LES AVIS DU CESE

RÉPUBLIQUE FRANÇAISE
LIBERTÉ - ÉGALITÉ - FRATERNITÉ
CONSEIL ÉCONOMIQUE SOCIAL ET ENVIRONNEMENTAL

Les éditions des Journaux officiels

Économie et gouvernance de la donnée

Soraya Duboc et Daniel-Julien Noël

CESE 06 FÉVRIER 2021

2021-06

NOR : CESL1100006X

mercredi 10 février 2021

JOURNAL OFFICIEL
DE LA REPUBLIQUE FRANCAISE

Mandature 2015-2021 – Séance du mercredi 10 février 2021

ÉCONOMIE ET GOUVERNANCE DE LA DONNÉE

Avis du Conseil économique, social et environnemental

présenté par

Soraya Duboc et Daniel-Julien Noël

au nom de la

section des activités économiques

Question dont le Conseil économique, social et environnemental a été saisi par décision de son bureau en date du 14 avril 2020 en application de l'article 3 de l'ordonnance no 58-1360 du 29 décembre 1958 modifiée portant loi organique relative au Conseil économique, social et environnemental. Le bureau a confié à la section des activités économiques la préparation d'un avis intitulé : *Économie et gouvernance de la donnée*. La section des activités économiques présidée par Mme Delphine Lalu, a désigné Mme Soraya Duboc comme rapporteure et M. Daniel-Julien Noël comme rapporteur.

Sommaire

Avis

Présenté au nom de la section des activités économiques

L'ensemble du projet d'avis a été adopté au scrutin public à l'unanimité

ÉCONOMIE ET GOUVERNANCE DE LA DONNÉE

Soraya Duboc et Daniel-Julien Noël

Synthèse de l'avis

L'exploitation de la donnée, enregistrement factuel sous forme numérique, offre un champ considérable d'opportunités économiques et de développements et ouvre aujourd'hui la possibilité de multiplier à l'infini les connaissances. Ces évolutions ont rendu plus aigus les enjeux industriels, économiques, commerciaux et génèrent une lutte mondiale implacable, pour la possession et la gouvernance des données et sont susceptibles de donner lieu à des violations aux droits et libertés fondamentales souverains régissant la vie en société.

L'économie de la donnée est en expansion (le marché mondial du *Big Data* représenterait plus de 200 Mds$ en 2020 et le volume mondial des données devrait augmenter de 530 % d'ici 2025, selon la Commission européenne) et offre des opportunités à saisir par les acteurs économiques. Il faut cependant constater que la France comme les autres Etats-membres de l'Union européenne ont pris un certain retard, à titre d'exemple, le stockage mondial actuel des données recourt essentiellement aux entreprises américaines (GAFAM) et chinoises (BATX), ce qui pousse aujourd'hui les États européens à vouloir renforcer leur souveraineté. Cette croissance des données s'est accompagnée de la mise en place de réglementations concourant aux conditions de la confiance, notamment en Europe avec le règlement général sur la protection des données (RGPD), devenu une référence mondiale. Cela n'a pas pour autant éliminé les vulnérabilités technologiques, sécuritaires et sociales liées à l'économie de la donnée.

Aujourd'hui, les défis de gouvernance et de régulation de l'économie de la donnée sont nombreux. Il s'agit tout d'abord d'une gouvernance à consolider notamment au niveau international, aucun organisme international régulateur n'existant. Se pose la question de l'extraterritorialité des lois étrangères (*Cloud Act* américain) et du triple défi des libertés, de la concurrence, de la sécurité. Enfin, on constate que les géants du « Net » viennent concurrencer les missions régaliennes des États comme le démontrent la création de la « cour suprême Facebook »la cryptomonnaie « Libra » de Facebook ou encore les conditions générales d'utilisation, analylisables comme un véritable pouvoir d'écrire la loi. Pour le Cese, il est donc nécessaire de mettre en place une régulation juridique et commerciale et doter les citoyens de capacités d'agir qui pourraient aller jusqu'à consacrer un droit de propriété des données. L'avis constate également que les souverainetés nationales sont remises en question par ces puissants acteurs internationaux, privés et publics, du numérique ; le Cese soutient la création d'un Commissariat à la souveraineté numérique. Le Cese considère que la France dispose d'atouts suffisants mais à renforcer par des coopérations solides au sein de l'Union européenne (UE). Il convient tout d'abord de consolider le cadre politique, réglementaire et normatif existant. À ce titre, l'Europe dispose déjà d'une réglementation de plus en plus harmonisée. Il faut cependant aller plus loin et mettre en place une politique publique de la donnée adaptée aux besoins du 21e siècle. Aujourd'hui, l'ouverture des données est cruciale pour le développement d'une intelligence artificielle et d'activités innovantes. L'avis propose également de renforcer le cadre éducatif, scientifique et technique, et notamment de développer les compétences et qualifications essentielles à l'économie de la donnée. Enfin, le cadre économique et social est à réinventer en permanence (compréhension des modèles économiques en mutation, soutien des pouvoirs publics aux PME, ETI à renforcer et à évaluer, acteurs dans les organisations à convaincre et à outiller).

À ce titre, le CESE a formulé les préconisations suivantes :

Préconisation 1 :

Recourir à la solution de chiffrement des données sensibles par les entreprises dont le code serait détenu par le client et non par l'intermédiaire technique, rendant ainsi impossible le décryptage par les autorités d'investigation.

Préconisation 2 :

Lorsque les autorités américaines en sollicitent la communication, subordonner la transmission des données personnelles à l'accord du client.

Préconisation 3 :

Obliger les hébergeurs à insérer dans leurs contrats des clauses spécifiques, afin de les rendre juridiquement responsables et ainsi mieux protéger les utilisateurs d'une communication à leur insu de leurs données personnelles.

Préconisation 4 :

Instaurer une procédure d'homologation des conditions générales d'utilisation (CGU) au niveau national, afin de vérifier leur compatibilité avec le droit positif.

Préconisation 5 :

Créer un titre V au Code de la propriété intellectuelle intitulé « Droit de propriété sur les données à caractère personnel » et qui serait complété par une disposition d'ordre public rendant inaliénable et incessible les données personnelles, afin de protéger l'internaute.

Préconisation 6 :

Faire adopter une loi triennale d'orientation et de suivi de la souveraineté numérique permettant de rationaliser, d'une part les efforts budgétaires de l'État et, d'autre part de fixer les lignes d'orientation de notre stratégie numérique, en fonction des évolutions et des innovations constatées dans le secteur.

Préconisation 7 :

Renforcer la dynamique du service public de la donnée pour constituer des « communs de la donnée » par un partage plus intense des données publiques et des données privées d'intérêt général.

Préconisation 8 :

Mettre en place, pour les outils basés sur l'intelligence artificielle (IA), une régulation et un cadre normatif européens en cohérence avec les principes de transparence, de traçabilité et de contrôle humain afin que les libertés et les droits fondamentaux soient renforcés. Les travaux de régulation et de normalisation doivent intégrer des compétences en sciences humaines.

Préconisation 9 :

Développer des compétences essentielles pour assurer l'avenir en formant davantage les décisionnels au caractère stratégique des données numériques et en renforçant les compétences et les qualifications de haut niveau en matière de recherche académique.

Préconisation 10 :

Lutter contre la captation des compétences utiles en matière de traitement des données et d'infrastructures matérielles.

Préconisation 11 :

Renforcer, en coopération avec les autres partenaires européens, les choix opérés dans les filières industrielles stratégiques du numérique, avec notamment le développement des infrastructures nécessaires au stockage des données.

Préconisation 12 :

Renforcer les compétences en cybersécurité à la hauteur des besoins d'une économie de la donnée en diversifiant les parcours de formation et en augmentant les effectifs formés (formation initiale et continue) et en renforçant la prise de conscience des opérateurs économiques conventionnels sur les risques dans ce domaine.

Préconisation 13 :

Mobiliser des moyens conséquents pour produire les connaissances théoriques sur les modèles économiques fondés sur la donnée et leurs enjeux, utiles pour les décideurs publics et aux opérateurs économiques

Préconisation 14 :

Engager une culture de l'usage de la donnée et de l'intelligence numérique dans les entreprises, en lien avec le haut fonctionnaire de défense ; renforcer le dialogue social pour mettre en place des outils efficaces de sensibilisation, d'information en amont de déploiement d'outil d'intelligence artificielle; adapter les modalités de coopération et les méthodes de management.

Préconisation 15 :

Responsabiliser les utilisateurs face au risque de consommation excessive de certains services numériques séducteurs et addictifs, puissants aspirateurs de données personnelles.

Introduction

La transformation numérique, le développement des techniques, ont permis d'accumuler puis de consolider une somme considérable de données. Le traitement massif de ces données, leur juxtaposition, leur corrélation ouvrent aujourd'hui la possibilité de multiplier à l'infini les connaissances, sur les sciences, les techniques, mais aussi sur les hommes.

Ainsi le simple cas du traitement des données massives (*Big Data*) aboutissant à des catégorisations algorithmiques des comportements et des préférences des individus, à des possibilités de décisions automatiques doit nous tenir en alerte collectivement sur une nouvelle forme de déterminisme numérique. Celui-ci peut aboutir, si l'on n'y prend pas garde, à une exclusion de certaines catégories sociales, et à l'asservissement d'autres. Il en va donc de notre aptitude à définir notre pacte social, à préserver les droits de l'homme et les libertés fondamentales. Et l'on ne peut s'exonérer d'affronter les problématiques éthiques, juridiques et politiques posées par une économie fondée sur la donnée.

La donnée qui peut être définie comme tout enregistrement factuel sous forme numérique (en fonction du contexte : images, textes, vidéos, caractéristiques physiques d'un objet, résultats d'analyses ou d'enquêtes, etc.) nécessite des équipements matériels et des logiciels pour sa collecte, sa sauvegarde, son traitement et sa réutilisation. L'exploitation de ces données offre un champ considérable d'opportunités économiques et de développements ; elle est cependant susceptible de générer des violations aux droits et libertés fondamentales souverains régissant la vie en société.

La numérisation a engendré de considérables progrès dans la vie quotidienne, par exemple dans l'accès à la culture et au savoir rendu plus facile, généralisé, diversifié, mais aussi dans les relations avec les administrations, la gestion des entreprises, permettant des gains de productivité importants.

Dans le domaine médical, les technologies les plus sophistiquées sont devenues accessibles : imagerie, scanners, miniaturisation de l'électronique pour des interventions chirurgicales de haute précision alliant l'efficacité à la suppression des effets opératoires invasifs, diagnostics connectés. Dans ce domaine si particulier qui touche à la préservation de la vie ou à la réduction de la souffrance, les avancées scientifiques ont apporté des progrès importants.

Ces prouesses technologiques s'accompagnent d'une collecte anonymisée des données de santé par les organismes gestionnaires de l'Assurance Maladie, alimentant la recherche médicale, permettant de développer les thérapies nouvelles ou des médicaments innovants.

Toutes ces opportunités avec lesquelles nous sommes familiarisés depuis plusieurs décennies, ne sont que l'expression visible, positive, d'enjeux industriels, économiques, commerciaux, qui génèrent une lutte mondiale implacable, pour la possession et la gouvernance des données permettant ces réalisations.

La détention de l'information, c'est-à-dire, la capacité de collecter, de croiser et d'analyser ces données confère une forme de pouvoir économique de première part, d'influence de deuxième part, puis de domination, de troisième part.

La gouvernance, selon l'acception commune, est la mise en œuvre d'un ensemble de dispositifs de règles, de normes, de conventions, pour assurer une meilleure coordination entre les différents détenteurs de pouvoirs afin de prendre ces décisions consensuelles.

La gouvernance de la donnée est aujourd'hui éloignée de cette définition idyllique, compte tenu des intérêts divergents et des tensions extrêmes entre les principaux acteurs de cette technologie.

Avant d'analyser les enjeux de la gouvernance de la donnée, il convient d'évoquer les trois défis essentiels qu'elle pose aux sociétés modernes :

- un défi de conscience, de préservation des libertés et des droits fondamentaux et d'intérêt général ;
- un défi de liberté économique et de concurrence libre et non faussée ;
- un défi de sécurité et de souveraineté nationale.

Ces trois défis, dont les conséquences s'interpénètrent sur chacun des aspects de la collecte et de l'exploitation des données, constituent un enjeu global qui appelle à la mise en œuvre de réponses appropriées, afin de sauvegarder les grands équilibres de nos démocraties. S'y ajoute le défi environnemental d'une économie de la donnée ; il constitue un sujet en soi, et sera traité pour partie seulement dans le présent avis ; il nécessite une étude approfondie et rigoureuse des hypothèses de développement technologique et des usages que le format de cet avis ne permet pas. Toutefois, des approches fécondes montrent que le numérique peut être mis au service de la transition écologique[1].

La France et l'Union européenne ont engagé une dynamique pour relever ces défis et préparent des réponses d'ordre institutionnel et socioéconomique en s'appuyant sur leurs atouts tout en se prémunissant de menaces de nature technologique et politique. Elles pourront compter dans l'économie et la gouvernance de la donnée à la condition d'une coopération accélérée dans les domaines critiques qu'a tenté d'identifier cet avis.

[1] Think Tank Fing, *Transitions : l'agenda pour un futur numérique et écologique,* 2019.

I - UNE ÉCONOMIE DE LA DONNÉE EN EXPANSION, DES OPPORTUNITÉS À SAISIR PAR LES ACTEURS ÉCONOMIQUES DANS UN ENVIRONNEMENT CONCURRENTIEL ET INTERNATIONAL

A - Les données dans l'économie et ses mutations : des effets massifs bien que difficiles à quantifier

« Pétrole du futur, lumière du soleil » : les métaphores et les expressions sont nombreuses pour évoquer la place croissante des données dans nos économies contemporaines, ouvertes et mondialisées. Aujourd'hui, l'on n'hésite plus à parler d'une économie de la donnée qui représente « l'économie qui est affectée, directement ou indirectement, par l'utilisation de données ».

Ce que l'on peut constater, c'est que le marché du *Big Data* (applications analytiques, data management) est en plein essor[2] en France et dans le monde entier même si les chiffres d'une source à l'autre sont très différents. Ainsi, le marché mondial du *Big Data* devrait représenter plus de 200 Md$ de chiffre d'affaires en 2020 (projection cabinet IDC 2016) et pèserait aujourd'hui plus de 4 Md€ en France en 2020[3].

La « Stratégie européenne de la Commission sur les données » du 19 février 2020 a identifié neuf espaces communs de données jugés déterminants : l'industrie (utilisation des données à caractère non personnel), le pacte vert (appui aux actions prioritaires sur le changement climatique, l'économie circulaire…), la mobilité (transport intelligent, voitures connectées…), la santé (prévention, détection et guérison des maladies…), la finance (transparence du marché, financement durable…), l'énergie (partage intersectoriel des données, solutions innovantes), l'agriculture (analyse des données de production…), l'administration publique (transparence, application effective du droit…), les compétences (renforcer l'adéquation compétences et marché du travail…).

Cette prise de conscience de l'importance croissante de la donnée est également très forte au niveau des entreprises puisqu'en 2015, 61 % des sociétés françaises

[2] On peut citer, entre autres, Palantir Technologies ainsi que Thalès et ses différentes filiales.

[3] Source : « Un marché en perpétuelle croissance »,12 février 2018, https://www.lebigdata.fr.

estimaient que le *Big Data* était devenu l'un des principaux moteurs de croissance aussi important pour elle que leurs produits et services existants[4].

Lors des auditions organisées au CESE, plusieurs intervenants ont illustré les incidences des données dans l'économie.

Mme Marianne Laigneau, présidente du directoire d'Enedis, a démontré l'impact des données sur l'activité et l'organisation de sa société. Concernant ses missions, Enedis, entreprise régulée de service public a une mission de collecte, de protection et de mise à disposition des données prévue par la loi[5]. Elle est ainsi devenue l'un des leaders du secteur énergétique en matière de données. Cet objectif affirmé de maitrise des données est vu comme un atout et lui a permis de développer des solutions industrielles, de répondre aux attentes des territoires en matière de disposition des données. Aujourd'hui, les 30 millions de compteurs Linky déployés sur le territoire (et 35 millions avant fin 2021) ont vocation à relever plus finement les consommations, à réaliser des interventions clients à distance, à faciliter l'intégration des énergies renouvelables et de la mobilité électrique, à faire de la maintenance prédictive grâce à l'intelligence artificielle. Concernant l'organisation, Enedis comme bien d'autres entreprises, s'est remise en question autour de la donnée et de son traitement et s'est restructurée avec la création d'une direction du numérique. Le fonctionnement de l'entreprise a été revu au prisme des problématiques transverses suivantes : gouvernance, cybersécurité, culture d'entreprise, savoir-faire industriel et évolution des métiers et des compétences…

Dans le domaine de l'agriculture, M. Maximin Charpentier, président de la chambre régionale d'agriculture du grand Est ainsi que de l'association Numagri, entendu en entretien par la section, a souligné que la création de valeur par le numérique était très importante car elle pouvait permettre de répondre aux difficultés de répartition de valeur économique entre l'amont et l'aval des filières. Les données en agriculture sont extrêmement variées et sont des vecteurs d'innovation et de productivité : la météorologie, le machinisme, le stockage, l'usage des intrants, la consommation d'énergie, la traçabilité des produits alimentaires... Pour M. Charpentier, le numérique permet aussi d'aider les agriculteurs à traiter de façon transversale avec les différentes filières aujourd'hui organisées en silos. Une stratégie numérique lui semble donc nécessaire et il importe de l'inscrire dans le cadre du *Green Deal* européen.

Enfin, dans le domaine de la santé, M. Gilles Bonnefond, président de l'Union des syndicats de pharmaciens d'officines (USPO), a rappelé les différents usages de la donnée dans le domaine médical. Par exemple, le dossier pharmaceutique (DP) contient des données qui permettent d'avoir des informations sur l'historique médicamenteux des patients (traitements, changements de dosage d'un médicament), ce qui permet de sécuriser la dispensation des médicaments. Il contient l'historique des médicaments prescrits et/ou délivrés au cours des 4 derniers mois ; la Commission nationale de l'informatique et des libertés (CNIL) a en effet empêché

[4] Chiffres de la société d'études Markess, *Big Data, analytique et gestion des données - Tendances clés*, 2015.

[5] La loi n° 2015-992 relative à la transition énergétique pour une croissance verte (LTECV) du 17 août 2015 et la loi n° 2016-1321 pour une République numérique du 7 octobre 2016 confèrent au distributeur une mission de mise à disposition des données.

d'aller au-delà. Ce DP pourrait être intégré au dossier médical partagé (DMP), déployé depuis 2018, qui a vocation à devenir la « bibliothèque » du patient (résultats d'examens et d'analyses, antécédents, allergies, etc.).

Dans le domaine médical, encore davantage que dans d'autres, se pose très rapidement la question de la propriété et de la protection des données. Ainsi le DMP est actuellement ouvert avec l'accord exprès du patient. Il va être ouvert automatiquement à partir de 2021 mais pourra toujours être supprimé sur demande. Le DMP est en outre destiné à intégrer « l'espace numérique de santé » qui doit être automatiquement créé pour chaque patient, là aussi sauf opposition de ce dernier, à partir du 1er janvier 2022. La crise de la Covid-19 a démontré qu'il faudrait envisager un niveau de partage européen de ces données pour la prévention des épidémies.

Le recours à la plateforme nationale de données de santé appelée *Health Data Hub* (notamment alimentée par le DMP et l'application Stop-Covid devenue TousAntiCovid) et hébergée par Microsoft a cependant mis en exergue les problèmes posés quant à la protection des données notamment quand elles sont hébergées par un prestataire étranger et donc sujettes à un transfert vers ce pays tiers (à l'occasion des traitements nécessitant des infrastructures particulières par exemple), et soumises au droit extraterritorial américain dans le cas des géants informatiques surnommés « Gafam ». La législation américaine, notamment le *USA Patriot Act* de 2001 et le *Cloud Act* de 2018, permet en effet aux autorités publiques nationales (services de renseignement et justice) de réquisitionner les données détenues par les ressortissants américains même en dehors du territoire des États-Unis, ce qui est le cas du Heath Data Hub aujourd'hui hébergé dans des centres de données aux Pays-Bas par les services de cloud Azure de Microsoft.

Outre le monde économique, l'État a également largement ouvert ses données dans une politique d'open data. Il est en effet depuis longtemps producteur mais aussi consommateur de données, pour ses propres besoins et ceux de la société.

Cet accès aux données s'inscrit dans une tradition française déjà longue d'ouverture des données publiques. On peut ainsi rappeler la loi n° 78-753 du 17 juillet 1978 portant diverses mesures d'amélioration des relations entre l'administration et le public.

Au-delà de cette volonté de transparence, l'État a compris que la mise à disposition de données génère de la valeur économique et sociale y compris pour ses propres services et ouvre de nouvelles possibilités dans le domaine des politiques publiques. Le gouvernement français s'est engagé dans une politique ambitieuse d'ouverture et de partage des données. C'est ce que l'on appelle « l'*Open Data* » qui désigne l'effort que font les institutions, notamment gouvernementales, qui partagent la donnée dont elles disposent. Le triple objectif de cette ouverture est d'améliorer le fonctionnement démocratique (transparence et ouverture), de renforcer l'efficacité de l'action publique et de proposer de nouvelles ressources pour l'innovation économique et sociale (les données partagées trouvent des « réutilisateurs » qui les intègrent dans de nouveaux services à forte valeur ajoutée).

Pour concrétiser cet engagement politique, le 18 juin 2013 lors d'un sommet du G8, la France a fait adopter à ses partenaires internationaux une charte pour l'ouverture des données publiques.

Au niveau institutionnel, le décret du 30 octobre 2019 a créé Étalab qui est chargé de coordonner la conception et la mise en œuvre de la stratégie de l'État dans le domaine de la donnée. L'article 14 de la loi pour une République numérique du 7 octobre 2016 lui a confié la mise en œuvre et la gouvernance de ce que l'on appelle désormais « le service public de la donnée » créé afin de *« mettre à disposition, en vue de faciliter leur réutilisation, les jeux de données de référence qui présentent le plus fort impact économique et social »*.

Étalab développe et anime donc la plateforme ouverte des données publiques françaises (data.gouv.fr) qui met à disposition librement l'ensemble des informations publiques de l'État, de ses établissements publics et si elles le souhaitent, des collectivités territoriales et des personnes de droit public ou de droit privé chargées d'une mission de service public. Ce site, lancé en 2011, met à disposition, fin 2020, 35 000 jeux de données et fait l'objet de 450 000 visites par an. Sa mise en ligne a permis une plus grande transparence de l'action publique (vie électorale, budget…), des gains d'efficience pour l'administration publique et la dynamisation du secteur privé. Par exemple, la base de demandes valeurs foncières produite par la Direction générale des finances publiques (DGFIP) a considérablement accru la transparence du marché immobilier. À l'heure actuelle neuf bases de données existent (base adresse nationale, base Sirene des entreprises, code officiel géographique, plan cadastral informatisé, répertoire national des associations…) et font de la France l'un des pays leaders en matière d'ouverture de données publiques[6].

