjeux numériques*, Annales des mines n°4

Chardel, P. (2014). Données personnelles et devenir des subjectivités. Questions d'éthique. *Sécurité et stratégie*, 17

Charlin L. (2017), « Intelligence artificielle : une mine d'or pour les entreprises », *Gestion*, vol. 42

De Filippi P. (2013), « Une charte éthique pour le big data », *Documentaliste - Sciences de l'Information*, ADBS

Davadie P., Teboul B., Kempf O. (2016), *La donnée n'est pas donnée*, éd. Kawa

Kocher I. (2018), « Le numérique chez ENGIE : quelle organisation pour quel business model ? », *Enjeux numériques*, Annales des mines n°4

Rouvroy A. et Berns T. (2010), « Le nouveau pouvoir statistique : Ou quand le contrôle s'exerce sur un réel normé, docile et sans événement car constitué de corps numériques », *Multitudes*, 40

Roux E. et Jan Krewer J. (2018), « Entreprise libérée et pratiques numériques », *Enjeux numériques*, Annales des mines n°4

Zolynski C. (2015). « Big data : pour une éthique des données », *I2D – Information, données & documents*, volume 52

Chaire Gouvernance et Régulation, Synthèse de conférence « Répondre à la menace cyber par la régulation », Université Paris Dauphine (lien)

Artiguelong M. (2018) « Numérique, vie privée et libertés », *Hommes et Libertés* n°183

Initiatives à l'attention des entreprises

Aproged, Atala, AFCP et Cap Digital, *Charte Ethique Big Data* (lien)

C3D, *Utilisation des données : comment concilier business et éthique en entreprise* ? (lien)

Francony J-M., Modoloni E. (2011), *Ethique et connaissance client dans le domaine de l'e-mailing publicitaire* (lien)

Imagin'able & Utopie (2017), *Data responsable. Livre Blanc, Principes et outils pour une utilisation responsable des données* (lien)

Paris Innovation Review, *Big Data et données personnelles : vers une gouvernance éthique des algorithmes* (lien)

Syntec numérique (2018), CIGREF, *Ethique et numérique, un référentiel pratique pour les acteurs du numérique*

Santé Publique France, *Note d'information relative au traitement des données à caractère personnel – Investigation relative au nouveau Coronavirus (SARS-CoV-2) – COVID-19*

BPI France le Lab (2017), *Histoire d'incompréhension - Dirigeants de PME et ETI face au digital* (lien)

Cooper T., Siu J., Wei K., *Corporate Digital Responsibilty – Doing well by doing good*, rapport Accenture (lien)

CFDT (2016), *Transition numérique, Analyse et propositions de la CFDT* (lien)

Articles de presse

J. Jacob, (2020) « J'appelle à la prudence concernant l'application de visio Zoom », Décideurs Magazine (lien)

Vitard A. (2020), « COVID-19 : La ville de New York interdit aux écoles d'utiliser Zoom et bascule vers Teams », L'Usine Digitale (lien)

Martin J. (2020), « Données personnelles et déconfinement : les points de vigilance de la CNIL », RSE Magazine (lien)

Fabre M. (2020), « Application Stopcovid : le Gouvernement se préparer à pister les français atteints du Coronavirus », Novethic (lien)

Newsletter de Socialter du 7 avril (lien)

Georges B. (2020), « Coronavirus : quelles données, pour quel suivi ? », Les Echos (lien)

Belot L. (2020), « Les données de santé, un trésor mondialement convoité », Le Monde (lien)

Damgé M. (2020), « Faut-il s'inquiéter de Gendnotes, le nouveau fichier de la gendarmerie ? », Le Monde (lien)

Datiche N. (2019), « Classement eCAC40 2019 : et les champions du numérique sont… », LesEchos.fr

Droit du Partage (2017) « Mais au fait, c'est quoi une Plateforme ? »

Hourdeaux J. (2020), « La CNIL s'inquiète d'un possible transferts de nos données de santé aux Etats-Unis », Mediapart https://www.mediapart.fr/journal/france/080520/la-cnil-s-inquiete-d-un-possible-transfert-de-nos-donnees-de-sante-aux-etats-unis

Zielinska A. et Pegny M. (2020), « L'épineuse question des données numériques de santé, The Conversation, https://theconversation.com/lepineuse-question-des-donnees-numeriques-de-sante-131586

L'Usine Digitale (2019), « Développer une stratégie d'échange de données, un enjeu d'avenir pour les entreprises françaises » https://www.usine-digitale.fr/article/developper-une-strategie-d-echange-de-donnees-un-enjeux-d-avenir-pour-les-entreprises-francaises.N904439

Arnulf S. (2013), « Avec l'affaire Prism, la nécessité d'avoir un cloud souverain se pose, selon Fleur Pellerin », L'Usine Digitale

Dèbes F. (2019), « Une page se tourne pour le cloud souverain français », Les Echos

Dèbes F. (2019), « La France cherche son cloud de confiance », Les Echos

Filippone D. (2019), « OVH-Outscale : le cloud souverain vraiment ressucité ? », LeMondeInformatique

