INSTITUT
MONTAIGNE

Données personnelles : comment gagner la bataille

ÉTUDE DÉCEMBRE 2019

Think tank indépendant créé en 2000, l'Institut Montaigne est une plateforme de réflexion, de propositions et d'expérimentations consacrée aux politiques publiques en France et en Europe. À travers ses publications et les événements qu'il organise, il souhaite jouer pleinement son rôle d'acteur du débat démocratique avec une approche transpartisane. Ses travaux sont le fruit d'une méthode d'analyse et de recherche rigoureuse et critique, ouverte sur les comparaisons internationales. Association à but non lucratif, l'Institut Montaigne réunit des chefs d'entreprise, des hauts fonctionnaires, des universitaires et des personnalités issues d'horizons divers. Ses financements sont exclusivement privés, aucune contribution n'excédant 1,5 % d'un budget annuel de 5,6 millions d'euros.

Il n'est désir plus naturel
que le désir de connaissance

INSTITUT
MONTAIGNE

Données personnelles : comment gagner la bataille

DÉCEMBRE 2019

À propos de l'auteur

François Godement, conseiller pour l'Asie, Institut Montaigne

François Godement est Conseiller pour l'Asie à l'Institut Montaigne. Il est également *Senior non resident fellow* du *Carnegie Endowment for International Peace,* et consultant externe au ministère de l'Europe et des Affaires étrangères français. François Godement était précédemment directeur du programme Asie de l'ECFR, professeur des universités à l'INALCO (Institut national des langues et civilisations orientales) puis à SciencesPo Paris. Il a fondé le Centre Asie de l'IFRI, le CSCAP Europe *(Council for Security Cooperation in the Asia-Pacific)*, et le *think tank* Asia Centre. Son dernier ouvrage publié est : *La Chine à nos portes – une stratégie pour l'Europe* (avec Abigael Vasselier), Odile Jacob, 2018.

SOMMAIRE

INTRODUCTION

« Les gentlemen ne lisent pas le courrier des autres ». En réalité, ils le font parfois, légalement ou subrepticement. La nouveauté, c'est qu'ils n'ont plus besoin d'ouvrir l'enveloppe à la vapeur. Si nous n'écrivons plus de lettres à l'ancienne, nous émettons des données personnelles jour et nuit. Sauf en cas de chiffrement de bout en bout, ou plus rarement, de chiffrement de contenu, ces données flottent dans le cyberespace.

Mais comment les gentlemen peuvent-ils s'y retrouver dans les exaoctets de données qui circulent à travers le cyberespace depuis le sanctuaire qu'est votre domicile, ou dans les 3 milliards de smartphones en circulation aujourd'hui, ou la multitude d'objets connectés de demain ? La sécurité est-elle encore assurée face à cette démesure ? La plupart des utilisateurs numériques ne croient pas que leurs données sont en totale sécurité, mais ils se fient au vieil adage : personne ne trouvera une aiguille dans une botte de foin.

Avec cette réserve à l'esprit, l'ère numérique est devenue la dernière frontière libre de notre époque. Pour utiliser une métaphore, l'ère numérique est aux ères précédentes ce que l'exploration maritime a été pour relier les États terrestres, « l'équivalent au XXIe siècle des « continents obscurs » qui ont attiré les spéculateurs européens du XIXe siècle sur leurs rivages »[1]. Ou alors ce que l'ouverture de l'Ouest américain a représenté pour les pionniers venus des premiers états de l'est : des terres d'opportunités où les lois n'étaient guère appliquées. Avec leurs inconvénients : l'utilisation de corsaires était

[1] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York: Publicaffairs, 2019, p. 103.

une pratique officielle des nations maritimes. On était libre en mer, y compris de devenir la proie de ces mêmes corsaires ou de maraudeurs. De même, la « loi du Far West » était un euphémisme. Les rumeurs sociales ou les *fake news,* la récupération à des fins commerciales des *small data* de tous les utilisateurs, les questions de cybersécurité en sont l'équivalent contemporain.

Vivre à la frontière numérique

La révolution numérique, une combinaison de big data[2], d'algorithmes prédictifs et d'informatique quantique promet de changer nos vies comme aucune autre avancée ne l'a fait. En effet, relier des nombres entre eux, même s'il s'agit « d'objets » comme dans « l'Internet des objets » (IdO), touche au cœur du comportement humain, et un jour de notre processus de pensée intérieur. Pour le moment, la révolution se contente de prédictions statistiques fondées sur l'exploration approfondie du comportement humain, mais un jour ces prédictions, et les variables de comportement sur lesquelles elles reposent, deviendront tellement granulaires et précises qu'elles seront contemporaines ou même synonymes des processus de la pensée humaine. Les performances combinées des algorithmes et du *big data* ne s'arrêtent pas là. Des machines battent des êtres humains aux échecs, au jeu de go – une expérience beaucoup plus multidimensionnelle, et maintenant au poker[3]. L'interprétation de l'imagerie thoracique (recherche de tumeurs, choix du traitement)

[2] Pour une présentation claire et un récit historique de ce phénomène : Gilles Babinet, *Big Data, penser l'homme et le monde autrement*, Paris : Le Passeur Éditeur, 2016, p. 25-51.

[3] Noam Brown et Tuomas Sandholm, « Superhuman AI for multiplayer poker », *Science,* 30 août 2019.

par l'intelligence artificielle (IA) surpasse constamment celle des meilleures équipes médicales.

Ces réalisations s'accompagnent de visions d'utopie. Qui a besoin de bibliothèques physiques lorsque les *clouds* internet fournissent beaucoup plus de capacités et les grandes bibliothèques deviennent elles aussi des *clouds* ? La Bibliothèque du Congrès américain, par exemple, a reçu en dépôt une archive complète de TOUS les tweets postés sur Twitter pendant les premières décennies. Un smartphone moyen donne accès à un volume d'informations auquel aucun individu de l'ère précédente n'a jamais eu accès, sous quelque forme que ce soit. Certains prétendent que la révolution numérique, accompagnée par l'informatique et les serveurs en périphérie de réseau (local) et des logiciels intégrant de l'IA, rendra obsolète la révolution industrielle fordiste et tayloriste. L'imagerie, le diagnostic à distance et le diagnostic prédictif vont révolutionner la médecine préventive et permettre de traiter des milliards de personnes qui n'avaient pas un accès approprié aux médecins et aux ressources médicales. Les décisions automatisées deviendront monnaie courante et allègeront le poids des corvées quotidiennes, tout comme le travail physique a diminué au cours des premières révolutions industrielles. Au bout du compte, nous serions donc de purs esprits concentrés sur l'innovation, les loisirs et la communication instantanée avec toutes les autres monades du monde, en surmontant les barrières physiques, linguistiques et culturelles.

Ou pas.

Le meilleur des mondes des données

L'autre vision est celle d'une dystopie, dont un aspect est économique, avec la perspective du chômage de masse : les emplois des « cols blancs », dont beaucoup étaient auparavant considérés comme qualifiés, seront automatisés. Mais la vision dystopique dominante est plutôt centrée sur la disparition de la notion de vie privée à des fins commerciales ou de contrôle. L'argument est presque le même que celui de la vision utopique, à tel point qu'on peut le considérer comme son envers.

Le conflit entre droits individuels et droits souverains est le plus vieux conflit de la philosophie politique. Mais à l'ère du numérique, on peut remplacer la notion d'individualisme par la question du respect de la vie privée. Il ne peut y avoir de droits individuels sans respect de la vie privée. Si un sondage devient suffisamment granulaire pour prédire le vote d'une personne donnée avec *une quasi-certitude,* le secret du vote n'existe plus. L'équipe de campagne d'Obama à l'élection présidentielle de 2008 a compilé des données sur plus de 250 millions d'Américains. Selon un participant, « nous savions… pour qui les gens allaient voter avant même qu'ils ne l'aient décidé. » L'équipe de campagne pour la réélection du président en 2012 connaissait « le nom, l'adresse, la race, le sexe et les revenus de tous les électeurs hésitants qu'il fallait convaincre de voter pour Obama » et a créé des « scores de persuasion » pour les électeurs indécis[4]. À notre connaissance, l'équipe de campagne d'Obama n'a enfreint aucune loi. Cette campagne est même devenue un modèle ailleurs dans le monde dans des contextes démocratiques ouverts. Certaines des personnes qui y avaient participé ont travaillé plus

[4] Cité par *Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power,* New York : Publicaffairs, 2019, p. 122-123.

tard sur la campagne de Trump et pour Cambridge Analytica, la société impliquée dans ce qui est probablement à ce jour le scandale de fuite des données personnelles le plus flagrant.

« Avec une quasi-certitude » : dans cet îlot minuscule où le hasard peut encore l'emporter sur la nécessité, peut-on vraiment trouver un reste de choix humain et d'autodétermination ? Cela n'est concevable que dans une société protégée par un droit positif et des institutions. Ailleurs, la quasi-certitude suffit à vous cataloguer ou vous juger.

Chaos prédictif

Le cœur du débat juridique sur les droits individuels, l'*habeas corpus,* a souvent porté sur la légalité des pratiques, et non sur leur réalité qui ne faisait guère de doute : *habeas corpus* signifie que le « corps » ou sujet doit être traduit en justice, et non traité autrement. En termes de données numériques, il s'agit de l'obligation légale de prévenir toute « intrusion dans l'intimité », et de l'utilisation publique et légalement admissible des données collectées. Les sociétés de technologies financières chinoises fonctionnent sur des grandes plateformes ayant accès à beaucoup plus de types de données que ce qui est légalement admissible en Occident : elles peuvent fournir une notation de crédit ou d'assurance en quelques secondes au plus petit des entrepreneurs sur la base d'un ensemble de données qui inclut de nombreuses habitudes personnelles et d'éventuels incidents. Il est presque certain qu'une personne physique ou morale possédant des ressources d'IA pourra jouer avec les marchés dans un avenir proche (on peut supposer le même résultat pour des scénarios de guerre). Cependant, si *plusieurs* personnes physiques ou morales

rivalisent avec des algorithmes, le chaos et une totale incertitude pourraient en résulter. La résistance du marché tient au fait, comme le suggère Friedrich Hayek, qu'aucun esprit humain individuel ne peut égaler « l'utilisation coordonnée de ressources basées sur des connaissances réparties équitablement »[5]. Fin de la partie. Mais même Hayek n'avait pas envisagé que les algorithmes puissent jouer l'un contre l'autre et créer une instabilité générale. Le principe d'incertitude n'est pas l'équivalent d'un jeu libre du marché.

Ce qui précède doit être nuancé par deux questions interdépendantes. La première est celle de la précision, étroitement liée à la qualité des algorithmes utilisés. Peu de domaines de l'IA concernant le comportement humain sont susceptibles d'atteindre le niveau de fiabilité acquis par le décryptage d'ADN (mais pas la manipulation et la conservation des échantillons). Et les banques de données volumineuses ne valent pas plus que le logiciel qui permet de les interpréter.

Mais tout cela doit être relativisé par une seconde question : celle de la certitude relative qui peut suffire dans certains systèmes. La reconnaissance faciale est devenue tellement courante qu'une application russe en vente libre met cette technologie à la disposition de tout internaute[6]. Mais elle est encore truffée de « faux positifs » et de « faux négatifs » (erreurs d'identification ou absence de correspondance réelle). La plupart des experts reconnaissent que le chemin à parcourir pour passer de 90 % à 100 % de précision est bien plus difficile que celui qui a permis de passer de 50 % à 90 %,

[5] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York : Publicaffairs, 2019, p. 497

[6] Kevin Webb, « Viral app that makes you look old with shocking precision may be quietly keeping all your data », *Business Insider France,* 17 juillet 2019, https://www.businessinsider.fr/us/faceapp-privacy-data-terms-service-russia-2019-7

sans compter les éventuelles tromperies et dissimulations. Pourtant, certains systèmes de gouvernance se contenteront de 90 % de précision, surtout si ce résultat est combiné à d'autres résultats prédictifs.

Les créateurs de l'ère numérique ne sont pas les premiers inventeurs de l'informatique, ni même d'Internet. Ce sont des entrepreneurs qui en ont fait un produit presque universel et qui ont créé un nouveau champ immense de médias sociaux et d'utilisation des données. Ils étaient souvent convaincus d'apporter une liberté illimitée aux individus, notamment en les libérant de réglementations pesantes. Cette liberté promettait un épanouissement. « Le monde en ligne n'est pas véritablement soumis aux lois terrestres… C'est le plus grand espace non gouverné du monde »[7]. En pratique, à l'ère numérique, les utilisateurs ont l'illusion que leur vie privée est bien mieux respectée qu'à n'importe quelle autre époque : en fait, d'une manière ou d'une autre, ils confient la plupart de leurs données privées à l'espace numérique.

N'est-il pas révélateur que les rencontres en ligne sont devenues le moyen le plus répandu (39 %) par lequel les couples se forment en assumant le rôle que la famille, les amis et l'espace public jouaient autrefois[8] ? On peut faire valoir que cette méthode de recherche de partenaires offre plus de confidentialité que les méthodes précédentes

[7] Eric Schmidt et Jared Cohen, T*he New Digital Age Reshaping the Future of People, Nations and Business,* London Murray, 2014.

[8] Ce pourcentage de 39 % s'applique aux couples hétérosexuels. D'après la même étude, le pourcentage de rencontre en ligne atteint 65 % chez les couples homosexuels.
Source : Michael J. Rosenfeld, Reuben J. Thomas et Sonia Hausen, « Disintermediating Your Friends: How Online Dating in the United States Displaces Other Ways of Meeting », *Proceedings of the National Academy of Sciences* 116, n° 36, 20 août 2019, p. 4, https://doi.org/10.1073/pnas.1908630116.

qui faisaient appel à des intermédiaires ou à des recherches publiques. Faire des recherches sur Google, vagabonder sur le net, échanger sur les médias sociaux sont autant d'activités qui semblent mettre en valeur l'individu face aux contraintes et inhibitions de la communauté. Le cyberespace est le plus grand espace public de tous les temps et pourtant, il est considéré comme un lieu de rencontre très privé. Si tel n'était pas le cas, les contenus réservés aux adultes n'auraient pas représenté 30 % du trafic Internet, comme cela fut le cas jusqu'à ce les nouveaux médias en streaming apportent une alternative à la maison et absorbent 60 % du trafic Internet total. Il convient tout de même de préciser que, selon toute vraisemblance, l'immense majorité des clients du premier type de contenus n'aurait jamais imaginé les confier à un bureau de poste, même si les gentlemen détournent le regard.

Cette nouvelle liberté est indéniable, de même que les nombreuses possibilités offertes par l'ère numérique. Mais le revers de la médaille apparaît de plus en plus évident : la récupération des données individuelles que nous laissons sur les médias numériques, la mesure même dans laquelle chacun de nos mouvements, de nos actes et, de plus en plus souvent nos pensées sont déclenchés *via* un média numérique et donc exposés à la surveillance, peut-être à jamais et sans rémission, tout cela crée un monde de transparence, où la surveillance est la coutume sinon la règle. Pour dire les choses simplement, nous adoptons de nouveaux outils numériques et de nouvelles plateformes de médias sociaux qui réduisent notre intimité. Trouver un équilibre entre liberté et vie privée est un choix extrêmement difficile, même au niveau individuel.

À l'instar de l'ère nucléaire, il est impossible de dés-inventer l'ère numérique

Le *big data* n'est pas seulement le « nouvel or noir ». Les algorithmes en font l'équivalent humain de la fission nucléaire, également connue sous le nom de bombe atomique. Pour reprendre les mots d'Eric Schmidt, « rien, à l'exception d'un virus biologique, ne peut évoluer aussi rapidement, efficacement et agressivement que ces plateformes technologiques, ce qui confère une certaine puissance aux personnes qui les construisent, les contrôlent et les utilisent »[9]. Ou comme l'explique Jim Balsillie, ancien PDG de RIM (Blackberry) : « Les données au niveau micro-personnel donnent à la technologie un pouvoir d'influence sans précédent. Les données ne sont pas le nouveau pétrole, elles sont le nouveau plutonium. Elles sont incroyablement puissantes, dangereuses quand elles se propagent, difficiles à nettoyer, et elles peuvent avoir des conséquences graves quand elles sont mal utilisées »[10]. Dans un avenir proche, l'expansion de l'ère numérique avec l'Internet des objets nous placera au cœur d'un réseau composé d'une multitude d'appareils interconnectés, dotés d'une forme d'IA et équipés de capteurs enregistrant leur environnement, et donc également le nôtre. Dans une certaine mesure, nous deviendrons les sujets de ces réseaux, ou c'est un opérateur qui le sera. Mais il est plus que probable que ces réseaux évolueront d'un objet que nous possédons vers un objet qui nous possède. Déjà, certaines des entreprises qui possèdent et vendent tous les éléments ou aspects de nos données personnelles sont des sociétés dont nous ne connaissons même pas le nom. Acxiom, une

[9] Eric Schmidt et Jared Cohen, *The New Digital Age Reshaping the Future of People, Nations and Business*, London Murray, 2014, p. 9-10.

[10] Jim Balsillie, « Data Is Not the New Oil – It's the New Plutonium », *Financial Post,* 28 mai 2019, https://business.financialpost.com/technology/jim-balsillie-data-is-not-the-new-oil-its-the-new-plutonium.

société de courtage en données indépendante désormais rebaptisée LiveRamp, affirme avoir accumulé en 2018 jusqu'à 10 000 attributs sur 2,5 milliards de personnes, soit une « représentation complète de 68 % de la population mondiale en ligne »[11].

Le fait de relier très peu de points de métadonnées provenant de sources dispersées, permet désormais d'identifier des individus, même lorsque chacun de ces points de données a été collecté de façon anonyme. L'IA, c'est une multitude de cerveaux réunis qui, dans tous les cas, ira plus vite que n'importe quelle pensée ou action humaines. La même chose peut arriver au cryptage, qui sera vaincu par l'informatique quantique. Ce qui importe dans ce qui précède, ce n'est pas seulement que le respect de la vie privée, défini comme la confidentialité et un principe d'incertitude quant aux actions humaines, soit remplacé par une connaissance presque complète de l'esprit individuel, ou du moins par la catégorisation et le caractère prévisible, c'est également qu'une énorme asymétrie a été créée entre les opérateurs des systèmes et leur objet, à savoir l'individu. Les prophètes de cette ère ont parfaitement anticipé cette dépossession. B.F. Skinner, un éminent psychologue du comportement, a écrit en 1971 : « *À l'homme en tant qu'homme,* nous disons sans hésiter : bon débarras. Ce n'est qu'en le dépossédant que nous [...] pourrons passer de l'inféré à l'observé, du miraculeux au naturel, de l'inaccessible au manipulable »[12].

[11] La société a changé de propriétaire après le scandale de Cambridge Analytica en 2018. Source : Alex Pasternack, « Here Are the Data Brokers Quietly Buying and Selling Your Personal Information », *Fast Company,* 2 mars 2019, https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information.

[12] Burrhus Frederic Skinner, *Beyond Freedom & Dignity* (Indianapolis, Ind.: Hackett Pub, 2002) [Traduction française : Par delà la liberté et la dignité]. Cité par Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York : Publicaffairs, 2019, p. 439.