1. Cycle de vie et chaîne de valeur de la donnée - Leur masse croissante, les conditions de leur utilité, leur diversité

Le poids croissant des données dans l'économie entraine de façon concomitante une hausse des volumes échangés, possible grâce à l'amélioration des réseaux d'échange (apparition de la 5G) et au développement de l'Internet des objets. La Commission européenne a ainsi estimé que le volume mondial des données devrait augmenter de 530 % d'ici 2025 en passant de 33 zettaoctets en 2018 à 175 zettaoctets en 2025 (1 zettaoctet correspondant à 10 puissance 21 octets, autrement dit mille milliards de gigaoctets)[7].

Il convient cependant de rappeler que la donnée brute en tant que telle n'a pas de valeur mais qu'elle devient importante à partir du moment où elle est retraitée, analysée, synthétisée. Elle devient significative lorsqu'elle est croisée et combinée avec d'autres données (série de données par exemple). En France, l'administrateur général des données[8] considérait en 2015 que la mise à disposition de données libres et ouvertes produisait de la valeur économique et sociale par le biais de cinq mécanismes générateurs de valeur : la réduction des coûts de transaction (la gratuité des données baisse le coût de transaction), l'innovation (création de nouveaux produits grâce aux données), la réduction des asymétries d'information (les acteurs

[6] Commission européenne, *Open data maturity report 2019,* Open Data Maturity Report 2019 | European Data Portal.

[7] *Stratégie européenne pour les données*, communication de la Commission européenne du 19 février 2020, www.europa.eu, projections pour 2025.

[8] Rapport au Premier ministre sur la gouvernance de la donnée, décembre 2015.

ont les mêmes données), la collaboration et les boucles de rétroaction (partager une information contribue à modifier les comportements).

Les entités économiques doivent cependant savoir tirer parti de l'ensemble des données disponibles. Or, certaines données, comme les données structurées ou semi-structurées, sont encore très peu utilisées à des fins d'analyses, tout en représentant pourtant 40 % des données disponibles dans leurs systèmes d'information. Les données existent et sont disponibles, mais elles sont encore peu exploitées par l'entreprise, faute, le plus souvent, d'une architecture capable de supporter la diversité des données et des solutions technologiques qui permettront d'absorber les volumétries de données dans des conditions optimales de performance et raisonnables de coûts. La donnée nécessite donc un système d'analyse pour être utile.

Enfin, la donnée est diverse. Les classifications sont en effet multiples. On peut ainsi évoquer les « données ouvertes » auxquelles tout le monde a accès et qui peuvent être utilisées et partagées par tous, les « données partagées » entre certaines entités publiques ou privées (souvent contre redevances) et les « données fermées » tenues confidentielles et qui ne sont accessibles qu'à quelques personnes.

Une autre distinction fondamentale, de nature juridique, consiste à distinguer les données à caractère non personnel et celles à caractère personnel. Selon la CNIL, *« une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. Mais, parce qu'elles concernent des personnes, celles-ci doivent en conserver la maîtrise »*. Elles jouissent de protections et de garanties particulières qui seront développées ci-après.

La Commission européenne définit les données à caractère non personnel, par opposition aux données personnelles au sens du Règlement général sur la protection des données (RGPD), en distinguant deux catégories : les données qui dès leur production ne concernaient pas une personne physique identifiée ou identifiable ; les données qui étaient initialement des données à caractère personnel mais qui ont ensuite été rendues anonymes.

Dans le domaine industriel, les données sont notamment au coeur du pilotage des procédés de fabrication et des opérations de maintenance. Les données issues des capteurs installés sur les équipements (internet des objets) et l'arrivée de la technologie 5G modifient en profondeur les modes de production dans les unités de production conventionnelles et bien évidemment dans les usines dites 4.0.

Encadré 1 : « Du pneu réel au pneu virtuel » ou comment se construit la valeur : l'exemple de Michelin[9]

1. L'exemple de Michelin illustre comment une entreprise industrielle a réussi à intégrer la donnée pour faire évoluer son modèle économique : de fabricant d'un pneu réel, Michelin peut mettre à disposition des « pneus virtuels » grâce à sa maîtrise des données et des traitements algorithmiques et d'intelligence artificielle.

[9] Entretien avec M. Yves Caseau, *Group Chief Information Officer* chez Michelin, le 1er juin 2020.

2. La définition des données utiles (internes ou externes) puis leur collecte constitue le premier maillon de la chaîne. Puis vient le stockage (création de base de données interrogée par des requêtes de façon classique) et l'utilisation en flux de données (données nouvelles collectées et traitées pour en générer de nouvelles, clé du succès de Google par exemple).
3. La donnée commence à produire de la valeur selon 4 niveaux croissants : lorsqu'elle est analysée pour comprendre et prédire, lorsqu'elle est traitée par l'intelligence artificielle pour adapter les produits et les services ou les automatiser (exemple : détection d'erreur automatique, maintenance prédictive) ; Exporter le savoir-faire avec des services ; exemple gestion des flottes de camions ou de bus (pneus connectés) permet de franchir un cap supplémentaire dans la production de la valeur économique.
4. Dans le futur, Michelin comme acteur du monde digital pourra proposer à la vente de la « data » comme produits, des données d'usage (par exemple à des constructeurs d'autoroute), ou un « pneu virtuel » comme modèle de calcul.

2. Le stockage des données : une dépendance aux BATX et GAFAM qui pousse les États européens à vouloir renforcer leur souveraineté

Aujourd'hui, l'essentiel des données et notamment les données personnelles des citoyens européens, transitant par internet, utilisent les GAFAM et sont donc sous le contrôle des États-Unis. À titre d'illustration, on peut rappeler que 2,45 milliards de personnes ont un compte Facebook.

La puissance économique et même politique de ces entreprises démontre leur toute puissance sur l'économie de la donnée.

L'acronyme GAFAM (apparu au milieu des années 2000 sous la forme GAFA) est formé par la lettre initiale des cinq entreprises Google, Apple, Facebook, Amazon et Microsoft. Un autre acronyme, BATX, est apparu plus récemment et désigne sur le même modèle que les GAFAM quatre entreprises du Web chinois : Baidu, Alibaba, Tencent et Xiaom. Leur réseau d'influence est pour l'instant moindre mais la Chine a fait bénéficier ces entreprises d'un cadre juridique protectionniste (interdiction de l'usage de Google dans le pays) et dispose de son réseau domestique d'1,4 milliards de consommateurs pour les développer. La croissance annuelle de leur chiffre d'affaires respectif est en 2020 largement supérieure à celle de leurs concurrents américains.

Le niveau de capitalisation boursière de ces entreprises démontre également leur poids économique. Les GAFAM pèsent désormais 4 900 milliards de dollars en Bourse et l'analyste Dan Ives, de la société d'investissement *Wedbush Securities*, anticipe déjà qu'Apple va bientôt devenir la première entreprise à dépasser les 2 000 milliards de dollars. Ils représentent à eux seuls trois fois la capitalisation du CAC 40. Quant aux BATX, leur capitalisation boursière est estimé à 950 milliards de dollars, chiffre moindre mais là aussi en constante hausse.

Par cette domination technique, ces entreprises disposent d'outils pour contrôler nos vies. Près de 80 000 requêtes sont effectuées chaque seconde sur Google, soit 6,9 milliards par jour ; plus de 720 000 heures de vidéos sont mises en ligne quotidiennement sur YouTube[10], et 145 milliards de courriels envoyés… En 2010, le monde ne comptait que deux zettaoctets de données numériques. En 2015, ce chiffre avait été multiplié par six. Le volume mondial de données sera multiplié encore par 3,7 entre 2020 et 2025, puis par 3,5 tous les cinq ans jusqu'en 2035, pour atteindre la somme vertigineuse de 2 142 zettaoctets[11]. Cela pose la question de la capacité de nos sociétés à fournir l'énergie nécessaire pour faire face à cette hausse exponentielle du volume de données échangées.

En profilant chaque utilisateur à travers ses comportements, ces données ne permettent pas seulement de cibler les messages publicitaires ; une fois traitées, elles sont également prescriptrices, dans la mesure où elles permettent de rassembler les avis ou les recommandations des internautes sur une plateforme.

Ce modèle économique soulève de nombreuses questions, comme l'a souligné Mme Angie Gaudion, co-directrice de l'association Framasoft. Il est toxique pour les raisons suivantes : domination technique (oligopole des systèmes d'exploitation Apple et Google sur les smartphones) ; domination économique (poids des capitalisations boursières et des chiffres d'affaires des GAFAM équivalents au PIB de certains pays) ; domination culturelle (normes et vision américaines) ; domination politique.

3. Les incidences des données sur l'environnement

Le recours accru au numérique a des impacts environnementaux. On estime ainsi qu'en 2018, 75 % des Français détiennent désormais un smartphone[12]. La commission de l'aménagement du territoire et du développement durable du Sénat, en juin 2019[13], a estimé que le numérique représentait une source importante d'émissions de gaz à effet de serre (GES) : 15 millions de tonnes équivalent carbone en 2019 soit 2 % des émissions totales de la France. En France, c'est la construction des terminaux et des équipements qui pèse le plus lourd dans les émissions et la consommation de matières premières, alors qu'au niveau international, selon les estimations de *Shift Project*[14], le poste pour la production (ordinateurs, télévisions, smartphones, et autres) représente 45 % en termes de consommation d'énergie finale du numérique, contre 55% pour l'utilisation (terminaux, *data centers*, réseaux).

---

[10] Chiffres Google : toutes les statistiques à connaître en 2020, actualité du digital, site Internet.

[11] « Big Data : le volume de données mondial multiplié par 5 d'ici 2025 », www.lebigdata.fr, 5 décembre 2018.

[12] Insee, *L'économie et la société à l'ère du numérique*, édition 2019.

[13] Guillaume Chevrollier et Jean-Michel Houllegatte, sénateurs, rapport d'information *Pour une transition numérique écologique*, fait au nom au nom de la commission de l'aménagement du territoire et du développement durable par la mission d'information sur l'empreinte environnementale du numérique, juin 2020.

[14] Source : Lean ICT, *The Shift Project 2018*.

En 2040, le numérique pourrait représenter 7 % des émissions de GES pour un coût collectif de 12 milliards d'euros si rien n'était fait. Les principaux responsables de ces émissions sont les terminaux qui engendrent 81 % des impacts environnementaux[15].

Pour le Sénat, la donnée numérique doit être considérée comme une « ressource précieuse ». Les consommateurs ont en effet été encouragés à consommer toujours plus de données grâce à des débits toujours plus rapides (le débit de la 5G sera 10 fois plus rapide que celui de la 4G et celui de la fibre est encore bien plus intense que la 5G). Les forfaits téléphoniques actuellement disponibles ont pour effet de faire baisser le coût unitaire de la donnée avec le volume téléchargé (plus le forfait est important, plus le prix de l'octet consommé décroit). Comme dans le même temps le coût des transmissions baisse, la consommation de données mobiles augmente ainsi de 30 % par an environ, comme indiqué dans le rapport du Sénat de juin 2020, ce qui multiplie aussi le besoin de puissance des data centers dont la consommation énergétique devrait être multipliée par trois en vingt ans[16]. Il s'agit là d'estimations.

Nous assistons ainsi partout dans le monde à une croissance importante de la consommation des données, qui est jusqu'à présent compensée, du point de vue de l'énergie, par une amélioration unitaire des consommations. Mais cette course ne peut pas durer toujours, d'autant que les utilisations ne sont pas nécessairement justifiées. Par exemple, le cas de l'Internet des objets induit des données très redondantes et peu optimisées. Il convient donc de changer de paradigme et de se diriger vers une sobriété en matière de consommation de données.

La crise liée à la Covid-19 a démontré que l'accès à la donnée n'était pas illimité et pose aussi de redoutables problèmes d'inégalités. Le gouvernement, lors de cette crise, a encouragé les géants de la vidéo américains à réduire leur trafic pour faciliter le travail de maintenance et de renforcement des réseaux pendant toute la durée de l'état d'urgence instauré à cause de la pandémie[17].

Le Sénat propose ainsi de consacrer la donnée, dans la loi, comme une ressource nécessitant une gestion durable, mais également de réguler l'offre téléphonique en interdisant à titre préventif les forfaits mobiles avec un accès illimité aux données et en rendant obligatoire une tarification proportionnelle au volume de données du forfait.

B - Des réglementations en place concourant aux conditions de la confiance

La transformation numérique de l'économie a imposé la mise en œuvre d'un cadre juridique. En effet, les technologies de l'information et de la communication sont

[15] Guillaume Chevrollier et Jean-Michel Houllegatte, sénateurs, rapport d'information *Pour une transition numérique écologique*, fait au nom au nom de la commission de l'aménagement du territoire et du développement durable par la mission d'information sur l'empreinte environnementale du numérique, juin 2020.

[16] *Idem.*

[17] Ordonnances prises en application de la loi d'urgence pour faire face à l'épidémie de covid-19, 25 mars 2020.

devenues la base de tous les systèmes économiques innovants et des sociétés modernes. L'utilisation des données électroniques, au cœur de ces systèmes sociaux, doit être encadrée afin de pouvoir se développer dans un environnement basé sur la confiance.

La protection des données est le résultat d'un long processus pour lequel la France est considérée comme l'un des pays leaders sur le plan juridique. L'article 2 de la Déclaration des droits de l'homme et du citoyen de 1789 consacrait la protection des libertés individuelles. De même, en vertu de l'article 34 de la Constitution de la cinquième République, il appartient au législateur de fixer les règles générales applicables aux fichiers nominatifs et aux traitements des données personnelles, celles-ci devant s'attacher à respecter la vie privée qui constitue un droit à valeur constitutionnelle. Avec l'évolution des technologies, il a été nécessaire d'élaborer une loi *ad hoc*, la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, plus connue sous le nom de « loi informatique et libertés » pour réglementer la liberté de traitement des données personnelles. Cette loi française sera source d'inspiration pour d'autres lois nationales mais aussi pour les réglementations européennes. Enfin, il faut mentionner la loi pour une République numérique du 7 octobre 2016 qui a créé de nouveaux droits dans le domaine de l'informatique et des libertés et a permis ainsi aux individus de mieux maîtriser leurs données personnelles. Elle a renforcé les pouvoirs de sanctions de la CNIL et lui a confié de nouvelles missions. Elle a contribué également à une meilleure ouverture des données publiques. Certaines de ses dispositions ont anticipé le règlement européen sur la protection des données personnelles applicable depuis mai 2018.

La mise en œuvre d'une réglementation européenne a également été le fruit d'une assez longue évolution.

Le texte européen majeur est le règlement général sur la protection des données (RGPD) (UE) 2016/679 entré en vigueur dans tous les États membres de l'Union européenne (UE) le 25 mai 2018. Il a permis la mise en place d'une réglementation unique au sein de l'UE, a renforcé la protection des données pour les individus et a aussi créé des conditions de concurrence équitables pour toutes les entreprises actives sur le marché de l'UE, quel que soit leur lieu d'établissement.

Mme Marie-Laure Denis, Présidente de la Commission nationale de l'informatique et des libertés (CNIL) a souligné lors de son audition au CESE que *« l'entrée en application du RGPD a eu des répercussions mondiales et européennes. Il a institué une sorte de marque européenne en matière de protection des données. C'est une sorte de référence mondiale dans les débats autour de la gouvernance et de la protection des données personnelles. Sur le plan international, entre un internet autorégulé et un internet surveillé par des régimes autoritaires, le RGPD est une troisième voie assise sur les droits fondamentaux qui fait des émules (Brésil, Japon, Inde, Californie – qui s'inspirent désormais du RGPD pour adopter leur propre législation) »*.

Ce règlement définit les données à caractère personnel comme « des informations se rapportant à une personne physique identifiée ou identifiable ». Il peut s'agir par exemple d'un nom, d'un prénom, d'une adresse mail, d'une localisation,

d'un numéro de carte d'identité, ou d'une adresse IP. Les règles s'appliquent lorsque les données sont utilisées, conservées ou collectées numériquement ou sur papier.

Le RGPD est un corpus unique de règles du droit de l'Union régissant, d'une part, la protection des particuliers à l'égard du traitement des données à caractère personnel et, d'autre part, la libre circulation de ces données. Il renforce les garanties en matière de protection des données, confère aux citoyens des droits supplémentaires et renforcés, accroît la transparence et rend tous les acteurs du traitement des données à caractère personnel davantage comptables de leurs actes et plus responsables.

L'application extraterritoriale de ce règlement (article 3) est l'une de ses forces. Il s'applique aux entreprises établies en dehors de l'UE qui traitent des données relatives aux activités des organisations de l'UE. Les sociétés non européennes sont également soumises au règlement dès qu'elles ciblent les résidents de l'UE par le profilage ou proposent des biens et services à des résidents européens.

Le RGPD fixe les grands principes suivants pour protéger les données personnelles :

- **le principe de finalité** (le responsable d'un fichier ne peut enregistrer et utiliser des informations sur des personnes physiques que dans un but précis, légal et légitime) ;
- **le principe de proportionnalité et de pertinence** (les informations enregistrées doivent être pertinentes et strictement nécessaires au regard de l'utilité du fichier) ;
- **le principe d'une durée de conservation limitée** (la durée doit être fixée précisément en fonction du type d'informations et ne peut être indéfinie) ;
- **le principe de sécurité et de confidentialité** (le responsable du fichier doit garantir la sécurité et la confidentialité des informations qu'il détient).

Les droits des citoyens sont également renforcés avec l'octroi des droits suivants : droit à l'oubli, droit à la portabilité des données, droit à l'information sur les failles de sécurité.

Dans le domaine de la gouvernance, le RGPD a doté les autorités nationales chargées de la protection des données de pouvoirs d'exécution harmonisés et renforcés et a instauré un nouveau système de gouvernance entre les autorités de protection des données. Pour cela, un comité européen de la protection des données (EDPB) a été créé, composé de représentants des autorités de protection des données de tous les États membres. Il vient compléter l'action du contrôleur européen de la protection des données (EDPS). L'EDPB s'assure que la loi sur la protection des données est bien appliquée par tous les États membres et que les autorités de protection des données coopèrent efficacement.

Le rôle de contrôle et de supervision des autorités nationales, comme la Commission nationale de l'informatique et des libertés (CNIL) en France, a également été renforcé (ex : nouvelles sanctions comme le prononcé d'une astreinte ou le retrait d'une certification ou d'un agrément en cas de violation des règles sur la protection des données, hausse du montant des amendes administratives…).

Enfin, le RGPD donne à l'Union européenne les armes pour lutter efficacement contre les fraudes perpétrées par des entreprises multinationales. Il introduit en effet

des sanctions en cas de violation de ses dispositions. Ainsi, en cas de non-respect du règlement, l'article 83 précise que les violations font l'objet *« d'amendes administratives pouvant s'élever jusqu'à 10 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu »*. De plus, en cas de non-respect d'une injonction émise par l'autorité de contrôle, des amendes administratives *« pouvant s'élever jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu »*.

Les sanctions sont devenues plus nombreuses et leur montant financier plus important.

La DGCCRF relève régulièrement des infractions à l'égard des géants du Net. La condamnation la plus importante a été prononcée en 2019 contre le groupe Apple qui a accepté de payer une amende de 25 millions d'euros dans le cadre d'une transaction pénale. Le parquet avait ouvert le 5 janvier 2018 une enquête préliminaire pour « obsolescence programmée ».

La CNIL, de son côté, prononce désormais des sanctions financières hors norme. Ainsi, en application du RGPD, la société Google LLC a été condamnée, en 2019, à une amende de 50 millions d'euros pour manque de transparence, information insatisfaisante et absence de consentement valable pour la personnalisation de la publicité. En décembre 2020, une amende record a été infligée à Google et Amazon (100 et 35 millions d'euros) pour non-respect des règles sur le ciblage publicitaire des internautes.

Si dans les faits les règles doivent être appliquées uniformément partout en Europe, quelques marges de manœuvre sont cependant laissées aux États membres. Entre autres, ils peuvent décider de fixer l'âge à partir duquel un mineur peut consentir au traitement de ses données personnelles de 13 à 16 ans. En cas de non-respect de la législation par une administration publique, les pays peuvent également choisir d'appliquer ou non des sanctions financières. Notons enfin que toutes les entreprises privées ne sont pas logées à la même enseigne : des exceptions sont prévues pour les petites et moyennes entreprises de moins de 250 salariés. Pour éviter une trop grande lourdeur administrative, elles sont en effet exemptées de désigner ou de recruter un délégué à la protection des données, ce qui est obligatoire dans les autres entreprises. Elles ne sont pas non plus tenues d'avoir un registre de traitement des données.

Enfin, concernant les données non personnelles, il convient de mentionner l'existence d'un règlement européen n° 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. Il vise à assurer le libre flux de données autres que les données à caractère personnel au sein de l'Union, en établissant des règles concernant les exigences de localisation des données, la disponibilité des données pour les autorités compétentes et le portage des données pour les utilisateurs. Pour l'UE, le libre flux des données joue un rôle important dans la croissance et l'innovation fondées sur le numérique.

C - Des vulnérabilités technologiques, sécuritaires et sociales

Malgré les règles qui ont été instaurées aux niveaux européen et national, l'utilisation massifiée du numérique et des données expose les acteurs économiques, les administrations et les citoyens français à des risques de nature diverse. Les vulnérabilités sont d'abord **d'ordre technologique** :

- un nombre significatif de **composants électroniques** stratégiques sont conçus et fabriqués par les États-Unis ou les pays asiatiques. Les Européens, qui possèdent pourtant une industrie solide de semi-conducteurs et des fleurons pour certains composants, notamment automobiles, sont dépendants d'autres continents pour les infrastructures constituant le support du numérique et le savoir-faire industriel nécessaire, ce qui nous fragilise en cas de tension de marché ou d'accident industriel chez nos fournisseurs étrangers ;
- la dépendance à des outils numériques de conception étrangère et extra-européenne, là aussi asiatiques et principalement américains, d'abord à travers l'utilisation massive des GAFAM pour les multiples produits et services numériques qu'ils offrent, y compris dans le cadre de l'activité professionnelle (matériel et logiciels, moteurs de recherche, hébergement de données, réseaux sociaux, plateformes de commerce,…). D'autres éditeurs américains développent des applications largement utilisées dans les organisations françaises (comme Zoom pour la visioconférence, Palantir Technologies pour l'analyse des données).

En outre, il existe de larges incertitudes sur l'utilisation de nos données par ces entreprises ressortissant d'États où la protection juridique des données est bien moins assurée qu'en Europe. En conséquence, les vulnérabilités françaises face au numérique sont aussi de l'ordre de la sécurité publique. M. Guillaume Poupard, Directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), a décrit, lors de son audition par la section des activités économiques du CESE, les trois types de menaces existant sur les données hébergées par les organisations (les données constituent selon lui des *« cibles de choix »*) :

• la menace cybercriminelle : la cybercriminalité est en développement et concerne de plus en plus d'entreprises ; c'est le développement des virus en un modèle criminel. Dans son rapport de mai 2019, la Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (DMISC), du ministère de l'Intérieur, indique que près de 80 % des entreprises ont constaté au moins une cyberattaque en 2018. En septembre 2020, l'ANSSI avait déjà traité 104 attaques par « rançongiciel » depuis le mois de janvier, contre 54 sur l'ensemble de l'année 2019. Les dommages collatéraux peuvent être dramatiques, comme dans le cas de l'attaque du CHU de Rouen en 2019.