Journal du Net (2019), « Jumeau numérique : l'IoT au service de la simulation »

Mann N. (2019), « La France et l'Allemagne veulent créer une infrastructure de données sécurisée », L'Usine Nouvelle

AMSILI S. (2020), « Télétravail : les salariés le plébiscitent mais veulent plus de garde-fous », Les Echos

Articles scientifiques

Basdevant A., « La propriété des donnée, une fausse bonne idée », Optic (lien)

Institut Veolia (2017), « Intelligence artificielle et robotique dans la ville » Numéro 17 (lien)

Renaissance Numérique (2020), « Réguler les plateformes numériques : Pourquoi ? Comment ? »

Autres

BPI France (2017), « Histoire d'incompréhension – Les dirigeants de PME et ETI face au digital » https://www.bpifrance-lelab.fr/Analyses-Reflexions/Les-Travaux-du-Lab/Dirigeants-de-PME-et-ETI-face-au-digital

Arcep (2019), « L'internet des objets », Grand dossier, mis à jour le 10 avril 2019 (lien)

Mon mandat Local (2019), « De la donnée mutualisée aux services : des plateformes de confiance pour le développement du territoire »

Ligue des Droits de l'Homme (2017), « Big data, Algorithmes et risques de discriminations, l'exemple de l'assurance »

Blog de l'Institut Mines-Telecom (2019), « Le partage des données : un enjeu du secteur agricole » https://blogrecherche.wp.imt.fr/2019/09/26/partage-de-donnees-secteur-agricole/

ANNEXE 5
ANALYSE DES DOCUMENTS DE REFERENCE DES ENTREPRISES DU CAC40

La Plateforme RSE s'est appuyée sur les documents de référence publiés par les entreprises du CAC 40 au printemps 2019 (les données portent ainsi sur l'années 2018).

Entreprises du numérique

- Les entreprises du numérique (Atos, Orange, Capgemini) sont bien plus avancées en matière de protection du numérique
- L'entreprise qui n'est pas du numérique et qui est la plus avancée est Kering

Message du DG / Président de Directoire

- Seulement 2 : Atos et Publicis

Exposé Stratégie Développement Durable

- Les enjeux de digitalisation sont parfois mentionnés mais ce n'est pas spécifique aux données personnelles ; excepté pour Atos et Dassault Systèmes
- Le développement durable est parfois mentionné comme un enjeu fondamental ; c'est notamment le cas dans la DPEF ou la partie Sustainability

Investissements et programmes mis en place

- Investissements dans les Systèmes d'Information
- Programme de mise en conformité avec le RGPD
- Certaines entreprises créent une Commission Spécialisée Protection des Données
- De nombreux programmes « éthiques » élargi à la protection des données ont été mis en place entre 2016 et 2019
- Parfois, programme Cyber sécurité

Mention d'un code de conduite, de chartes, de labels d'engagements

- Les Chartes Ethiques de l'entreprise sont souvent étendues à la protection des données
- Normes ISO
- Normes PMI ou PSSI
- Il y a rarement de politiques spécifiques

Mention du RGPD

- 38 entreprises du CAC 40 mentionne le RGPD

Type de données collectées

- Le type de données collectées est rès rarement explicité. La mention la plus courante est celles des clients puis fournisseurs

Risques identifiés

- Cyber attaque / Vol / Compromission de données
- Protection des données
- Non-conformité avec le RGPD, et sanctions encourues
- Failles dans les systèmes d'informations
- Evolution ou renforcement complexe de la Réglementation
- Nouvelles technologies : IOT, voitures connectées ; vues comme de nouveaux défis

Qui gère les données de l'entreprise

- C'est majoritairement le ou la *data protection officer*. Placée au niveau groupe et dans chaque Business unit, la personne est en charge de la mise en conformité avec le RGPD et la protection des données personnelles
- Comité Spécifique pour les données dans certains cas
- Direction des Systèmes d'informations / de la Cyber sécurité
- Direction Ethique / Compliance
- Il est fréquent que plusieurs directions travaillent de concert sur ces questions

Bonnes pratiques

- La partie sur les bonnes pratiques s'avère la plus fournie dans les documents de référence
- Binding Corporate Rules (BCR) : assez régulièrement (politiques de protection des données intra-groupe en matière de transferts de données personnelles hors de l'Union européenne. Elles sont juridiquement contraignantes et respectées par les entités signataires du groupe, quel que soit leur pays d'implantation, ainsi que par tous leurs salariés d'une même entreprise ou d'un même groupe. Les BCR se retrouvent à l'article 47 du RGPD)
- Explicite les actions de mise en conformité RGPD
- Détail des mesures organisationnelles
- Souvent : « *privacy by design* »
- Souvent : systèmes d'alertes et de notifications en cas de faille
- Souvent : système de Contrôle Interne au groupe, due diligence
- Assez souvent : tests d'intrusion
- Assez souvent : *data privacy impact assessment*
- Parfois : cartographie de traitement des données personnelles
- Parfois : gestion du consentement
- Rarement : ne pas vendre les données des clients à de tierces parties
- Rarement : audit relatif à la protection des données
- Rarement : principe de transparence