La dépossession s'étend à des caractéristiques humaines incontrôlables : déduire des préférences et des sentiments humains. « Avec suffisamment de données, les chiffres parlent d'eux-mêmes »[13]. Les « J'aime » sur Facebook permettent de déduire l'orientation sexuelle avec une précision de 88 %. Des schémas de frappe sur un clavier permettent également de détecter le sentiment de tristesse avec une précision de 88 % : ces résultats remontent à 2011, et l'on ne peut que deviner les progrès réalisés depuis[14]. Et bien entendu, il existe également des asymétries entre les opérateurs, ce que l'on reconnaît habituellement à leur part de marché respective, car le premier arrivé bénéficie d'une prime énorme. Mais cette inégalité est bien compensée par une autre : les opérateurs qui peuvent accéder légalement à des bases de données plus importantes dans différents domaines, et les utiliser de manière moins restrictive, deviendront plus efficaces que ceux qui sont assujettis à des réglementations anti-monopole, de protection de la vie privée ou à d'autres contraintes.

De nombreux autres pays ont une base de départ et un programme pour l'ère numérique très diverse par rapport à ceux des États-Unis. Nous examinerons trois cas : l'Union européenne (UE) et son cadre réglementaire par le haut, la Chine et sa vision étatiste du contrôle et de l'innovation associée au dynamisme par le bas, et l'Inde qui présente des caractéristiques à la fois de l'UE et de la Chine tout en étant très intégrée à l'économie numérique américaine. Des différences existent, tant du point de vue technologique et sociétal que réglementaire.

[13] Chris Anderson, « The End of Theory: The Data Deluge Makes the Scientific Method Obsolete », *Wired,* 23 juin 2008, https://www.wired.com/2008/06/pb-theory/.

[14] Wolfie Christl, « Corporate Surveillance in Everyday Life - How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions », *Cracked Labs,* juin 2017, https://crackedlabs.org/dl/CrackedLabs_Christl_CorporateSurveillance.pdf

Au-delà de ces cas, des distinctions plus générales peuvent être faites: soit les pays sont trop petits ou trop peu développés pour réglementer un espace numérique sur lequel ils n'ont aucune emprise. Ils sont alors axés sur le marché et opteront pour des solutions rentables et efficaces pour les clients, au mépris du respect de la vie privée et du contrôle gouvernemental sur le contenu des communications. Soit leur gouvernance est autoritaire et ils choisiront des environnements numériques qui facilitent la surveillance et une éventuelle fermeture. Comme nous le verrons, l'équilibre réglementaire qui a toujours été au cœur du choix européen n'est pas facile à définir. Il est également très difficile à mettre en œuvre et exige des règles sophistiquées ainsi que des ressources humaines importantes.

Cette étude identifie les principaux acteurs du débat sur la confidentialité des données (I), étudie ses formulations juridiques (II), examine les trois cas que nous avons choisi d'ausculter (III, IV et V), procède à une analyse plus particulière de la question des données de santé (VI) et conclut par les questions en suspens et des propositions de régime de protection des données (VII).

I

DÉFINITION DE LA QUESTION ET DU DÉBAT

L'objectif de la protection des données à caractère personnel et du respect de la vie privée s'inscrit dans le cadre d'un équilibre réglementaire que l'on peut définir en termes très simples d'un triangle. Comme un juge de la Cour suprême indienne l'a exprimé en juillet 2018 : « Les droits des citoyens doivent être protégés, les responsabilités des États doivent être définies, mais la protection des données ne peut se faire au détriment du commerce et de l'industrie »[15]. Cependant, l'analyse de ces définitions élémentaires ne fait qu'aggraver le problème. Ce n'est pas seulement le droit des citoyens au respect de la vie privée qui doit être protégé, mais également les données des entreprises et les données relatives aux droits de propriété intellectuelle. L'intérêt de l'État ne concerne pas uniquement la sécurité nationale ou publique. Il implique également de définir l'intérêt public, et ce sont les exemples les plus évidents, la priorité des banques de données de santé par rapport au droit des patients à la vie privée ou le droit des médias libres à enquêter par rapport à la protection de l'individu. L'efficacité, ou la logique économique, peuvent impliquer de constituer des banques de données de plus en plus importantes dans différents domaines qui non seulement remettent en question la protection de la vie privée, mais créent également des oligopoles.

[15] ET Bureau, « Justice Srikrishna Committee Submits Report on Data Protection. Here're Its Top 10 Suggestions », *The Economic Times,* 27 juillet 2018, https://economictimes.indiatimes.com/articleshow/65164663.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

Du plus, cet équilibre réglementaire est une cible mouvante. Depuis le début de l'ère numérique, les innovations technologiques ou commerciales ont eu tendance à devancer les règles. C'est encore plus vrai de l'IA et d'autres avancées récentes qui reposent sur la puissance de calcul des algorithmes.

Il n'est pas surprenant que la question de la collecte des données et de la protection de la vie privée soit omniprésente. C'est un point de départ naturel, à moins de désinventer les techniques algorithmiques qui transforment les données en arme, comme les suggèrent les propos accusateurs de Shoshana Zuboff : *« Si de nouvelles lois interdisaient les activités d'extraction de données, le modèle de surveillance imploserait »*[16]. Rappelons que la législation antérieure sur la collecte des données n'était qu'une simple traduction à l'ère informatique naissante des réserves contre le fichage des individus. La loi suédoise de 1973 relative aux données exigeait d'abord l'autorisation d'une autorité nationale de protection des données pour conserver des données à caractère personnel, puis des directives de cette autorité. Le texte français de 1978, la Loi Informatique et Libertés, était un document d'une seule page. Il interdisait l'utilisation pour toute décision publique ou privée de données reposant sur l'utilisation exclusive de fichiers automatisés établissant le profil de la personnalité d'un individu ou contenant des informations à son sujet. Ces fichiers automatisés ne pouvaient absolument pas être utilisés dans le cadre de décisions judiciaires[17]. En bref, la loi n'interdisait ni la collecte ni l'utilisation de fichiers, mais seulement leur recoupement et les décisions qui en découlaient.

[16] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, New York : Publicaffairs, 2019, p. 105.

[17] Assemblée nationale et Sénat, « Loi N° 78-17 du 6 Janvier 1978 Relative à l'informatique, Aux Fichiers et Aux Libertés », https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460

Ces restrictions étaient originales, mais elles semblent encore plus fragiles aujourd'hui qu'elles ne l'étaient à l'époque.

Mais jusqu'où aller et dans quelle direction ? Ce qui est certain, c'est que les flux de données sont trop bénéfiques à la croissance mondiale pour être fortement entravés par la réglementation ou le contrôle, à moins d'accepter un coût très important. Au cours de la seule décennie 2005-2014, les flux de données (informations, recherches, communications, transactions, vidéos et trafic intra-entreprise) ont été multipliés par 45. Leur contribution à l'augmentation du PIB est supérieure à celle des flux de marchandises. Le commerce électronique a également représenté 12 % de l'ensemble des biens échangés en 2015. L'avènement de l'impression 3D devrait réduire les échanges de biens dans un avenir proche, car la production sera souvent relocalisée. Cette évaluation économique abrupte ne tient pas compte des multiples avantages que l'ère numérique apportera de manière croissante. Contrairement au travail ou aux machines de l'ère industrielle, l'information est évolutive et ne s'épuise pas lorsqu'elle est consommée. « En bref, l'économie de l'information numérique n'est pas une économie de pénurie, mais une économie de l'abondance. Il s'agit d'un changement fondamental et fondamentalement bénéfique. Aujourd'hui, si vous avez accès à Internet et disposez d'un appareil connecté, il est facile et gratuit de rester en contact avec les personnes qui comptent pour vous, vos proches, même lorsque vous êtes en déplacement. Les technologies numériques améliorant l'efficacité des marchés et des entreprises, elles profitent à nous tous, les consommateurs »[18]. Même l'asymétrie d'information entre opérateurs décrite ci-dessus n'est pas complète.

[18] Erik Brynjolfsson et Andrew McAfee, *Race Against the Machine: How the Revolution Is Accelerating Inovation, Driving Productivity, and Irreversibly Transforming Employment and the Economy,* Lexington : Digital Frontier Press, 2011, p. 46.

Si les besoins en matière d'éducation ont été satisfaits, la diffusion des technologies de l'information peut donner des moyens aux microentreprises et aux entreprises jusqu'alors considérées comme éloignées des principaux centres de production.

La prise de conscience de leur danger provient de l'expérience des États autoritaires. George Orwell est la référence littéraire incontournable, de même que son nouvel homologue cinématographique, *Black Mirror.* La marche de la Chine vers une dystopie où l'État collecte des données en masse et les utilise en est un exemple. Mais cette réalité ne se limite pas aux systèmes autoritaires. Les lois peuvent être différentes, mais souvent les outils se ressemblent beaucoup, ne serait-ce que parce qu'il y a eu de nombreux croisements, par exemple entre la Silicon Valley ou la scène numérique américaine, et les concurrents apparus en Chine et qui ont parfois dépassé leurs modèles en taille. Pour évaluer sereinement ce qu'un « État de la surveillance » peut réaliser, il faut également comprendre les outils déjà développés par ce que Shoshana Zuboff, par exemple, appelle le nouveau « capitalisme de surveillance ».

De toute évidence, l'environnement juridique fait une différence, même dans une situation où la collecte de données ne peut être désinventée et où les technologies disponibles créent une asymétrie forte entre l'individu et l'État, ou l'entreprise. Dans nos sociétés, le fait d'utiliser le moteur de recherche de Google ne vous conduira pas en prison (sauf s'il s'agit du *dark web*), alors qu'au Xinjiang (Chine), plus d'un million de citoyens issus de minorités qui se sont retrouvés dans les algorithmes de la plateforme *Integrated Joint Operations Platform* (IJOP, 一体化联合作战平台, l'application téléphonique qui collecte des données pour le ministère de la Sécurité

publique), ont été internés dans des camps de rééducation[19]. Pourtant, les différents outils (collecte de données, établissement de lien entre diverses sources et utilisation d'algorithmes prédictifs) ont une certaine parenté entre eux. C'est encore plus évident quand on compare le système de crédit social de la Chine, qui connaît une croissance rapide, avec le système de notation de crédit vieux de plusieurs décennies et particulièrement répandu aux États-Unis. Ce dernier est constamment affiné par l'introduction de nouveaux algorithmes. En Chine, des centaines de milliers de personnes se voient refuser des réservations de billets de train à grande vitesse, d'avion et autres, parce qu'ils ont reçu une mauvaise notation de crédit social n'ayant aucun lien avec les voyages en train. Ils disposent de peu de moyens de corriger leur score. Aux États-Unis, si vous ne payez pas les primes d'assurance de votre voiture, la compagnie d'assurance a parfois la possibilité de couper le moteur à distance au moment de son choix : la sanction est assez grave, mais au moins elle est directement liée au défaut de paiement[20].

[19] « China's Algorithms of Repression | Reverse Engineering a Xinjiang Police Mass Surveillance App », *Human Rights Watch,* 1er mai 2019, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance.

[20] Gary Hoffman, « Car Payment or Else: Engine Shut off Systems », *Autoblog,* 19 décembre 2016, https://www.autoblog.com/2009/06/27/engine-shut-off-systems/?guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAC8mFb3frqN6hIkaLhdvtwsLC0OW6P1A5Sn7mS8i9tvO6Lc8qsEm0fjWMPZk7SkW8_kirojwhauEJtoFnbnBbORFaKKrrjtqBaJnvN_0I2V_mNKAEniWBrGz1dOYbcTr5hZIHRDTODW-q6F2npEHCZeJSXExx6d9aiZqLTd8YLV5&guccounter=2

La matrice américaine

La façon dont les sociétés relèvent ce défi, impliquant à la fois les utilisations positives de l'ère numérique, ses inconvénients et ses possibilités terrifiantes, est une question qui nous concerne tous. Elle a de multiples facettes, mais celle du respect de la vie privée et des débats autour de ce droit est pertinente, parce qu'elle se trouve à l'intersection de l'individuel et du collectif, de la technologie et de la réglementation. Elle illustre les grandes différences entre les sociétés et les systèmes politiques et, à certains égards, elle évoque deux débats antérieurs. De façon directe, ce sont les débats autour des lois sur la diffamation qui ont surgi avec la presse écrite. Dans une perspective plus large, c'est le débat pour ou contre l'énergie nucléaire. Comme les premiers, elle est directement liée à la question de la liberté et de ses restrictions. Comme ce dernier, elle oppose les promoteurs de l'efficacité à ceux qui donnent la priorité au principe de précaution. Et elle a la même ampleur que ces deux débats. L'ère numérique combine une centralisation extrême des données, des plateformes et des opérateurs, jusqu'aux grandes entreprises publiques et aux sociétés géantes, avec une diffusion extrêmement large de certaines de ses fonctions. Avant même que l'informatique en périphérie de réseau ne devienne monnaie courante, les médias sociaux ont créé des réactions en chaîne qui s'apparentent à des événements biologiques tels que les épidémies. Les rumeurs et les *fake news* avaient cours aux siècles passés. Elles avaient été remplacées par la propagande de masse au XX^{e} siècle. Elles sont de retour.

Le débat sur le respect de la vie privée a deux matrices. L'une est clairement celle des États-Unis, pays où une grande partie des technologies numériques a été inventée. Les entreprises qui les ont lancées, qu'elles soient grandes ou non, ont une influence mondiale.

En raison de la liberté académique qui règne dans ce pays et du goût des Américains pour les débats de fond, le concept même de vie privée a été largement redéfini outre-Atlantique. La culture de la litigation juridique y est tout aussi importante. De nombreuses affaires impliquant les *big data* et le respect de la vie privée sont arbitrées par des tribunaux. Elles font jurisprudence et ont de lourdes conséquences financières. Les vents dominants ont également tourné et l'opinion publique est passée d'une foi aveugle dans les promesses de l'ère numérique à une prise de conscience de ses dangers pour la vie privée et la liberté. Dans une certaine mesure, la génération Apple (qui a débuté dans un garage en 1976) avait emboîté le pas à la génération précédente du festival de Woodstock (1969) et à sa rébellion contre la culture d'entreprise dominante. Aujourd'hui, la génération suivante se bat contre les entreprises du numérique pour son droit à la vie privée. Les militants des données personnelles sont les héritiers de Ralph Nader et du combat en faveur des droits des consommateurs contre les entreprises, notamment dans l'affaire de la Chevrolet Corvair.

L'Amérique est donc la mère de tous les débats sur le respect de la vie privée. Elle a dans le passé promulgué des textes de loi importants. En se fondant sur le Quatrième Amendement à la Constitution des États-Unis d'Amérique, « tout homme est maître chez lui… », la loi Wiretap (1968) et l'*Electronic Communications Privacy Act* (ECPA, 1986, Loi sur la confidentialité des communications électroniques) ont défini les limites de la collecte et de la conservation des données (avec des lacunes et des oublis importants), telles que l'utilisation de données à caractère personnel par des tiers. D'autres lois ont souvent porté sur le renseignement extérieur et sont liées au terrorisme, ou justifiées par ce dernier, jusqu'aux révélations de l'affaire Snowden (2013). Pour autant, le respect de la vie privée

n'a pas été la priorité de la législation fédérale, du moins au cours des dernières décennies, et ce pour plusieurs raisons. Au lieu de cela, des régimes réglementaires sectoriels ont été mis en place, en particulier dans le secteur de la santé et des données financières. Ils s'inspirent des principes du commerce équitable de la *Federal Trade Commission* (FTC, agence indépendante du gouvernement des États-Unis dont la mission principale est l'application du droit de la consommation et le contrôle des pratiques commerciales anti-concurrentielles telles que les monopoles déloyaux). Le respect et la protection de la vie privée sont laissés en grande partie à l'arbitrage des tribunaux, les litiges et les délits étant un moyen lent et procédural de créer des précédents à partir de cas individuels plutôt que de statuer *ex ante* sur les questions ci-dessus. Ce n'est peut-être pas moins efficace, comme nous le verrons, mais c'est infiniment plus difficile à décrire, surtout lorsque le processus judiciaire est réparti entre 51 États. En fait, les règles relatives aux données personnelles diffèrent dans ces 51 États, mais aucune d'elles n'est systématisée. Le gouvernement fédéral a tardé à s'emparer de cette question, pour ne pas dire à la reconnaître pleinement. Deux administrations successives ont chacune eu leurs propres priorités : sous G.W. Bush, la lutte contre le terrorisme a coïncidé avec une nette baisse de l'importance des questions de respect de la vie privée dès lors que la sécurité nationale était en jeu. L'administration Obama n'a pas rompu avec cette tendance. Elle a presque été unanimement soutenue, et donc influencée, par la « Valley », cette constellation de nouveaux magnats des affaires, de jeunes entrepreneurs et de *geeks* talentueux qui ont en commun une foi illimitée dans l'ère numérique. En termes de politique générale, elle a plaidé en faveur d'une approche des droits de

données personnelles qui diffère de l'approche européenne, mais elle a manqué de détermination dans ses propres recommandations[21].

Les administrations Bush et Obama ont également reconnu l'extraordinaire avantage que les nouvelles technologies numériques confèrent à l'économie américaine en compensant ce qui a été perdu dans le secteur manufacturier. Mais les liens de la Silicon Valley avec l'administration Trump sont beaucoup moins symbiotiques qu'ils ne l'étaient avec son prédécesseur. Cette administration fait une analyse différente de la situation. Elle peut encourager des décisions anti-trust qui entravent la croissance horizontale des grandes plateformes et des entreprises du numérique dans tous les secteurs et peuvent limiter l'agrégation de données volumineuses, et dès lors favoriser les droits à la vie privée. Mais cette administration vit également dans un contexte où la concurrence avec la Chine est la priorité en matière de politique étrangère. Or, avancer dans le domaine du *big data*, des algorithmes etc. avec un bras attaché dans le dos n'est certainement pas la meilleure option politique. Les développements intéressants en matière de respect de la vie privée, y compris, comme nous allons le voir, l'influence du très apprécié Règlement Général sur la Protection des Données (RGPD), sont essentiellement le fait des États. Le *Cloud Act* (2018)[22] est avant tout la réponse du Congrès américain aux problèmes liés au partage international de données. Cet exemple illustre la portée extraterritoriale du droit américain et constitue une victoire du gouvernement fédéral sur les entreprises du numérique en ce qui concerne la transmission des données conservées en dehors des États-Unis.

[21] Voir notamment, Executive Office of the President, « Big Data and Privacy: A Technological Perspective », *President's Council of Advisors on Science and Technology,* mai 2014, https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf.

[22] « Text - H.R.4943 - 115th Congress (2017-2018): CLOUD Act », *Congress,* 2018, https://www.congress.gov/bill/115th-congress/house-bill/4943/text.

Inévitablement, les débats sur le respect de la vie privée portent sur des entreprises, des experts et souvent sur des décisions judiciaires émanant des États-Unis. Pourtant, la scène américaine est tellement diversifiée qu'elle échappe à toute caractérisation. Elle n'est donc pas l'objet de notre étude. De l'avis d'un expert juridique, « La loi américaine sur la protection de la vie privée est un patchwork (…) de lois sectorielles, de délits couvrant un comportement étroitement défini et de certaines interdictions constitutionnelles complémentaires qui s'appliquent aux activités du gouvernement. Mais les activités de traitement des données les plus privées aux États-Unis ne tombent pas sous le coup de ces lois. En l'absence de loi générale sur la protection de la vie privée telle que le règlement de l'UE, les organismes de réglementation de la protection des consommateurs comme la FTC sont intervenus pour combler le vide »[23]. Les États-Unis restent donc un point de référence complexe.