• l'espionnage : l'impact économique peut être colossal mais reste inchiffrable (par exemple, comment mesurer le bénéfice d'un accès aux boîtes mails d'une entreprise stratégique ?). On peut ici faire référence aux révélations d'Edward Snowden en 2013 sur l'accès aux données des principaux prestataires et producteurs numériques par les services de renseignement américains. Un développeur français,

Julien Bouquillon, a réalisé une étude en octobre 2020 révélant que 66 % des sites du service public français contiennent au moins un « service externe » (bouton de partage sur les réseaux sociaux, géolocalisation, etc.), dissimulant des mouchards qui envoient les données de consultation du site aux firmes fournisseurs de ces « services » numériques ;

• la menace matérielle : ce sont ici des effets physiques qui sont recherchés : sabotage, destruction. Par le biais d'une attaque informatique, on peut en effet faire exploser une usine ou une raffinerie (et demain menacer le fonctionnement d'objets connectés sensibles tels que des dispositifs médicaux). En France, les « opérateurs d'importance vitale » (OIV) sont régulés depuis 2013 : ils ont l'obligation de faire de la cybersécurité à haut niveau en raison de la sensibilité de leur activité pour le pays. Le nom de ces OIV est classifié mais les secteurs sont définis par la réglementation et donc publics, et répartis en quatre dominantes: humaine (eau, alimentation, santé); régalienne (défense, justice, activités civiles de l'État); économique (énergie, transports, finances), et technologique (industrie,espace, recherche, communications électroniques, audio-visuel et information).

La cybersécurité est cependant globalement insuffisante au sein des entreprises et des administrations françaises qui font face aux exigences techniques et financières élevées pour mettre en place une protection informatique de qualité. Le défi ne vient pas seulement des capacités d'attaques extérieures mais aussi de la naïveté des employeurs et des employés qui interagissent avec leurs machines de façon trop individuelle et instinctive, comme dans la sphère privée, ce qui est incompatible avec la gestion d'une organisation où les données sont plus nombreuses et sensibles. Le développement du télétravail à l'occasion de la crise sanitaire de la Covid-19 rend encore plus fort le besoin d'appropriation des impératifs de la cybersécurité.

M. Poupard a indiqué les orientations promues par l'ANSSI : faire de la cybersécurité un sujet de gouvernance au niveau des comités exécutifs des entreprises (afin de concerner tous les métiers et pas seulement les services informatiques), faire la cartographie des risques dans tous les processus internes, reconstruire du cloisonnement informatique entre activités, limiter l'externalisation et viser la sobriété numérique plutôt que poursuivre dans la voie technophile. Le développement et l'accès aux techniques de cryptographie telles que le chiffrement des données (rendant celles-ci inintelligibles aux utilisateurs non autorisés, voire à l'hébergeur lui-même dans le cas d'un intermédiaire, par exemple de messagerie) ont également été évoqués lors de nos auditions.

L'ANSSI, qui bénéficie d'un effectif relativement faible (600-700 personnes alors que le BSI, l'équivalent allemand, compte 2000-2500 agents), mène une activité d'accompagnement des plus petites structures vers la cybersécurité, et publie des guides de prévention destinés aux acteurs économiques. Mme Denis nous a également indiqué que la Cnil allait renforcer son action dans ce sens, en complément de l'ANSSI. CCI France forme également des référents cybersécurité pour aider les TPE-PME, avec le soutien de l'ANSSI. Celle-ci a par ailleurs développé une activité de certification du niveau de cybersécurité des organisations (réalisée directement ou indirectement par des tiers agréés).

C'est aussi la sécurité individuelle de chaque consommateur ou administré qui peut être directement atteinte par une attaque numérique. La cyberfraude peut notamment frapper par l'escroquerie (techniques de social engineering telles que le hameçonnage/*phishing*) ou l'usurpation d'identité, le pirate informatique se faisant passer par exemple pour une banque par un courriel adressé à un individu. Le nombre de plaintes traitées par la Gendarmerie pour des infractions relevant du champ « cyber » est en constante augmentation ces dernières années (+32 % en 2017, +7 % en 2018) et atteint près de 67 890 faits en 2018 ; plus de 73 % de ces infractions sont des escroqueries liées à Internet. La sécurité et la vie privée d'une personne peuvent aussi être mises en danger par la diffusion de données personnelles sans son autorisation (sur un site internet, sur les réseaux sociaux, ou bien par envoi à un tiers) : sur les 14 137 plaintes reçues par la CNIL en 2019, en hausse de 79 % en cinq ans, 2 287 portent sur la violation de données personnelles.

La cybersécurité doit aussi être développée au niveau des citoyens : le site public cybermalveillance.gouv.fr fait de la prévention vers les citoyens et les petits acteurs économiques et permet de réorienter ceux-ci vers des prestataires techniques de qualité.

Enfin, les vulnérabilités auxquelles nous expose l'envahissement de notre vie quotidienne par le numérique sont d'ordre social. Lors de son audition, le Pr Claude Kirchner (INRIA) a indiqué à la section que les systèmes biologiques et numériques de traitement de l'information interagissaient souvent vertueusement, mais pas toujours : des applications peuvent « hacker » des algorithmes mais aussi notre système biologique de traitement de l'information, avec des conséquences par exemple politiques : la modification numérique d'une photo de visage pour rendre celui-ci plus familier et donc plus désirable (sur le plan politique par exemple) ou bien le scandale en 2015 de l'agence *Cambridge Analytica* récoltant des données individuelles d'utilisateurs de Facebook à leur insu afin de cibler l'envoi de messages électoraux. On passe ainsi du risque cyber au risque démocratique. À terme, on peut aussi redouter le piratage de votes électroniques organisés au niveau professionnel, voire politique.

On peut également citer les risques culturels que présentent les réseaux dits « sociaux » :

- la propagation des *Fake News* (infox) : dans le documentaire *The Social Dilemma* du cinéaste Jeff Orlowski (produit et diffusé par Netflix en septembre 2020), Tristan Harris, ex-designer de Google, déclare que *« les fausses informations rapportent plus d'argent aux entreprises. Sur Twitter, les Fake News se diffusent six fois plus que les vraies. »* ;
- la diffusion publique et la propagation de propos haineux ou insultants, comme on l'observe quotidiennement.

II - DES DÉFIS DE GOUVERNANCE ET DE RÉGULATION POUR UN DÉVELOPPEMENT PARTAGÉ ET SÉCURISÉ DE L'ÉCONOMIE DE LA DONNÉE

A - Une gouvernance à consolider

1. Une gouvernance internationale instable face aux enjeux géopolitiques et économiques

Les enjeux de gouvernance de la donnée dépassent le cadre des économies nationales mais également le pouvoir d'action des États et parfois même celui des institutions internationales. Certains économistes parlent désormais de *« ces géants qui défient les États »*[18], d'autres évoquent des *« entreprises souveraines »*[19]. La puissance numérique alliée à la robustesse économique des grandes mégapoles numériques, constitue une force multilatérale avec laquelle tous les pays du monde doivent désormais compter.

Les déséquilibres de puissance, de contrôle sur leurs activités, d'empiètement sur le pouvoir régalien des États, ne cessent cependant de s'accentuer en faveur des grands majors du Net. Par rapport aux États, ils exercent une emprise sur les utilisateurs que les gouvernements peinent à combattre devant l'absence de règlementations internationales efficaces.

Là réside, sans doute, la véritable menace pour les États, et principalement pour les démocraties occidentales dont les fondements sont parfois remis en cause par des populismes latents.

La constatation la plus frappante réside sans doute dans le fait, que la montée des individualismes qui fragilise le pacte social noué entre les citoyens et le pouvoir politique élu, trouve un refuge dans les services proposés par les grands acteurs, renforçant l'emprise économique de ceux-ci, en affaiblissant simultanément l'autorité des États.

Le rapport de force n'est cependant pas aussi écrasant qu'il pourrait y paraitre, car les démocraties ont des ressources, et des outils de régulation et de coercition pour défendre leur souveraineté, Cependant, une observation de détail permet d'analyser la puissance grandissante qui s'insinue dans des domaines touchant aux missions régaliennes des États.

---

[18] Catherine Morin-Desailly, sénatrice, *L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne*, rapport d'information n° 696 fait au nom de la mission commune d'information « Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet », 8 juillet 2014.

[19] Annie Blandin-Obernesser (sous la direction de), *Droit et souveraineté numérique en Europe*, Bruylant, collection « Rencontres européennes », mars 2016.

Les États peuvent se défendre grâce aux axes traditionnels que sont la mise en place de règles fiscales et l'affirmation de normes protectrices des libertés individuelles et collectives fondamentales.

Face à ces outils régaliens, les risques sont multiples : déstabilisation des économies nationales (violation des règles de concurrence libre et non faussée), concentration des opérateurs, effets multiplicateurs de réseau portant atteinte aux potentiels économiques des Nations.

Ces atteintes sont en outre, amplifiées par la détention de masses de données considérables par des opérateurs susceptibles de renforcer, par les informations qu'ils peuvent extraire, leur efficacité économique. Placés en position de monopole, technologique et de marché, ils interdisent ainsi l'apparition d'entreprises concurrentes.

2. Une absence d'organisme international régulateur

L'utilisation de la donnée numérique constitue un élément sans cesse plus important dans les champs critiques de l'activité humaine. Or, il convient de faire le constat qu'il n'existe à ce jour aucune organisation internationale ayant vocation à procéder aux investigations nécessaires dans ce domaine. Dans des domaines éminemment sensibles tels que le nucléaire, la santé ou l'aviation civile, trois grandes agences dépendant des Nations-Unies (OACI, OMS, AIEA)[20] se sont dotées de moyens d'intervention nécessaires à leurs domaines respectifs de compétence. Il n'existe en revanche aucun organisme similaire, pour ce qui concerne la protection des données et leur utilisation.

S'il existe trois organisations, assurant une gestion technique de l'Internet, par coopération mondiale, leur domaine est limité à mettre en place des standards de fonctionnement (attribution et gestion des noms de domaine, veille technique).

Ainsi, alors qu'une cyber puissance appelle des risques importants pour les libertés, pour l'économie et pour la sécurité, les organismes de régulation mondiale n'ont à ce jour pas réussi à s'entendre sur la création d'une agence contrôlant les activités en ce domaine, et susceptibles d'émettre des règles et d'en assurer le respect, dans un domaine où la circulation et l'exploitation des données revêtent une importance stratégique et économique mondiale.

Pour autant, la gouvernance de la donnée n'échappe pas à toute règlementation. Ainsi, les outils internationaux de régulation, de normalisation et de contrôle portent uniquement sur le fonctionnement structurel des vecteurs de données et non sur le contenu logistique ou la conformité du message aux règles couramment admises par les institutions internationales.

Néanmoins l'effort de normalisation réalisé au niveau européen (RGPD) ne reste pas sans effet sur les rapports mondiaux puisque cent pays (parmi lesquels la plupart des pays africains) ont adopté des dispositions similaires.

[20] Organisation de l'aviation civile internationale (OACI), Organisation mondiale de la santé (OMS) et Agence internationale de l'énergie atomique (AIEA).

3. L'extraterritorialité des lois étrangères : le triple défi des libertés, de la concurrence, de la sécurité

3.1. Le Cloud Act

Les États-Unis ont adopté en 2018, le *Cloud Act*[21], loi fédérale extraterritoriale sur l'accès aux données de communication.

Elle permet aux administrations américaines d'accéder aux données hébergées dans les serveurs informatiques, que ceux-ci soient situés aux États-Unis, ou dans d'autres pays. Cette loi a été votée *« au nom de la protection de la sécurité publique des États-Unis et de la lutte contre les infractions les plus graves, les crimes, et le terrorisme »*. Son objet particulièrement vague n'a trompé personne quant à la volonté des autorités américaines de pouvoir disposer facilement d'un droit de regard sur les données stockées dans les *Clouds*. Les fournisseurs de service peuvent être contraints à livrer toutes les informations détenues sur une simple autorisation d'un juge fédéral ou local, que ces données soient situées aux États-Unis ou à l'étranger, les prestataires de service doivent communiquer *« les contenus de communications électroniques, tout enregistrement, toute information relative à un client ou un abonné, y compris les données personnelles. La personne propriétaire de ces données ne sera pas prévenue »*. Cette loi qui contrevient aux règles élémentaires de protection des données personnelles, protection des données des entreprises et protection des éléments hautement confidentiels stratégique de sécurité stratégique des États a un champ d'application très vaste puisqu'il porte, compte tenu du caractère général de la loi sur les personnes physiques, les entreprises, les États, sur l'ensemble des échanges ou des données, où que celles-ci soient stockées.

Dans son rapport établi à la demande du Premier ministre français, Raphaël Gauvin[22] souligne que : *« Les entreprises françaises ne disposent pas des outils juridiques efficaces pour se défendre contre les actions extraterritoriales engagées à leur encontre »*. Selon le député, les poursuites engagées le seraient pour des motifs économiques et viseraient les grandes entreprises européennes ou asiatiques, les grandes entreprises américaines étant généralement, épargnées de toutes poursuites. Presque toutes les entreprises françaises sont potentiellement concernées par ce régime, en l'état du marché mondial de stockage numérique détenu à 85 % par trois géants américains.

3.2. La loi chinoise sur le renseignement de 2017

La Chine suscite également les mêmes préoccupations après le vote de sa loi sur le renseignement en 2017, dont l'article 14 dispose clairement que : *« les services de renseignements chinois peuvent requérir la coopération de tout citoyen chinois et de toute organisation »*. Les contours très flous de cette loi peuvent faire craindre une application extensive, à l'identique du *Cloud Act* américain.

---

[21] *Clarifying Lawful Overseas Use of Data Act*.

[22] Raphaël Gauvin, député, *Rétablir la souveraineté de la France et de l'Europe et protéger les entreprises des lois et mesures à portée extraterritoriales*, rapport au Premier ministre, juin 2019.

Les craintes des observateurs semblent d'autant plus fondées en raison d'une certaine porosité entre le gouvernement chinois et le géant Huawei. En effet, le fondateur de l'entreprise Ren Zhengfei ne détiendrait que 1,14 % du capital, alors qu'un « Comité Syndical », dont l'élection reste soumise à un vote politique, détiendrait 98,86 % du capital.

Face à de telles menaces, pour les libertés et le respect de la vie privée d'une part, mais aussi pour la protection de nos entreprises, une riposte européenne est indispensable.

Elle est d'ores et déjà portée par le RGPD, qui protège les entreprises ou les ressortissants européens ou que soient stockées leurs données. Il existe dès lors un conflit de lois territoriales qui ne pourrait être jugé que par une instance internationale. Malheureusement aucune juridiction ne semble pouvoir s'emparer de ce type de contentieux.

Préconisation 1 :

Le Cese préconise la solution de chiffrement des données sensibles par les entreprises dont le code serait détenu par le client et non par l'intermédiaire technique, rendant ainsi impossible le décryptage par les autorités d'investigation. Cette solution a été proposée par de nombreux acteurs de la numérisation. Elle a l'inconvénient d'un coût élevé et devrait être accompagnée d'aides ciblées pour rendre la mesure moins pénalisante.

Microsoft s'est engagé par ses représentants en France et en Europe :

- à répondre aux autorités américaines qui les solliciteraient de demander les données aux clients ;
- à avertir le client que l'entreprise qui stocke les données est saisie d'une telle demande, lui permettant ainsi de mettre en œuvre les réponses juridiques, techniques ou judiciaires, en s'opposant à une telle demande.

Préconisation 2 :

Le Cese préconise, lorsque les autorités américaines en sollicitent la communication, de subordonner la transmission des données personnelles à l'accord du client.

Préconisation 3 :

Le Cese préconise d'obliger les hébergeurs à insérer dans leurs contrats des clauses, afin de les rendre juridiquement responsables et ainsi de mieux protéger les utilisateurs d'une communication à leur insu de leurs données personnelles.

La concurrence étant vive entre les acteurs du secteur, il est possible d'atteindre un résultat tangible, avec une telle démarche.

B - Des prérogatives venant concurrencer les missions régaliennes des États

1. Les droits régaliens

Les droits régaliens des États n'ont guère subi de modifications malgré les vicissitudes constitutionnelles et politiques des États. Les quatre attributs principaux des missions régaliennes des États sont :

- de garantir la sécurité et la défense des citoyens et de l'État ;
- de dire le droit et rendre la justice ;
- de lever l'impôt et battre monnaie ;
- d'écrire des lois pour satisfaire au fonctionnement harmonieux de l'État.

Sur ces fondements se retrouvent tous les États de la planète. Les démocraties les ont déclinés pour les intégrer dans leurs constitutions ou dans leurs lois, mais ils demeurent les fondements qui assurent l'équilibre des nations et le dialogue international. Les géants du Net viennent n'ont de cesse cependant que d'élargir leur emprise en s'inscrivant dans une concurrence de puissance en ce domaine.

2. La « Cour suprême Facebook »-Le droit de rendre justice

En mai 2020, Facebook installait sa « Cour suprême » chargée de dire souverainement le droit sur les règles de publication ou de censure des contenus de sa plateforme. Ce « Comité de supervision » pourra être saisi dans le cas où un différend viendrait à exister sur la censure d'un contenu. Il a pour mission notamment d'imposer sa « jurisprudence ». Les co-présidents et les membres éminents de cette instance sont des personnalités indiscutables quant à leurs engagements pour les droits de l'homme.

Ce comité a été financé grâce à un fonds de 130 millions de dollars et Facebook a déjà accepté, dans des documents légaux authentifiables, de se soumettre à l'ensemble des décisions de ce comité. Il s'agit d'un exemple de justice privée.

Ce type de justice prédictive peut être efficace auprès de personnes vulnérables, devant les difficultés d'accès à la justice d'État en raison de son coût et de sa lenteur.

Une telle initiative se heurte au pouvoir des États de rendre la justice, même si elle peut apparaitre comme une forme de régularisation sur les contenus permettant de lutter contre les appels à la haine, au meurtre, à la discrimination…

3. « Libra » ou le privilège de battre monnaie

Facebook lancera en janvier 2021, « Libra » une cryptomonnaie adossée au dollar. La devise permettra, dans premier temps aux utilisateurs des applications Messenger et WhatsApp de réaliser des paiements en ligne.

À l'origine Mark Zuckerberg, le PDG de Facebook avait souhaité adosser Libra à un panier de plusieurs monnaies (Dollar, Livre sterling, Euro, Yen…), mais devant l'hostilité du congrès américain, il a dû revoir ses prétentions à la baisse. L'adossement à une monnaie d'État semble être une digue bien fragile pour protéger

les utilisateurs et les instituts d'émission. Avec plus de 2 milliards de comptes clients, d'utilisateurs ou de terminaux actifs par mois, c'est une formidable puissance financière qui peut concurrencer les monnaies d'État.

4. Les conditions générales d'utilisation : le pouvoir d'écrire la loi

Le caractère transnational des plateformes soumet tous leurs utilisateurs à des conditions générales d'utilisation (CGU) qui ne sont ni discutables, ni partiellement refusables. Elles créent ainsi par une forme d'inversion de la hiérarchie des normes juridiques un nouveau droit international applicable à leurs entreprises, une législation au-dessus des États. Le Professeur Annie Blandin considère que les CGU *« se présentent comme de véritables lois de l'Internet »*[23].

Cette souveraineté étant en France un droit régalien constitutionnel, une telle pratique se présente comme une captation de souveraineté. Il convient, de protéger les usagers contre de telles clauses.

L'ordonnance n° 2016-131 du 10 février 2016 complétée par la loi n° 2018-287 du 20 avril 2018 a inscrit dans la loi, la notion auparavant jurisprudentielle de « contrat d'adhésion ». L'alinéa 2 de l'article 1110 du Code Civil est désormais ainsi rédigé : *« Le contrat d'adhésion est celui qui comporte un ensemble de clauses non négociables, déterminées à l'avance par l'une des parties »*. Les mêmes lois ont créé des dispositions spécifiques à l'article 1171 pour réputer « non écrites » les clauses non-négociables d'un contrat d'adhésion.

Ainsi, les clauses qui enfreindraient les règles protectrices éditées par les États ou par l'Union européenne (UE) pourraient faire l'objet d'une annulation par les tribunaux français.

Préconisation 4 :

Le Cese propose, dans le prolongement de son avis *La coproduction à l'heure du numérique. Risques et opportunités pour le.la consommateur.rice et l'emploi* qu'une procédure d'homologation des Conditions Générales d'Utilisation soit instaurée au niveau national, afin de vérifier leur compatibilité avec le droit positif. L'introduction d'actions de groupe par les personnes intéressées pourra alors être plus aisément engagée pour faire reconnaitre par une juridiction française, la nullité du contrat conformément à la loi nationale.

[23] Annie Blandin-Obernesser, *op. cit.*

5. Le pouvoir d'imposer des règles de sécurité

On pourrait encore citer le *Facebook Safety Check*, qui vient concourir à la sécurité intérieure et qui constitue un outil de solidarité face au danger, mais qui intervient dans le domaine de la sécurité intérieure, dont le monopole est attribué constitutionnellement à l'État

De même, l'établissement d'une cartographie qui se décline en un cadastre, avec *Google Maps*, alors que les délimitations des propriétés ressortissent du pouvoir souverain de l'État[24].

Ainsi, dans les quatre prérogatives régaliennes des États, les grands acteurs du numérique ont, *motu proprio*, pris les initiatives d'assumer, des fonctions régaliennes, qu'elles agrègent au panel des services qu'elles offrent.

La concurrence avec l'État, conduit à son affaiblissement dans l'exercice de ses fonctions régaliennes. En effet, malgré les déclarations de bonne volonté, et parfois les initiatives de régulation ou de coopération avec les États, les grandes plateformes semblent guidées par une pensée d'inspiration « libertarienne » récusant les tutelles étatiques et faisant des acteurs économiques les promoteurs éclairés de la vie en société.

Ce n'est pas une logique d'appropriation du pouvoir des États, mais une logique d'affaiblissement, au service d'une ambition de contrôle, de monopole économique et d'intervention dans l'ensemble des secteurs de la vie en société.

Google décrypte les centres d'intérêts des internautes grâce à des sites consultés ou des vidéos visionnés sur *YouTube* et établit des profils de consommateurs. *Google Maps* enregistre les déplacements à des fins commerciales. Des données personnelles sont stockées, comparées à l'insu des utilisateurs. Une base de données de visages sans autorisation des personnes concernées est enregistrée par Microsoft.

Un nombre incalculable de données sensibles (sujets de discussion, goûts, opinions politiques…), mène à un traçage numérique constant, qui implique une surveillance sur le droit d'aller et de venir, reconnu constitutionnellement.

Sont ainsi mis en œuvre de façon systématique et générale, la constitution de vastes fichiers d'intérêts stratégiques et économiques, rendant possible une surveillance de tous les instants. De véritables capacités de manipulation existent pour les opérateurs et nécessiteraient la mise en œuvre d'un principe de transparence.

L'ampleur et la concordance des moyens ainsi mis en œuvre portent atteinte aux pouvoirs régaliens des États, à la protection des citoyens et au caractère pérenne de nos modèles économiques et sociaux.

[24] Les géomètres-experts utilisent génériquement l'outil pour une aide au bornage.

C - Une nécessaire régulation juridique et commerciale

1. Des citoyens à doter de capacités d'agir – La propriété des données

La protection de la vie privée est reconnue comme un droit fondamental dans toutes les démocraties. Ainsi que nous l'avons rappelé, la Charte des droits fondamentaux adoptée par le Parlement européen, la Commission et le Conseil promeut les valeurs indivisibles et universelles de dignité humaine.