Valorisation dans la Politique RSE :

- Il y a assez souvent une sous-partie consacrée dans la DPEF / RSE, mais la longueur et la qualité est inégale
- Ça fait souvent doublon avec ce qui est dit ailleurs, notamment dans la partie sur les risques
- La protection des données est davantage perçue comme un risque que comme une opportunité mais il y a des exceptions

Sensibilisation des collaborateurs / Formation

- Une grande majorité ont mis en place une formation au RGPD, et plus rarement à la protection des données
- E-learning majoritaire
- Sensibilisation avec des campagnes d'hameçonnage
- Mise à disposition de règles ou de chartes sur l'intranet
- Rarement : formation des dirigeants / VP / Codir

Politique volontaire de gestion des données personnelles

- Hétéroclite, à voir au cas par cas, ça fait parfois doublon avec les autres processus
- Les mieux-disant (souvent les entreprises du numérique) ont une politique de gouvernance en matière de protection des données

Grille de matérialité

- Beaucoup d'entreprises n'ont pas (ou n'ont pas publicisé) de grilles de matérialité
- Les entreprises qui mentionnent cet enjeu le place en haut à droite
- ACCOR : "Protection des données" → parties prenantes : important /impact sur activité du groupe : important (en haut à droite)
- ATOS : "Protection des données" → parties prenantes : important /impact sur activité du groupe : important (en haut à droite)
- KERING : Pas de matrice mais indications pertinentes tout de même → Probabilité d'occurrence : 2/4 - Impacts :clients, financier, fournisseur, réputation, juridique
- LEGRAND : "Protection des données" → parties prenantes : important /impact sur activité du groupe : important (en haut à droite)
- PUBLICIS : "Protection des données" → parties prenantes : important /impact sur activité du groupe : important (en haut à droite)
- RENAULT : "Protection des données" → parties prenantes : important /impact sur activité du groupe : important (en haut à droite)

Inclusion / Exclusion

- Seule l'entreprise Orange mentionne l'inclusion au début de son document de référence ; dans son modèle d'affaires.

ANNEXE 6
GLOSSAIRE

AIPD / PIA : analyse d'impact relative à la protection des données / *privacy impact assesment*

ANSSI : Agence nationale de la sécurité des systèmes d'informations

ARCEP : Autorité de régulation des communications électroniques et des postes

BCR : Binding Corporate Rules

CCNE : Comité consultatif national d'éthique

CDO : *chief data officer*

CDR: *corporate digital responsibility*

CEO : *chief executive officer*

CNIL : Commission nationale de l'informatique et des libertés

CNNUM : Conseil national du numérique

DDOS : *distributed denial-of-service attack* (attaque par déni de service)

DPO/DPD : *data privacy officer* / délégué à la protection des données

DSI : Direction des systèmes d'information

EDI : échanges de données informatisées / *electronic data interchange*

FING : Fondation internet nouvelle génération

G29 : Groupe de travail article 29 sur la protection des données ; aujourd'hui : Conseil européen de la protection des données

GAFAM : Google Apple Facebook Amazon Microsoft

IA : intelligence artificielle

IaaS : Infrastructure as a service

IdO / IoT : internet des objets / *internet of things*

INRIA : Institut national de recherche en informatique et en automatique

OCDE : Organisation de coopération et de développement économiques

PaaS : *platform as a service*

PGI / ERP : progiciel de gestion intégrée / *enterprise resource planning*

PSSI : Politique de sécurtité des systèmes d'information

RGPD : Règlement général sur la protection des données

RNE : Responsabilité numérique des entreprises

RSSI : responsable de la sécurité des systèmes d'information

SaaS : *software as a service*

TIC : *technologies de l'information et de la communication*

VPN : *virtual private network* (réseau privé virtuel)

RETROUVEZ
LES DERNIÈRES ACTUALITÉS
DE FRANCE STRATÉGIE SUR :

www.strategie.gouv.fr

@Strategie_Gouv

france-strategie

FranceStrategie

@FranceStrategie_

StrategieGouv

Les opinions exprimées dans ce rapport engagent leurs auteurs et n'ont pas vocation à refléter la position du gouvernement.

FRANCE STRATÉGIE

PLATEFORME RSE
Responsabilité sociétale des entreprises

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
Premier ministre

France Stratégie

Institution autonome placée auprès du Premier ministre, France Stratégie contribue à l'action publique par ses analyses et ses propositions. Elle anime le débat public et éclaire les choix collectifs sur les enjeux sociaux, économiques et environnementaux. Elle produit également des évaluations de politiques publiques à la demande du gouvernement. Les résultats de ses travaux s'adressent aux pouvoirs publics, à la société civile et aux citoyens.

FRANCE STRATÉGIE – 20, AVENUE DE SÉGUR – TSA 90725 – 75334 PARIS CEDEX 07 – TÉL. 01 42 75 60 00