Il y a des différences importantes entre les visions américaine et européenne de la protection de la vie privée. « Un régime de protection des consommateurs autorise généralement la collecte et le traitement des données à caractère personnel, à moins que cela ne soit expressément interdit. Par défaut, une loi sur la protection des données adopte le point de vue opposé. Elle autorise la collecte et le traitement des données uniquement dans un cadre défini légalement. En d'autres termes : « la collecte et le traitement des données est généralement autorisé aux États-Unis sauf si la loi dit que c'est interdit, tandis que dans l'UE, la collecte et le traitement des données sont interdits sauf si la loi dit que c'est autorisé »[24].

[23] William McGeveran, « Friending the Privacy Regulators », *Arizona Law Review* 58, n° 4 (2016): 959–1026, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820683.

[24] *Ibid.*

Cela ressort clairement dans différentes opinions sur les options par défaut.

La puissance normative de l'Europe en action

L'influence de l'Europe sur ce débat n'a cessé de grandir jusqu'à ce qu'elle en devienne l'autre acteur principal. La Convention 108 a longtemps été le seul accord international contraignant sur la protection des données. Elle a été ouverte à la signature en janvier 1981 par le Conseil de l'Europe et compte actuellement 55 signataires, y compris des États qui ne sont pas membres du Conseil. Elle constitue une première base pour la protection des données, bien qu'en termes très généraux : la Russie, par exemple, a pu signer cette première version. La convention a été modernisée en 2018, dans le but de l'harmoniser avec le RGPD. Elle comprend désormais le traitement manuel et le traitement automatisé, empêche les États de créer des exemptions de traitement pour certaines catégories et met à jour les notifications de violation. Elle crée également un Comité conventionnel qui contrôle et supervise l'application des principes de la Convention par les parties. Jusqu'à présent, la Convention modernisée a été signée par 33 États.

L'Union européenne a atteint un nouveau niveau de protection avec son RGPD novateur, qui est entré en vigueur en mai 2018. Il est intéressant de noter que le terme « vie privée » ne revient que deux fois dans les 88 pages de ce texte superbement écrit, dans une note de bas de page faisant référence à une directive européenne de 2002 sur la protection de la vie privée dans le secteur des communications électroniques (souvent surnommée la « Loi cookies »). La seule autre mention qui s'en rapproche est celle de

la « vie privée et familiale » qui apparaît au paragraphe 4 du Préambule. Ce règlement a un objectif plus large : protéger les personnes physiques à l'égard du traitement de leurs données à caractère personnel et assurer la libre circulation des données au sein de l'Union. Centré sur la collecte et le traitement des données à caractère personnel (plutôt que sur leur utilisation, une question sur laquelle nous reviendrons), ce texte est un subtil équilibre entre la protection des personnes physiques, la nécessité commerciale explicitement reconnue de libre circulation des données à l'intérieur et à l'extérieur de l'UE, et une série d'exemptions lorsque des exigences légales (portant essentiellement sur la sécurité) ou l'intérêt public (allant de la recherche médicale au droit d'investigation des médias) sont en jeu. Il s'agit surtout d'un règlement partant du sommet plus que de la base, mais qui prévoit des exceptions nationales. Règlement et non directive européenne, il se substitue aux règles et lois nationales (sauf lorsqu'elles pourraient aller au-delà des dispositions du RGPD), et oblige chaque État membre à créer une autorité de contrôle chargée de sa mise en œuvre, du traitement des réclamations et de la communication avec la Commission européenne.

Le RGPD devrait être complété par un règlement intitulé « vie privée et communications électroniques » (remplaçant une directive de 2002), qui est à l'étude depuis janvier 2017. Il aura un impact plus large que les directives précédentes : il traitera de la vie privée et de la confidentialité de toutes les communications électroniques (y compris les nouvelles applications de messagerie et de communication par exemple), et pas uniquement de la collecte commerciale de données à caractère personnel par l'intermédiaire de cookies. Peu de gens savent que ces nouveaux moyens de communication sont des sources privilégiées de récupération de données à caractère

personnel. De ce fait, le règlement « vie privée et communications électroniques » fait toujours l'objet de nombreux débats. Il pourrait avoir des répercussions beaucoup plus lourdes sur le secteur de la publicité, tout en offrant aux fournisseurs de télécommunications et de messagerie un environnement juridique plus sûr pour les communications *Over the Top* (OTT) (c'est-à-dire contournant les offres des fournisseurs d'accès à l'Internet) en termes de métadonnées admissibles. Le règlement « vie privée et communications électroniques » progresse très lentement au sein des institutions européennes et sera débattu par le Parlement européen nouvellement élu.

Pour l'utilisateur numérique moyen en Europe, le RGPD représente essentiellement un processus assez peu systématique d'acceptation des cookies avant d'accéder pour la première fois à un site Web.La première année a fait apparaître des divergences entre les États membres ainsi que des problèmes de mise en œuvre. Mais cela ne rend guère justice aux obligations qui incombent aux « responsables du traitement », c'est-à-dire aux entreprises et institutions qui conservent et gèrent des données à caractère personnel, par exemple. En outre, ce règlement illustre la grande influence que l'approche normative européenne peut avoir sur les débats mondiaux et son incidence sur les règles adoptées dans de nombreux autres pays. Ce n'est pas le seul résultat d'une persuasion morale. Le marché européen et ses flux numériques sont énormes. Y accéder est une nécessité économique. Par conséquent, afin de préserver les intérêts des États membres, il n'est pas surprenant que même le nouveau règlement européen de filtrage des investissements, entré en vigueur en avril 2019, a listé « l'accès à des informations sensibles, y compris des données à caractère personnel, ou la capacité de contrôler de telles informations » comme des facteurs déterminants de la sécurité

ou du risque pour le public d'un investissement direct étranger[25].

L'UE a également mis en place un règlement[26] qui définit les critères d'une « décision d'adéquation » concernant des pays tiers ou des organisations internationales et qui permettra le libre transfert de données entre l'UE et ces pays. Jusqu'à présent, 13 pays ont fait l'objet d'une décision d'adéquation, les États-Unis étant un cas à part puisqu'un « Bouclier de protection des données » *(Privacy Shield)* qui compense l'impact de lois comme le *Cloud Act* a été mis en place[27]. En préparation de ses négociations avec l'UE, le Japon a adopté une loi sur la protection des renseignements personnels en 2017[28]. De nombreux autres pays, dont le Brésil, l'Inde et la Corée du Sud, ont présenté une demande d'adéquation. Certains états des États-Unis, souvent ceux qui prennent les devants en matière de protection de l'environnement, instaurent une législation similaire : le *California Consumer Privacy Act* (juin 2018), le *State of Washington Privacy Act* (qui a finalement été rejeté en avril 2019). Le Texas, le Massachusetts, l'état de New York et d'autres états envisagent des projets de loi similaires. D'éminents experts universitaires en matière de données personnelles qualifient

[25] « Règlement (UE) 2019/452 du Parlement européen et du Conseil du 19 mars 2019 établissant un cadre pour le filtrage des investissements directs étrangers dans l'Union », *EUR-Lex,* 2019, https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32019R0452&from=EN

[26] « Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/EC (Règlement général sur la protection des données) », *EUR-Lex,* 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A119%3ATOC.

[27] « Décisions d'adéquation », *Commission européenne,* 2019, https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

[28] Texte et résumés disponibles à la rubrique « Laws and Policies » sur le site de la Personal Information Protection Commission Japan, https://www.ppc.go.jp/en/legal/.

régulièrement le RGPD de précédent important. Il convient d'ajouter que de nombreux concepts et une part de la terminologie utilisés dans le RGPD sont également issus des débats américains.

Il est donc indéniable que l'Europe est un acteur clé des débats sur la protection de la vie privée et du processus d'arbitrage entre les trois côtés du triangle décrit ci-dessus : respect de la vie privée, efficacité économique et sécurité étatique. À ce titre, elle est l'objet principal de notre étude. Pour compléter notre compréhension de la protection des données, nous étudierons simultanément deux autres cas, deux pays qui s'imposent de plus en plus dans le débat numérique.

L'Inde à la croisée des modèles

Le cas de l'Inde est le plus évident pour examiner l'impact international du RGPD et le rôle de modèle que ce règlement peut jouer pour la législation récemment proposée en matière de protection des données. Le projet de loi *Personal Data Protection Bill* (ci-après « PDPB ») a recours à des concepts tels que le contrôle des transferts de données transfrontaliers, l'avis de notification et le consentement par le biais de politiques de confidentialité et la création d'une autorité de contrôle de la protection des données. Il semble donc avoir été largement inspiré du RGPD. La sphère numérique de l'Inde surpasse celle de l'Europe en taille, si ce n'est en chiffre d'affaires. À l'instar de l'Europe, la sphère numérique indienne est dominée par des acteurs extérieurs : les plateformes, applications et logiciels américains. Cette sphère est également partagée avec les acteurs chinois qui occupent déjà le devant de la scène des smartphones et tendent à devenir très actifs dans les médias sociaux et les jeux.

La question de la reconquête de l'économie numérique par les entreprises indiennes face à de puissantes entreprises étrangères se pose de manière plus pressante encore en Inde qu'en Europe. Les similitudes et les différences entre le cas de l'Europe et celui de l'Inde font du second un test comparatif important pour le régime européen de protection des données.

Contrairement à l'Europe, l'Inde est dotée d'un système constitutionnel au sommet, ainsi que d'une société et d'une économie informelles prédominantes au bas de l'échelle. Comme l'a relevé un projet de politique nationale, « Aujourd'hui, deux tiers des Indiens n'ont pas accès au type de connectivité nécessaire au commerce numérique et électronique. De plus, il existe un problème de compétences : seulement 15 % des ménages ruraux possèdent une culture numérique »[29]. Mais le pays a continué de lutter contre les obstacles infrastructurels à la numérisation, le nombre d'utilisateurs d'Internet en Inde est passé de 4 millions en 2007 à 420 millions en 2017 (l'équivalent des utilisateurs des États-Unis, du Royaume-Uni et de l'Allemagne réunis). Il s'agit d'une base de consommateurs en constante augmentation qui devrait atteindre l'équivalent du nombre total d'utilisateurs des pays du G7 d'ici à 2025[30]. En plus d'une large base de consommateurs, l'Inde dispose de ressources humaines importantes dans le domaine numérique. En termes d'industrie et d'emploi, l'Inde numérique est beaucoup plus étroitement liée aux entreprises américaines qu'européennes. En 2017, les premières ont généré plus de 11 milliards de dollars américains de chiffre

[29] La culture numérique est définie comme suit : « au moins une personne au sein du ménage est capable d'utiliser un ordinateur, une tablette ou un smartphone ». Source : « Draft National E-Commerce Policy », 16 février 2019, p. 30, https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf.

[30] Rishi Iyengar, « The Future of the Internet Is Indian », *CNN,* 27 novembre 2018, https://edition.cnn.com/interactive/2018/11/business/internet-usage-india-future/.

d'affaires pour l'énorme secteur indien d'analyse des données ; le Royaume-Uni a généré 170 millions de dollars américains (part la plus importante au sein de l'UE) et les Pays-Bas 37 millions de dollars américains (troisième part la plus importante)[31]. « L'Inde numérique », ses objectifs et les politiques proactives mises en œuvre dans ce domaine sont un volet déterminant de la politique menée par le gouvernement de Narendra Modi. Cependant, cette administration n'est pas à l'origine de l'initiative. Le système national d'identification unique Aadhaar fondé sur des données biométriques et démographiques a été lancé en 2010. Projet ambitieux, la carte Aadhaar a également été, à bien des égards, le point de départ du débat sur la confidentialité des données juridiques en Inde. Ce débat s'étend également aux failles de sécurité dans la mise en place d'Aadhaar[32].

Bien que le projet de loi s'étende également aux acteurs privés, il semble contenir un courant sous-jacent visant à protéger l'économie locale des entreprises étrangères, en particulier des entreprises technologiques américaines et chinoises qui dominent actuellement la scène technologique[33]. À cet égard, l'Inde semble se tourner vers les instruments politiques utilisés par la Chine, comme l'indiquent, à titre d'exemple, les exigences en matière de localisation des données présentes dans le PDPB. « Nous ne voulons pas construire des murs, mais en même temps, nous reconnaissons expressément que les

[31] Source : Analytics India Magazine, AnalytixLabs, cité par Sandhya Keelery, « Infographic: India: Decoding Data for the Dollar », *Statista Infographics,* 23 mai 2018, https://www.statista.com/chart/13935/decoding-data-for-the-dollar-india-analytics/.

[32] À titre d'exemple, voir l'article : « Indian state government leaks thousands of Aadhaar names », *TechCrunch,* 1er février 2019, https://techcrunch.com/2019/01/31/aadhaar-data-leak/

[33] Newley Purnell, « India Looks to Curb U.S. Tech Giants' Power », *The Wall Street Journal,* 13 août 2018, https://www.wsj.com/articles/india-looks-to-curb-u-s-tech-giants-power-1534178721.

données sont un atout stratégique », a déclaré Aruna Sundararajan, la secrétaire d'État indien aux télécommunications. Celle-ci a par ailleurs été très impliquée dans le débat politique en faveur d'un autre projet politique, la politique nationale du commerce électronique qui appelle à des « règles du jeu équitables » pour les entreprises indiennes[34]. Le PDPB propose également des exemptions pour l'État, souvent formulées en termes vagues et donnant des pouvoirs très étendus à l'appareil d'État. Pourtant, l'Inde est un système démocratique et constitutionnel, et l'exécutif doit rendre des comptes au pouvoir judiciaire.

D'une certaine manière, l'Inde semble être un pont entre les cas européen et chinois. Elle calque sa législation sur le RGPD tout en l'utilisant comme un instrument de sa politique industrielle. Forte de son expertise naissante et de sa présence dans ce domaine, elle veut jouer un rôle important pour briser l'hégémonie sino-américaine dans la sphère numérique. Mais surtout, en termes d'adéquation, le cas indien reste important pour l'UE. Les évolutions du régime de protection des données de cette dernière pourraient faciliter ou perturber les flux commerciaux entre l'Inde et l'UE, car ils impliquent de nombreux transferts de données. La participation active de la Commission européenne au processus de consultation de l'Inde dans le domaine de la protection des données témoigne également de cette importance[35]. Dans les sections suivantes, qui ne constituent en aucun cas une analyse complète d'une scène numérique indienne

[34] Vindu Goel, « India Pushes Back Against Tech 'Colonization' by Internet Giants », *The New York Times,* 31 août 2018, https://www.nytimes.com/2018/08/31/technology/india-technology-american-giants.html?module=inline.

[35] Bruno Gencarelli, « Submission on Draft Personal Data Protection Bill of India 2018 by the Directorate-General for Justice & Consumers to the Ministry of Electronics and Information Technology (MeitY) », *Service européen pour l'action extérieure,* 29 septembre 2018, https://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en.

à la fois vaste, diversifiée et souvent ignorée par les Européens, nous tentons d'examiner la situation juridique et les débats sur la protection de la vie privée et des données à caractère personnel en Inde.

Les règles chinoises

Le deuxième cas que nous étudierons est celui de la Chine, qui a déjà été présentée dans ce chapitre comme une dystopie autoritaire du monde numérique. Pour certains, c'est un modèle de technologies de surveillance et de sujétion des médias sociaux. Le quasi-intranet chinois, considérablement renforcé par les récentes règles régissant le transfert international de données, est une source d'inspiration pour certains. « Nous devons créer un segment [de l'Internet] qui ne dépend de personne », a déclaré Vladimir Poutine, dévoilant ainsi le penchant de la Russie pour un intranet à la chinoise[36]. Le 1er novembre 2019, la loi russe sur un « Internet souverain » est entrée en vigueur, donnant au gouvernement, en cas d'urgence, le pouvoir de couper son réseau Internet du reste du monde[37]. Les règles chinoises ne visent pas à garantir la confidentialité des données mais à protéger la sécurité nationale dans le sens le plus large possible, tout en écartant les informations et opinions indésirables, également au nom de la sécurité. « Les fournisseurs de services d'information sur Internet ne doivent pas produire, reproduire, distribuer ou diffuser des informations qui (…) portent atteinte à la sécurité nationale, divulguent des secrets d'État, portent atteinte à la souveraineté de l'État ou compromettent l'unité nationale »,

[36] Andrew Roth, « Russia's Great Firewall: Is It Meant to Keep Information in – or Out? », *The Guardian,* 28 avril 2019, https://www.theguardian.com/technology/2019/apr/28/russia-great-firewall-sovereign-internet-bill-keeping-information-in-or-out.

[37] « Russia Internet: Law Introducing New Controls Comes into Force », *BBC News,* 1er Novembre 2019, https://www.bbc.com/news/world-europe-50259597.

indiquent les mesures administratives de 2000 relatives aux services d'information sur Internet. L'article 1 de la loi de 2017 sur la cybersécurité dit clairement que cette loi est formulée pour garantir la cybersécurité, mais également pour sauvegarder la souveraineté du cyberespace et la sécurité nationale. La spécification de 2018 sur la sécurité des renseignements personnels dispense de l'obligation d'obtenir un consentement lorsqu'il est question de sécurité nationale. La liste est longue, et la sécurité nationale est un aspect visible des règles chinoises que le pays ne cherche pas à cacher.

La Chine exerce un contrôle vertical sur l'Internet et les données numériques, mais les utilisations sont horizontales. Chacune des énormes plateformes chinoises recoupe différents secteurs et couvre de nombreuses activités. Le caractère horizontal des entreprises chinoises ne passe guère inaperçu. Il est particulièrement évident lorsqu'il est question du système de crédit social abondamment traité dans les médias occidentaux. Alibaba, l'entreprise de commerce électronique, est parvenue à couvrir tous les aspects de la vie d'un citoyen chinois à travers les services qu'elle fournit, et à prendre des participations dans d'autres entreprises. A travers son propre accès et celui de ses sociétés apparentées, Alibaba a une vision inégalée des clients chinois à travers leurs différentes activités. Le tableau ci-dessous montre les principaux secteurs concernés.

Données volumineuses d'Alibaba : Sources internes		
1	Données du commerce électronique	Taobao, Tmall, Alibaba
2	Données de paiement	Alipay
3	Donnée des sites de rencontre	Wangwang, Laiwang
4	Données vidéo	Youku
5	Données des navigateurs	Navigateur Taobao
6	Données de recherche	etao
7	Données de jeux	AliGame
8	Données musicales	Xiami Music
9	Données de voyage	Qyer
10	Données cartographiques	Gaode Map
11	Données d'identification	Taobao Account

Données volumineuses d'Alibaba : Sources externes		
	Partie achetée	Part d'Alibaba
Moteur de recherche	Yahoo China	40
Vie quotidienne	Koubei	100
	Meituan	10
	Kuaidi Dache	100
	Gaode Map	100
Réseaux sociaux et Internet mobile	Sina Weibo	18
	Navigateur UC	100
Culture	Xiami Music	100
	Culture China	60
	Wasu TV	20
	Youku Tudou	16
	Evergrande Football	50
	21st Century Media	20
Finance	Tianhong Asset Management	51
	Hundsun Technologies	100
Logistique	Singapore Post	10

Source du tableau : Chu Zhang and Leng Xin, « Research on the Application of Big Data in E-Commerce Enterprises 大数据在电商企业的应用研究 », *Journal of Chuzhou Vocational & Technical College 15, n° 5, mars 2018.*

C'est un avantage avec lequel les entreprises non chinoises ont du mal à rivaliser. Le fait que les Chinois sont comparativement moins sensibilisés à la problématique du respect de la vie privée, et que le gouvernement chinois donne la priorité aux objectifs de l'État plutôt qu'à toute autre considération rendent le cas chinois unique. Cela vaut pour la sécurité nationale dont la définition est large, pour ne pas dire illimitée. L'accent mis par l'État sur le développement économique en est également un exemple. Le système de crédit social, visant à créer une société digne de confiance qui favorise la croissance et la stratégie *Internet plus* en vue de créer de nouveaux secteurs d'activité, en témoigne. L'essor de l'économie en ligne a créé de nouvelles opportunités commerciales, y compris d'ailleurs le vol et les ventes illégales de données personnelles. Un article récent du *China Daily* se réjouit de l'arrestation de 7 460 personnes par la police de Guangdong lors d'une campagne spéciale menée au cours des huit premiers mois de l'année 2019. Comme le signale l'article, 400 millions de données personnelles volées et utilisées par des organisations criminelles à des fins de fraude ont été identifiées[38]. Cette affaire donne une indication de l'ampleur des enjeux ayant trait à la protection des renseignements personnels.