L'article 8 de la Charte dispose que :

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.

La notion de dignité humaine proclamée par les instances européennes fonde le droit imprescriptible d'avoir une vie privée, de contrôler les informations privées concernant chacun, de ne pas subir l'ingérence, dans sa sphère intime de l'État ou de quiconque.

Le Droit au respect de la vie privée est inscrit dans la déclaration universelle des droits de l'Homme (article 12) dans la Convention européenne des droits de l'Homme (article 8) et reprise dans la Charte des droits fondamentaux (article 7).

Ainsi, la vie privée et la protection des données sont reconnues, dans l'Union européenne (UE) comme deux droits fondamentaux à valeur constitutionnelle. Le citoyen européen est donc protégé dans le respect de sa vie privée par l'arsenal législatif et ses déclinaisons judiciaires mis en place dans l'Union.

Cette protection peut cependant apparaître comme illusoire devant l'utilisation qui peut être faite de données librement communiquées ou obtenues après un consentement donné à un contrat d'adhésion.

Pour autant, sur le plan juridique, il n'existe aucun droit de propriété sur les données personnelles.

Le droit de propriété sur les données constitue d'ailleurs un sujet de divergence profonde entre les organes de régulation, les représentants des usagers, et tous ceux qui cherchent à poser des jalons protecteurs sur le chemin de la gouvernance des données numériques.

Pour certains, il devient indispensable de consacrer un droit de propriété sur les données personnelles aux fins de réguler l'environnement et redonner le pouvoir aux citoyens. En revanche, le Conseil national du numérique (CNNum), en mai 2014 a

estimé que ce concept *« renforcerait l'individualisme et nierait le rapport de force entre consommateurs et entreprise »*. Ce même argument est développé par la CNIL qui appelait dans son rapport d'activité 2017 *« qu'un tel droit ne permettrait aucunement d'accroitre le retour vers l'individu de la valeur créée à partir de ses données, mais fragiliserait le cadre historique de protection des données »*. Elle voit dans l'application du RGPD *« une occasion de renforcer les droits d'usage, y compris exercés collectivement, des personnes sur leurs données »*.

Le problème sous-jacent à la reconnaissance d'un droit de propriété sur les données est la monétarisation de celles-ci par les internautes. Un droit de propriété sur leurs données leur ayant été reconnu, ils pourraient alors céder l'usage de ce droit aux plateformes, et pour une somme dérisoire, être ensuite démunis de toute revendication même en cas d'exploitation abusive de données ainsi cédées.

Deux conceptions s'affrontent, fondées sur une même finalité : la protection des données personnelles, la protection de la vie privée et surtout la protection de l'utilisateur qui se retrouve seul face aux plateformes confortées par une technologie et une puissance financière susceptible de résister, même aux États.

La finalité louable, ne doit pas cependant occulter la nécessité de reconnaitre un droit de propriété sur les données.

La Cour de Cassation a déjà en partie tranché la difficulté à plusieurs reprises en condamnant le « vol de données ». Or chacun le sait, le vol est la soustraction frauduleuse de la chose d'autrui. Ainsi, reconnaitre le vol c'est aussi reconnaitre le droit de propriété ! Certes, il s'agit d'une reconnaissance prétorienne, mais le sujet ne pourra pas indéfiniment rester en suspens.

Au-delà de l'organisation économique du marché dans lequel une force économique dominante accepterait de payer une aumône pour utiliser sans restriction les données personnelles, se profilent des revendications qui tendent à placer l'internaute et l'ensemble de la collectivité au centre de l'économie numérique.

Le droit offre des possibilités de reconnaitre le droit de propriété, afin de permettre le contrôle sur l'utilisation des données collectées ou l'interdiction d'en faire usage. La reconnaissance d'un droit de propriété sur les données personnelles, peut en effet s'accompagner de la possibilité de rendre celles-ci incessibles, ou inaliénables, de sorte que l'on ne puisse en faire commerce.

Le débat pourrait donc être ainsi tranché, il mettrait l'internaute dans une situation de sécurité lui ouvrant l'exercice de droits qui lui sont propres : contrôle de l'utilisation, interdiction d'utilisation. Ces actions légitimes pourraient alors être exercées en toute sécurité juridique dans des actions de groupe ainsi que le suggère la CNIL.

Préconisation 5 :

Le Cese préconise la création d'un titre V au Code de la propriété intellectuelle intitulé « Droit de propriété sur les données à caractère personnel » qui viendrait à la suite du titre IV sur « le droit des producteurs de base de données ». Ce texte serait complété par une disposition d'ordre public rendant inaliénable et incessible les données personnelles, afin de protéger l'internaute.

2. La souveraineté numérique en question

La souveraineté en France appartient au peuple qui l'exerce par ses représentants et par la voie du référendum[25]. Elle est réglée par le titre Premier de la Constitution du 4 octobre 1958.

La souveraineté nationale se trouve cependant concurrencée par la concentration quasi monopolistique des acteurs du numérique, par le volume d'informations qu'ils traitent, les services qu'ils offrent et le stockage des données personnelles auxquelles ils accèdent. Les prérogatives quasi régaliennes[26] investies par les géants du numérique font surgir la nécessaire réflexion sur l'affirmation par les États, d'un principe de souveraineté numérique qui préserverait leurs prérogatives et la liberté des peuples.

2.1. Les adversaires invisibles d'une guerre numérique

Les GAFAM, les géants chinois sont visibles, connus, implantés dans des pays qui peuvent, généralement exercer sur eux des mesures d'autorité ou de coercition.

Mais il existe dans le monde des armées « invisibles », déterminées, outillées, susceptibles de porter de graves atteintes à la sécurité intérieure ou aux libertés. La puissance numérique constitue une arme redoutable contre les sociétés organisées.

Elle allie les trois paramètres fondamentaux de l'efficacité en matière de confrontation :

- la puissance qui lui apporte un effet multiplicateur des dégâts causés par une attaque ;
- la vitesse d'exécution qui interdit les parades des systèmes de protection informatique. Lorsque l'attaque est détectée, elle a déjà produit ses effets ;
- la portée des armes numériques qui est planétaire et qui peuvent frapper de petits systèmes ou de grande concentration de données ;
- la saturation des réseaux et le refus d'accès.

Les cyber-attaques se démarquent ainsi par leur efficacité, leur instantanéité, d'autres attaques physiques, détectables et auxquelles il est possible de répondre.

Elles constituent des menaces absolues. Ainsi, l'attaque de *Wanna-Cry* a paralysé des hôpitaux britanniques en 2017.

La puissance numérique acquise de façon frauduleuse ou régulièrement n'entraine pas nécessairement une capacité stratégique d'infliger des dégâts matériels considérables, L'arme numérique donne la puissance de paralyser la cible. Puissance qui s'exerce sans dégât direct majeur et qui est réversible : faire pression sur un corps constitué sur une entreprise, sur un État devient alors un but, une stratégie.

Ainsi, les risques d'une atteinte au fonctionnement régulier des États, c'est-à-dire de fait à leur souveraineté demeure un risque prégnant et permanent.

[25] Article 3 de la Constitution de la V[e] République, 4 octobre 1958.

[26] Voir *supra*.

3. Le débat sur la souveraineté numérique en France

La dimension destructrice des armes cyber est bien réelle et présente une menace constante sur les États. Leur dangerosité provient de leur caractère furtif, d'une capacité d'agir à distance, de cibler l'attaque sans encourir généralement de responsabilité ou de ripostes.

Les services de renseignement des États montent une veille, attentive de chaque instant pour préserver leur sécurité nationale.

La souveraineté numérique, conception post-moderne de la souveraineté, mais sans référence à un territoire géographique délimité, s'entend comme espace constitué par les réseaux, s'appréciant comme un outil de maîtrise, d'influence des entités souveraines[27].

Jusqu'alors, la souveraineté était liée à la notion de « territoire » mais une représentation nouvelle est apparue qui dépasse par ses développements les frontières, les souverainetés nationales et le périmètre d'intervention des Nations.

La notion, jusqu'alors réservée aux réflexions des acteurs et des chercheurs est apparue à la suite des révélations d'Edward Snowden sur les programmes de surveillance américaines, en juin 2013. Dès ce moment, le concept est devenu un enjeu politique et un sujet constitutionnel.

C'est ainsi que fut votée le 7 octobre 2016, la loi pour une République numérique, après un « débat citoyen » qui a permis de recueillir les avis et les positions des acteurs.

La loi qui se voulait résolument progressiste ne fut pas accueillie de façon très enthousiaste. Bien que réalisant un effort d'approfondissement et de regroupement des règlementations, le projet qui s'était donné pour mission de *« doter la France d'une longueur d'avance dans le domaine numérique »*[28] ne dotait cependant pas la France de pouvoirs nouveaux ou d'outils pertinents pour réaliser cet objectif. La défense des droits individuels y était rappelée, mais l'absence d'un dispositif centralisé permettant de maitriser la gouvernance des données et d'assurer une véritable souveraineté numérique de l'État faisait cependant défaut.

Le *Cloud* souverain qui avait été initié en 2009 avec l'adoption du programme Andromède et qui visait à la construction d'un centre national unique d'hébergement de données informatiques n'a pas connu l'effet escompté et n'a pas été, à tout le moins relayé par la loi de 2016, alors que Microsoft annonçait le 3 octobre 2016, après Amazon, l'ouverture de *Data Center* en France pour 2017, afin de pouvoir répondre aux demandes de clients, acteurs publics, souhaitant voir leurs données stockées sur le territoire national. Aujourd'hui, l'Union européenne se doit d'accélérer les investissements indispensables pour un cloud européen souverain. C'est la condition de notre indépendance technologique.

---

[27] Boris Barraud, « L'État territorial face au cyberespace mondial - L'informatique en nuage… de Tchernobyl », Revue Lamy, Droit de l'immatériel, janvier 2016.

[28] Exposé des motifs du projet de loi au nom du Premier ministre par M. Emmanuel Macron, ministre de l'Économie, de l'industrie et du numérique, Assemblée nationale, 9 décembre 2015, p. 3.

D - La création d'un Commissariat à la souveraineté numérique

Le vote de la loi « Pour une République numérique » avait ouvert un vaste débat par les consultations publiques qui l'avait précédé. Ce débat se poursuivit après le vote d'un amendement visant à la création d'un **« Commissariat à la souveraineté numérique »**. L'article 29 de la loi disposait que le Gouvernement remette au Parlement un rapport *« sur la possibilité de créer un commissariat à la souveraineté numérique rattaché aux services du Premier ministre, dont les missions concourent à l'exercice, dans le cyberespace, de la souveraineté nationale et des droits et libertés individuels et collectifs que la République protège »*. Cette idée était reprise lors de l'examen de la loi au Sénat, la haute assemblée insistant alors sur le *« nouveau rôle et la nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet »* et la nécessité de coordonner, les politiques industrielles.

La guerre contre le terrorisme, mais aussi l'urgente nécessité de protéger dans le cyberespace les droits et libertés des citoyens alors qu'une décision de la Cour de Justice de l'Union européenne (CJUE) prouvait que leurs données à caractère personnel étaient exploitées en toute illégalité, appelaient de la part de la représentation nationale une prise de conscience nouvelle sur ces enjeux.

Trois années plus tard, cet engagement n'avait toujours pas été tenu, alors que les rapporteurs avaient été désignés et avaient rempli leur mission. Le rapport au demeurant indiquait dans sa seconde recommandation que *« pour la sphère régalienne, la création d'un commissariat à la souveraineté numérique ne se justifie pas car les structures actuelles apparaissent à même de régler ou faire arbitrer les choix de l'administration »*. Le sujet demeura au carrefour de toutes les interrogations face à la montée en puissance des géants du net et à leur investissement dans une multitude de services annexes.

Dans son rapport au nom de la commission d'enquête sur la souveraineté numérique du Sénat[29], le rapporteur Gérard Longuet, reprend l'initiative d'une création d'un organe d'État fédératif, afin de coordonner les initiatives, appelant à une *« stratégie globale lisible qui fédèrerait les énergies et les efforts »*. C'est au demeurant la première de ses recommandations. Le rapport propose *« un nouveau pilotage et la fédération de tous les acteurs dans le numérique »* en transformant le Conseil national du numérique en un *« Forum institutionnel de concertation temporaire »*. Ayant une existence temporaire Il réunirait les acteurs du public et du privé, administrations et industries, universités et collectivités territoriales. Il donnerait au Parlement et au Gouvernement l'occasion d'arbitrer sur ses principales recommandations, aiguillant ainsi sur le long terme l'action des ministères pour défendre la souveraineté numérique française.

En complément le rapport propose l'élaboration d'une loi triennale d'orientation et de suivi de la souveraineté numérique afin de garantir davantage de lisibilité aux

[29] Gérard Longuet, sénateur, *Le devoir de souveraineté numérique*, rapport fait au nom de la Commission d'enquête sur la souveraineté numérique, n° 7, 1er octobre 2019.

entreprises, de bénéficier d'un pilotage plus rigoureux des innovations et des actions à mettre en œuvre en faveur de la souveraineté numérique française. Le suivi de l'exécution de la loi d'orientation et de suivi de la souveraineté numérique (LOSSN) par le Parlement garantirait la gestion politique de ces choix stratégiques.

Préconisation 6 :

Le Cese est favorable au principe d'une loi triennale d'orientation et de suivi de la souveraineté numérique permettant de rationaliser d'une part les efforts budgétaires de l'État et d'autre part de fixer les lignes d'orientation de notre stratégie numérique, en fonction des évolutions et des innovations constatées dans le secteur.

E - Les régulations

1. La place du droit dans la gouvernance des données

2020 semble marquer une prise de conscience multilatérale des États pour lesquels le concept de souveraineté nationale doit être complété par celui de « souveraineté numérique ». Ils engagent de nouveaux moyens, affichent une volonté nouvelle de reprendre un champ qui leur a échappé lors de la décennie précédente.

Les initiatives se multiplient pour rechercher la pleine gouvernance des données et ne plus dépendre économiquement, technologiquement et juridiquement d'aucune entreprise même si les résultats sont insuffisants. Assurer la protection et lutter contre la captation, des données produites sur son territoire, semble devenu aujourd'hui un enjeu politique.

Cet enjeu est un enjeu non de guerre ou de concurrence, mais un enjeu de régulation.

2. Une position modifiée mais toujours ambiguë des États-Unis

2.1. Des procédures initiées à tous niveaux

Après avoir eu une attitude complaisante, pour les activités à l'étranger des GAFAM, en adoptant notamment le *Cloud Act*, les États-Unis ont pris conscience de l'importance monopolistique des GAFAM. Une série d'enquêtes visant la loi anti-trust ont été ouvertes en 2019, et se poursuivent cette année. Plusieurs instances judiciaires avaient déjà été ouvertes dans des États visant à condamner un abus de position dominante. Désormais c'est l'ouverture d'enquêtes fédérales qui semblent vouloir enrayer la suprématie des GAFAM. De nombreuses initiatives étaient prises.

- En juillet 2019, le Département de la justice qui mettait en place, une commission d'enquête, sur le fondement des lois anti-trust.
- La *Federal Trade Commission* (FTC), gendarme de la concurrence aux États-Unis a confirmé en août 2019 que plusieurs enquêtes fédérales étaient menées. La Commission fédérale du commerce, relayant les inquiétudes du monde économique américain, accuse les GAFAM d'étouffer la concurrence en

rachetant, ou en faisant disparaitre avant leur maturité des petites entreprises du secteur et ainsi limiter l'innovation dans le secteur technologique, substituant ainsi leurs propres intérêts financiers à ceux du peuple américain.

- Un rapport de la Chambre des représentants signé par les élus démocrates (majoritaires de la Chambre des représentants) dénonçait l'attitude désinvolte des patrons de ces géants qui n'ont répondu que superficiellement aux questions posées, et leur manque de coopération pour fournir les documents demandés, nécessaires à l'enquête ont posé le véritable enjeu de cette procédure parlementaire : réguler ou démanteler.
- Des procédures et des enquêtes fédérales sont également ouvertes dans près de la moitié des États de l'Union (48 États).

Ainsi, de toute part, les pouvoirs publics américains, fédéraux ou locaux, se mobilisent pour rétablir une forme d'éthique dans ce dérèglement économique. Si l'argument économique domine, les groupes de pressions et les associations de défense des consommateurs se mobilisent depuis très longtemps sur le sujet de la protection de la vie privée des internautes, ou sur la passivité des plateformes à l'égard des discours de haine ou des propagandes racistes.

Le démantèlement étant évoqué comme une sorte d'arme dissuasive, la priorité pour les parlementaires semble être de promulguer de nouvelles lois restrictives empêchant ces entreprises d'imposer leurs propres produits et ainsi de fournir un avantage concurrentiel aux plateformes qu'elles contrôlent.

2.2. Des effets limités à attendre des lois Anti-trust

Pour les GAFAM, le spectre du démantèlement demeure une menace irréelle qui entraînerait le chaos dans le monde des plateformes et des technologies numériques. Le secrétaire d'État français au numérique, monsieur Cédric O a déclaré que *« même si Facebook était démantelé en 10 entités différentes, il resterait toujours 240 millions d'utilisateurs dans chaque entité »*. Cette remarque qui caractérise parfaitement l'enjeu des régulations, met en évidence la puissance de géants économiques.

Cette menace semble d'autant plus illusoire que l'esprit de Milton Friedman est toujours vivace au cœur de l'économie américaine et que les tensions internationales incitent le congrès à la prudence. Adversaire de l'intervention de l'État dans l'économie, Friedman avait jeté les jalons de la pensée « libertarienne » voulant écarter la main de l'État dans toutes les activités économiques. Aussi, les adversaires d'une intervention publique, se mobilisent. Peut-être moins pour sauver la suprématie des GAFAM que pour imposer leurs visions de l'économie. Leurs arguments ont l'avantage du pragmatisme : la recherche dans de nouvelles technologies exige des moyens importants, des investissements en hommes et en matériel, et, souvent ces investissements se font sans retour immédiat de dividendes. Découper les géants américains, diviser leur potentiel économique de recherche et d'innovation reviendrait alors à affaiblir la capacité de recherche de l'industrie américaine, à limiter ou réduire son avance technologique.

L'argument a d'autant plus de poids que la suprématie américaine n'est pas indéfiniment acquise.

2.3. Les dangers chinois et russes

Un tel découpage qui interviendrait en application des lois d'équilibre de la concurrence, qui fait figure de théorie économique première aux États-Unis, révèlerait un véritable danger dans le contexte international actuel de tension.

La question primordiale, aux yeux du congrès et de dirigeants américains, reste l'attitude conquérante de la Chine et la puissance numérique souterraine de la Russie.

Le gouvernement chinois est-il prêt à démanteler Alibaba, Tencent ou Baidu ? Poser la question est déjà en affirmer la réponse négative.

Les tensions avec le géant asiatique permettent aux GAFAM, de rester sereins face aux enquêtes parlementaires, et aux condamnations.

La Russie est également un facteur intense de réflexion. Dotée d'une capacité numérique importante elle intervient peu dans le domaine économique. Elle reste cependant une puissance en sommeil dans le cyberespace où la sécurité vitale des États impose une veille minutieuse et continuelle.

Ainsi les grands principes se heurtent-ils à la défense pragmatique de l'avance technologique des États-Unis sur le monde numérique.

Il convient sans doute d'espérer des enquêtes en cours et des procédures ouvertes un assouplissement des positions des GAFAM, sur le plan concurrentiel d'une part, et sur le plan du respect de la vie privée d'autre part, il ne faut en attendre guère plus.

Ces victoires seront cependant des avancées significatives pour aboutir aux indispensables régulations d'un marché débridé.

F - L'Europe : le temps des régulations

Si la souveraineté numérique s'est imposée en France comme un thème majeur de réflexions et de propositions, l'Union européenne vient de faire de ce sujet l'une de ses priorités.

La Commission, après avoir eu une attitude timorée, malgré les révélations d'Edward Snowden en 2013, s'est engagée dans une nouvelle stratégie européenne pour les données.

1. La stratégie européenne des données.

La Commission, issue du scrutin européen de juin 2019, a affiché des ambitions nouvelles et multiplie les initiatives pour réguler le numérique et pour poser les principes d'un ordre juste, centré sur la sauvegarde des valeurs humanistes.

Dans une communication officielle au Parlement européen, au Conseil, au Comité économique et social européen (Cese) et au Comité des Régions (CdR), la

Commission européenne a fait part, le 19 février 2020, de sa **« stratégie pour les données »**[30]**.**

La vision de la Commission découle des valeurs fondamentales de l'Union, des droits fondamentaux et de la conviction que l'être humain est et doit rester au centre des activités économiques.

L'Union européenne se fixe pour objectif de devenir un modèle de premier plan pour une société à laquelle les données confèrent les moyens de prendre les meilleures décisions tant dans les entreprises que dans le secteur public.

Après avoir évoqué longuement les finalités humaines et sociales d'une appropriation vertueuse des données, la Commission évoque de façon générique les déséquilibres en termes de pouvoir de marché, tant dans la concentration *« dans la fourniture des services en nuage et d'infrastructures de données que de déséquilibres en ce qui concerne l'accès aux données et leur utilisation par les PME »*. En insistant sur le « pouvoir de marché » on avance dans l'affirmation de régulations à venir.

La Commission insiste également sur la nécessaire *« interopérabilité des données »* que les utilisateurs doivent pouvoir exercer sans entrave.

La stratégie présentée le 19 février 2020, présente une société européenne soutenue par des solutions numériques qui placent les citoyens au premier plan, ouvrent de nouvelles perspectives aux entreprises et encouragent le développement de technologies fiables pour promouvoir une société ouverte et démocratique et une économie dynamique et durable. La présidente de la Commission européenne, Mme Ursula von der Leyen, a affirmé vouloir *« présenter les ambitions de l'Europe, dont la stratégie englobe des domaines aussi variés que la cybersécurité, les infrastructures critiques, la formation numérique, les compétences, la démocratie et les médias, l'ouverture, l'équité, la diversité, la démocratie et la confiance »*.

2. L'offensive de la Commission pour renforcer la lutte contre les monopoles numériques

2.1. La protection du bien-être des consommateurs demeure un droit affirmé par l'Union

Les traités de l'Union définissent parfaitement le principe de « préjudice des consommateurs »[31] comme facteur déclenchant de la répression des pratiques abusives. Ils permettent cependant des exemptions si *« une partie équitable du profit qui en résulte »* est transmise aux *« utilisateurs »*. Le contrôle des concentrations est également défini dans les traités.

La jurisprudence de la Cour de Justice de l'Union européenne (CJUE) a mis en œuvre un droit à réparation des victimes de pratiques anticoncurrentielles[32]. Ces décisions juridictionnelles ont permis la publication de directives favorisant les droits

[30] Commission européenne, communication *Stratégie européenne pour les données,* COM(2020) 66 final, 19 février 2020. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020DC0066&from=EN.

[31] Traité sur le fonctionnement de l'Union européenne (TFUE), article 101(b).

[32] Arrêts *Courage CJUE, 20 septembre 2001, Courage Ltd. C. Bernard Crehan et Bernard Crehan c. Courage Ltd. et autres, aff. C-453/99* et *Manfredi CJUE, 13 juillet 2006, Manfredi, aff. Jointes C-295-298/04*.

ainsi reconnus. La directive du 26 novembre 2014 a ainsi réglementé les dispositions régissant les actions en dommage et intérêt en droit national pour les infractions aux dispositions du droit de la concurrence des États membres et de l'Union européenne.

Cette construction prétorienne d'abord, législative ensuite, ne fait que décliner les traités qui font de l'exigence de la protection des consommateurs une composante de la définition et de la mise en œuvre des politiques de l'Union[33].

Cependant, l'intervention du droit et de la jurisprudence, ne peuvent pallier une absence de politique volontariste. Le bon fonctionnement du marché et la compétitivité des entreprises européennes ne constituent pas, en l'état actuel des traités, un objectif du droit européen de la concurrence. Une réécriture de ceux-ci devait donc être faite avec l'apparition des géants du numérique, qui ont faussé, par ce gigantisme et par les moyens qu'il procure, les équilibres du marché européen du numérique.

Ainsi la nouvelle Commission après avoir défini sa stratégie pour le numérique, et sans doute aussi, constaté les formidables profits enregistrés par les GAFAM durant la crise de la Covid-19, a lancé une offensive au printemps 2020 aux fins de réviser les textes régissant la concurrence et principalement la directive de 2000, intervenue alors que l'Internet était balbutiant.

2.2. Les tentatives de nouvelles règlementations lancées par la Commission

Ces initiatives interviennent, alors que l'Organisation de coopération et de développement économiques (OCDE) qui avait lancé en 2013, le projet BEPS (érosion de la base d'imposition et transfert des bénéfices) avait réuni un cycle de travail pour adapter le système fiscal international, face aux stratégies de contournement de l'imposition de certaines multinationales. Les lignes directrices de cette adaptation seraient de :

- définir le lieu et la base d'imposition pour le paiement de l'impôt sur les bénéfices ;
- l'instauration d'où taux d'imposition minimal pour les multinationales.

Les travaux n'ont pas à ce jour abouti.

2.3. Les initiatives de la France.

(a) L'initiative de régulation des plateformes numériques.

Le 25 février 2020, la France avait pris l'initiative en créant un groupe de travail réunissant des experts et des représentants des États, membres intéressés par la protection de l'espace numérique européen, qui se donnait pour mission de calibrer des propositions efficientes sur les notions « d'abus de position dominante » et « d'infrastructures essentielles » et d'amplifier nos efforts pour développer une vision stratégique au service de l'innovation de rupture et des technologies critiques.

(b) L'initiative française d'une taxe sur les GAFAM

Le levier fiscal, demeure l'un des piliers structurant de la souveraineté de l'État et l'outil le plus efficace pour atteindre les plateformes en position de monopole.

[33] TFUE, article 12.

Les difficultés sont cependant nombreuses pour atteindre un objectif pertinent et admissible, sur le plan des règles internationales. En effet, l'importance des actifs incorporels de ces sociétés, rend leur valorisation comptable aléatoire, la définition de la valeur ajoutée taxable en est de ce seul fait difficile. À cet inconvénient s'ajoute la localisation de la création du service taxable et le découpage qui peut être fait entre lieu de création de la valeur et lieu de fourniture du service.

Les règles fiscales traditionnelles, tant nationales qu'internationales ne sont plus adaptées à la taxation des profits de l'économique numérique.

Le levier de la taxation d'office au terme d'une procédure contentieuse n'offre qu'une alternative médiocre, en raison d'une part de sa lourdeur et d'autre part, de l'incertitude quant à l'adéquation du montant taxé et la réalité du profit réalisé. Il en résulte un « chiffre noir » qui donne à penser aux économistes que la taxation est sans doute dérisoire face au profit réalisé.

La France s'est dotée depuis 2019, d'une taxe sur les services numériques (TSN) qui s'applique au taux de 3 % sur le chiffre d'affaires réalisé au titre de la fourniture en France de services d'intermédiation numérique ayant réalisé plus de 25 millions d'euros au titre de la fourniture de tels services en France. Pour les sociétés françaises soumises à l'impôt sur les sociétés, cette taxe sera déductible des bénéfices imposables. La perception en avait été que suspendue *« le temps que les négociations avec l'OCDE aboutissent »*. Après l'échec des négociations au niveau européen, la taxe dite « GAFAM », va finalement être recouvrée dès décembre 2020.

Les mesures de rétorsion annoncées par l'administration Trump, annoncent cependant de possibles rétorsions dans d'organisation des échanges commerciaux

La conjonction des ripostes, aux États-Unis, en Europe et en France indique clairement que les États ont pris pleinement conscience des dangers que la situation de quasi-monopole de certaines plateformes leur faisait courir.

3. Un dialogue social européen sur la manière d'accompagner au travail la transformation numérique

Des négociations engagées en juin 2019 entre la Confédération européenne des syndicats (CES) et Business Europe, le Centre européen des employeurs et entreprises fournissant des services publics (CEEP) et le SMEunited ont abouti le 22 juin 2020 à un accord européen sur la digitalisation qui doit être transposé dans notre pays. Pour le CESE, cette transposition est urgente et devrait intervenir dans le courant de l'année 2021. Cet accord établit un cadre européen sur le déploiement des technologies numériques au travail et pense la transformation numérique à partir de l'humain. Il met notamment l'accent sur deux points :

3.1. L'intelligence artificielle (IA) et le maintien du contrôle humain

Les systèmes d'IA fiables doivent être légitimes, justes, transparents, sûrs, sécurisés, conformes à toutes les lois et réglementations applicables, ainsi qu'aux droits et libertés fondamentales, avec les principes de non-discrimination. Ces systèmes doivent respecter des normes éthiques reconnues, veiller au respect des droits de l'Homme et être conformes aux valeurs définies par la charte européenne des droits fondamentaux de l'UE. Ils doivent être fiables et durables techniquement,

dans le domaine social car même avec les meilleures intentions, les systèmes d'IA sont susceptibles de causer des préjudices involontaires.

3.2. Le respect de la dignité humaine et la surveillance

La transparence, une collecte minimum de données personnelles, ainsi que l'élaboration de règles claires sur le traitement de celles-ci, limitent les risques de contrôle intrusif et d'utilisation abusive des données personnelles.

Les règles définies par le RGPD sur le traitement des données personnelles des travailleurs dans le contexte professionnel, doivent être respectées.

A cet effet, les partenaires sociaux liés juridiquement par cet accord, rappellent l'article 88 du RGPD qui mentionne la possibilité de prévoir, au moyen de conventions collectives, des règles plus spécifiques pour assurer la protection des droits et libertés en ce qui concerne le traitement des données à caractère personnel des salariés dans le cadre des relations de travail.

III - DES ATOUTS SUFFISANTS EN FRANCE, MAIS À RENFORCER PAR DES COOPÉRATIONS SOLIDES AU SEIN DE L'UE

La complexité de la question des données et les ramifications en lien avec les aspects nombreux du numérique nous conduisent à élaborer des choix dans cet avis. Ainsi le parti pris est le suivant : sans entrer dans des considérations trop générales, il s'agit de proposer des solutions opérationnelles de court-moyen terme dans l'optique de résoudre des problèmes de long terme.

Comme développé précédemment, l'enjeu global de toute stratégie en matière de données et de gouvernance est de créer un écosystème institutionnel et technologique autonome, dans lequel les entreprises pourront se développer et où, la place des citoyens sera consolidée. Face aux moyens déployés par les États-Unis[34] et par la Chine et à leur avance dans le domaine du digital, on ne peut que constater que le niveau pertinent pour être concurrentiel avec l'écosystème en place est nécessairement européen.

En effet, à ce jour aucun secteur ni aucune entreprise en Europe ne peut peser face aux États-Unis et à la Chine. Cependant, la France en tant qu'État membre engagé de longue date dans la construction de l'Union européenne, peut s'appuyer sur ses atouts et les synergies avec d'autres États membres au rang desquels en premier lieu l'Allemagne. L'exemple emblématique de coopération est à ce jour le projet GAIA-X.

[34] Recherche publique depuis les années 1960, puis privée depuis l'avènement des GAFAM.

La confiance des citoyens et des acteurs économiques n'est cependant pas encore acquise, comme la présidente de la Commission européenne, Ursula von der Leyen, en dressait le constat dans une tribune intitulée « *Façonner l'avenir numérique de l'Europe* »[35]. Le problème est peut-être moins de faire confiance, que de disposer d'institutions et d'outils dignes de confiance. Etre digne de confiance, selon les travaux de la philosophe Onara O'Neill (professeur honoraire de philosophie à l'université de Cambridge, Grande-Bretagne) suppose tout à la fois : honnêteté, compétence et fiabilité (*honesty*, *competence and reliability*)[36]. Comme les travaux récents d'économistes l'ont aussi montré, la confiance est la condition nécessaire à toute coopération.

A - Le cadre politique, réglementaire et normatif : renforcer l'existant

L'enjeu est donc de créer un environnement attrayant, juridiquement prévisible où les données à caractère personnel et non personnel, de haute qualité sont échangées pour stimuler la croissance tout en limitant l'empreinte environnementale.

1. Un espace européen digital bénéficiant d'une réglementation de plus en plus harmonisée : un avantage comparatif en devenir

Au sein de l'Union européenne, un certain nombre de stratégies et d'initiatives réglementaires ont été prises par la Commission européenne pendant la mandature 2014-2019 pour combler le retard pris en matière de réglementation du numérique.

En février 2020, la Commission a proposé une vision d'ensemble sur cette question en publiant la « Stratégie européenne pour les données »[37] complétée par le livre blanc pour l'intelligence artificielle[38], ainsi qu'un cadre législatif générique pour la gouvernance des espaces européens communs des données.

Cette stratégie s'est fixé comme objectif la mise en place pour fin 2020 d'un cadre législatif pour la gouvernance des espaces européens communs des données. Le

[35] Communiqué de presse « Façonner l'avenir numérique de l'Europe : la Commission présente des stratégies en matière de données et d'intelligence artificielle », Bruxelles, le 19 février 2020.

[36] La confiance est une ressource précieuse, dans des situations critiques (crise sanitaire notamment). Voir Roberto Frega, « Les dimensions de la confiance », *Revue Esprit*, n° 468, octobre 2020 et Éloi Laurent, *L'économie de la confiance*, Éditions La Découverte, 2019.

[37] Commission européenne, communication *Stratégie européenne pour les données,* COM(2020) 66 final, 19 février 2020. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020DC0066&from=EN.

[38] Commission européenne, livre blanc *Intelligence artificielle - Une approche européenne axée sur l'excellence et la confiance*, COM(2020) 65 final, 19 février 2020. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf.

projet de *Governance Act* dont l'objectif est de faciliter le partage des données prévoit dans sa version du 25 novembre 2020 que les données sensibles devront être traitées soit au sein d'une structure publique, soit dans une entité privée basée en Europe de façon à garantir l'application du cadre réglementaire approprié aux données européennes. Les discussions sur le plan juridique sont engagées quant à la compatibilité de ce type de disposition avec les accords OMC de libre-échange.

Le renforcement de la stratégie des données au niveau européen dans un contexte politique et réglementaire porteur ne peut qu'inciter la France à saisir cette opportunité pour continuer à développer cette économie de la donnée. Dans cette perspective, en juin dernier, le Premier ministre a ainsi confié au député Éric Bothorel une mission relative à la politique publique de la donnée dont le rapport a été remis le 23 décembre 2020[39].

2. Pour une politique publique de la donnée en phase avec les besoins d'une démocratie et d'une économie du 21e siècle

2.1. Une politique d'ouverture des données publiques par défaut : un principe toujours valable, mais à affiner

Parmi les pays pionniers, la France s'est engagée dans une politique affirmée d'ouverture des données publiques (droit d'accès et de réutilisation des documents administratifs dans le cadre de la loi « CADA » du 18 janvier 1978, ouverture des données publiques avec la Loi n° 2016-1321 du 7 octobre 2016 « pour une République numérique »). Ces bases de données publiques sont constituées à partir des ressources propres des établissements producteurs et souvent en partenariat avec différents acteurs publics ou privés. Dans le cas du Répertoire opérationnel des métiers et des emplois (ROME), par exemple, Pôle Emploi a fait appel à différents acteurs tels que des entreprises, branches et syndicats professionnels, AFPA…Comme les administrations, certaines entreprises publiques (comme Enedis, voir partie I), ou les organismes de recherche ont également des obligations légales à l'ouverture de leurs données.

Mais toutes les données produites par les administrations, les organismes de recherche publique et les entreprises publiques n'ont pas vocation à être ouvertes sans discernement[40]. Dans le cas d'Enedis, les données à caractère personnel, et les informations commerciales sensibles (données d'un producteur ou d'un fournisseur par exemple) ne sont pas partagées. Une équipe « gouvernance de la donnée » est en charge des 200 types de données collectées et traitées par Enedis. Cet exemple illustre les ressources nécessaires pour répondre à la politique d'ouverture des données.

S'agissant en particulier des données issues de la recherche publique, les pratiques de partage ont profondément évolué au cours des dernières années,

[39] Mission confiée par le Premier ministre à Éric Bothorel, député, *Pour une politique publique de la donnée*, décembre 2020. https://www.gouvernement.fr/remise-du-rapport-sur-la-politique-publique-de-la-donnee-des-algorithmes-et-des-codes-sources. https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2020/12/rapport_-_pour_une_politique_publique_de_la_donnee_-_23.12.2020__0.pdf.

[40] Comité consultatif commun d'éthique pour la recherche agronomique, INRA-CIRAD, *Avis 8 sur les enjeux éthiques et déontologiques du partage et de la gestion des données issues de la recherche*, février 2016.

caractérisées par un accroissement des exigences liées à l'accessibilité aux données et à la reproductibilité des résultats. Le développement de plateformes pour stocker et partager des jeux de données de toutes natures a facilité l'ouverture et la circulation des données de recherche. Leur ouverture doit répondre aux principes dits « FAIR » (*Findable*, *Accessible*, *Interoperable*, *Reusable*) qui définissent un partage de données faciles à trouver, accessibles, interopérables et réutilisables.

Cela implique trois exigences : documenter (métadonnées), standardiser la structure et le vocabulaire, mettre à disposition des API (interfaces de programmation applicative), et gérer les droits d'accès avec des profils adaptés aux différents usages, dont des usages gratuits et anonymes.

Il apparaît donc que l'ouverture des données nécessite des compétences, des infrastructures matérielles qui ne sont pas nécessairement à la portée de toutes les entités publiques, telles que les collectivités locales par exemple. Si des partenariats avec le secteur privé restent possibles, les éventuels candidats sont peu incités à investir dans des données qui pourront être acquises gratuitement par leurs concurrents.

Par ailleurs, les besoins de professionnels qui fondent leurs activités et leurs innovations sur les données publiques, notamment pour entraîner les algorithmes utilisés dans des outils d'intelligence artificielle ont des besoins spécifiques en termes de qualité des données et de format.

Le Groupement français des industries de l'information (GFII)[41], n'est pas hostile à une monétisation de certaines données publiques, élaborée pour des usages prédéfinis avec un secteur économique.

Cette question mérite d'être examinée de façon approfondie afin d'évaluer les effets bénéfiques (notamment en terme de financement des opérations coûteuses qui permettent de conférer de la valeur à des données, et de fournir donc des données de qualité) ou négatifs (exclusion de certaines entreprises en raison d'une tarification dissuasive ce qui limiterait le potentiel d'innovation, et doterait des entreprises déjà bien positionnées d'un avantage concurrentiel supplémentaire).

2.2. Des données d'intérêt général issues du secteur privé qui doivent trouver un cadre juridique adéquat

La notion de données d'intérêt général a été introduite par la loi « pour une République numérique »[42]. Elle recouvre des données qui sont particulièrement importantes pour l'action publique ou pour le fonctionnement du marché. Ainsi le rapport relatif aux données d'intérêt général, établi en 2015,[43] tout en reconnaissant le caractère d'actifs stratégiques des données d'entreprises privées, recommandait

[41] Association loi 1901 regroupant des acteurs œuvrant dans le domaine de la donnée (administrations publiques, banques, énergie, éditeurs juridiques, avocats…). Entretien avec les rapporteurs de MM. Denis Berthault, Président du GFII, Frédéric Cantat et Mme Claire-Élisabeth Fritz, membres du GFII devant la section des activités économiques, le 3 novembre 2020.

[42] Loi n° 2016-1321 pour une République numérique du 7 octobre 2016.

[43] Laurent Cytermann (sous la direction de), *Rapport relatif aux données générales*, établi par le Conseil général de l'économie, de l'industrie, de l'énergie et des technologies et l'Inspection générale des finances. https://www.economie.gouv.fr/files/files/PDF/DIG-Rapport-final2015-09.pdf.

de *« procéder de manière sectorielle et au cas par cas à l'ouverture de données détenues par des personnes privées, à condition que cette ouverture soit justifiée par des motifs d'intérêt général et repose sur des modalités proportionnées. »*

Ce rapport mettait donc en garde contre la mise sous un même statut de toutes les données d'intérêt général, ce qui soulèverait des problématiques inextricables au regard de la diversité des données en cause et du risque sous-jacent que cette ouverture bénéficie principalement aux géants du numérique et porte atteinte à la liberté d'entreprendre.

La stratégie de la donnée de la Commission européenne recommande aux États membres de créer des structures nationales pour le partage des données d'entreprises à pouvoirs publics (*Business to Government* – B2G).

Par ailleurs, le GFII, très mobilisé sur ce sujet, propose que les acteurs privés puissent être rémunérés pour les données d'intérêt général qu'ils seraient amenés à partager avec les pouvoirs publics.

Que les données proviennent du secteur public (« open data ») ou du secteur privé, certaines d'entre elles, de par leur importance pour la conduite de l'action publique, pour l'exercice de la démocratie (information du citoyen), pour le fonctionnement de l'économie, constituent de fait des « communs ».

- Les communs, tels que théorisés par Elinor Ostrom[44] sont définis par les trois caractéristiques suivantes : une ressource en accès partagé ; une communauté bénéficie de droits particuliers sur cette ressource ; un mode de gouvernance mis en place pour que chacun n'outrepasse pas ses droits et pour assurer la reproduction de cette ressource.

Il existe un débat au niveau des économistes sur l'estimation de la valeur créée grâce à l'utilisation des communs de la donnée et de sa restitution à la collectivité (financement des infrastructures, des formations, etc.)[45].

Il reste à orienter les opérateurs économiques (PME notamment) pour un repérage et un usage des données ouvertes dans leurs propres champs d'activité pour leur permettre de doter de plus de services leurs produits existants ou pour innover sur de nouveaux créneaux.

Préconisation 7 :

Le Cese préconise de renforcer la dynamique du service public de la donnée pour constituer des « communs de la donnée » par un partage plus intense des données publiques et des données privées d'intérêt général.

[44] Elinor Ostrom, *Governing the commons: The evolution of collective action*, 1990.

[45] Organisation des Nations-unies, *Digital economy report. 2019: value creation and capture: implications for developing countries,* janvier 2020. https://digitallibrary.un.org/record/3833647?ln=fr. Clara Dallaire-Fortier, « Le travail sous le capitalisme .de plateforme », Institut de recherche et d'informations socioéconomiques (IRIS, Canada), janvier 2020. Arnaud Anciaux, Joëlle Farchy, « Données personnelles et droit de propriété : quatre chantiers et un enterrement », De Boeck Supérieur, *Revue internationale de droit économique*, 2015.

Cela conduira notamment à :

- interroger le modèle de gratuité systématique des données publiques à destination des professionnels ;

- adopter une approche sectorielle pour les données privées d'intérêt général, et un cadre juridique sécurisé ;

- mettre en place des modalités de concertation continue entre producteurs, transformateurs et utilisateurs des données publiques et privés.

Concernant l'échange des données entre entreprises privées, il reste peu développé alors même que le potentiel en termes d'innovation est important. Des raisons multiples expliquent les freins : manque de confiance entre opérateurs économiques, asymétrie dans le pouvoir de négociation et cadre juridique peu développé (notamment pour les données issues de l'internet des objets).

Il conviendrait donc d'articuler la stratégie des données de la France avec celles des pays de l'UE afin de contribuer à la construction d'un espace unique de la donnée et garantir ainsi un niveau élevé de sécurité juridique lorsqu'il s'agit du partage de données d'intérêt général produites par le secteur privé ou de données à caractère personnel (données de santé) et des données d'entreprises privées vers d'autres entreprises privées (*Business to Business* B2B) dans la perspective notamment du développement de l'intelligence artificielle, domaine dans lequel l'Union européenne a été distancée jusqu'à présent par les États-Unis et la Chine[46].

3. Une ouverture des données cruciale pour le développement d'une intelligence artificielle digne de confiance au sens de l'Union européenne

La disponibilité et l'accès à des données de qualité sont au cœur du développement des technologies de l'intelligence artificielle. Les deux autres facteurs déterminants en sont les algorithmes et les capacités de calcul.

Les pays les plus avancés ont comparativement beaucoup plus de données disponibles (États-Unis, Chine). En revanche ces données ne sont pas toujours accessibles ni standardisées et sont stockées dans des *Data Centers* contrôlés par des opérateurs non européens.

Concernant les algorithmes de *Machine Learning* et de *Deep Learning*, ils se font de plus en plus avec des logiciels en *Open Source* et des outils en ligne. Plusieurs géants de la technologie, tels que Google proposent des plateformes *Open source* et des outils permettant d'exploiter cette innovation sans expertise en codage informatique. Ces mêmes géants du numérique établissent également des partenariats stratégiques avec des organismes de recherche dans l'optique principale de collecter encore davantage de données.

[46] Voir étude menée par la Fondation Bertelsmann sur les brevets déposés entre 2000 et 2019 dans 58 technologies de rupture : *"World class patents in cutting-edge technologies. The innovation power of East Asia, North America and Europe"*, juin 2020.
https://www.bertelsmann-stiftung.de/fileadmin/files/user_upload/BST_World_class_patents_2020_ENG.pdf.

La stratégie européenne pour les données qui vise à établir **un espace européen de la donnée** prend tout son relief face aux géants du numérique qui se sont développés grâce à leur capacité à collecter des données sur la planète entière.

Ces constats permettent de confirmer que les enjeux pour l'intelligence artificielle (IA) résident d'une part dans l'accès à des données de qualité, et d'autre part dans la puissance de calcul.

L'aperçu des usages des données par les technologies de l'intelligence artificielle, et les applications qui en dérivent font que ces dernières sont capables du meilleur (application pour la santé prédictive, optimisation des procédés de fabrication, de gestion des systèmes d'information[47] comme du pire[48] (décision automatique sur des aspects importants de la vie des citoyens). La consultation lancée par la Commission[49] sur le « Livre blanc pour l'intelligence artificielle », publié en février 2020, va permettre aux Etats-membres de définir le niveau pertinent d'encadrement juridique et normatif. Les principes énoncés par la Commission sont en cohérence avec les recommandations du rapport de Cédric Villani intitulé *Donner du sens à l'intelligence artificielle* (2017).

Les notions d'IA à haut risque et à faible risque ont été définies dans ce livre blanc. La Commission vise à légiférer sur l'IA à haut risque, IA qui cumule deux critères :

- un secteur impliqué à risque (santé, énergie, transport, etc.) ;
- des applications d'IA dans ce secteur à risque susceptibles de faire émerger un risque.