Les cas de la Chine et de l'Inde illustrent les tensions existantes entre respect de la vie privée, intérêts commerciaux et contrôle de l'État par des solutions très différentes. La protection des données personnelles est une priorité qui se heurte à d'autres objectifs. Les Européens doivent tenir compte du fait que ces objectifs sont mis en avant différemment en Chine, en Inde ou aux États-Unis, les trois autres grands marchés numériques.

[38] Caixiong Zheng, « Guangdong Police to Intensify Fight against Personal Data Theft - Chinadaily.Com.Cn », *Chinadaily,* 19 septembre 2019, https://www.chinadaily.com.cn/a/201909/19/WS5d833fd8a310cf3e3556c711.html.

L'innovation est l'un de ces objectifs, pour ne pas dire une exigence. Les multiples applications et l'amélioration de la productivité que les développements numériques permettent ne peuvent se résumer aux notions d'efficacité ou de productivité : ce sont des mesures de la performance économique, or l'ère numérique offre bien plus que cela. De plus, les réglementations européennes n'existent pas en dehors de tout contexte. Elles peuvent espérer exercer une certaine pression grâce à la taille et à l'attractivité du marché européen des données. Mais l'innovation peut prospérer dans des environnements réglementaires moins exigeants.

L'intérêt général est une autre exigence que la sécurité, voire l'ordre public, n'englobent pas complètement : l'exemple du secteur de la santé en est une illustration, mais nous aurions tout aussi bien pu parler de l'éducation, de la conduite autonome et de nombreux autres domaines prometteurs. Les exigences d'intérêt général peuvent entrer en conflit avec les objectifs de confidentialité des données : il s'agit d'un enjeu à double sens. Il est clair que l'objectif de respect de la vie privée doit trouver un compromis avec l'objectif de défense de l'intérêt général, une définition qui dépasse les seules notions d'ordre public ou de sécurité.

II

QU'EST-CE QUE LE RESPECT DE LA VIE PRIVÉE ET COMMENT LE GARANTIR ?

La confidentialité des données est un terme générique, intuitivement compris de tous, mais qui n'est pas facile à définir. Il ne s'agit ni de confidentialité ni de cybersécurité, bien qu'il y ait un peu des deux. Vous pouvez communiquer des informations, y compris des informations à caractère personnel en sélectionnant des personnes, sans pour autant rendre ces informations publiques : c'est le cas de nombreuses données à caractère personnel qui étaient auparavant conservées sur votre disquette ou votre disque dur et qui se trouvent désormais dans un *cloud*. Il s'agit alors de respect de la vie privée et de confidentialité. Vous pouvez souhaiter que ces données soient protégées contre un piratage informatique par une personne physique ou morale. Dans ce cas, il s'agit de respect de la vie privée et de sécurité. Vous pouvez souhaiter que les données à caractère personnel soient traitées de façon anonyme (ce qui est souvent le cas pour les informations médicales) dans votre intérêt médical immédiat ou à long terme, mais ne pas vouloir qu'elles soient utilisées pour évaluer votre profil de risque d'assurance : il est alors plutôt question d'utilisation que de collecte des données à caractère personnel. Prendre des décisions à l'abri du regard du gouvernement, et ne pas subir de discrimination fondée sur ces décisions ou sur vos caractéristiques personnelles est également étroitement lié au respect de la vie privée.

La protection de la vie privée est à la fois une sphère en expansion et une réalité qui s'estompe. Le Quatrième Amendement à la Constitution américaine stipule que « tout homme est maître chez lui » : nombre de querelles juridiques au cours des dernières

décennies ont porté sur le droit de fouiller les voitures et la question de savoir si celles-ci sont des extensions du domicile, avec des interprétations diverses. Cependant, se prémunir contre une intrusion n'est pas la même chose que garantir le respect de la vie privée. Pour cela, la loi américaine compense largement le respect de la vie privée par la liberté, y compris la liberté d'enquêter. Dans le contexte juridique européen, l'idée même que les données à caractère personnel d'un être humain puissent faire l'objet d'un commerce est discutable : vendre son esprit n'est pas plus acceptable pour certains que la gestation pour autrui pour de nombreuses personnes, ou la vente d'organes pour la majorité. Cette dernière pratique est néanmoins légale en Iran, y compris pour les condamnés à mort : les attitudes diffèrent. Sur le plan juridique, le respect de la vie privée s'exprime en termes de protection des données. Les données à caractère personnel sont au cœur des réglementations en matière de protection des données et du débat sur le respect de la vie privée. Selon le RGPD, les données à caractère personnel se réfèrent à « toute information se rapportant à une personne physique identifiée ou identifiable » soit directement, soit indirectement.

Les données à caractère personnel ne peuvent pas être séparées de la personne physique, pas plus que l'esprit ne peut être séparé du corps. Mais l'opposition est dans ce cas moins répandue, puisqu'il ne s'agit ni d'une effraction ni d'hameçonnage. Ouvrir du courrier ou même déchiffrer des communications cryptées sont des formes d'intrusion, puisque la personne qui ouvre la lettre ou celle qui casse le code ne sont pas les destinataires légitimes de ces messages. Recombiner des informations déjà transformées en données, avec l'aide d'algorithmes par exemple, est un processus analytique plutôt qu'intrusif. Après avoir pénétré les domaines de la collecte et du traitement des *big data,* on a longtemps accepté de faire une

distinction entre les données (qu'elles soient numériques ou analogiques) qui soutirent des informations aux personnes physiques, et les métadonnées qui servent à décrire des données réelles : à titre de comparaison, enregistrer une conversation téléphonique entre deux personnes et simplement noter l'heure à laquelle elle a eu lieu et sa durée, ne sont pas la même chose. S'agissant des fichiers numériques, les métadonnées permettent de conserver, sélectionner et communiquer des données avec une garantie d'authenticité assurée par des normes de métadonnées.

Mais que faire d'une fusion de données provenant de sources de collecte distinctes et associée à des algorithmes ? Cette combinaison transforme le plomb en or, ou des points de données isolés en procédé capable d'identifier des personnes et d'accumuler des connaissances sur elles, sans casser de code, sans effraction virtuelle. Chaque étape de l'opération peut être totalement légale, bien que le résultat soit une mine de données personnelles souvent sensibles. La question des données anonymes ou métadonnées illustre bien ces possibilités depuis un certain temps. Dans la pratique, il est de plus en plus souvent possible, pour ne pas dire presque toujours, de « désanonymiser » des données qui ont été rendues anonymes. Lors de démonstrations classiques, des chercheurs ont été capables de réidentifier des personnes en combinant leur code postal, leur sexe et leur date de naissance, avec 84 % de certitude, ou en faisant correspondre les recherches de films sur le site IMDB avec les données de Netflix, ou simplement à partir des requêtes de recherche sur AOL qui ont été publiées[39]. Qui plus est, ces exemples montrent quelques-unes des façons par lesquelles le champ des données

[39] Ces trois cas sont bien documentés dans Paul Ohm, « Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization », *UCLA Law Review* 57, 2010, p. 1701, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.

d'identification personnelles s'est élargi, certainement bien au-delà de la capacité d'une personne à comprendre les conséquences des données inoffensives qu'elle cède lorsqu'elle laisse des traces sur Internet. La façon de cliquer ou de taper sur le clavier permet de déduire des changements d'humeur, mais aussi l'apparition de la maladie d'Alzheimer. Dans ce cas, les métadonnées se transforment en données à caractère personnel et les distinctions établies par les réglementations existantes peuvent être considérées comme caduques. L'alternative consiste à imposer des normes tellement larges qu'elles créent une obligation de résultat, et pas simplement de processus, pour les opérateurs de données. En fait, c'est souvent le cas avec le RGPD européen qui met l'accent sur les résultats plutôt que sur les processus techniques, mais avec des conséquences imprévues : la prescription risque de ne pas être mise en œuvre ou de devenir un obstacle majeur pour les activités numériques. Comme nous le verrons plus loin, c'est un choix politique dont les conséquences n'ont pas encore été évaluées ou ne pourront peut-être jamais l'être pleinement.

Il n'en demeure pas moins qu'il est facile de justifier une réglementation qui dépasse son objectif, c'est-à-dire de légiférer sur les résultats plutôt que sur les moyens. Les garanties de respect de la vie privée données actuellement sont risquées. Il est impossible de prédire comment la fusion de données (qui consiste à regrouper des champs de données en constante expansion) et des algorithmes qui n'ont pas encore été identifiés peuvent rendre obsolète la protection technologique ou réglementaire actuelle de la vie privée. Selon une commission présidentielle de la Maison-Blanche dirigée par Barack Obama, « la sécurité, c'est faire face aux menaces de demain contre les plateformes d'aujourd'hui. C'est déjà assez difficile. Le respect

de la vie privée, c'est faire face aux menaces de demain contre les plateformes de demain »[40].

Anonymisation et pseudonymisation des données à caractère personnel

Les méthodes d'anonymisation sont devenues plus complètes et comprennent notamment l'obligation d'utiliser des échantillons de données limités pour empêcher la fusion de données à grande échelle. Des recherches récentes prouvent que cela devient plus difficile. Il faudra probablement que les techniques d'anonymisation deviennent de plus en plus sophistiquées. Actuellement, seulement cinq points de données disponibles sur 210 populations différentes permettent de désanonymiser une personne dans 84% à 97% des cas. Avec 15 points de données, il est possible de réidentifier 99,98 % des Américains. Les résultats ne sont pas très différents sur des échantillons plus petits. De plus, le taux d'échec absolu moyen est très faible : il est inférieur à 0,041 sur un échantillon de 1 % de la population. Ce point est important, parce ce que cela signifie que « vous savez ce que vous ne savez pas ». L'incapacité à identifier n'a pas les mêmes conséquences que des erreurs d'identification. En d'autres termes, les résultats ont tendance à être de moins en moins contestables : ils approchent de la certitude à mesure que le nombre de points de données augmente[41]. Selon une

[40] Executive Office of the President, « Big Data and Privacy: A Technological Perspective », *President's Council of Advisors on Science and Technology,* mai 2014, https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf.

[41] Luc Rocher, Julien M. Hendrickx et Yves-Alexandre de Montjoye, « Estimating the Success of Re-Identifications in Incomplete Datasets Using Generative Models », *Nature Communications* 10, n° 1, 23 juillet 2019, https://doi.org/10.1038/s41467-019-10933-3.

estimation basse pour les populations équipées d'appareils numériques, chaque personne a créé en moyenne 5 000 points de données, un chiffre qui continuera de se multiplier avec les utilisations autorisées (qui souvent n'ont pas encore été inventées) pour la 5G et l'IdO. Les villes et les maisons intelligentes entraîneront ou permettront techniquement la collecte d'infiniment plus de points de données (les caméras vidéo en sont l'exemple le plus évident). Un appareil existant, le thermostat Nest, mémorise vos températures préférées, « sait quand vous êtes absent, apprend à connaître votre maison et la contrôle en votre absence »[42]. Pour ce faire, il détecte les mouvements et le bruit de tous les autres appareils, et il suit leur consommation électrique. Il ne lui manque plus qu'une caméra avant, dont tous les autres appareils Nest sont équipés.

D'après ce qui précède, on voit clairement que le respect de la vie privée n'est pas assuré par la seule anonymisation. Il s'agit pourtant d'un objectif ambitieux et, comme nous le verrons plus loin, l'anonymat figure en bonne place dans presque tous les règlements sur la protection des données. Il est plus sûr d'adopter une définition très large du respect de la vie privée, un terme générique englobant les « règles et normes d'action et d'inaction à l'égard de nos informations personnelles »[43]. Woodrow Hartzog lie également le respect de la vie privée à « la confiance, à l'obscurité et à l'autonomie ». La confiance s'oppose au contrôle : comme nous le verrons, personne ne peut espérer gérer et contrôler efficacement ses données à caractère personnel. L'obscurité est préférable au secret : un but encore inatteignable pour les individus. L'autonomie est la préservation

[42] Nest appartient aujourd'hui à Google. Ces déclarations sont tirées de la page « Real Savings » sur le site Internet de Nest, https://nest.com/thermostats/real-savings/.

[43] Woodrow Hartzog, *Privacy's Blueprint : The Battle to Control the Design of New Technologies,* Cambridge : Harvard University Press, 2018, p. 10.

d'un jardin secret dans le but de se faire sa propre opinion, y compris le droit pour les individus de s'engager dans un échange constructif entre partenaires de leur choix.

Médias sociaux et données à caractère personnel

L'ère numérique élargit considérablement notre horizon social, même si beaucoup diront que cela se fait au détriment de la profondeur des relations. Selon un célèbre psychologue social, une personne ne peut pas entretenir plus de 150 « vraies relations », tandis que notre capacité à reconnaître un nom irait jusqu'à 2 000[44]. Les réseaux sociaux utilisent des paramètres de filtre : on dit souvent que Facebook limite le nombre d' « amis » à 5 000 et que Twitter limite à 1 000 le nombre de messages que l'on peut recevoir par jour. Cela protège en réalité l'ergonomie de l'application. Mais les algorithmes commandent également le classement des messages dans la boîte de réception, censément en fonction des préférences observées.

Une forme de respect de la vie privée, la protection des données, est une exigence commerciale pour le « *data scraping* »[45] lui-même. Facebook doit protéger ses données simplement parce qu'il vend leur utilisation. À l'inverse, l'attrait de la gratuité des informations et des services sur Internet est la principale incitation à ne pas exiger le respect de la vie privée. Parce qu'Internet est gratuit pour les utilisateurs (à l'exception de l'abonnement chez le fournisseur

[44] Robin I. M. Dunbar, « The Social Brain Hypothesis », *Evolutionary Anthropology: Issues, News, and Reviews* 6, no. 5 (1998), p. 184, https://doi.org/10.1002/(sici)1520-6505(1998)6:5<178::aid-evan5>3.0.co;2-8. Cité par Woodrow Hartzog, *Privacy's Blueprint : The Battle to Control the Design of New Technologies*, Cambridge: Harvard University Press, 2018, p. 109.

[45] L'image fait allusion aux exploitations minières à ciel ouvert.

d'accès), il est payé par d'autres, à savoir par la publicité, souvent surnommée « le péché originel de l'Internet », d'où cette conclusion en miroir : « si c'est gratuit, c'est que vous êtes le produit ». Certains des mots-clés servant à extraire des données proviennent directement du vocabulaire de l'exploitation de mines à ciel ouvert ou du conditionnement de la viande : le « *data scraping* », littéralement le « raclage ou grattage de données », après quoi ce qu'il reste d'une individualité est la « carcasse » sans valeur. Les réseaux privés virtuels (VPN) sont un remède partiel masquant la véritable adresse IP (Internet Protocol) d'un utilisateur (et pas beaucoup plus). Mais attention, peu d'utilisateurs s'arrêtent pour se demander à qui appartiennent ces VPN et quelle pourrait être leur utilité secondaire. Une étude de 2019 montre qu'un tiers des principaux VPN du monde appartiennent à la Chine, souvent par l'intermédiaire de filiales. Le Pakistan, qui possède le « pire droit informatique au monde », arrive en deuxième position. Les VPN basés aux États-Unis n'excluent évidemment pas la surveillance des non-citoyens[46]. En bref, un VPN peut assurer une protection contre une partie des menaces, mais rarement contre toutes.

En termes de surveillance gouvernementale, les « portes dérobées », intentionnellement installées lors de la conception de matériel ou de logiciels, ont un défaut majeur : s'il existe une porte dérobée, d'autres peuvent également l'emprunter, les « méchants » proverbiaux. Cela revient à laisser la clé sous le paillasson devant chez soi. Les gouvernements eux-mêmes, en dehors de toute considération juridique, se heurtent à deux exigences contradictoires de sécurité, que ce soit dans le domaine du cryptage ou celui de leur propre

[46] Jan Youngren, « Hidden VPN Owners Unveiled: 99 VPNs Run by 23 Companies | VPNpro », *VPNpro,* 2 juin 2019, https://vpnpro.com/blog/hidden-vpn-owners-unveiled-97-vpns-23-companies/.

accès secret aux données. Pour ce qui est du cryptage, augmenter le niveau de codage augmente la protection, mais des clés interminables sont également plus fastidieuses à utiliser. La protection marche aussi pour les communications illégales. La France a d'abord exigé que toutes les clés de cryptage soient communiquées aux autorités publiques, puis, de 1999 à 2004, les clés supérieures à 128 bits uniquement. De même, l'installation de portes dérobées (comme cela a pu être le cas pour les routeurs Cisco, ainsi que l'a exposé Edward Snowden) peut créer des points d'entrée pour d'autres. À l'inverse, la création d'une architecture infaillible donnera lieu à des batailles juridiques pour accéder aux données : Apple a gagné un avantage en termes de réputation en refusant au FBI d'accéder à l'iPhone d'un terroriste tué aux États-Unis, au détriment de la lutte contre le terrorisme.

Localisation et souveraineté des données

Étant donné que le respect de la vie privée est lié à la sécurité des données collectées, l'un des principaux enjeux a été le contrôle des réseaux, ainsi que l'emplacement des *clouds* de données et l'accès à ces *clouds*. Le réseau mondial, et de fait les données et communications numérisées, ont été fondés sur le principe de libre circulation des données par-delà les frontières. La situation géographique des serveurs (dans des bâtiments géants qui constituent en réalité le *cloud*) est souvent déterminée en fonction des coûts d'opportunité (principalement la température locale moyenne et/ou le prix de l'électricité), plutôt qu'en fonction de facteurs de sécurité. Les chiffres varient beaucoup, mais un décompte fin 2018 comprenait 24 grandes entreprises qui devraient exploiter 420 centres de données classés comme serveurs *hyperscale*. Non seulement ils

remplaceront votre disque dur ou les serveurs localisés de votre entreprise, mais également la première génération de *clouds*[47]. Les centres *hyperscale* permettent de collecter et de relier davantage de données. Ils devraient remplacer de nombreux équipements des réseaux physiques, par exemple dans les communications mobiles. 45 % de ces centres étaient situés aux États-Unis en 2017, et 8 % en Chine, son concurrent le plus proche. Microsoft, le *leader* des solutions de *cloud,* dépense chaque année 15 milliards de dollars pour son architecture *cloud,* y compris pour sa marque signature Azure. À titre de comparaison, la Commission européenne estime qu'au total 2 milliards d'euros de financement du programme Horizon 2020 seront alloués à l'initiative de *cloud* européen sur cinq ans[48]. En France, deux tentatives de *clouds* nationaux financés par des fonds publics ont échoué[49].

La question de l'accès aux données et de leur contrôle a cédé la place à des politiques gouvernementales visant à localiser les données sur leur territoire. La souveraineté sur les données est un sujet politique sensible. C'est également une réponse possible à un autre problème : la privatisation des données par des métaplateformes, qui reprennent de plus en plus d'activités (santé, éducation) qui étaient précédemment celles de systèmes publics. Pour le meilleur ou pour le pire, les États délèguent désormais la mise en place de leurs tâches répétitives, telles que le paiement des fonctionnaires, à des sociétés informatiques. Les systèmes de cartographie sont de

[47] Jeff Borker, « What Is Hyperscale? », *Digital Realt,* 15 novembre 2017, https://www.digitalrealty.com/blog/what-is-hyperscale.

[48] « The European Cloud Initiative », *Commission européenne,* 17 août 2018, https://ec.europa.eu/digital-single-market/en/%20european-cloud-initiative.

[49] Florian Dèbes, « Une page se tourne pour le cloud souverain français », *Les Échos,* 1er août 2019, https://www.lesechos.fr/tech-medias/hightech/une-page-se-tourne-pour-le-cloud-souverain-francais-1118112.

plus en plus souvent dirigés par des acteurs privés comme Google et Apple. Un seul pays, l'Estonie, a fait de l'État une plateforme multitâches[50]. Le problème du contrôle de ces données privatisées occupe une place importante. La solution de la Chine est un contrôle hybride assuré par des moyens largement coutumiers entre plateformes théoriquement privées et l'État-parti, et par un contrôle rigoureux de tous les transferts de données. D'autres pays, comme l'Inde, acceptent les plateformes mondiales, mais s'efforcent au moins de localiser les données à l'intérieur du pays.

À l'inverse, le *Cloud Act* américain *(Clarifying Lawful Overseas Use of Data Act)*[51] est un très bon exemple de la portée extraterritoriale des juridictions américaines, puisqu'il oblige les entreprises américaines conservant des données à l'étranger, à les transmettre à la demande des autorités nationales chargées de l'application des lois. Ces demandes ne peuvent pas être effectuées en bloc. Elles doivent être exigées par un tribunal et motivées par une probable cause criminelle (et non pas en invoquant la sécurité nationale par exemple). Les entreprises qui prétendent être en conflit avec une loi étrangère peuvent refuser ce transfert des données. C'est une disposition très importante puisque l'application du *Cloud Act* est fondamentalement liée à l'existence de règles compatibles dans d'autres pays. En réalité, cette loi autorise le pouvoir exécutif à signer des accords d'échange de données avec des gouvernements étrangers, ce qui a ravivé une querelle sur les flux de données transatlantiques, flux qui restent les plus importants au monde. Un traité relatif à la sphère de sécurité qui avait déjà été négocié a été

[50] Voir la série en quatre parties de Gilles Babinet, « La fin de l'État-nation ? », *Institut Montaigne,* 2019, https://www.institutmontaigne.org/en/series/end-nation-states.

[51] « Text - H.R.4943 - 115th Congress (2017-2018): CLOUD Act », *Congress,* 2018, https://www.congress.gov/bill/115th-congress/house-bill/4943/text.

invalidé par la Cour de Justice de l'Union Européenne (CJUE). Le *Privacy Shield* entre l'UE et les États-Unis, parfois présenté comme une réponse au *Cloud Act*, a en fait été adopté dés 2016. Il autorise le libre transfert de données, y compris de données à caractère personnel, à des entreprises certifiées aux États-Unis dans le cadre du *Privacy Shield*, et il est révisé chaque année. Il est également complété par un accord-cadre entre l'UE et les États-Unis sur la protection des données à caractère personnel. Celui-ci définit des règles pour l'échange de données entre les autorités chargées de l'application des lois[52].

Le *Cloud Act* et le *Privacy Shield* font tous deux l'objet de nombreuses polémiques. Les rapports annuels de la Commission donnent un aperçu des questions en suspens. Les principaux points d'achoppement sont actuellement la supervision effective de la mise en œuvre par le ministère américain du Commerce ainsi que la nomination, longtemps différée, d'un médiateur qui donnerait une possibilité de recours permanente aux personnes physiques et aux entreprises. La Commission a également « encouragé les États-Unis à adopter un système complet de protection de la vie privée et des données »[53].

[52] Le *Privacy Shield*, l'accord-cadre entre les États-Unis et l'Union européenne ainsi que des examens annuels sont disponibles à l'adresse suivante : « EU-US Data Transfers », *Commission européenne,* https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/eu-us-data-transfers_en.

[53] « The Second Annual Review of the Functioning of the EU-U.S. Privacy Shield », *Commission européenne,* 19 décembre 2018, https://ec.europa.eu/info/sites/info/files/report_on_the_second_annual_review_of_the_eu-us_privacy_shield_2018.pdf.

Politiques de confidentialité, avis de notification et de consentement

La notification et l'avis de consentement sont l'élément le plus caractéristique de la protection de la vie privée des consommateurs. Il s'agit de l'obligation d'informer les consommateurs sur la collecte et l'utilisation de leurs données afin qu'ils puissent y consentir. Cela se fait le plus souvent par le biais de politiques de confidentialité. Bien entendu, les exigences en matière de respect de la vie privée peuvent également diverger d'une société à l'autre et d'une époque à l'autre. Avec la brusquerie qui le caractérise, Jack Ma, le fondateur d'Alibaba, déclare préférer l'Afrique à l'Europe parce que « l'Europe se soucie trop du respect de la vie privée et de règles »[54]. Pour ce que cela vaut (les sondages d'opinion dans l'environnement contrôlé de la Chine étant une entreprise discutable), 38 % du public chinois serait prêt à renoncer à la confidentialité des données, dans l'intérêt de la sécurité et de la confiance dans les transactions généralement. Aadhaar, l'enregistrement à grande échelle de tous les citoyens indiens, reposant en partie sur un système de reconnaissance biométrique, aurait rencontré une opposition plus forte s'il avait été appliqué en Europe (qui accepte néanmoins une collecte plus dispersée de données à caractère personnel). Une récente étude australienne sur les plateformes Internet a collationné les règles de confidentialité de Google depuis le début et présenté, sous forme de tableau, les catégories de données à caractère personnel que Google admet détenir. Cette détention n'implique pas une retransmission, car l'entreprise met l'accent sur son développement interne et dément le fait qu'elle vendrait des données identifiables.

[54] Yunyu Qu, « Ma Yun: Europeans Worry Too Much, Alibaba Chooses Africa, Which Is More Willing to Believe in Technology 马云：欧洲人担忧太多，阿里选择更愿相信技术的非洲 », *Caixin,* 23 janvier 2019, http://companies.caixin.com/2019-01-23/101373592.html.

Informations par Google dans ses règles de confidentialité de 1999 à 2019 sur les données collectées auprès des utilisateurs

	Juin 1999	Juil. 2004	Jan. 2009	Déc. 2014	Jan. 2019
Nom	✘	✔	✔	✔	✔
Anniversaire	✘	✘	✘	✔	✔
Numéro de téléphone	✘	✘	✘	✔	✔
Adresse e-mail	✘	✔	✔	✔	✔
Informations vocales et audio	✘	✘	✘	✘	✔
Informations de paiement	✘	✔	✔	✔	✔
Lieu	✘	✘	✘	✔	✔
GPS	✘	✘	✘	✔	✔
Données de capteurs *via* des tours Wifi, Bluetooth, etc.	✘	✘	✘	✔	✔
Adresses IP	✘	✔	✔	✔	✔
Vos e-mails sur Gmail (lancement en avril 2004)	N/A	✘	✔	✔	✔
Les photos que vous téléchargez	✘	✘	✘	✔	✔
Les vidéos que vous téléchargez	✘	✘	✘	✔	✔
Vos messages	✘	✘	✘	✔	✔
Vos appels téléphoniques	✘	✘	✘	✔	✔
Commentaires que vous postez	✘	✘	✘	✔	✔
Les événements de votre calendrier sur Google Agenda (lancement général en juil. 2009)	N/A	N/A	N/A	✔	✔
Votre historique de recherche	✘	✘	✘	✔	✔
Vidéos que vous regardez sur YouTube (acquisition en nov. 2006)	N/A	N/A	✘	✔	✔
Appareils que vous utilisez	✘	✘	✘	✔	✔
Applications que vous avez installées	✘	✘	✘	✘	✔
Navigateur que vous utilisez	✘	✔	✔	✔	✔

	Juin 1999	Juil. 2004	Jan. 2009	Déc. 2014	Jan. 2019
Site Web de tiers visités en utilisant les services de publicité de Google	✘	✔	✔	✔	✔
Historique de navigation de Chrome (lancement sept. 2008)	N/A	N/A	✘	✔	✔
Informations sur le navigateur	✘	✔	✔	✔	✔
Informations sur l'appareil	✘	✘	✘	✔	✔
Cookies en général	✔	✔	✔	✔	✔
Activité d'achat	✘	✘	✘	✘	✔
Informations sur les cookies Doubleclick (acquisition de Doubleclick en mars 2008)	N/A	N/A	✘	✔	✔
Information sur le réseau mobile	✘	✘	✘	✔	✔

Source : Australian Competition and Consumer Commission, « Digital Platforms Inquiry Final Report », juin 2019, p. 380, https://www.accc.gov.au/system/files/Digital%20platforms%20inquiry%20-%20final%20report.pdf.

Il suffit de jeter un coup d'œil sur le tableau ci-dessus pour juger du bien-fondé des règles de confidentialité actuelles qui sont basées sur l'information des personnes physiques et le consentement. Il serait contre-productif d'abandonner ces obligations et de réduire Internet à une chasse à vos données. Mais la réalité est que personne ne lit les politiques de confidentialité, car il faudrait en lire des centaines, ainsi que leurs mises à jour, tout en comprenant le jargon juridique. Ce tableau révèle également comment les cookies, qui étaient autrefois le principal outil de collecte des données, ne sont désormais plus qu'un élément d'un ensemble beaucoup plus vaste. Il est utile de prendre le cas de la plus grande plateforme mondiale en exemple, à savoir Google. Mais Google est loin d'être unique, et les revendeurs tiers des données issues de vos clics se livrent à des pratiques beaucoup plus choquantes. Avec 7 906 mots dans sa version américaine, la dernière déclaration de Google en matière de

règles de confidentialité[55] est également loin d'être la plus longue du genre, bien que son texte incorpore de nombreux segments cliquables renvoyant à de nouvelles descriptions et à d'autres choix difficiles à faire.

Une entreprise comme Google se distingue par la quantité et la diversité de ses données. Seules les plus grandes entreprises chinoises en ligne sont capables de rivaliser avec Google, car elles ont beaucoup moins de restrictions concernant les activités qu'elles peuvent exercer simultanément, y compris bancaire, d'assurance et celles liées à l'industrie florissante des paiements. Ce qui motive les grandes entreprises américaines de haute technologie à procéder à de nombreuses acquisitions, ce n'est pas uniquement la taille de la cible, mais la possibilité d'acquérir et de consolider des données personnelles ou le « surplus comportemental ». Et ce qui rend Google unique, c'est la qualité de ses algorithmes et sa capacité financière à acheter d'autres entreprises pionnières pour leurs algorithmes et leurs domaines d'utilisation. Deux millions d'entreprises dépendent des résultats marketing produits par le *big data* et les algorithmes de Google. Pourtant, à bien des égards, Google est plus soucieuse de protéger l'énorme quantité de données qu'elle acquiert que ne le font de nombreux médias et éditeurs numériques. Ces derniers dépendent directement des revenus de la publicité pour survivre et ouvrent sans discernement leurs sites Web à des courtiers et revendeurs tiers. Parce qu'ils ont besoin de ces revenus en ligne, ces médias d'information « défendent une surveillance de masse qui va à l'encontre tant de leurs lecteurs que des journalistes », commente une ONG à vocation privée[56].

[55] Au 22 janvier 2019, « Règles de confidentialité », *Google,* https://policies.google.com/privacy?hl=en-US.

[56] « Règlement EPrivacy : Ne laissons pas l'UE vendre notre vie privée », *La Quadrature du Net,* 2017, https://eprivacy.laquadrature.net/en/.

Les consommateurs manifestent un intérêt fort pour la protection de leurs données personnelles. Aux États-Unis, 90 % des adultes estiment qu'il est important de contrôler les informations collectées à leur sujet, 93 % considèrent qu'il est important de pouvoir contrôler qui a accès à ces informations[57], et 86 % ont fait des efforts pour masquer leurs empreintes numériques[58] ; ces chiffres trouvent un écho similaire en Europe selon le rapport de 2018 sur les attitudes numériques[59]. Pourtant, ces mouvements d'opinion sont en contradiction avec le comportement observé en ligne. Les gens acceptent souvent de partager leurs données pour avoir accès à des applications gratuites telles que le Wi-Fi et les sites Web. C'est le *privacy paradox*.

Les consommateurs ont souvent le choix entre renoncer au respect de leur vie privée et de longues politiques de confidentialité truffées de jargon juridique[60]. D'après une étude, il faudrait plus de 25 jours à un Américain moyen pour lire toutes les politiques de confidentialité auxquelles il est exposé au cours d'une année[61]. Ensuite, les consommateurs peuvent se voir refuser des biens ou des services s'ils ne consentent pas à la collecte de leurs données. Ainsi,

[57] Mary Madden et Lee Rainie, « Americans' Attitudes About Privacy, Security and Surveillance », *Pew Research Center,* 20 mai 2015, https://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/.

[58] Lee Rainie et al., « Anonymity, Privacy, and Security Online », *Pew Research Center,* 5 septembre 2013, https://www.pewinternet.org/2013/09/05/anonymity-privacy-and-security-online/.

[59] Joe Toscano, « Privacy By Design: What Changes Are Necessary, How To Do It, and How To Sell Your Boss », *Medium,* 30 octobre 2018, https://medium.com/greater-than-experience-design/privacy-by-design-7b1165d045e0.

[60] Kai Burkhardt, « The Privacy Paradox Is a Privacy Dilemma – Internet Citizen », *Internet Citizen,* 24 août 2018, https://blog.mozilla.org/internetcitizen/2018/08/24/the-privacy-paradox-is-a-privacy-dilemma/.

[61] Alexis C Madrigal, « Reading the Privacy Policies You Encounter in a Year Would Take 76 Work Days », *The Atlantic*, 1er mars 2012, https://www.theatlantic.com/technology/archive/2012/03/reading-the-privacy-policies-you-encounter-in-a-year-would-take-76-work-days/253851/.

l'argument intuitif selon lequel chaque individu sait mieux que quiconque ce qu'il doit faire de ses données personnelles est facilement battu en brèche. De nombreuses études l'ont déjà démontré, et pourtant, de nombreux règlements et la perception du grand public reposent sur les notions d'avis de notification et de consentement. Comme nous le verrons, les efforts déployés dans le cadre du RGPD portent en partie sur l'amélioration de l'ergonomie de l'avis de notification et de consentement, y compris la normalisation et l'universalité de l'utilisation : ces efforts sont louables. Ne pas y souscrire ne ferait qu'aggraver la situation en matière de confidentialité des données. Pourtant, ils ne font qu'effleurer la question. En réalité, il est impossible pour une personne de lire les informations nécessaires, et encore plus impossible, même pour les experts, de comprendre quel type de données (ou métadonnées) pourrait être utilisé à l'avenir pour obtenir des renseignements sur un individu.

Ce qui est inaccessible aux experts et aux utilisateurs compétents et expérimentés a encore moins de chances d'être accessible aux utilisateurs de smartphones, médias sociaux et autres applications populaires peu instruits. Parmi les marchés ouverts, l'Inde est en passe de devenir la plus grande base de smartphones et d'abonnés à Internet. Ce marché est âprement disputé par les entreprises de télécommunications et les plateformes. Le semi-analphabétisme encourage les applications vocales, comme en témoigne l'augmentation de 270 % par an du nombre de requêtes par recherche vocale sur Google en Inde[62]. La probabilité que le grand public puisse gérer efficacement une conception du respect de la vie privée fondée sur l'avis de notification et de consentement des utilisateurs y est donc pratiquement nulle.

[62] Rishi Iyengar, « The Future of the Internet Is Indian », *CNN,* 27 novembre 2018, https://edition.cnn.com/interactive/2018/11/business/internet-usage-india-future/.

Droit à l'oubli

Il en va de même pour d'autres aspects importants du respect de la vie privée, comme le droit de savoir ce que l'on sait de vous ou « droit à l'oubli », qui sont des applications concrètes du besoin d'anonymat pour garantir le respect de la vie privée. Là encore, un article ingénieux sur Google et Facebook souligne à quel point ces objectifs sont inatteignables[63]. Le volume moyen d'informations téléchargées pour une seule personne sur Google est de 687,5 Mo soit 3 millions de mots ou plus de deux volumes de l'Encyclopedia Britannica. En pratique, à la question que sait-on de vous, la réponse est tout simplement la suivante : « nous en savons vraiment beaucoup ». Trier les données est d'autant plus difficile que les mêmes informations sont conservées de façon redondante par différentes sources. « Du point de vue de l'élaboration des politiques, la seule hypothèse viable aujourd'hui et dans un avenir prévisible, est qu'une fois créées, les données sont permanentes »[64].

Ainsi, la technologie porte atteinte au « droit à l'oubli », l'un des fondements de la loi sur le respect de la vie privée. En 2014, la CJUE a condamné Google et lui a ordonné de retirer de la liste de ses résultats des données concernant deux citoyens espagnols (mention sur Internet d'une vente immobilière qui avait eu lieu des années auparavant)[65]. Il est important que la Cour ait mentionné

[63] Dylan Curran, « Are You Ready? This Is All the Data Facebook and Google Have on You | Dylan Curran », *The Guardian,* 19 décembre 2018, https://www.theguardian.com/commentisfree/2018/mar/28/all-the-data-facebook-google-has-on-you-privacy.

[64] Executive Office of the President, « Big Data and Privacy: A Technological Perspective », *President's Council of Advisors on Science and Technology,* mai 2014, p. 40, https://bigdatawg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf.

[65] Cour de justice de l'Union européenne, « Google Spain, C 131/12 », *EUR-Lex,* 13 mai 2014, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

qu'il s'agissait de simples citoyens et non de personnalités publiques. Cet arrêt est devenu le fondement du « droit à l'oubli ». S'appliquant uniquement aux mineurs de moins de 18 ans, la loi dite *eraser law* de l'État de Californie est quant à elle entrée en vigueur en janvier 2015[66].

L'un des développements connexes concerne l'étendue de la conservation des données et le droit des autorités publiques à y accéder. Lorsque les entreprises n'attachent aucune valeur aux données, elles n'ont pas d'intérêt particulier à les conserver, car c'est un processus onéreux. En revanche, l'État peut y voir un intérêt beaucoup plus important, justifié par des affaires criminelles par exemple. Les métadonnées des appels téléphoniques en particulier, et dans certains cas, l'hameçonnage de toutes les communications d'une antenne-relais de téléphonie mobile sont des outils d'investigation importants. L'utilisation de telles informations fait pourtant débat. En décembre 2016, le CJUE a jugé que la conservation des métadonnées des entreprises de télécommunications (heure de l'appel, numéro appelé) et la possibilité d'y accéder ne sont appropriées que dans le cadre d'enquêtes pénales individuelles et ne peuvent être effectuées en bloc[67]. Des États membres se sont opposés à cet arrêt[68] et ont entamé un lent processus de consultation pour trouver des alternatives acceptables. Trouver une méthode

[66] « Senate Bill No. 568 », *California Legislative Information,* 2013, http://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201320140SB568.