D'autres applications seront considérées à haut risque dès lors qu'elles sont susceptibles de porter atteinte aux droits fondamentaux (égalité professionnelle et algorithmes de recrutement par exemple) ou qu'elles concernent les identifications biométriques à distance. Ainsi les outils IA déployés affectant les conditions de travail en milieu professionnel doivent être classés par défaut dans la catégorie à haut risque.

Par ailleurs, des travaux de normalisation ont été lancés au niveau de l'ISO avec un groupe miroir mis en place par l'AFNOR et le Conseil européen de normalisation (CEN)[50]. Dans la feuille de route sont inscrites les thématiques d'importance : responsabilité, qualité, données pour l'IA, sécurité et protection de la vie privée, éthique, ingénierie de l'IA et sécurité de l'IA.

Les débats actuels entre États membres font apparaître deux visions différentes sur le degré de régulation de l'IA : l'une défendue par l'Allemagne qui préconise une réglementation stricte pour éviter l'envahissement des citoyens par des outils d'IA, l'autre soutenue par la France qui opte pour une régulation souple de façon à ne pas brider l'innovation et ne pas freiner le rattrapage technologique amorcé.

---

[47] C. Obez, M.-C. Duboc, K. Chen, *Artificial intelligence as a solution to your complex issues in IT operations*, novembre 2019. https://www.wavestone.com/en/insight/artificial-intelligence-it-operations.

[48] Roman S.A.R. R.A de David Gruson. Entretien au CESE du 10/06/2020.

[49] Consultation de la Commission européenne portant sur le *Livre blanc sur l'intelligence artificielle*, ouverte du 20 février au 14 juin 2020.

[50] Échange avec Philippe Saint-Aubin, membre de notre section et participant, en tant qu'expert, aux travaux du CEN Focus group au titre de la Confédération européenne des syndicats (CES) sur l'IA.

Dans tous les cas, il convient que, quel que soit le cadre législatif ou l'outil normatif d'ordre privé et volontaire, toute application d'IA se conforme pleinement à l'article 22 du RGPD relatif à toute décision automatisée, y compris le profilage : l'IA ne doit pas s'appliquer sans supervision humaine dans des prises de décision aux conséquences graves.

Ces considérations montrent l'importance d'associer des représentants de disciplines qui relèvent des sciences humaines (géopolitique, sociologie, éthique, etc.) aux travaux de régulation et de normalisation de façon à donner une traduction opérationnelle aux « Lignes directrices en matière d'éthique pour une IA digne de confiance » établies en 2019 par le Groupe d'experts de haut niveau sur l'intelligence artificielle[51].

Préconisation 8 :

Pour les outils basés sur l'intelligence artificielle (IA), le Cese préconise de mettre en place une régulation et un cadre normatif européens en cohérence avec les principes de transparence, de traçabilité et de contrôle humain afin que les libertés et les droits fondamentaux soient renforcés. Les travaux de régulation, de normalisation doivent intégrer des compétences en sciences humaines.

Dès la conception et avant leur mise sur le marché, les systèmes d'IA doivent respecter les droits fondamentaux et les exigences éthiques (écarter la subordination de l'humain et valoriser l'aide à l'activité).

En particulier, les algorithmes ouvrant ou limitant des droits aux personnes doivent répondre aux obligations de transparence.

B - Le Cadre éducatif, scientifique et technique : plus d'ambition et dans la durée

1. Des ressources en matière de formation et de recherche de haut niveau à renforcer

La France dispose de ressources en matière de formations et de la recherche de haut niveau (Pôles de compétitivité Systematics et Cap Digital, INRIA), mais le marché est en pénurie de main d'œuvre qualifiée comme l'attestent différentes études.[52]

Au niveau européen, la Commission estime à un million la pénurie globale de spécialistes du numérique. La participation plus forte des femmes, sous représentées dans ces métiers, doit être encouragée, en complément notamment des fonds que prévoit de dégager la Commission en vue de former 250 000 professionnels supplémentaires à horizon 2025.

[51] Groupe d'experts indépendants constitué par la Commission européenne.

[52] Voir notamment celle menée en 2017 par Cap Gemini Research Institute et LinkedIn intitulée *The digital talent gap - Are companies doing enough ?*

Les métiers sous tension concernent généralement les managers, ingénieurs et cadres techniques. Les métiers émergents sont également difficiles à pourvoir : responsables des réseaux sociaux, analystes des données, (*data scientists*, *data analysts),* spécialistes de l'informatique en nuage (*cloud computing*) et de la cybersécurité.

Les formations ne sont pas suffisantes en nombre et en contenu tant en formation initiale dans les grandes écoles et les universités qu'en formation continue au sein des entreprises, voire en reconversion *via* l'APEC et Pôle Emploi, et cela concerne également les qualifications intermédiaires post-bac.

Par ailleurs, les décisionnaires et l'encadrement de façon générale doivent pouvoir piloter les investissements en matière d'infrastructures techniques, toujours très coûteux, d'achats de prestations intellectuelles et de données. Une étude de Mc Kinsey[53] donne une idée du volume et de la structure des postes de dépense liés à la donnée : les coûts des personnels internes et externes, les contrats de protection des données contre les risques, coûts liés aux infrastructures, aux logiciels, etc. Les répondants à l'enquête sur laquelle se base cette étude anticipent une inflation des dépenses d'environ 47% par an sur l'ensemble des secteurs d'activités, et de plus de 80 % pour les secteurs de la grande consommation.

Pour ce qui est de la recherche académique, les points faibles concernant la recherche française, étayés à nouveau à l'occasion des débats sur la Loi de programmation pluriannuelle de la recherche (LPPR)[54], sont d'autant plus critiques pour les disciplines qui concernent l'économie et la gouvernance de la donnée (mathématiques, informatique, sciences des matériaux, sciences sociales…

Au regard des enjeux climatiques et environnementaux, les connaissances et compétences techniques doivent s'étoffer. Si tout le discours ambiant concourt à « invisibiliser » la matérialité du numérique (monde virtuelle, nuage, etc.), ses impacts sont bien réels : dématérialiser ce n'est rien d'autre que rematérialiser[55]. Le numérique est une ressource non renouvelable[56] et sa matérialité concerne à la fois les équipements et les usages que les ingénieurs doivent optimiser dès les phases de conception et .de prototypage.

Enfin, la conception des outils d'intelligence artificielle, l'utilité sociale de certaines applications destinées au grand public basées sur la captation et le contrôle de l'attention emportent des implications éthiques dont il est essentiel de tenir compte en amont de toute activité de conception.

---

[53] Mc Kinsey digital, *Reducing data cost without jeopardizing growth*, 31 juillet 2020. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/reducing-data-costs-without-jeopardizing-growth.

[54] Loi n° 2020-1674 du 24 décembre 2020 de programmation de la recherche pour les années 2021 à 2030 et portant diverses dispositions relatives à la recherche et à l'enseignement supérieur.

[55] Bruno Latour, « On est passé du virtuel au réel, et non du réel au virtuel », entretien du 20 novembre 2009, site Internetactu.net.

[56] Les travaux de *Shift Project*, *Think tank* de la transition carbone menés avec des chercheurs pourraient trouver bonne place dans les maquettes de formation initiale et continue.

Préconisation 9 :

Pour le Cese il faut des compétences essentielles pour assurer l'avenir en :

- formant davantage les décisionnels (ingénieurs R&D, enseignements, les diplômés des écoles de commerce, etc.) au caractère stratégique des données numériques avec une place substantielle aux aspects éthiques, juridiques et environnementaux ;

- renforçant les compétences et les qualifications de haut niveau en matière de recherche académique notamment sur les aspects sociotechniques des technologies actuelles et émergentes.

2. Des liens entre le monde de la recherche et des entreprises européennes à tisser sur la question de la donnée

Former ne suffit pas. Maintenir notre indépendance géopolitique et économique en Europe par l'avance technologique est devenu très délicat en raison de l'aspiration des compétences par les GAFAM ou les entreprises chinoises (Huawei notamment). Les exemples de laboratoires publics (INRIA par exemple) en sous-effectif car les chercheurs sont en « disponibilité » pour travailler pour Facebook ou Google ne manquent pas[57]. Or, il est primordial de maintenir un tissu de recherche et d'enseignement fort, à la fois pour former les étudiants et pour éviter la privatisation encore plus grande des données et des connaissances.

Il semble aussi qu'il ne faille pas négliger un autre aspect fondamental : les travaux critiques sur les données collectées et les algorithmes développés seront significativement amoindris par le captage des compétences construites au moyen des deniers publics.

La reconnaissance financière est un levier, mais probablement pas le plus opérant concernant les chercheurs : des infrastructures de recherche de qualité, des moyens alloués pour la recherche à la hauteur des enjeux, une gestion dynamique de leurs carrières au sein de l'écosystème européen peuvent constituer des pistes efficientes.

Préconisation 10 :

Le Cese préconise de lutter contre la captation des compétences utiles en matière de traitement des données et d'infrastructures matérielles (notamment la maîtrise du secteur du semi-conducteur et du calcul de haute fréquence par le développement des technologies quantiques, la technologie *Block Chain*, et l'IA) :

- en créant, à partir des pôles d'excellence des synergies fortes pour mettre en cohérence et développer les talents, sur la durée grâce à des programmes ambitieux et suivis sur le moyen et long terme, avec des évaluations et des réévaluations permanentes ;

[57] *Le Monde*, article intitulé « Numérique - Main basse sur les données », 18 septembre 2019.

- en sécurisant et regroupant les connaissances industrielles et techniques considérées comme particulièrement sensibles et stratégiques et en retenant les compétences critiques au sein de l'UE ;

- en renforçant en la matière le rôle proactif de la DGSI, DGSE et de l'ANSSI à l'image des pratiques des États-Unis et de la Chine.

Pour protéger les données, il faut protéger les supports des données et les moyens de traitement. Cela vaut tout particulièrement pour les données de santé, données sensibles par excellence et les données industrielles par exemple.

Cette protection implique l'implantation des entrepôts de stockage dans l'UE pour éviter que les données brutes ou lors de leurs traitements ne tombent sous des juridictions extraterritoriales.

Comme analysé dans la partie I, l'étape de traitement des données est cruciale pour les aspects de souveraineté et la dynamique économique. La capacité de traitement nécessite l'accès à des infrastructures techniques de plus en plus lourdes et complexes et à des moyens financiers conséquents.

Le projet de GAIA X constitue une étape importante dans la coopération au sein de l'Union européenne. Par ailleurs en France, la filière « Infrastructures numériques » a été labellisée en novembre 2018 par le Conseil national de l'industrie (CNI). Des politiques structurantes ont également été engagées par la Commission et le Conseil conjointement avec les États membres. L'Union européenne a mis en place une infrastructure de supercalculateurs de classe mondiale à l'échelle européenne afin de *« soutenir le développement d'un écosystème intégré pour le calcul à haute performance dans l'Union, couvrant tous les segments de la chaîne de valeur scientifique et industrielle, notamment le matériel informatique, les logiciels, les applications, les services, l'ingénierie, le savoir-faire et les compétences »*. Un règlement du Conseil a permis de créer cette entreprise en la dotant d'1 milliard d'euros[58].

Préconisation 11 :

En coopération avec les autres partenaires européens, la France doit renforcer les choix opérés dans les filières industrielles stratégiques du numérique, avec notamment le développement des infrastructures nécessaires au stockage des données. Cela implique notamment la maîtrise du secteur du semi-conducteur et du calcul de haute performance, le développement des technologies quantiques, de la technologie *Block Chain*[59] et des technologies d'intelligence artificielle.

[58] Règlement du Conseil établissant l'entreprise commune européenne pour le calcul à haute performance, 11 février 2018. https://eur-lex.europa.eu/resource.html?uri=cellar:c48188c9-f6bb-11e7-b8f5-01aa75ed71a1.0002.02/DOC_1&format=PDF.

[59] Sur la technologie Block Chain, voir article de Julien Hardellin et Vanina Forget, *Les perspectives offertes par la Block Chain en agriculture et agroalimentaire*, juillet 2029 - https://agreste.agriculture.gouv.fr/agreste-web/download/publication/publie/Ana140/Analyse_1401907.pdf.

3. Un atout majeur : la cyber-sécurité française et européenne. Des engagements des pouvoirs publics à renforcer

Alors que le rapport sur les risques mondiaux 2019 du Forum économique mondial classe le vol de données et les cyberattaques parmi les cinq principaux risques mondiaux, avec un coût estimé à 90 000 milliards de dollars, un nombre insuffisant de personnes sont formées dans ce domaine.

Le problème de déficit de professionnels en cybersécurité dans l'Union européenne[60] peut être résolu selon le rapport de l'Agence européenne en cybersécurité en redéfinissant les parcours d'éducation et de formation avant et après entrée sur le marché du travail. La France a remis à plat son système de formation et de certification avec l'appui de l'ANSSI.

Aujourd'hui, plus d'une centaine de formations sont proposées par 23 pays de l'Union européenne et la Suisse. La France fait preuve d'un certain « malthusianisme » : seuls deux établissements sont référencés dans la base de données de l'*European Union Agency for Cybersecurity* (ENISA)[61] tandis que la Suisse en compte 6 (niveau master et baccalauréat).

La France dispose de grands groupes (Airbus, Deloitte, Thalès, Orange, Safran, Sopra Steria, Atos) bien positionnés dans le domaine de la cybersécurité mais aussi de start-ups particulièrement innovantes et qui se développent à l'international : 134 au total en 2019, selon l'étude menée par le cabinet Wavestone[62]. Leur positionnement concerne aussi bien les sujets matures en matière de cybersécurité (sécurité de la donnée, gestion des identités et des accès, sécurité réseaux, etc.) que les sujets émergents (vie privée, collaboration sécurisé, gestion de crise, digitalisation des parcours client, sécurité de l'IoT).

Pour ce qui est de la maturité des entreprises en matière de cybersécurité, un travail de fond doit être entrepris, car plusieurs études tendent à montrer une sous-estimation du risque cybersécurité, encore plus prononcée lorsqu'il s'agit des technologies émergentes (IA, 5G, informatique quantique, réalité virtuelle, réalité augmentée). De plus, les entreprises mettent en place des plans de sécurisation trop tardivement[63]. Certains opérateurs d'importance vitale (OIV) sont accompagnés par l'ANSSI dans le dispositif interministériel plus large de sécurité des activités d'importance vitale (SAIV) inscrit dans le code de la défense mais il reste tous les autres opérateurs, dit conventionnels et notamment les PME/ETI. Des actions sont menées pour sensibiliser et accompagner ces dernières ; ainsi la Chambre de commerce et d'industrie (CCI) Paris Ile-de-France diffuse depuis septembre 2020 une remarquable brochure intitulée *Pérenniser l'entreprise face au risque cyber : de la cybersécurité à la cyber-résilience*.

---

[60] ENISA, « Cybersecutity skills development in EU », décembre 2019.

[61] Université de Grenoble (40 étudiants niveau master) et Télécom Sud Paris (24 étudiants niveau master).

[62] Radar Wavestone, première société de consulting française en matière de transformation digitale, spécialisée en cybersécurité.

[63] Étude Accenture. https://www.usine-digitale.fr/article/etude-les-entreprises-sous-evaluent-les-risques-cyber-lies-aux-technologies-emergentes.N1024859.

Préconisation 12 :

Pour le CESE, il faut renforcer les compétences en cybersécurité à la hauteur des besoins d'une économie de la donnée en :

- diversifiant les parcours de formation et en augmentant les effectifs formés (formation initiale et continue) ;

- renforçant la prise de conscience des opérateurs économiques conventionnels sur les risques de cybersécurité de façon à augmenter leur maturité en ce domaine, notamment lors d'introduction de technologies émergentes.

C - Un cadre économique et social à réinventer en permanence

Les avancées rapides des technologies stimulent l'innovation et permettent la création de nouveaux services mais exigent un effort permanent d'adaptation aussi bien pour les institutions, les organisations publiques et privées, que pour les individus dans des environnements en transformation continue.

1. De multiples modèles économiques en mutation

Comme l'a souligné M. Jacques Crémer, directeur du Centre numérique de *Toulouse School of Economics*, il n'existe pas deux ou trois mais plusieurs modèles économiques fondés sur la donnée y compris lorsqu'il s'agit du plus emblématique d'entre eux, celui des plateformes qui bouleversent la dynamique des marchés conventionnels sur le court et le long terme, rendent inopérantes les règles de la concurrence et créent des formes inédites de précarité du travail.

Les données et l'algorithmique constituent la base fondamentale des modèles de plateformes. Elles bénéficient des effets de réseau nés de leurs positions d'intermédiaires sur des marchés multi-faces, à l'origine de concentration capitalistique.

Pour identifier les modèles économiques, il convient de rappeler le processus de création de valeur par la donnée[64].

La donnée en tant que telle n'a pas de valeur intrinsèque *ex ante*. Elle en acquiert une fois transformée en plusieurs étapes, avec introduction de ressources et de compétences calibrées à cet effet. La métaphore usuelle de la donnée comme « pétrole » ou « d'or » du XXI^{e} renvoie à cette étape indispensable de transformation.

[64] Voir notamment Henri Isaac, Données, Valeur et Business models, 2016. hal-01821836. https://hal.archives-ouvertes.fr/hal-01821836.

Mais si la donnée nécessite d'être transformée pour produire de la valeur elle ne constitue pas pour autant un bien rival, comme les ressources minières : son utilisation par un acteur économique ne la détruit pas et ne la rend pas impropre à l'utilisation par un autre.

Le procédé de de création de la valeur comporte quatre étapes principales : la production de données, le stockage (stock ou flux), le traitement algorithmique puis l'utilisation ou la mise à disposition à des tiers qui vont les réutiliser[65]. Les étapes qui consistent à garantir la qualité de la donnée sont indispensables et la valeur produite va dépendre également des métadonnées qui décrivent des données et permettent leur exploitation.

Chaque étape fait appel à des ressources et des compétences spécifiques et de natures très différentes que peu d'entreprises sont en mesure de maîtriser dans leur totalité :

- compétences stratégiques pour définir le modèle d'affaires le plus approprié pour extraire le potentiel de valeur contenue dans la donnée ;
- compétences managériales pour coordonner et faire travailler ensemble la diversité des métiers nécessaires ou utiles à une activité centrée sur la donnée ;
- ressources et compétences techniques (pour le choix de la plateforme, des infrastructures techniques, le traitement des données ;
- compétences organisationnelles pour assurer la gouvernance de la donnée.

Les opérateurs de l'industrie de la donnée peuvent choisir de se positionner sur l'un des maillons de la chaîne de valeur pour déployer leurs activités.

Une typologie empirique partant de l'analyse d'une centaine de cas d'entreprises spécialisées dans la donnée a mis en évidence 6 modèles d'affaires en fonction de l'origine de la donnée traitée : données librement accessibles et gratuite, ou données fournies par des clients, données générées et collectées.

1.1. La donnée dans un modèle d'affaires classique : du plus basique au plus innovant

La donnée dans les modèles d'affaires classiques peut simplement être collectée dans le cadre de l'activité principale, puis revendue à une autre entreprise (exemple : Orange-Business avec l'offre Flux-vision pour les entreprises qui sont intéressées d'évaluer la fréquentation d'un lieu par leurs clients ou connaître les déplacements de ces derniers). Un deuxième modèle consiste à utiliser les données issues d'une activité principale (banque par exemple) pour développer un autre segment d'activités (assurances). Un troisième modèle se caractérise par la commercialisation d'un service payant ou gratuit, basé sur la donnée (exemple : compteur électrique intelligent - modèle dit *Commodity Swap*). Un troisième modèle observé repose sur l'intégration des acteurs positionnés sur une chaîne de valeur en vue d'améliorer le service au client final (exemple : chaîne logistique intégrée dans les métiers de la distribution, ou de l'automobile). Un quatrième modèle, plus élaboré, consiste en le regroupement de plusieurs partenaires travaillant en réseau pour améliorer l'expérience globale du client (partenariat KLM-Hertz).

[65] Voir l'exemple de Michelin dans l'encadré 1, pp. 16 et 17.

Le modèle de partenariat de Dassault Systèmes avec sa plateforme 3Dexpérience va encore plus loin en regroupant plus de 25 millions d'utilisateurs pour tous types de modélisation. Plus précisément la plateforme 3DS Medidata, une plateforme de santé unique au monde qui vise à transformer le cycle de développement des médicaments (45 milliards de données de patients). Les tests actuels pour la mise au point d'un futur vaccin anti-Covid sont réalisés sur cette plateforme acquise l'année dernière par Dassault Systèmes. Pour cette entreprise, *« La valeur du virtuel excède désormais l'économie " matérielle " »* par la création de jumeaux numériques non seulement d'objets inertes, mais aussi d'organes complexes tels que le cœur ou le cerveau.

Enfin un nouveau modèle économique voit le jour sous la forme d'une société coopérative d'intérêt collectif (SCIC) pour structurer les données de toute la filière agroalimentaire de « la fourche à la fourchette ». Il s'agit de la plateforme NumAlim dont le lancement est prévu pour le printemps 2021.[66] Il s'agit d'une initiative suscitée par le succès d'applications (type Yuka) qui notent et classent les produits alimentaires. L'influence des recommandations formulées par ces applications basées sur des données pas toujours fiables a incité les pouvoirs publics (ministère de l'Agriculture, avec l'appui de Bpifrance) et les acteurs de la filière à créer cette SCIC dotée d'un comité d'éthique, d'un conseil scientifique et d'une gouvernance dans laquelle des associations de consommateurs ont leur place. L'une des missions de NumAlim est de former ses sociétaires et d'accompagner les acteurs de la filière dans la maîtrise et l'usage de leurs données.

Ces deux derniers modèles originaux concernent deux domaines d'excellence de notre pays en matière d'innovation : la santé et la nutrition/alimentation comme le confirme l'édition 2020 de l'analyse des brevets de classe mondiale portant sur les technologies de rupture, réalisée par la fondation allemande Bertelsmann[67]. En la matière il n'y a pas de position définitivement acquise comme le démontre hélas le recul de la France sur les 20 dernières années dans les brevets liés aux technologies de pointe en matière de sécurité (sécurité des réseaux, des transactions financières, *etc.*).

[66] Plateforme numérique de l'alimentation (Numalim), Livre blanc *Ces données qui nourrissent la confiance et la valeur dans l'alimentation*, septembre 2020.

[67] Voir référence plus haut.

1.2. Les données dans les modèles d'affaires de l'Internet des objets

L'Internet des objets peut être décrit comme l'imbrication ou l'encapsulation du réseau Internet dans les objets physiques.

La connectivité des objets conditionne selon Henri Isaac le modèle d'affaires. Le degré de connectivité va de la simple carte électronique à la possibilité de transmettre des données qui peuvent être traitées, analysées et combinées à d'autres données externes à l'objet-lui-même, en agrégeant plusieurs partenaires (*cf.* annexe 4).

Le volume des données produites par l'internet des objets est appelé à croître très rapidement, avec des opportunités de développement de nouvelles activités. Comme le note la Commission européenne, si à l'heure actuelle 80 % des opérations de traitement des données sont réalisées dans des installations centralisées, et 20 % dans des objets connectés et les installations proches des utilisateurs (*Edge Computing*), à l'horizon 2025, cette proportion va s'inverser. Cette évolution donne ainsi la possibilité de développer des outils pour les producteurs de données pour un meilleur contrôle de leurs propres données.