[67] Cet arrêt de la CJUE sur l'affaire Tele2 Sverige est disponible sur le site de la Cour de Justice de l'Union européenne, ECLI:EU:C:2016:970, *europa.eu*, 2016, http://curia.europa.eu/juris/document/document.jsf?docid=186492&text=&dir=&doclang=EN&part=1&occ=first&mode=DOC&pageIndex=0&cid=4147224

[68] Pour une critique de la réticence des États membres à accepter les conséquences de l'arrêt de la CJUE, voir Jesper Lund, « EU Member States Willing to Retain Illegal Data Retention - EDRi », *European Digital Rights,* 16 janvier 2019, https://edri.org/eu-member-states-willing-to-retain-illegal-data-retention/.

d'accès ciblé plutôt qu'un régime de conservation généralisée des données semble difficile[69].

Même sur une plateforme ou une application unique, le seul moyen de mettre en œuvre le droit à l'oubli, entériné par les lois dites « eraser laws », consiste à appuyer sur le bouton nucléaire, c'est-à-dire à supprimer TOUTES les données. Cela vous fera gagner un court instant d'anonymat jusqu'à ce que vous recommenciez à taper sur un clavier, ouvriez votre téléphone, vous déplaciez ou démarriez toute autre activité enregistrée. Même ce court instant d'anonymat est incertain. Ces mêmes données ont probablement été dupliquées ailleurs : sur vos autres appareils, par des partenaires ou par des tiers hors de votre portée. Là encore, Google et Facebook sont les coupables évidents (certains parleraient de boucs émissaires) simplement à cause de leur omniprésence et de la diversité de leur gamme d'activités concernées (même si là encore, cela n'a rien à voir avec leurs concurrents chinois). Mais, souvent à l'insu de leurs utilisateurs, un grand nombre d'autres plateformes et applications présentent des problèmes similaires, avec la difficulté supplémentaire de les identifier.

[69] Document de travail soumis au Conseil « Justice et affaires intérieures » de décembre 2018, 23 novembre 2018, disponible à l'adresse suivante : http://data.consilium.europa.eu/doc/document/ST-14319-2018-INIT/en/pdf

Respect de la vie privée et *privacy by design*

Il faut donc s'éloigner des notions d'avis de notification et de consentement, d'ergonomie et d'expérience utilisateur (UX) dans ces processus pour s'orienter vers d'autres méthodes assurant la confidentialité des données. Le « respect de la vie privée dès la conception » *(privacy by design)*, ou la prise en compte de la vie privée dans la conception d'un projet IT, est un concept générique. Il s'agit d'une approche privilégiée par les grandes entreprises numériques parce qu'elle repose sur des prouesses technologiques qui leur sont plus accessibles. Cette approche ne déroge pas à la thèse fondamentale selon laquelle « le code fait loi » (*Code is law,* Lawrence Lessig), ni à la conviction selon laquelle le droit doit garder ses distances avec la technologie car le droit évolue beaucoup plus lentement et ne peut pas rattraper l'innovation, ou seulement en l'étouffant ou en l'arrêtant. Le concept de *privacy by design* donne un maximum de pouvoir aux choix faits par les concepteurs de logiciels. Citons par exemple le cryptage des iPhones par Apple. Ces choix, tels que le chiffrement de bout en bout, créent des dilemmes pour les autorités qui craignent que les criminels puissent par exemple échapper à leur surveillance. Dans ce jeu du chat et de la souris, la balance semble de plus en plus pencher du côté des nouvelles technologies disponibles pour les outils de surveillance. Les chefs de la mafia sicilienne parviennent à déjouer la surveillance en communicant exclusivement depuis leurs retraites cachées avec des *pizzi,* des bouts de papier. Ils doivent se méfier du moindre équipement électronique dans leur environnement.

Certains outils visant à garantir la confidentialité des données impliquent également des compromis avec les principes de concurrence. Récemment, plusieurs grandes plateformes de données

et leurs PDG se sont tournées vers les lois de protection de la vie privée, notamment le RGPD et le règlement européen « vie privée et communications électroniques ». Ils prennent peut-être progressivement conscience des dommages déjà causés. Mais il existe également un aspect commercial : rejeter une multitude de gestionnaires et de revendeurs de données tiers, élargir la portée des plateformes à de nouveaux domaines tout en s'assurant que les données restent à l'intérieur de la boîte noire de la plateforme, tout cela favorisera effectivement plus de confidentialité (en supposant que l'entreprise et ses employés sont dignes de confiance) mais étendra également la puissance des algorithmes basés sur des banques de données encore plus grandes et plus larges. C'est peut-être aussi la façon par laquelle les grandes plateformes occidentales peuvent espérer s'imposer face aux plateformes chinoises qui, certes sont entièrement contrôlées par leur gouvernement, mais qui sont aussi beaucoup moins réglementées, ce dont elles se servent pour s'étendre à l'international. Cette situation est à l'origine d'une contre-offensive du ministère américain de la Justice qui envisage un démembrement de Google, voire d'autres grandes plateformes informatiques.

Pour éviter l'asymétrie des connaissances entre opérateurs de données, il a été fortement suggéré d'imposer une norme ouverte aux plus grandes plateformes. Celles-ci seraient obligées de partager des catégories de données avec leurs concurrents. Prenons l'exemple d'Amazon : cette plateforme est désormais capable de concevoir et de commercialiser des ampoules électriques ayant le meilleur rapport qualité/prix parce qu'elle a étudié les clics et les achats de ses client et connaît bien leurs préférences. Elle serait obligée de partager cette information marketing avec d'autres fabricants et vendeurs d'ampoules électriques. Aussi attrayante que soit l'idée pour assurer la symétrie

de l'information, elle implique de transférer d'importantes ressources de données à un nombre indéterminé de tiers. Dans ce cas, le fait d'accroître la concurrence va à l'encontre de la notion de respect de la propriété privée dès la conception.

Les entreprises ne peuvent pas protéger les données personnelles dès la conception si elles ne connaissent pas les règles et ne reçoivent pas de lignes directrices. Ni elles ni les utilisateurs n'auront de points de référence ou en cas de litige. Une évaluation saisissante oppose le « choix de fournisseurs d'infrastructures numériques critiques qui se mêlent aux débats sur la sécurité et le respect de la vie privée et celui de fournisseurs qui écartent activement ces débats et optent pour l'autoritarisme numérique ou les intérêts chinois »[70]. Elle note par exemple que les pays impliqués dans des projets de connectivité dans le cadre de l'initiative *Belt & Road* n'ont peut-être pas ce choix. Jusqu'à présent, 18 États ont opté pour les systèmes de surveillance chinois.

Mais il est difficile de légiférer sur la *privacy by design* et cela va peut-être même à l'encontre de l'innovation. « La *privacy by design* dès la conception fait beaucoup de bruit pour très peu de substance. Même si ce concept permettrait très certainement de rétablir l'équilibre entre les collecteurs de données et les utilisateurs, il souffre d'une trop grande ambiguïté »[71]. Les obligations de chaque acteur doivent être clairement identifiées pour éviter que les différents types d'opérateurs ne rejettent par exemple les responsabilités sur les autres. Si la loi est formulée dans des termes trop généraux, elle

[70] « Is The Innovation Winter Coming? – Analysis », *Eurasia Review,* 27 juin 2019, https://www.eurasiareview.com/27062019-is-the-innovation-winter-coming-analysis/.

[71] Ari Ezra Waldman, « Privacy's Law of Design », *UC Irvine Law Review,* 31 octobre 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3263000.

devient inapplicable ; si elle est définie de manière trop stricte, elle passe à côté d'une grande partie de la cible. Des exigences et conditions vagues favorisent une conformité de façade et les utilisateurs ont du mal à savoir si la loi est respectée. Cela laisse également la possibilité aux diverses institutions et personnes physiques chargées de contrôler la conformité d'avoir des interprétations différentes, voire opposées, de la loi. Les responsabilités doivent être réparties entre les concepteurs de logiciels, les opérateurs et les utilisateurs organisés : si des groupes extrémistes abusent du potentiel d'un réseau social pour le transformer en arme, cela ne relève pas de la seule responsabilité de ce réseau. La loi devrait être appliquée de manière coopérative. En effet, compte tenu de la multitude d'organisations impliquées dans les échanges numériques, il faut expliquer la loi et convaincre, avant d'influencer par des incitations indirectes *(nudging)* ou de punir.

Seul ce processus itératif entre la loi et les acteurs peut éviter l'inconvénient majeur d'une législation *ex ante,* qui se trompera en passant à côté de questions de confidentialité cachées ou manquera sa cible et inhibera les activités numériques en étant trop générale et trop vague. Il faut ajouter à cela que les Européens sont particulièrement vulnérables à ce dernier travers, en raison de la popularité du fameux « principe de précaution », une véritable philosophie sociale anti-innovation. Une réglementation excessive et irréaliste conduit généralement à une mauvaise application de la loi. Un autre enjeu majeur est le choix entre une application d'en haut de la loi et une approche par le bas, par exemple par le biais de plaintes et de recours individuels ou par l'émancipation de groupes de la société civile capables de mieux représenter les intérêts des individus. Ce point est particulièrement important pour les préoccupations en matière de protection de la vie privée. L'un des

principaux objectifs du concept de *privacy by design*, et de ses prescriptions légales, devrait être de libérer l'individu des choix qu'il ne peut pas faire, soit parce qu'ils sont indéchiffrables, soit parce qu'il y en a trop. « Faire confiance, mais vérifier » : seule l'accumulation d'institutions chargées de faire appliquer la loi et d'organisations représentatives de la société civile permet d'exercer un contrôle permanent sur les opérateurs. Cela est d'autant plus nécessaire que le monde numérique est en constante évolution. Les mises à jour, les correctifs, les améliorations, les utilisations non prévues au départ apparaissent tout le temps et posent de nouveau les mêmes risques.

Et pourtant, le principe de précaution a ses limites car il est souvent fondé sur le consensus actuel et les habitudes. Sans innovations technologiques radicales, nos sociétés resteraient figées. Il existe très peu de consensus durables. Parce que le monde numérique remodèle nos coutumes sociales et nos habitudes personnelles en étendant la portée de notre esprit, à l'instar d'un exosquelette qui augmente les capacités de notre corps, il faut considérer qu'arrêter d'innover a des conséquences éthiques aussi importantes que de continuer. En 2006, alors que Facebook comptait 8 millions de membres étudiants, le réseau social a lancé le « fil d'actualité », une fonction qui permettait à ses membres de suivre les activités de leurs amis Facebook en temps réel[72]. Des centaines de milliers de membres ont organisé des manifestations contre cette fonctionnalité. Aujourd'hui, peut-être pour le pire, le fil d'actualité représente le principal attrait de Facebook pour ses 2,4 milliards d'utilisateurs. Il apparaît très clairement que le service rendu par les applications

[72] Tracy Samantha Schmidt, « Inside the Backlash Against Facebook », *TIME,* 6 septembre 2006, http://content.time.com/time/nation/article/0,8599,1532225,00.html. Cité par William McGeveran, « Friending the Privacy Regulators », *Arizona Law Review* 58, n° 4 (2016), p. 1004, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820683.

VTC l'emporte sur la perte évidente qu'ils impliquent en termes de protection de la vie privée. Être évalué et noté à chaque fois que l'on monte dans l'un de ces véhicules aurait été inconcevable il y a seulement quelques années. Cela est aujourd'hui pourtant considéré comme normal, et ceci est de plus en plus le cas dans d'autres secteurs de l'économie à la tâche et de l'économie de troc. Les libertaires peuvent toujours prendre le métro - à condition de payer en espèces plutôt qu'avec une carte, comme de nombreux manifestants de Hong Kong ont choisi de le faire en juillet 2019 pour échapper à l'identification personnelle.

L'argument libéral en faveur d'un marché des données a également ses limites. Les utilisateurs ou consommateurs qui « paient » avec leurs données n'ont pratiquement aucune idée de ce qu'il adviendra de leurs données et des risques encourus. Le « marché » est faussé par le déni de service qu'un opérateur peut prononcer et par l'absence de « tarification » des données cédées[73]. Nous voilà dès lors revenus au besoin initial de trouver un équilibre entre respect de la vie privée, efficacité et sécurité. Des compromis sont nécessaires, peut-être de la part de tout le monde : une des raisons pour lesquelles les utilisateurs se détournent de la télévision traditionnelle au profit des services de streaming est qu'ils sont épargnés par la publicité incessante. Mais en retour, ils renoncent au respect de leur vie privée.

[73] Katherine J. Strandburg, « Free Fall: The Online Market's Consumer Preference Disconnect », *University of Chicago Legal Forum* 2013, n° 5, 2013, https://chicagounbound.uchicago.edu/uclf/vol2013/iss1/5/.

III

LE RGPD, UNE PROUESSE RÉGLEMENTAIRE EUROPÉENNE

En l'espace d'un an, le RGPD est devenu la référence la plus couramment utilisée pour évaluer la protection de la vie privée, même si ce règlement concerne en réalité le traitement des données à caractère personnel par les opérateurs et les sociétés.

Il y a des raisons à cela. Il vise à créer un outil unique pour la prise de décisions relatives à la protection des données à caractère personnel (bien que les directives et les lignes directrices concernant la mise en œuvre revêtent une grande importance). C'est un texte de 88 pages superbement écrit, qui commence par énoncer les objectifs et la portée du règlement (173 « considérants »), puis poursuit par les dispositions à proprement parler (99 articles). Comme il s'agit d'un règlement, et non d'une directive comme le document précédent qu'il remplace, il a force de loi pour les 28 États membres, au moins dans des conditions « équivalentes ». Il permet de fait d'assurer la sécurité juridique dans tous les États membres de l'UE et sur ses flux de données externes. Dans certaines conditions, les règles nationales peuvent aller au-delà, mais non en deçà, des protections mises en place. Ce règlement aborde bon nombre, si ce n'est la totalité des questions relatives à la protection de la vie privée qui ont été évoquées précédemment dans la Partie II. Par exemple, les exigences relatives au consentement ont été renforcées par rapport à la directive européenne précédente : il doit être affirmatif, clairement énoncé, réversible et explicite pour les données à caractère personnel « sensibles ». Une utilisation différente des données à caractère personnel doit faire l'objet d'un consentement

distinct de la part de la personne concernée. Les données à caractère personnel sont définies au sens large. Elles comprennent les données financières, l'identité internationale d'équipement mobile (numéro IMEI) ou les adresses IP.

Le traitement des données ne peut s'effectuer qu'en respectant six obligations juridiques spécifiques, notamment le consentement. Le droit à l'effacement s'étend aux cas où la conservation des données n'est plus nécessaire à sa finalité initiale. Le droit à la portabilité des données est introduit. Le règlement traite par ailleurs de l'ergonomie, de l'anonymisation, de la responsabilité des fiduciaires de données en général et des opérateurs (respectivement décrits dans le RGPD comme les « responsables du traitement »[74] et les « sous-traitants »[75]), d'une approche coopérative, mais également de sanctions très sévères, de l'inclusion de toute entité traitant des données à caractère personnel de résidents l'UE, ainsi que de l'épineuse question de l'équivalence avec d'autres régimes de protection des données. Le *privacy by design* a lui aussi été intégré au RGPD : dans les faits, il incombe aux responsables du traitement de prendre les « mesures techniques et organisationnelles appropriées » pour se conformer au règlement. La minimisation de la collecte des données et la limitation de l'accès à celles strictement nécessaires à leur traitement sont également des obligations. Les violations de la confidentialité des données qui « engendrent un risque pour les droits et libertés » doivent impérativement être

[74] Selon l'article 4, le responsable du traitement est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et moyens du traitement des données à caractère personnel ».

[75] Selon l'article 4, le sous-traitant est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».

notifiées dans un délai de 72 heures. Il est également obligatoire pour les responsables du traitement des données, ou les sous-traitants, de désigner un délégué à la protection des données chargé des questions de formation et de conformité au règlement au sein de l'entreprise. Enfin, le RGPD fournit un cadre pratique pour la mise en œuvre, confiée aux institutions nationales responsables des données, mais avec un nouveau comité européen de la protection des données chargé du contrôle. Il a remplacé le groupe de travail dit « Article 29 » (GT29) qui avait lui un rôle consultatif. Ceci est de fait devenu un aspect essentiel du RGPD.

Les États-Unis ne fournissent tout simplement aucun modèle qui puisse être reproduit dans une autre société : leur législation est dispersée et conditionnée par des lois et des organismes d'État et fédéraux extrêmement divers. La justice joue un rôle important dans les litiges au cas par cas. Le RGPD, y compris son système de dispositions nationales équivalentes et d'autorités de contrôle, est un modèle cartésien en comparaison. Dans la mesure où il apporte certitude et simplicité, il est facilement transférable, ou tout du moins ses principes. Enfin, l'Europe est l'un des quatre grands marchés de données numériques (avec la Chine, l'Inde et les États-Unis), et le RGPD aura progressivement des implications importantes pour la libre circulation mondiale des données. Alors que l'« équivalence » sert de guide pour la mise en œuvre du RGPD dans les États membres, l'« adéquation » est la référence pour conclure des accords de libre circulation des données avec des pays tiers. Cette notion vise à reconnaître que les environnements juridique et sociétal diffèrent, et que divers processus peuvent être utilisés pour atteindre un niveau de protection adéquat mais non identique à celui des normes de l'UE. La décision d'adéquation n'est pas transférable à un autre pays, et elle n'est prise qu'à l'issue d'un processus itératif

entre l'UE et son partenaire, qui entraîne des changements dans les règles régissant la protection des données dans ce pays. La décision d'adéquation est régulièrement examinée et peut ultérieurement faire l'objet d'améliorations[76].

Les inconvénients évidents

Il y a bien sûr des inconvénients. Le RGPD est un texte fourre-tout reposant sur la recherche d'un équilibre entre objectifs opposés. En effet, il affirme que la protection des données à caractère personnel « n'est pas un droit absolu ». Ce droit est limité par tout « intérêt légitime ». Ce règlement est censé encourager la libre circulation des données, une revendication contestée par ceux qui voient de lourdes obligations et des risques de litiges poindre à l'horizon. Les PME et organisations comptant moins de 250 employés sont dispensées de tenir un registre de leurs activités de traitement. Cette exemption ne s'applique pas si le traitement effectué par l'entreprise n'est pas occasionnel, une exception utile à cette exception. La société Cambridge Analytica comptait par exemple moins de 250 salariés[77]. Il n'en demeure pas moins qu'un nombre louable de droits des personnes physiques sont reconnus : le contrôle par les

[76] À titre d'exemple, la décision d'adéquation concernant le Japon compte 48 pages et 28 000 mots.

Source : Commission européenne, « Décision d'exécution (UE) 2019/419 de la Commission du 23 janvier 2019 constatant, conformément au règlement (UE) 2016/679 du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par le Japon en vertu de la loi sur la protection des informations à caractère personnel », *EUR-Lex,* 2019, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2019.076.01.0001.01.ENG&toc=OJ:L:2019:076:TOC.

[77] « Cambridge Analytica », *Crunchbase,* 2019, https://www.crunchbase.com/organization/cambridge-analytica#section-overview or https://www.owler.com/company/cambridgeanalytica.

personnes physiques de leurs données à caractère personnel, le consentement explicite et facilité à la collecte des données, le traitement minimal (ex. lorsqu'aucun autre moyen n'est disponible), le droit à la rectification et à l'oubli, la portabilité des données, les principes de protection des données dès la conception et par défaut, ainsi que des normes strictes en matière de droits de l'homme et d'État de droit pour les accords d'adéquation avec les pays non membres de l'UE.

Mais ce règlement ne contient pratiquement aucune prescription en matière d'ergonomie, à savoir l'expérience utilisateur. Ce n'est pas inhabituel pour un texte juridique, mais il est clair que des études en expérience utilisateur, des lignes directrices pour la mise en œuvre et des processus standard sont nécessaires, tout comme le conducteur de voiture moyen doit comprendre les règles de circulation. Dans ces conditions, l'idée de permettre aux personnes physiques de contrôler leurs données à caractère personnel est envisageable, du moins partiellement. De même, ce règlement n'a littéralement aucune mention relative à l'IA : les mots « algorithmes » ou « fusion de données » n'y figurent pas. Bien qu'elles soient requises, l'anonymisation ou la pseudonymisation ne tiennent pas compte des nouvelles capacités d'apprentissage automatique pour déjouer ces processus.

Les exemptions : intérêt public et prérogatives des États membres

Il existe un grand nombre d'exemptions au Règlement : la liste la plus longue figure à l'article 23, comme suit :

« 1. (…)a) la sécurité nationale; b) la défense nationale; c) la sécurité publique; d) la prévention et la détection d'infractions pénales, ainsi que les enquêtes et les poursuites en la matière ou l'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces ; e) d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale; f) la protection de l'indépendance de la justice et des procédures judiciaires; g) la prévention et la détection de manquements à la déontologie des professions réglementées, ainsi que les enquêtes et les poursuites en la matière; h) une mission de contrôle, d'inspection ou de réglementation liée, même occasionnellement, à l'exercice de l'autorité publique, dans les cas visés aux points a) à e) et g); i) la protection de la personne concernée ou des droits et libertés d'autrui; j) l'exécution des demandes de droit civil.

2. En particulier, toute mesure législative visée au paragraphe 1 contient des dispositions spécifiques relatives, au moins, le cas échéant: a) aux finalités du traitement ou des catégories de traitement; b) aux catégories de données à caractère personnel; c) à l'étendue des limitations introduites; d) aux garanties destinées à prévenir les abus ou l'accès ou le transfert illicites; e) à la détermination du responsable du traitement ou des catégories de responsables du

traitement; f) aux durées de conservation et aux garanties applicables, en tenant compte de la nature, de la portée et des finalités du traitement ou des catégories de traitement; g) aux risques pour les droits et libertés des personnes concernées; et h) au droit des personnes concernées d'être informées de la limitation, à moins que cela risque de nuire à la finalité de la limitation. »

Ce règlement ne peut pas non plus être invoqué contre l'archivage de données à des fins historiques, scientifiques et statistiques, un ajout apprécié des chercheurs, mais qui met en doute, au moins dans un sens absolu, le « droit à l'oubli ». Il est clair que le RGPD a été conçu en direction des opérateurs privés et les fiduciaires de données plutôt que des gouvernements et des entités publiques. Dans le triangle entre respect de la vie privée, efficacité et sécurité évoqué ci-dessus, il a surtout fait pencher la balance en faveur du respect de la vie privée, en imposant des obligations aux opérateurs et aux fiduciaires de données, y compris parfois les organismes publics. Pourtant, il a reculé devant de nombreuses décisions qui auraient pu diminuer la sécurité ou compromettre les objectifs de politique publique en général. Lorsque le RPGD est examiné sous cet angle, le contraste avec des règles plus explicitement axées sur le consommateur ou les décisions de justice en matière de vie privée aux États-Unis est moins évident. Le règlement prévoit également des exceptions importantes, mais définies de manière très générale, aux règles de transfert de données en dehors de l'UE. Comme indiqué au considérant 114 et aux articles 48 et 49, la conclusion sur ce point est que c'est la Commission qui a le pouvoir de décider au cas par cas et conformément aux principes généraux.

Le bâton dissuasif

Les sanctions potentielles sont un domaine où le RGPD fait vraiment la différence. Elles doivent être « effectives, proportionnées et dissuasives ». Pour les violations des obligations strictes incombant au responsable du traitement, au sous-traitant et aux organismes de certification et de contrôle, les amendes peuvent atteindre 10 millions d'euros ou 2 % du chiffre d'affaires mondial, le montant le plus élevé étant retenu. Pour les « principes de base », les droits des personnes concernées, les transferts en dehors de l'UE et le non-respect d'une injonction de cessation, elles s'élèvent à 20 millions d'euros ou 4 % du chiffre d'affaires. Comme nous le verrons, le fait de placer la barre très haute en matière de sanctions a attiré l'attention des grandes entreprises au cours de la première année de mise en œuvre. En vertu de l'article 58, le traitement de données par-delà les frontières de l'UE peut également être exclu en tant que mesure correctrice.

Évaluation du RGPD, un an après

Après sa première année d'existence, le RGPD de l'UE est examiné et évalué par diverses sources, dont la Commission et le Comité européen de la protection des données (*European Data Protection Board,* EDPB), ainsi que par les autorités nationales de contrôle. C'est dans ce contexte que l'on peut juger de l'impact réel du RGPD. Le texte avait de nombreuses intentions déclarées et représentait un exercice d'équilibriste. La façon dont il est mis en œuvre, même dans sa phase initiale, nous en dit plus sur son impact. Le rôle qu'il joue pour la protection des données et de la vie privée par d'autres législations dans le monde, y compris aux États-Unis, peut également

être évalué. En revanche, sa pertinence pour les lois et règles de la Chine en matière de protection de la vie privée, semble n'être qu'un élément secondaire de ce qui est aujourd'hui l'État le plus avancé du monde en matière de surveillance ouverte. Par ailleurs, la distance entre textes juridiques et pratiques effectives y est telle que ce sont ces dernières qui importent.

Retour d'expérience et silos nationaux

Comme il se doit d'un règlement garantissant la protection des données à caractère personnel, le principal critère de l'EDPB pour mesurer le succès du RGPD après un an a été la sensibilisation des citoyens et leur volonté à porter plainte. En mars 2019, 67 % des citoyens de l'UE interrogés étaient au courant de l'existence du RGPD et 57 % connaissaient l'existence des autorités nationales de contrôle, un résultat louable. Les chiffres sont impressionnants : 281 088 requêtes adressées simultanément aux autorités nationales de contrôle des données, dont 144 376 plaintes et 89 271 rapports de violation de données.

L'une des principales innovations du RGPD est de prévoir une coopération entre les autorités nationales pour les affaires transfrontalières. Ces affaires sont enregistrées dans le système d'information sur le marché intérieur (IMI). Au-delà d'une assistance mutuelle (444 demandes ont été déposées à ce titre), bon nombre de ces cas passent par un mécanisme de guichet unique *(one stop shop)* dans lequel une autorité de contrôle chef de file doit d'abord être désignée. Jusqu'ici, les chiffres réels sont moins impressionnants. En mars 2019, seuls 466 cas transfrontaliers avaient été signalés, dont 19 seulement avaient trouvé une solution. Sur ce total,

45 étaient des cas relevant du mécanisme de guichet unique, dont six ont abouti à une décision définitive. L'EDPB donne également des avis de cohérence afin de garantir systématiquement l'équivalence entre les autorités de contrôle. 29 de ces avis ont été donnés. Le mécanisme de guichet unique ne s'applique pas lorsque l'entité concernée exerce ses activités en dehors de l'UE : celle-ci est alors responsable devant chacune des autorités de contrôle nationales.

L'EDPB et la Commission reconnaissent implicitement certaines des critiques des parties prenantes. L'une de ces critiques porte sur les différences pratiques persistant entre les États membres pour assurer l'adéquation au règlement. Un an après, trois États membres n'ont toujours pas modifié leur législation. La Commission ne dévoile pas leur nom, mais il s'agit de la Grèce, du Portugal et de la Slovénie. Des différences telles que l'âge minimum du consentement des enfants créent des difficultés pour les plateformes transnationales. Bien que la Commission privilégie actuellement le dialogue aux sanctions, elle ne reconnaît pas toujours le manque de clarté et de réalisme de certaines autorités de contrôle. En Pologne, l'autorité de contrôle PUODO a infligé une amende de 220 000 euros (la troisième plus grosse amende infligée sur la base du RGPD la première année) à une plateforme suédoise (Bisnode) pour avoir omis de contacter six millions de personnes par lettre recommandée au sujet de l'acquisition de leurs données à caractère personnel par des registres publics. La bataille juridique oppose les ardents défenseurs de l'article 14 du RGPD à ceux qui plaident en faveur de la proportionnalité : le coût de six millions de lettres recommandées serait en effet prohibitif[78]. Ni le PUODO ni le RGPD lui-même ne prêtent une grande attention au réalisme de ces règles.

[78] Karolina Gałęzowska, « Why You Should Pay Close Attention to the Polish DPA's First GDPR Fine », *Iapp.org,* 22 avril 2019, https://iapp.org/news/a/polish-dpas-first-fine-pay-close-attention/.

Mais où est le bâton ?

Au total, 56 millions d'euros d'amende ont été infligés au cours de la première année, chiffre qui comprend l'amende de 50 millions d'euros infligée par la CNIL, l'autorité de contrôle française, à Google. Google a cependant fait appel. Le Royaume-Uni est allé plus loin depuis, en août 2019, avec une amende de 99 millions de livres sterling contre Marriott et une autre de 183 millions de livres sterling contre British Airways : à ce jour, le Royaume-Uni, qui s'apprête à quitter l'UE, est le pays qui impose les sanctions du RGPD de la façon la plus stricte ! Ces chiffres parlent d'eux-mêmes. Bien qu'élevé en apparence, le nombre de plaintes est très faible par rapport à l'utilisation globale. La mise en œuvre reste largement à l'intérieur des frontières. L'arme magique des 4 % du chiffre d'affaires mondial s'est muée en amendes très limitées, parfois décrites comme appropriées pour une première année de mise en œuvre. Phénomène bien plus encourageant, les entreprises ont dépensé de l'argent et recruté des collaborateurs pour se conformer au RGPD. L'*International Association of Privacy Professionals* (IAPP) estime qu'un an après, 500 000 organisations ont enregistré des délégués à la protection des données en Europe[79]. Les grandes entreprises informatiques mettent effectivement en avant leur investissement pour se conformer au règlement. Microsoft affirme par exemple avoir mobilisé 1 600 ingénieurs-année pour se mettre en conformité avec le RGPD dans le monde entier, et pas seulement en Europe.

[79] Pour une explication de l'estimation : IAPP, « Approaching One Year GDPR Anniversary, IAPP Reports Estimated 500,000 Organizations Registered DPOs in Europe », *Iapp.org,* 16 mai 2019, https://iapp.org/about/approaching-one-year-gdpr-anniversary-iapp-reports-estimated-500000-organizations-registered-dpos-in-europe/.

Le nombre total de plaintes, en particulier les plaintes transfrontalières, la lenteur du rythme de résolution et le montant minimal des amendes infligées soulèvent la question de la mise en œuvre. L'EDPB constate que les autorités de contrôle nationales n'ont pas toutes obtenu les augmentations de budget correspondant à leurs nouvelles missions. Cinq d'entre elles ont vu leur budget diminuer (la Pologne et la République tchèque) ou ne pas augmenter (l'Autriche, la Belgique et la Lettonie). L'effectif de huit autorités de contrôle n'a pas changé, il a même diminué pour l'une d'elles (République tchèque)[80].

Le point de vue des entreprises et le problème de la taille

L'attitude générale des grandes entreprises à l'égard du RGPD est, du moins extérieurement, positive. Mais une des principales plateformes de partage interrogées lors de notre recherche explique qu'aucune grande entreprise ne se prononcerait publiquement contre le RGPD dans son ensemble et a souligné que la satisfaction des utilisateurs et leur sécurité étaient prioritaires par rapport aux règles de confidentialité. Les plaintes se concentrent sur les différentes législations « équivalentes » de chaque État membre, et l'uniformisation ne semble pas en vue. Ces différences engendrent une perte de temps et, en fin de compte, des amendes. Tous les sous-traitants et opérateurs ne sont pas sur un pied d'égalité. Il est clair que les courtiers en données indépendants, et paradoxalement les sites Web et applications de moindre envergure (y compris les médias

[80] Pour connaître les chiffres réels, voir : EDPB, « First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities », 8 mars 2019, p.11-12, https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf.

d'information les plus réputés qui sont passés au contenu gratuit en ligne) sont les plus vulnérables aux restrictions en termes d'avis de notification et de consentement, puisque leur source de revenus provient strictement de la revente des données émises par les utilisateurs. La *Oath Privacy platform* à laquelle appartiennent plusieurs publications respectées comme le *Huffington Post,* et qui appartenait à l'origine à Yahoo et AOL, a adopté une approche particulièrement choquante de « l'avis de notification et de consentement » du RGPD. Elle compte désormais 43 « partenaires fondateurs » qui récupèrent vos données. Pour gérer les contrôles de confidentialité, il faut lire et cliquer sur un dédale d'écrans, y compris une liste des règles de confidentialité mises au point par 45 pays différents, pour ensuite parcourir la politique de confidentialité en petits caractères de chaque propriétaire de cookie et enfin arriver sur un tableau de bord des règles de confidentialité[81]. En bref, Oath a rendu pratiquement impossible la mise en œuvre des règles du RGPD sur ses sites Web associés.

Une étude intéressante, qui a fait appel à l'apprentissage automatique pour tester les politiques de confidentialité affichées par quatorze grandes entreprises du Web (Google, Facebook, Instagram, Amazon, Apple, Microsoft, WhatsApp, Twitter, Uber, AirBnB, Booking.com, Skyscanner, Netflix, Steam et Epic Games), a trouvé qu'aucune d'elles n'était en pleine conformité avec le RGPD. Selon les auteurs de ce rapport[82], « le corpus évalué de 3 658 phrases (80 398 mots) contient 401 phrases (11,0 %) marquées comme contenant un

[81] Giuseppe Contissa et al., « CLAUDETTE Meets GDPR. Automating the Evaluation of Privacy Policies Using Artificial Intelligence », *CLAUDETTE,* 2 juillet 2018 https://www.beuc.eu/publications/beuc-x-2018-066_claudette_meets_gdpr_report.pdf

[82] Giuseppe Contissa et al., « CLAUDETTE Meets GDPR. Automating the Evaluation of Privacy Policies Using Artificial Intelligence », *CLAUDETTE,* 2 juillet 2018 https://www.beuc.eu/publications/beuc-x-2018-066_claudette_meets_gdpr_report.pdf

langage pas clair et 1 240 phrases (33,9 %) marquées comme constituant une clause potentiellement illégale, c'est-à-dire soit une clause de « traitement problématique », soit une clause « d'information insuffisante » (conformément aux articles 13 et 14 du RGPD) ». Ce rapport a également été cité dans le rapport multipartite de la Commission européenne qui évalue la première année d'application du RGPD[83].

Ces remarques doivent être mises en balance avec l'affrontement perçu entre clarté et caractère inclusif, compte tenu de la complexité des exigences du RGPD. Dans le rapport multipartite de la Commission, les remarques des entreprises, de la société civile ou des organisations de consommateurs vont souvent dans des directions opposées. En lisant entre les lignes de ce compte-rendu poli mais candide, on s'imagine très bien en spectateur d'un match de tennis. Il peut sembler étonnant que les intervenants des entreprises, tout en soulignant le travail exigé par le RGPD, en reconnaissent également les fruits positifs, en particulier lorsqu'il s'agit d'évaluer les risques du traitement des données numériques. Les intervenants des PME et du secteur public sont quant à eux éprouvés par les efforts déployés[84].

Pourtant, le RGPD a eu des effets mesurables immédiats sur la collecte de données par des tiers au moyen de cookies sur les sites Web. Une étude portant sur les trois premiers mois de mise en œuvre dans sept pays de l'UE révèle une baisse de 22 % de la collecte de

[83] Multistakeholder Expert Group to support the application of Regulation (EU) 2016/679, « Contribution from the Multistakeholder Expert Group to the Stock-Taking Exercise of June 2019 on One Year of GDPR Application », *Commission européenne,* 13 juin 2019, https://ec.europa.eu/commission/sites/beta-political/files/report_from_multistakeholder_expert_group_on_gdpr_application.pdf

[84] *Ibid.,* p. 14-15.

données sur les sites d'information, la plus importante ayant été enregistrée au Royaume-Uni (45 %) et la moins importante en Allemagne (6 %). Parmi celles-ci, les grandes plateformes – Google, Amazon, Facebook et Twitter – ont enregistré une très petite réduction de leur présence[85].

Les plateformes intégrées comme Google et Facebook font leur propre « tambouille » à l'aide d'algorithmes, puis elles vendent le produit de l'analyse et non les données brutes. Elles occupent une position suffisamment dominante auprès des utilisateurs pour ne pas courir le risque de se voir refuser beaucoup de données à caractère personnel. Cela peut représenter une activité énorme. Grâce à son minuscule bureau à Shenzhen, Facebook, qui n'est pourtant pas accessible depuis la Chine, génère 5 milliards de dollars de recettes publicitaires (9 % de son chiffre d'affaires annuel) provenant d'annonceurs chinois qui souhaitent s'adresser aux utilisateurs internationaux de Facebook[86]. Quant aux grandes plateformes de commerce électronique comme Amazon, le risque est moins celui d'une atteinte à la vie privée que d'une concurrence inégale : Amazon acquiert, et utilise, plus de données sur les goûts de ses clients que n'importe quel fabricant pourrait l'espérer. Les gestionnaires de réseaux de données, qu'il s'agisse d'opérateurs de télécommunication comme Orange ou de gestionnaires d'infrastructure comme Microsoft, tirent leurs revenus du service direct qu'ils fournissent, y compris la

[85] Timothy Libert, Lucas Graves et Rasmus Kleis Nielsen, « Changes in Third-Party Content on European News Websites after GDPR », *Reuters Institute for the Study of Journalism,* août 2018, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-08/Changes%20in%20Third-Party%20Content%20on%20European%20News%20Websites%20after%20GDPR_0_0.pdf

[86] L'estimation de 9 % est basée sur les derniers chiffres d'affaires de Facebook.
Source : Paul Mozur et Lin Qiqing, « How Facebook's Tiny China Sales Floor Helps Generate Big Ad Money », *The New York Times,* 7 février 2019, https://www.nytimes.com/2019/02/07/technology/facebook-china-internet.html.

sécurité des données, et sont donc moins vulnérables aux règles de confidentialité.

Cependant, les grandes entreprises n'hésitent pas à reconnaître qu'elles sont favorisées par rapport aux plus petites entreprises, tout simplement parce qu'elles disposent de plus de moyens financiers et de ressources humaines pour faire face aux exigences du RGPD. Elles peuvent également manœuvrer plus facilement. La priorité accordée par le RGPD à l'avis de notification et de consentement leur laisse une marge de manœuvre. Google a transféré la charge des demandes de consentement à ses fournisseurs de données externes. Une entreprise d'infrastructure numérique interrogée fait une distinction entre ses grands et ses petits clients : il est facile d'établir un partenariat avec les premiers pour le RGPD, mais beaucoup moins pour les seconds. C'est ce qu'avaient anticipé les concepteurs du RGPD en imposant moins d'exigences aux entreprises de moins de 250 employés. Un rapport récent de la Commission reproche à une autorité allemande de contrôle des données d'avoir abaissé unilatéralement ce plafond à 20 employés.