La littérature académique s'accorde à considérer que la recherche théorique sur les modèles économiques tirés par la donnée n'est pas encore assez développée et que les acteurs économiques peinent à identifier les modèles pertinents pour évoluer vers des activités à forte valeur ajoutée centrées sur la donnée.

Préconisation 13 :

Le Cese préconise de mobiliser des moyens conséquents pour produire les connaissances théoriques sur les modèles économiques fondés sur la donnée et leurs enjeux afin :

- de permettre aux décideurs publics et privés de décrypter, de comprendre les modèles d'affaires fondés sur la donnée et leurs enjeux ;

- d'aider les opérateurs économiques à identifier les modèles ou combinaisons de modèles à fort potentiel pour créer de la valeur socio-économique équitablement partagée, sobre et durable ;

- de contribuer à créer des communs numériques au service des besoins sociétaux avec notamment l'essor de l'internet des objets.

2. Un soutien des pouvoirs publics aux PME, ETI à renforcer et à évaluer

Une dispersion des organismes ou institutions compétents, des redondances et des carences entre les régions, l'État et les divers organismes *ad hoc* (Bpifrance, fonds européens, fonds pour l'innovation, etc.) ne sont pas de nature à aider les acteurs économiques à engager des transformations de fond. Il apparaît clairement que les PME et les ETI ne savent pas à quel interlocuteur identifié s'adresser et se sentent isolées face au problème dans sa globalité.[68]

[68] Une table ronde a été organisée par le CESE, dans le cadre du présent avis, sur ce sujet avec des représentants d'entreprises

Pourtant de nombreux dispositifs sont mis en place pour accompagner les PME et ETI en vue d'une meilleure appropriation de la question de la donnée : pacte productif, plan de relance *post* Covid-19.

Une évaluation de l'effectivité des mesures prises pour soutenir la digitalisation des PME mériterait cependant d'être conduite afin de dégager la vision stratégique qui devra orienter l'intégration de la donnée dans la conduite des affaires et la gouvernance de la donnée.

La collaboration entre organismes de recherche en matière de numérique et avec les entreprises est trop faible en France : peu de chercheurs font un passage dans les PME. C'est l'un des facteurs qui expliquerait une innovation moins dynamique en France qu'aux États-Unis[69]. Il semble donc urgent, pour accélérer la maîtrise de la donnée au sein des PME, de densifier l'écosystème autour d'elles afin de leur permettre de bénéficier des avancées technologiques et des nouvelles connaissances.

3. Des acteurs dans les organisations à convaincre et à outiller

3.1. Au niveau des organisations

Pour ce qui est du secteur public, la mise en place de la direction interministérielle du numérique (DINum), en charge de la transformation numérique de l'État contribue fortement à la modernisation du système d'information de l'État, qualité des services publics numériques, création de services innovants pour les citoyens, outils numériques de travail collaboratif pour les agents.

Pour ce qui est des entreprises privées, les organisations professionnelles, les chambres de commerce et de l'industrie (CCI) ont pris la mesure des enjeux et ont entrepris de sensibiliser leurs adhérents à la fois sur les opportunités comme sur les aspects plus défensifs (modifications des règles du jeu économique, propriété intellectuelle et partage de données, cybersécurité). La question du secret des affaires, du secret professionnel (pour les professions libérales notamment) et le partage des données sécurisé reste souvent en suspens, et constitue l'un des freins identifiés par les représentants des entreprises dans l'entrée dans l'économie de la donnée.

La mise en application du RGPD a permis néanmoins une véritable évolution dans la prise de conscience de la sensibilité sur les données relatives au personnel selon les représentants des entreprises et des salariés. Les entreprises font aussi l'objet de démarches commerciales et des propositions de solutions pour lesquelles il est difficile d'opérer des choix judicieux.

Lorsqu'il s'agit d'outils qui vont modifier les conditions de travail, et notamment les modalités de recrutement ou d'évaluation des personnels, il convient d'ouvrir un débat avec les représentants du personnel. Plus précisément, il importe de consulter ces derniers en amont du déploiement d'outils IA pour décider si un système doit être

[69] Audition au CESE de Jacques Crémer, Professeur d'économie à la *Toulouse School of Economics*, dans le cadre du présent avis.

introduit. Son introduction devrait être soumise au respect des valeurs sociales et éthiques et respecter la marge d'autonomie humaine.

Par ailleurs, l'entrée dans l'économie de la donnée nécessite d'articuler et de coordonner des métiers très différents, ce qui nécessite un profond changement de culture managériale, et de rapport à l'incertitude.

Préconisation 14 :

Le Cese préconise :

- d'engager une culture de l'usage de la donnée et de l'intelligence numérique dans les entreprises, en lien avec le haut fonctionnaire de défense ;

- de renforcer le dialogue social pour mettre en place des outils efficaces de sensibilisation, d'information en amont de déploiement d'outil IA, et pour revisiter les méthodes de formation continue, dans le respect des normes retenues par les accords européens ;

- d'adapter les modalités de coopération et les méthodes de management (décloisonnement des spécialités, croisement des expertises sectorielles avec expertises numériques notamment).

3.2. Au niveau des individus

L'exercice des droits inscrits dans le RGPD n'est pas pleinement effectif, comme le droit à la portabilité de l'article 20 de ce règlement. Il s'agit de permettre à chacun de décider avec qui partager ses données à caractère personnel, de contrôler qui a accès à ces données et à celles produites par les machines « intelligentes » de plus en plus répandues dans les lieux d'habitation ou encore les données collectées par les fournisseurs d'applications à caractère personnel (caméra de téléphone portable, etc.).

Par ailleurs, la collecte des données personnelles ou l'abandon de façon insouciante des données personnelles est favorisée par l'attrait des applications mises au point par les géants du numérique qui ont construit leurs modèles économiques sur la publicité ciblée en ayant recours à des méthodes dérivées de sciences cognitives pour créer une forme d'addiction et un besoin irrépressible de se connecter[70].

Préconisation 15 :

Pour le Cese, il est nécessaire de responsabiliser les utilisateurs face au risque de consommation excessive de certains services numériques séducteurs et addictifs, puissants aspirateurs de données personnelles et de soutenir les actions en faveur de la transparence (connaissance de sa consommation personnelle).

[70] Joëlle Toledano, *Gafa : reprenons le pouvoir*, Éd. Odile Jacob, septembre. 2020. Voir également Shoshana Zuboff, *L'âge du capitalisme de surveillance*, 2019 traduit de l'anglais par les Éd. Zulma, octobre 2020. Voir aussi l'article publié dans *Le Monde*, rubrique « Idées », l'article de Mireille Delmas-Marty « Nous basculons vers un droit pénal de la sécurité », 24 octobre 2020.

Avis

Ces actions doivent s'ajouter à un effort massif de formation dès le plus jeune âge aux outils numériques et en milieu professionnel, à l'organisation de formations exigeantes en situation de travail et à la reconnaissance des qualifications acquises.

Ces efforts doivent s’inscrire dans des campagnes de sensibilisation plus larges d’éducation au numérique tout au long de la vie personnelle et professionnelle, afin de maintenir en éveil l’esprit critique en matière de données et des technologies associées, pour ainsi assurer une maîtrise sociale, économique et environnementale des enjeux de la donnée.

Conclusion

L'enjeu global de toute stratégie en matière de données et de gouvernance est de créer un écosystème institutionnel et technologique souverain, dans lequel les entreprises pourront se développer et où la place des citoyens sera consolidée.

La gestion des données est devenue cruciale : c'est un facteur de création de richesse et d'innovation, son développement fait cependant peser des menaces sur les droits fondamentaux, les libertés individuelles et la souveraineté des États.

Au sein des réseaux mondiaux tissés par les données et les technologies du numérique, les institutions et les entreprises françaises ont pris du retard ; un retard qu'elles rattrapent grâce à des atouts qu'il convient de préserver et de développer de façon continue et accélérée, avec des coopérations stratégiques fortes au sein de l'Union européenne, dans les domaines technologiques, institutionnels et organisationnels.

Le numérique nécessite un haut niveau de coopération, un certain confort dans les situations incertaines et mobilise des compétences exigeantes en matière de relations humaines. À cet effet, le développement de l'économie de la donnée conduit à interroger l'efficacité et l'adéquation de nos dispositifs de formation initiale et continue sous-dimensionnés. En particulier, des études fournies en matière d'impact de l'intelligence artificielle[71] ont abondamment démontré les effets prévisibles sur les emplois et les qualifications (en nature et en quantité), concluant toutes à l'impératif de développer massivement des formations généralistes permettant d'acquérir des compétences transversales pour apprendre à apprendre.

Les outils de gouvernance de plus en plus sophistiqués, les réglementations créent une interdépendance poussée entre les États, mais aussi entre les différentes disciplines du savoir, souvent en cours de construction. Les aspects éthiques, environnementaux, légaux et sociaux doivent être pris en compte simultanément. La question qui se pose à nos sociétés est peut-être moins de faire confiance, que de disposer d'institutions et d'outils sécurisés et durables dans un cadre éthique partagé. Une éthique, qui pour reprendre Paul Ricœur, vise la *« recherche d'une vie bonne avec et pour les autres dans des institutions justes »*.[72]

[71] Voir notamment France Stratégie et Conseil national du numérique *Anticiper les impacts économiques et sociaux de l'intelligence artificielle*, mars 2017.

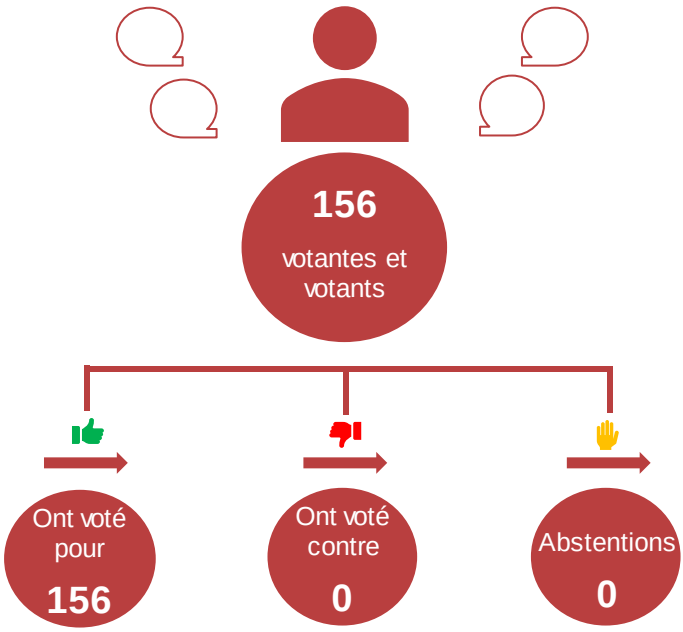
[72] Paul Ricœur, *Soi-même comme un autre*, éditions du Seuil, 1990.

Déclarations/ Scrutin

Déclarations des groupes

Scrutin

Sur l'ensemble du projet d'avis présenté par Soraya Duboc et Daniel-Julien Noël



L'ensemble du projet d'avis a été adopté au scrutin public lors de la séance plénière du Conseil économique, social et environnemental, le 10 février 2021

Annexes

N°1 COMPOSITION DE LA SECTION DES ACTIVITÉS ÉCONOMIQUES À LA DATE DU VOTE

Présidente : Delphine LALU
Vice-présidente : Renée INGELAERE
Vice-président : Philippe GUGLIELMI

❒	**Agriculture**
✓	Eric LAINÉ
✓	Manon PISANI
❒	**Artisanat**
✓	Jean-Pierre CROUZET
❒	**Associations**
✓	Delphine LALU
❒	**CFDT**
✓	Soraya DUBOC
✓	Sébastien MARIANI
✓	Philippe SAINT-AUBIN
❒	**CFE-CGC**
✓	Gabriel ARTERO
❒	**CFTC**
✓	Bernard SAGEZ
❒	**CGT**
✓	Marie-Claire CAILLETAUD
✓	Sylviane LEJEUNE
❒	**CGT-FO**
✓	Martine DEROBERT
✓	Frédéric HOMEZ
❒	**Coopération**
✓	Jacques LANDRIOT
❒	**Entreprises**
✓	Renée INGELAERE
✓	Frédéric GRIVOT
✓	Gontran LEJEUNE
❒	**Environnement et nature**
✓	Anne de BETHENCOURT
✓	Antoine BONDUELLE
❒	**Mutualité**
✓	Stéphane JUNIQUE

❒	**Outre-mer**
✓	Joël LOBEAU
❒	**Organisations étudiantes et mouvements de la jeunesse**
✓	Lilâ LE BAS
❒	**Personnalités qualifiées**
✓	Bernard AMSALEM
✓	Nathalie COLLIN
✓	Stéphanie GOUJON
✓	Philippe GUGLIELMI
✓	Nicole VERDIER-NAVES
❒	**Professions libérales**
✓	Daniel-Julien NOEL
❒	**UNAF**
✓	Bernard TRANCHAND
❒	**UNSA**
✓	Fanny ARAV
❒	**Personnalités associées**
✓	Kat BORLONGAN
✓	Patrick JOLY
✓	Marie-Vorgan LE BARZIC
✓	Didier RIDORET

N°2 LISTE DES AUDITIONNÉS

- ✓ **M. Mehdi AL BOUFARISSI,**
  Chargé des questions numériques au Mouvement associatif

- ✓ **M. Vincent BARBEY,**
  Président d'Ocentis, cabinet de conseil en business et digital process, président du groupe de travail sur la valorisation des données du Mouvement des entreprises de France (Medef)

- ✓ **Maître Alain BENSOUSSAN,**
  Avocat à la Cour d'appel de Paris, spécialiste en droit des nouvelles technologies de l'informatique et de la robotique, fondateur du cabinet Alain Bensoussan Avocats Lexing

- ✓ **Mme Raphaëlle BERTHOLON,**
  Secrétaire nationale à l'économie, l'industrie, le numérique et le logement à la Confédération française de l'encadrement-Confédération générale des cadres (CFE-CGC)

- ✓ **Mme Delphine BORNE,**
  Juriste en charge du numérique à la Confédération des petites et moyennes entreprises (CPME)

- ✓ **M. Thierry BORRAT,**
  Président de DécoAder, PME spécialisée dans l'impression numérique et la pose d'adhésif sur tous supports

- ✓ **M. Philippe CLERC,**
  Conseiller études et prospective de Chambres de commerce et d'industrie (CCI) France

- ✓ **M. Jacques CRÉMER,**
  Professeur d'économie à la Toulouse School of Economics, spécialiste de l'Internet et de l'industrie du logiciel

- ✓ **Mme Marie-Laure DENIS,**
  Présidente de la Commission nationale de l'informatique et des libertés (CNIL)

- ✓ **M. Louis DUVAUX,**
  Président du Syndicat de l'ingénierie du conseil et de techniques de l'information (SICSTI) CFTC

- ✓ **Mme Julie GALLAND,**
  Sous-directrice de l'électronique et du logiciel à la Direction générale des entreprises (DGE) du ministère de l'Économie, des finances et de la relance

- ✓ **M. Serge GARRIGOU,**
  Représentant de l'Union nationale des géomètres-experts (UNGE), président de la commission numérique de l'Union nationale des professions libérales (UNAPL)

- ✓ **M. Philippe JAHSHAN,**
  Conseiller du CESE, président de Coordination Sud, membre du Mouvement associatif

- ✓ **Mme Nathalie JAMMES,**
  Déléguée générale de la Fédération des Sociétés coopératives et participatives (Scop) de la communication

- ✓ **M. Gérard KARSENTI,**
  Président de SAP France, accompagné de Mme Sarah MAHROUF

- ✓ **M. Claude KIRCHNER,**
  Directeur de recherche émérite à l'Institut national de recherche en informatique et en automatique (INRIA), membre du Comité consultation national d'éthique (CCNE), directeur du Comité national pilote d'éthique du numérique, ancien président du Comité opérationnel d'évaluation des risques légaux et éthiques (COERLE) de l'INRIA, membre de la Commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique (CERNA) de l'Alliance des sciences et des technologies du numérique (ALLISTENE)

- ✓ **Mme Marianne LAIGNEAU,**
  Présidente du Directoire d'Enedis

- ✓ **M. Bastien LE QUERREC,**
  Doctorant en droit public, membre de La Quadrature du Net

- ✓ **M. Christian MATHOREL,**
  Secrétaire général de la Fédération des activités postales et de télécommunications (FAPT) de la CGT, représentant de la CGT au sein du Conseil national de l'industrie (CNI) numérique

- ✓ **M. Aziz MEKKAOUI,**
  Conseiller stratégique auprès du secrétariat national de l'Union nationale des syndicats autonomes (UNSA)

- ✓ **Mme Élise N'GUYEN,**
  Chargée de mission à l'UNAPL

- ✓ **M. Éric PÉRÈS,**
  Conseiller du CESE, Secrétaire général Force-ouvrière (FO)-Cadres

- ✓ **M. Benoît PIÉDALLU,**
  Ingénieur en développement informatique, membre de La Quadrature du Net

- ✓ **M. Guillaume POUPARD,**
  Directeur général de l'Agence nationale de la sécurité des systèmes d'information (ANSSI)

- ✓ **M. Amir REZA-TOFIGHI,**
  Président de la commission innovation de la Confédération des petites et moyennes entreprises (CPME), président de Vitalliance, prestataire d'aide à domicile et de services à la personne

- ✓ **Mme Juliette ROUILLOUX-SICRE,**
  Vice-president legal de Thales, membre du Groupement des industries françaises aéronautiques et spatiales (GIFAS), présidente du comité « régulations du numérique » du Medef

- ✓ **Mme Franca SALIS-MADINIER,**
  Secrétaire nationale CFDT-Cadres, membre du Comité économique et social européen

- ✓ **M. Salim SHADID,**
  Directeur numérique de Chambres de métiers et de l'artisanat (CMA) France

- ✓ **M. Jean-Luc TAVERNIER,**
  Directeur général de l'Institut national de la statistique et des études économiques (INSEE)

Par ailleurs, la rapporteure et le rapporteur se sont entretenus avec :

- ✓ **M. Denis BERTHAULT,**
  Président du Groupement français de l'industrie de l'information (GFII), Directeur des contenus en ligne chez LexisNexis

- ✓ **Mme Pascale BREUIL,**
  Directrice statistiques, prospective et recherche de la Caisse nationale d'assurance vieillesse (CNAV)

- ✓ **M. Gilles BONNEFOND,**
  Président de l'Union des syndicats de pharmaciens d'officine (USPO)

- ✓ **M. Frédéric CANTAT,**
  Chargé du service des études et du marketing de l'Institut national de l'information géographique et forestière (IGN), membre du GFII

- ✓ **M. Yves CASEAU,**
  Group Chief Information Officer chez Michelin

- ✓ **M. Maximin CHARPENTIER,**
  Président de la Chambre régionale d'agriculture Grand-Est, membre du bureau de l'Assemblée permanente des chambres d'agriculture (APCA)

- ✓ **Mme Claire-Élisabeth FRITZ,**
  Chargée du suivi réglementaire chez Ellisphère, membre du GFII

- ✓ **Mme Angie GAUDION,**
  Co-directrice et chargée des relations publiques de l'association Framasoft

- ✓ **M. David GRUSON**
  Directeur du programme santé du cabinet de conseil Jouve

- ✓ **Mme Anne-Claire MARQUET,**
  Déléguée générale du GFII

- ✓ **M. Sébastien MASSART,**
  Directeur de la stratégie chez Dassault Systèmes

- ✓ **M. Hadi QUESNEVILLE,**
  Administrateur des données scientifiques de l'Institut national de recherche pour l'agriculture, l'alimentation et l'environnement (INRAE)

N°3 GLOSSAIRE

Les définitions sont principalement issues du glossaire du site Internet de la CNIL et du RGPD.

ALGORITHME

Un algorithme est la description d'une suite d'étapes permettant d'obtenir un résultat à partir d'éléments fournis en entrée. Par exemple, une recette de cuisine est un algorithme permettant d'obtenir un plat à partir de ses ingrédients. Dans le monde de plus en plus numérique dans lequel nous vivons, les algorithmes mathématiques permettent de combiner les informations les plus diverses pour produire une grande variété de résultats : simuler l'évolution de la propagation de la grippe en hiver, recommander des livres à des clients sur la base des choix déjà effectués par d'autres clients, comparer des images numériques de visages ou d'empreintes digitales, piloter de façon autonome des automobiles ou des sondes spatiales, etc.

Pour qu'un algorithme puisse être mis en œuvre par un ordinateur, il faut qu'il soit exprimé dans un langage informatique, sous la forme d'un logiciel (souvent aussi appelé « application »). Un logiciel combine en général de nombreux algorithmes : pour la saisie des données, le calcul du résultat, leur affichage, la communication avec d'autres logiciels, etc.

Certains algorithmes ont été conçus de sorte que leur comportement évolue dans le temps, en fonction des données qui leur ont été fournies. Ces algorithmes « auto-apprenants » relèvent du domaine de recherche des systèmes experts et de l'« intelligence artificielle ». Ils sont utilisés dans un nombre croissant de domaines, allant de la prédiction du trafic routier à l'analyse d'images médicales.

ANONYMISATION

L'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et ce de manière irréversible.

BIG DATA

On parle depuis quelques années du phénomène de *Big Data*, que l'on traduit souvent par « données massives ». Avec le développement des nouvelles technologies, d'internet et des réseaux sociaux ces vingt dernières années, la production de données numériques a été de plus en plus nombreuse : textes, photos, vidéos, etc. Le gigantesque volume de données numériques produites combiné aux capacités sans cesse accrues de stockage et à des outils d'analyse en temps réel de plus en plus sophistiqués offre aujourd'hui des possibilités inégalées d'exploitation des informations. Les ensembles de données traités correspondant à la définition du *Big Data* répondent à trois caractéristiques principales : volume, vélocité et variété.

CALCUL DE HAUTE PERFORMANCE

Le calcul haute performance (en anglais : *high performance computing* ou HPC) consiste à associer un grand nombre de processeurs - de plusieurs milliers à plusieurs millions - pour construire des architectures de calcul en parallèle et diminuer les temps de calcul.

CLOUD COMPUTING

Le *Cloud Computing* (en français, « informatique dans les nuages ») fait référence à

l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. Les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage (*cloud*) composé de nombreux serveurs distants interconnectés.

COMMISSION NATIONALE INFORMATIQUE ET LIBERTÉS

Autorité administrative indépendante créée en 1978, composée d'un collège pluraliste de 17 commissaires, provenant d'horizons divers (4 parlementaires, 2 membres du Conseil économique et social, 6 représentants des hautes juridictions, 5 personnalités qualifiées désignées par le Président de l'Assemblée nationale (1), par le Président du Sénat (1), par le Conseil des ministres (3). Le mandat de ses membres est de 5 ans.

DONNÉE PERSONNELLE

Une donnée personnelle est toute information se rapportant à une personne physique identifiée ou identifiable. Mais, parce qu'elles concernent des personnes, celles-ci doivent en conserver la maîtrise.

Une personne physique peut être identifiée :

- directement (exemple : nom et prénom) ;
- indirectement (exemple : par un numéro de téléphone ou de plaque d'immatriculation, un identifiant tel que le numéro de sécurité sociale, une adresse postale ou courriel, mais aussi la voix ou l'image).

L'identification d'une personne physique peut être réalisée :

- à partir d'une seule donnée (exemple : nom) ;
- à partir du croisement d'un ensemble de données (exemple : une femme vivant à telle adresse, née tel jour et membre dans telle association) :

Par contre, des coordonnées d'entreprises (par exemple, l'entreprise « Compagnie A » avec son adresse postale, le numéro de téléphone de son standard et un courriel de contact générique « compagnie1@email.fr ») ne sont pas, en principe, des données personnelles.

DONNÉE SENSIBLE

Les données sensibles forment une catégorie particulière des données personnelles.

Ce sont des informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Le règlement européen interdit de recueillir ou d'utiliser ces données, sauf, notamment, dans les cas suivants :

- si la personne concernée a donné son consentement exprès (démarche active, explicite et de préférence écrite, qui doit être libre, spécifique, et informée) ;
- si les informations sont manifestement rendues publiques par la personne concernée ;
- si elles sont nécessaires à la sauvegarde de la vie humaine ;
- si leur utilisation est justifiée par l'intérêt public et autorisé par la CNIL ;
- si elles concernent les membres ou adhérents d'une association ou d'une organisation politique, religieuse, philosophique, politique ou syndicale.

DONNÉE BIOMÉTRIQUE

Caractéristique physique ou biologique permettant d'identifier une personne (ADN, contour de la main, empreintes digitales...).

DROIT À L'INFORMATION

Toute personne a un droit de regard sur ses propres données ; par conséquent, quiconque met en œuvre un fichier ou un traitement de données personnelles est obligé d'informer les personnes fichées de son identité, de l'objectif de la collecte d'informations et de son caractère obligatoire ou facultatif, des destinataires des informations, des droits reconnus à la personne, des éventuels transferts de données vers un pays hors de l'Union européenne.

DROIT D'ACCÈS

Toute personne peut prendre connaissance de l'intégralité des données la concernant dans un fichier en s'adressant directement à ceux qui les détiennent, et en obtenir une copie dont le coût ne peut dépasser celui de la reproduction.

DROIT DE RECTIFICATION

Toute personne peut faire rectifier, compléter, actualiser, verrouiller ou effacer des informations la concernant lorsqu'ont été décelées des erreurs, des inexactitudes ou la présence de données dont la collecte, l'utilisation, la communication ou la conservation est interdite.

DROIT D'OPPOSITION

Toute personne a la possibilité de s'opposer, pour des motifs légitimes, à figurer dans un fichier, et peut refuser sans avoir à se justifier, que les données qui la concernent soient utilisées à des fins de prospection commerciale.

FICHIER

Un fichier est un traitement de données qui s'organise dans un ensemble stable et structuré de données. Les données d'un fichier sont accessibles selon des critères déterminés.

INTELLIGENCE ARTIFICIELLE

L'intelligence artificielle (IA, ou AI en anglais pour Artificial Intelligence) consiste à mettre en œuvre un certain nombre de techniques visant à permettre aux machines d'imiter une forme d'intelligence réelle. L'IA se retrouve implémentée dans un nombre grandissant de domaines d'application.

INTERNET DES OBJETS

Selon l'Union internationale des télécommunications, l'Internet des objets (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 ». En réalité, la définition de ce qu'est l'Internet des objets n'est pas figée. Elle recoupe des dimensions d'ordres conceptuel et technique.

OPEN DATA

L'*Open Data* désigne un mouvement, né en Grande-Bretagne et aux États-Unis, d'ouverture et de mise à disposition des données produites et collectées par les services publics (administrations, collectivités locales...).

ORDINATEUR QUANTIQUE

Un ordinateur ou calculateur quantique utilise les propriétés quantiques de la matière, telle que la superposition et l'intrication afin d'effectuer des opérations sur des données. À la différence d'un ordinateur classique basé sur des transistors travaillant sur des données binaires (codées sur des bits, valant 0 ou 1), le calculateur quantique travaille sur des qubits dont l'état quantique peut posséder une infinité de valeurs.

PSEUDONYMISATION

Le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;

SANCTION

À l'issue de contrôle ou de plaintes, en cas de méconnaissance des dispositions du RGPD ou de la loi de la part des responsables de traitement et des sous-traitants, la formation restreinte de la CNIL peut prononcer des sanctions à l'égard des responsables de traitements qui ne respecteraient pas ces textes.

Avec le Règlement général sur la protection des données (RGPD), le montant des sanctions pécuniaires peut s'élever jusqu'à 20 millions d'euros ou dans le cas d'une entreprise jusqu'à 4 % du chiffre d'affaires annuel mondial. Ces sanctions peuvent être rendues publiques. Lorsque des manquements au RGPD ou à la loi sont portés à sa connaissance, la formation restreinte de la CNIL peut :

- prononcer un rappel à l'ordre ;
- enjoindre de mettre le traitement en conformité, y compris sous astreinte ;
- limiter temporairement ou définitivement un traitement ;
- suspendre les flux de données ;
- ordonner de satisfaire aux demandes d'exercice des droits des personnes, y compris sous astreinte ;
- prononcer une amende administrative.

TRAITEMENT DE DONNÉES PERSONNELLES

Un traitement de données personnelles est une opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement).

Un traitement de données personnelles n'est pas nécessairement informatisé : les fichiers papier sont également concernés et doivent être protégés dans les mêmes conditions.

Un traitement de données doit avoir un objectif, une finalité déterminée préalablement au recueil des données et à leur exploitation.

Exemples de traitements : tenue du registre des sous-traitants, gestion des paies, gestion des ressources humaines, etc.

TRANSFERT DE DONNÉES

Toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne.

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.

Exemples : suppression accidentelle de données médicales conservées par un établissement de santé et non sauvegardées par ailleurs ; perte d'une clef USB non sécurisée contenant une copie de la base clients d'une société…

N°4 INTERNET DES OBJETS : L'EXEMPLE DE L'AGRICULTURE

Texte et graphique à traduire ultérieurement

FIGURE 11 DU PRODUIT À LA PLATEFORME: LES DIFFÉRENTS MODÈLES D'AFFAIRES DES OBJETS CONNECTÉS, SOURCE PORTER & HEPPELMANN, 2014

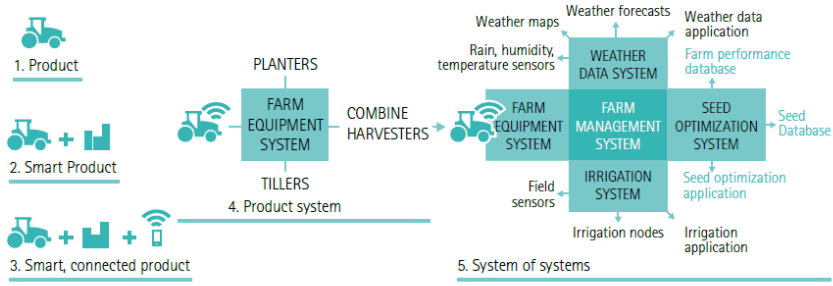
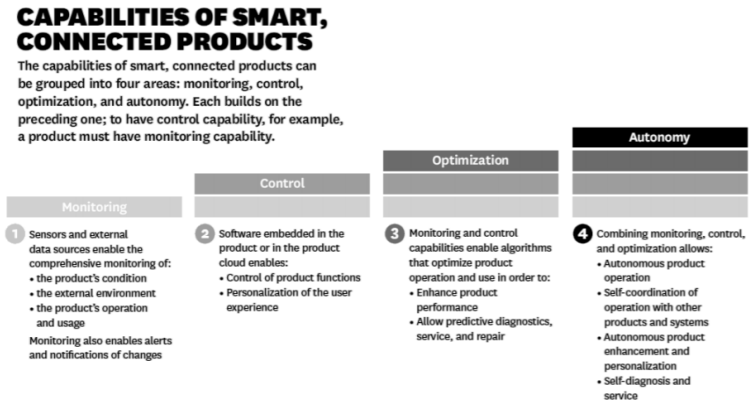


Figure 1 – Capabilities of Smart, Connected Products. Source: Porter and Heppelmann (2014, p. 8)



N°5 BIBLIOGRAPHIE

Accenture, https://www.usine-digitale.fr/article/etude-les-entreprises-sous-evaluent-les-risques-cyber-lies-aux-technologies-emergentes.N1024859

Administrateur général des données, *Rapport au Premier ministre sur la gouvernance de la donnée 2015 – Les données au service de la transformation de l'action publique*, décembre 2015

Arnaud Anciaux, Joëlle Farchy, « Données personnelles et droit de propriété : quatre chantiers et un enterrement », De Boeck Supérieur, *Revue internationale de droit économique,* 2015

Arrêts *Courage CJUE, 20 septembre 2001, Courage Ltd. C. Bernard Crehan et Bernard Crehan c. Courage Ltd. et autres, aff. C-453/99* et *Manfredi CJUE, 13 juillet 2006, Manfredi, aff. Jointes C-295-298/04*

Boris Barraud, « L'État territorial face au cyberespace mondial - L'informatique en nuage… de Tchernobyl », *Revue Lamy*, Droit de l'immatériel, janvier 2016

Annie Blandin-Obernesser (sous la direction de), *Droit et souveraineté numérique en Europe,* Bruylant, collection « Rencontres européennes », mars 2016

Chambre de commerce et d'industrie (CCI) Paris Ile-de-France, *Pérenniser l'entreprise face au risque cyber : de la cybersécurité à la cyber-résilience*

Cap Gemini Research Institute et LinkedIn, *The digital talent gap - Are companies doing enough ?*, 2017

Guillaume Chevrollier et Jean-Michel Houllegatte, sénateurs, rapport d'information *Pour une transition numérique écologique*, fait au nom au nom de la commission de l'aménagement du territoire et du développement durable par la mission d'information sur l'empreinte environnementale du numérique, juin 2020

Comité consultatif commun d'éthique pour la recherche agronomique, INRA-CIRAD, *Avis 8 sur les enjeux éthiques et déontologiques du partage et de la gestion des données issues de la recherche*, février 2016

Commission européenne, livre blanc *Intelligence artificielle - Une approche européenne axée sur l'excellence et la confiance*, COM(2020) 65 final, 19 février 2020. https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_fr.pdf

Commission européenne, *communication Stratégie européenne pour les données*, COM(2020) 66 final, 19 février 2020. https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52020DC0066&from=EN

Commission européenne, communiqué de presse « Façonner l'avenir numérique de l'Europe : la Commission présente des stratégies en matière de données et d'intelligence artificielle », Bruxelles, le 19 février 2020

Commission européenne, Open data maturity report 2019. Open Data Maturity Report 2019 | European Data Portal

Constitution de la Ve République, 4 octobre 1958

Laurent Cytermann (sous la direction de), *Rapport relatif aux données générales*, établi par le Conseil général de l'économie, de l'industrie, de l'énergie et des technologies et l'Inspection générale des finances. https://www.economie.gouv.fr/files/files/PDF/DIG-Rapport-final2015-09.pdf

Clara Dallaire-Fortier, « Le travail sous le capitalisme .de plateforme », Institut de recherche et d'informations socioéconomiques (IRIS, Canada), janvier 2020

Mireille Delmas-Marty, article « Nous basculons vers un droit pénal de la sécurité », *Le Monde*, rubrique « Idées », 24 octobre 2020

European Union Agency for Cybersecurity (ENISA), « Cybersecutity skills development in EU », décembre 2019

Exposé des motifs du projet de loi au nom du Premier ministre par M. Emmanuel Macron, ministre de l'Économie, de l'industrie et du numérique, Assemblée nationale, 9 décembre 2015

Fondation Bertelsmann, étude sur les brevets déposés entre 2000 et 2019 dans 58 technologies de rupture : *« World class patents in cutting-edge technologies. The innovation power of East Asia, North America and Europe »*, juin 2020. https://www.bertelsmann-stiftung.de/fileadmin/files/user_upload/BST_World_class_patents_2020_ENG.pdf

France Stratégie et Conseil national du numérique Anticiper les impacts économiques et sociaux de l'intelligence artificielle, mars 2017

Roberto Frega, « Les dimensions de la confiance », *Revue Esprit*, n 68, octobre 2020

Raphaël Gauvin, député, *Rétablir la souveraineté de la France et de l'Europe et protéger les entreprises des lois et mesures à portée extraterritoriales*, rapport au Premier ministre, juin 2019

Julien Hardellin et Vanina Forget, *Les perspectives offertes par la Block Chain en agriculture et agroalimentaire*, juillet 2029. https://agreste.agriculture.gouv.fr/agreste-web/download/publication/publie/Ana140/Analyse_1401907.pdf

Insee, *L'économie et la société à l'ère du numérique*, édition 2019

Henri Isaac, *Données, Valeur et Business models*, 2016. hal-01821836. https://hal.archives-ouvertes.fr/hal-01821836

Bruno Latour, « On est passé du virtuel au réel, et non du réel au virtuel », entretien du 20 novembre 2009, site Internetactu.net

Éloi Laurent, *L'économie de la confiance*, éditions La Découverte, 2019

Lean ICT, *The Shift Project 2018*

Le Big Data, « Un marché en perpétuelle croissance », 12 février 2018, https://www.lebigdata.fr

Le Big Data, « le volume de données mondial multiplié par 5 d'ici 2025 », 5 décembre 2018, https://www.lebigdata.fr

Le Monde, article « Numérique - Main basse sur les données », 18 septembre 2019

Gérard Longuet, sénateur, *Le devoir de souveraineté numérique*, rapport fait au nom de la Commission d'enquête sur la souveraineté numérique, n° 7, 1er octobre 2019

Loi n° 2015-992 relative à la transition énergétique pour une croissance verte (LTECV) du 17 août 2015

Loi n° 2016-1321 pour une République numérique du 7 octobre 2016

Loi n° 2020-1674 du 24 décembre 2020 de programmation de la recherche pour les années 2021 à 2030 et portant diverses dispositions relatives à la recherche et à l'enseignement supérieur

Mc Kinsey digital, *Reducing data cost without jeopardizing growth*, 31 juillet 2020. https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/reducing-data-costs-without-jeopardizing-growth

Markess, Big Data, analytique et gestion des données - Tendances clés, 2015

Mission confiée par le Premier ministre à Éric Bothorel, député, *Pour une politique publique de la donnée*, décembre 2020. https://www.gouvernement.fr/remise-du-rapport-sur-la-politique-publique-de-la-donnee-des-algorithmes-et-des-codes-sources. https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2020/12/rapport_-_pour_une_politique_publique_de_la_donnee_-_23.12.2020__0.pdf

Catherine Morin-Desailly, sénatrice, *L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne*, rapport d'information n° 696 fait au nom de la mission commune d'information « Nouveau rôle et nouvelle stratégie pour l'Union européenne dans la gouvernance mondiale de l'Internet », 8 juillet 2014

C. Obez, M.-C. Duboc, K. Chen, *Artificial intelligence as a solution to your complex issues in IT operations*, novembre 2019. https://www.wavestone.com/en/insight/artificial-intelligence-it-operations

Ordonnances prises en application de la loi d'urgence pour faire face à l'épidémie de covid-19, 25 mars 2020.

Organisation des Nations-unies, *Digital economy report. 2019: value creation and capture: implications for developing countries*, janvier 2020. https://digitallibrary.un.org/record/3833647?ln=fr

Elinor Ostrom, Governing the commons: The evolution of collective action, 1990

Plateforme numérique de l'alimentation (Numalim), Livre blanc *Ces données qui nourrissent la confiance et la valeur dans l'alimentation*, septembre 2020

Règlement du Conseil établissant l'entreprise commune européenne pour le calcul à haute performance, 11 février 2018. https://eur-lex.europa.eu/resource.html?uri=cellar:c48188c9-f6bb-11e7-b8f5-01aa75ed71a1.0002.02/DOC_1&format=PDF

Paul Ricœur, *Soi-même comme un autre*, éditions du Seuil, 1990

Think Tank Fing, *Transitions : l'agenda pour un futur numérique et écologique*, 2019

Joëlle Toledano, *Gafa : reprenons le pouvoir*, éditions Odile Jacob, septembre. 2020

Traité sur le fonctionnement de l'Union européenne (TFUE), articles 12 et 101(b)

Shoshana Zuboff*, L'âge du capitalisme de surveillance*, 2019 traduit de l'anglais par les éditions Zulma, octobre 2020

N°6 TABLE DES SIGLES

AFPA	Agence nationale pour la formation profressionnelle des adultes
AIEA	Agence internationale de l'énergie atomique
ALLISTENE	Alliance des sciences et des technologies du numérique
ANSSI	Agence nationale de la sécurité des systèmes d'information
APCA	Assemblée permanente des chambres d'agriculture
API	*Application Programming Interface* (Interface de programmation applicative)
BATX	Baidu, Alibaba, Tencent, Xiaom
B2G	*Business to Government*
BEPS	Érosion de la base d'imposition et transfert de bénéfices
CADA	Commission d'accès aux documents administratifs
CCI	Chambre de commerce et d'industrie
CCNE	Comité consultatif national d'éthique
CdR	Comité des régions
CEEP	Centre européen des employeurs et entreprises fournissant des services publics
CEN	Conseil européen de normalisation
CERNA	Commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique
CES	Confédération européenne des syndicats
CESE	Comité économique et social européen
CESE	Conseil économique, social et environnemental
CFDT	Confédération française démocratique du travail
CFE-CGC	Confédération française de l'encadrement-Confédération générale des cadres
CFTC	Confédération française des travailleurs chrétiens
CGT	Confédération générale du travail
CGU	Conditions générales d'utilisation
CIRAD	Centre de coopération internationale en recherche agronomique pour le développement
CJUE	Cour de Justice de l'Union européenne
CMA	Chambre de métiers et de l'artisanat
CNAV	Caisse nationale d'assurance vieillesse
CNI	Conseil national de l'industrie
CNIL	Commission nationale de l'informatique et des libertés
CNNum	Conseil national du numérique
COERLE	Comité opérationnel d'évaluation des risques légaux et éthiques
CPME	Confédération des petites et moyennes entreprises
DGCCRF	Direction générale de la concurrence, de la consommation et de la répression des fraudes
DGE	Direction générale des entreprises
DGFIP	Direction générale des finances publiques
DGSE	Direction générale de la securité extérieure

DGSI	Direction générale de la securité intérieure
DINum	Direction interministérielle du numérique
DMISC	Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces
DMP	Dossier médical partagé
DP	Dossier pharmaceutique
EDPB	*European Data Protection Board* (Comité européen de la protection des données)
EDPS	*European Data Protection Supervisor* (Contrôleur européen de la protection des données)
ENISA	*European Union Agency for Cybersecurity*
ETI	Entreprise de taille intermédiaire
FAIR	*Findable, Accessible, Interoperable, Reusable*
FAPT CGT	Fédération des activités postales et de télécommunications de la Confédération générale du travail
FTC	*Federal Trade Commission* (Commission fédérale du commerce)
GAFAM	Google, Apple, Facebook, Amazon, Microsoft
GES	Gaz à effet de serre
GFII	Groupement français de l'industrie de l'information
GIFAS	Groupement des industries françaises aéronautiques et spatiales
IA	Intelligence artificielle
IGN	Institut national de l'information géographique et forestière
INRAE	Institut national de recherche pour l'agriculture, l'alimentation et l'environnement
INRIA	Institut national de recherche en informatique et en automatique
INSEE	Institut national de la statistique et des études économiques
IoD	Internet des objets
IoT	*Internet on things*
LTECV	Loi relative à la transition énergétique pour une croissance verte
LOSSN	Loi d'orientation et de suivi de la souveraineté numérique
LPPR	Loi de programation pluriannuelle de la recherche
MEDEF	Mouvement des entreprises de France
NUMALIM	Plateforme numérique de l'alimentation
OACI	Organisation de l'aviation civile internationale
OCDE	Organisation de coopération et de développement économiques
OIV	Opérateur d'importance vitale
OMS	Organisation mondiale de la santé
PME	Petite et moyenne entreprise
RGPD	Règlement général sur la protection des données
ROME	Répertoire opérationnel des métiers et des emplois

SAIV	Sécurité des activités d'importance vitale
SCIC	Société coopérative d'intérêt collectif
SCOP	Sociétés coopératives et participatives
SICSTI CFTC	Syndicat de l'ingénierie du conseil et de techniques de l'information de la Confédération française des travailleurs chrétiens
TSN	Taxe sur les services numériques
UE	Union européenne
UNAPL	Union nationale des professions libérales
UNGE	Union nationale des géomètres-experts
UNSA	Union nationale des syndicats autonomes
USPO	Union des syndicats de pharmaciens d'officine

Dernières publications de la section section des activités économiques

Avis du CESE sur la programmation budgétaire du projet de loi de programmation pluriannuelle de la recherche

Sylviane Lejeune

Contribution du CESE au projet de loi de programmation pluriannuelle de la recherche

Sylviane Lejeune

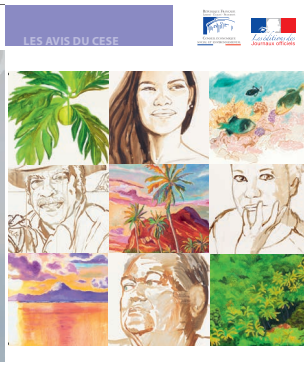
Filières stratégiques : définir et mettre en œuvre les priorités

Marie-Claire Cailletaud et Fréderic Grivot

Dernières publications du Conseil économique, social et environnemental

Filières stratégiques : définir et mettre en œuvre les priorités

Marie-Claire Cailletaud et Fréderic Grivot



Plan de relance et déclinaison territoriale dans les Outre-mer

Inès Bouchaut-Choisy, Olivier Mugnier et Christian Vernaudon

Climat, neutralité carbone et justice sociale

Avis du CESE sur le projet de loi portant lutte contre le dérèglement climatique et renforcement de la résilience face à ses effets

Michel Badré et Claire Bordenave

Retrouvez l'intégralité des travaux du CESE sur le site

www.lecese.fr

Imprimé par la Direction de l'information légale et administrative, 26, rue Desaix, Paris 15e,
d'après les documents fournis par le Conseil économique, social et environnemental.
N° 411210006-000221 - Dépôt légal : février 2021

Crédit photo : Getty images

PEFC Certifié PEFC 70 % FCBA/10-01283 IMPRIM'VERT®

Le développement massif des données et de leur exploitation offre un champ considérable d'opportunités économiques et d'accroissement des connaissances. Ces évolutions ont rendu plus aigus les enjeux industriels, économiques, commerciaux et génèrent une lutte mondiale implacable, pour la possession, la gouvernance et l'appropriation des données.

Ainsi, la défense des droits fondamentaux et des libertés individuelles et collectives constituent des enjeux d'une importance primordiale, au même titre que la préservation des souverainetés nationales remises en question par de puissants acteurs internationaux du numérique.

Dans cet avis, le Cese fait état des principaux défis de gouvernance et de régulation de l'économie de la donnée et formule des propositions pour qu'ils soient affrontés. Si la France dispose d'atouts institutionnels, industriels et de recherche, le Cese estime qu'elle doit les renforcer par des coopérations accélérées et solides au sein de l'Union européenne, dans un dialogue nourri avec les acteurs.

CONSEIL ÉCONOMIQUE, SOCIAL
ET ENVIRONNEMENTAL
9, place d'Iéna
75775 Paris Cedex 16
Tél. : 01 44 43 60 00
www.lecese.fr

N° 41121-0006
ISSN 0767-4538 ISBN 978-2-11-155695-9

9 782111 556959

Direction de l'information légale et administrative
Les éditions des *Journaux officiels*

www.vie-publique.fr/publications