Apprendre à aimer le RGPD … tout en continuant de détester la directive « vie privée et communications électroniques » qui va suivre

Le revirement des grandes entreprises informatiques est spectaculaire. Mark Zuckerberg s'est déclaré favorable au RGPD[87], de même que Sundar Pichai, le PDG de Google[88] ou Satya Nadella, le PDG de Microsoft, qui qualifie le RGPD de « début fantastique »[89] et milite en faveur d'une norme mondiale. Tim Cook chez Apple va encore plus loin en soutenant une loi fédérale sur la protection de la vie privée intégrant notamment la question de l'IA qui, comme nous l'avons vu, est presque totalement absente du RGPD. Il prend également ses distances avec une grande partie du secteur en soulignant la « méfiance saine d'Apple envers l'autorité » qui fait partie de son attrait pour le consommateur : « Certains s'opposent à toute forme de législation sur la protection de la vie privée. D'autres soutiendront une réforme en public, puis résisteront et la dénigreront en privé »[90]. Cette pique n'est pas sans raison. Dans le climat actuel où l'affaire Edward Snowden, les *fake news* et l'affaire Cambridge Analytica ont fait basculer l'opinion, le RGPD peut apparaître comme

[87] Henry Farrell, « Facebook Is Finally Learning to Love Privacy Laws », *Financial Times,* 4 avril 2019, https://www.ft.com/content/67b25894-5621-11e9-8b71-f5b0066105fe.

[88] Jon Porter, « Google's Sundar Pichai Snipes at Apple with Privacy Defense », *The Verge,* 8 mai 2019, https://www.theverge.com/2019/5/8/18536604/google-sundar-pichai-privacy-op-ed-nyt-regulation-apple-cook-advertising-targeting-user-data.

[89] Isobel Asher Hamilton, « Microsoft CEO Satya Nadella Made a Global Call for Countries to Come Together to Create New GDPR-Style Data Privacy Laws », *Business Insider France,* 24 janvier 2019, http://www.businessinsider.fr/us/satya-nadella-on-gdpr-2019-1.

[90] La transcription du discours de Tim Cook à la Conférence internationale des commissaires à la protection des données et de la vie privée de 2018 à Bruxelles le 24 octobre 2018 est disponible à l'adresse suivante : Jonny Evans, « Complete Transcript, Video of Apple CEO Tim Cook's EU Privacy Speech », *Computerworld,* 24 octobre 2018, https://www.computerworld.com/article/3315623/complete-transcript-video-of-apple-ceo-tim-cooks-eu-privacy-speech.html.

un règlement raisonnablement stable et avec une portée limitée. Notamment, il ne dit pas grand-chose de l'étendue de la mission des responsables du traitement des données, ce qui peut considérablement limiter la concurrence. De même, il est largement axé sur les droits des utilisateurs, que les entreprises les mieux équipées savent contourner.

En bref, ce qui apparaissait comme une hantise en 2015 est aujourd'hui une tentative limitée de garantir le respect de la vie privée. En effet, comme l'avait prédit le monde de l'informatique, « la technologie fait loi » *(technology is law)* et elle continue d'avancer impitoyablement. La préoccupation actuelle des entreprises qui échangent des données est davantage liée à la prochaine étape de la Commission européenne : un règlement « vie privée et communications électroniques » qui mettra la réglementation des données de télécommunications au goût du jour et qui aura une portée beaucoup plus large que l'ancienne directive de 2002 sur la « protection de la vie privée dans le secteur des communications électroniques ». Parce que ce règlement exigerait le consentement de l'utilisateur final pour les transmissions de données, y compris des données de l'IdO (potentiellement des centaines d'appareils par utilisateur), il va au-delà de la « loi cookies » qu'il remplace et fait maintenant l'objet de nombreuses pressions de la part des lobbies. En effet, ce texte législatif est bloqué au Conseil depuis qu'il a été proposé par la Commission en octobre 2017[91].

[91] Parlement européen et Conseil, « Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « vie privée et communications électroniques») », *EUR-Lex,* 2017, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0010&from=FR.

Les pièges du consentement de l'utilisateur

L'écart entre les grandes et les petites entreprises ou organisations est particulièrement visible au niveau de l'expérience des utilisateurs dans la mise en œuvre de l'avis de notification et de consentement. Les plateformes et entités plus importantes, qui attirent des utilisateurs à de multiples occasions et par différentes activités, ont tendance à proposer un système d'approbation initial lorsqu'on arrive sur leurs services. Ce système est fondé sur une déclaration de politique de confidentialité souvent interminable. Elle sera ensuite régulièrement mise à jour, généralement avec de nouvelles politiques d'une longueur comparable, dont le contenu peut ne différer que sur certains points, mais des points potentiellement critiques. La grande majorité des utilisateurs se dispensera de lire ces interminables politiques de confidentialité, en partie parce qu'ils ont confiance dans la marque, en partie parce qu'ils n'ont pas le temps. Et de la même manière ils ne liront pas non plus les fréquentes mises à jour. Les plus petites organisations qui attirent des visites variées, souvent uniques ou quasi uniques, proposent généralement un questionnaire. Leur conception varie considérablement, nombre d'entre elles enfreignant l'esprit si ce n'est la lettre du RGPD. Devoir parcourir une liste comptant des dizaines, si ce ne sont des centaines de partenaires tiers et les cocher un par un est une tâche redoutable, surtout si elle se répète à l'occasion d'autres visites et sur un grand nombre de sites Web. D'autres encore donnent simplement la possibilité de lire de longues politiques de confidentialité ou explications sur leur politique, mais le seul choix possible est de les accepter ou de quitter le site Web.

En exigeant un consentement séparé pour les différentes utilisations des données à caractère personnel, sans imposer un cadre unique pour les questions et les réponses, le RGPD a lui-même contribué

de manière involontaire à cette complexité. Les sous-traitants utiliseront ce que l'on appelle des *dark patterns* (interfaces truquées) et le *nudging* afin d'inciter les utilisateurs à donner leur consentement. En fait, chacun de nous a pu constater les énormes différences qui existent entre les sites Web : il y a ceux qui fournissent par défaut des paramètres garantissant le respect de la vie privée et demandent simplement de les accepter, ceux qui exigent des modifications élément par élément, ceux qui vous demandent d'examiner une politique de confidentialité interminable, éventuellement sur différents sites Web, et enfin ceux qui vous offrent la possibilité d'accepter leur politique de confidentialité ou de quitter le site, ce qui revient à exercer un chantage sur les visiteurs[92]. En raison du « paradoxe de la protection de la vie privée » *(privacy paradox)* (les utilisateurs se livreront volontiers, pour des raisons d'efficacité, à des pratiques qui menacent leur vie privée), le RGPD n'atteint qu'une partie de ses objectifs déclarés, même dans le domaine de l'avis de notification et de consentement. Le récent communiqué victorieux de la Commission sur le RGPD[93] reconnaît que 44 % des utilisateurs n'ont pas changé leurs paramètres de confidentialité par défaut depuis la mise en œuvre du RGPD. En réalité, tout comme il existe des règles du Code de la route, il faudrait publier des règles de conduite sur la route virtuelle ainsi que des processus pratiques et faciles à mettre en œuvre. Le fait de cocher des cases n'est que le début de ce qui devrait conduire

[92] Pour un regard cinglant sur la mise en œuvre du RGPD par plusieurs grandes plateformes au cours des premiers mois qui suivent son entrée en vigueur, voir : Forbrukerrådet, « Deceived by Design. How Tech Companies Use Dark Patterns to Discourage Us from Exercising Our Rights to Privacy », 27 juin 2018, https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

[93] Commission européenne, « Communication de la Commission au Parlement européen et au Conseil. Les règles en matière de protection des données comme instrument pour créer un climat de confiance dans l'UE et au-delà – bilan », 24 juillet 2019, https://ec.europa.eu/commission/sites/beta-political/files/communication_from_the_commission_to_the_european_parliament_and_the_council.pdf.

à une relation de confidentialité mutuellement acceptée entre fournisseurs et utilisateurs finaux. On en revient à l'idée que l'utilisateur ne peut porter seul la responsabilité de protéger sa propre vie privée.

Le RGPD et la possibilité d'une convergence mondiale

Alors que nous quittons l'Europe, et surtout compte tenu de l'immensité des marchés dans des pays où le taux moyen d'alphabétisation est plus faible, le besoin de protéger la vie privée devient encore plus évident. L'une des premières réussites du RGPD tient au nombre de législations qui se sont récemment construites sur certaines de ses parties et certains de ses concepts. L'intérêt manifesté par d'autres États pour une décision d'adéquation de l'UE permettant la libre circulation des données vers le pays concerné est une autre de ses réussites. Avec un certain battage médiatique, la Commission conclut que cela a entraîné « une convergence mondiale des règles en matière de protection des données. (…) Ces règles présentent souvent plusieurs points communs qui sont partagés par le régime de protection des données de l'UE, comme une législation globale plutôt que des règles sectorielles, droits individuels opposables et une autorité de contrôle indépendante. Cette tendance est véritablement mondiale et s'observe de la Corée du Sud au Brésil, en passant par le Chili, la Thaïlande, l'Inde et l'Indonésie »[94]. La Commission reconnaît qu'il ne s'agit pas d'une solution transposable à toutes les situations et cite d'autres modèles potentiels tels que l'initiative « libre flux de données en toute confiance *(Data Free Flow with Trust)* » lancée par Shinzo Abe au sommet du G20 à Osaka en juin 2019. Cependant, le projet du Japon ne couvre pas la question du transfert des données à caractère personnel.

[94] *Ibid.,* p.1 et p.11

Le rapport de la Commission cite les décisions d'adéquation telles que l'accord UE-Japon comme la voie la plus prometteuse[95]. Il évoque brièvement et indirectement la compétence excessive d'autres États, en mentionnant les négociations sur le processus de transfert des données des dossiers passagers (PNR), ainsi que la question du partage des preuves électroniques dans les enquêtes pénales : le partage des données avec des pays tiers à des fins répressives relève d'une directive distincte de l'UE sur la police[96]. Jusqu'à présent, l'UE a pris 13 décisions d'adéquation, dont deux accords limités avec les États-Unis et le Canada. Parmi les onze autres, six sont des centres financiers, voire des marchés *offshore* comme Andorre ou les îles Féroé. La Commission négocie officiellement avec la Corée du Sud. D'autres pays comme l'Inde, le Brésil, l'Indonésie, ont exprimé leur intérêt pour une décision d'adéquation de l'EU. De plus en plus de pays adoptent en principe une législation de type RGPD.

Sans cadre humain ni ressources pour la mettre en œuvre, cela peut rester symbolique, même si cela témoigne de l'attrait général de la législation.

[95] Pour une description du processus ayant mené à l'accord d'adéquation EU-Japon, voir : Hiroshi Miyashita, « The Impact of GDPR in Japan », in *National Adaptations of the GDPR* (Luxemburg: Collection Open Access Book, Blogdroiteuropeen, 2019), 122–27, https://blogdroiteuropeen.files.wordpress.com/2019/02/national-adaptations-of-the-gdpr-final-version-27-february-1.pdf.

[96] Parlement européen et Conseil, « Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil », 2016, https://publications.europa.eu/en/publication-detail/-/publication/182703d1-11bd-11e6-ba9a-01aa75ed71a1/language-en.

IV

L'INDE, UN MIX NUMÉRIQUE

Le droit constitutionnel à la vie privée, un sujet controversé

En Inde, les débats sur la confidentialité des données sont apparus avec les discussions autour de la carte d'identité Aadhaar. La base de données biométrique a été piratée à plusieurs reprises. Cette carte est également devenue obligatoire pour accéder à certains services publics et certaines prestations publiques. Les entreprises privées ont par ailleurs accès aux données à caractère personnel[97]. Dans ce contexte, une décision historique de la Cour suprême de l'Inde a orienté le débat sur la protection de la vie privée. En 2017, un groupe de neuf juges a rendu une décision qui reconnaît le respect de la vie privée comme un droit constitutionnel et a ordonné au gouvernement de créer un comité spécial visant à faciliter la création d'un régime de protection des données en Inde. Le comité Srikrishna a été créé en 2018 pour rédiger le projet de loi *Personal Data Protection Bill* (PDPB). Ce projet de loi n'a pas encore franchi le stade législatif, stade ultime pour que la loi devienne juridiquement contraignante.

Cette même année, le comité Srikrishna a également publié un rapport qui a renversé la question en plaçant le respect de la vie privée dans le contexte d'une « économie numérique libre et

[97] Bloomberg, « Amazon's Real Rival in India Isn't Walmart », *The Economic Times*, 16 août 2018, https://economictimes.indiatimes.com/industry/services/retail/amazons-real-rival-in-india-isnt-walmart/articleshow/65418425.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

équitable » et de la « responsabilisation des Indiens ». Ses motivations étaient clairement affichées dans son titre. Le projet de loi lui-même réduit la portée de l'arrêt de la Cour suprême en affirmant (à l'instar du RGPD) que le droit à la vie privée n'est pas un droit absolu. Ce n'est pas une surprise totale. Selon un avocat représentant les plaignants lors de l'appel initial devant la Cour suprême, un an plus tard « le jugement n'a guère contribué à modifier les pratiques de l'État »[98]. Ce rapport met en lumière les motivations du PDPB, et présente les États-Unis, l'UE et la Chine comme les trois voies possibles : les États-Unis avec un système de laisser-faire, l'UE avec une approche réglementaire de protection des consommateurs et la Chine qui privilégie la protection des données comme un moyen d'assurer la sécurité nationale. À partir de ces choix, il propose ensuite une « quatrième voie synthétique » et souligne que le projet de loi indien « protège la vie privée de l'individu, garantit l'autonomie, permet la circulation des données pour un écosystème de données en expansion et crée une économie numérique libre et équitable »[99].

Un projet de loi qui ressemble au RGPD

La portée du projet de loi PDPB est très vaste, puisqu'il s'applique aux données collectées ou traitées sur le territoire indien par les fiduciaires de données indiens et étrangers, mais également aux données collectées en dehors de l'Inde lorsqu'elles concernent des citoyens indiens. Il comprend également une dernière clause assez

[98] Apoorva Mandhani, « The Right To Privacy Judgment Is A Year Old, But Not A Year Wiser », *Livelaw.In,* 24 août 2018, www.livelaw.in/the-right-to-privacy-judgment-is-a-year-old-but-not-a-year-wiser/.

[99] Comité d'experts sous la présidence du juge B.N. Srikrishna, « A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians », 27 juillet 2018, https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf.

vague, mais qui va au-delà du champ d'application du RGPD. Elle concerne les données collectées ou traitées dans le cadre de toute activité exercée en dehors de l'Inde. Il s'inscrit largement dans la lignée du RGPD en imposant des obligations aux fiduciaires et aux sous-traitants de données[100], tout en soulignant les droits des individus (personnes concernées). Ces droits comprennent la confirmation et l'accès, la rectification, la portabilité des données ainsi que le droit à l'effacement. Les fiduciaires de données incluent les organismes gouvernementaux et entités publiques assimilées, ce qui constitue un pas en avant par rapport aux obligations de protection des données préexistantes prévues par la loi *Information Technology (Amendement) Act* de 2008 et le règlement *Information technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules* de 2011[101].

Le projet de loi énumère les divers motifs de traitement des données à caractère personnel pour diverses raisons, notamment le consentement. Il suit le RGPD en prescrivant de la même manière une collecte, une finalité et une conservation limitées, ainsi que le modèle de consentement fondé sur un avis. Aspect intéressant, il recommande d'inclure, dans la mesure du possible, des avis en plusieurs langues. Il impose des audits des données et, en vertu de l'article 35, il autorise les auditeurs à attribuer une notation aux fiduciaires de données. Cette notation doit être affichée dans les avis de confidentialité aux utilisateurs. Il établit également une distinction

[100] Selon le PDPB, le terme « sous-traitant » désigne toute personne, y compris l'État, une entreprise, une personne morale ou physique qui traite des données à caractère personnel pour le compte d'un fiduciaire de données, à l'exclusion des employés du fiduciaire de données.

[101] EPW Engage, « What Enables the State to Disregard the Right to Privacy? », *Economic and Political* Weekly, 16 janvier 2019, p. 7 et 8, www.epw.in/engage/article/what-enables-state-disregard-right.

entre les données à caractère personnel et les données personnelles « sensibles ». Des règles différenciées sont définies pour le traitement de chacune de ces catégories de données. Ces règles ajoutent une étape supplémentaire au traitement des données sensibles, sur la base du « consentement explicite » qui est considéré différemment du consentement. Le projet de loi crée également une catégorie distincte de fiduciaires de données : les « fiduciaires de données importants » qui doivent être désignés par l'autorité nationale de protection des données en fonction de certains critères, notamment la quantité de données qu'ils traitent. Les transferts de données à des tiers ne sont pas expressément mentionnés, ce qui signifie qu'ils sont autorisés pour les motifs de traitement précisés.

Comme le RGPD, le PDPB met en place une autorité nationale de protection des données et un tribunal d'appel. Le premier serait un organe consultatif, de contrôle, et de réglementation quasi législatif, tandis que le second serait une autorité juridictionnelle investie des pouvoirs d'un tribunal civil. Le projet de loi soumet l'autorité à des obligations de collecte et de traitement des données lorsqu'elle traite des données à caractère personnel. Ce qu'il est intéressant de noter, c'est l'absence flagrante de détails et de précisions dans les deux chapitres établissant ces organes. Ils sont pour la plupart laissés à l'appréciation ultérieure du Parlement ou du pouvoir exécutif. L'autonomie de cette autorité, qui est essentielle à l'exercice de ses fonctions, est donc contestée à juste titre par des observateurs[102]. Le projet de loi mentionne également la nécessité de mettre en œuvre la notion de *privacy by design,* l'évaluation de l'impact sur la protection

[102] Bruno Gencarelli, « Submission on Draft Personal Data Protection Bill of India 2018 by the Directorate-General for Justice & Consumers to the Ministry of Electronics and Information Technology (MeitY) », *Service européen pour l'action extérieure - Commission européenne,* 19 novembre 2018, eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en.

des données et la notification de violations de données. Il exige des fiduciaires de données qu'ils nomment des délégués à la protection des données (*data protection officers,* DPO) pour faire respecter ses dispositions. Même les sanctions ont un plafond identique à celui prévu par le RPGD. Il est fixé dans certains cas à 4 % du chiffre d'affaires mondial (article 69.2). La liste des exemptions suit un schéma similaire. Sont prévues des exemptions à des fins de sécurité nationale, d'application de la loi, journalistiques et de recherche, ainsi que des exceptions pour les données manuelles collectées par les foyers et les petites entreprises.

Rien de ce qui précède ne distingue vraiment le projet de loi indien du RGPD. Il insiste de la même manière sur la libre circulation des données, impose des limites sous la forme d'exemptions à la protection des données à caractère personnel et souligne les obligations des opérateurs privés avec plus de précision que celles des pouvoirs publics. Le projet de loi indien n'est pourtant pas complètement identique au RGPD, comme l'a fait remarquer le directeur de l'unité flux et protection des données internationales de la Commission européenne[103]. L'évaluation européenne mentionne sur plusieurs pages des différences, des ambiguïtés ou un manque de protection juridique du projet de loi. À l'inverse, une récente analyse de Carnegie India[104] souligne les multiples éléments qui imitent le RGPD, mais seulement pour conclure que ce projet n'est pas applicable dans le contexte indien à cause des coûts énormes de mise en conformité et de l'impossibilité pour les petites et moyennes entreprises (PME) indiennes d'exécuter ces tâches. L'étude de Carnegie

[103] *Ibid.*

[104] Anirudh Burman, « Will a GDPR-Style Data Protection Law Work For India? », *Carnegie India*, 15 mai 2019, carnegieindia.org/2019/05/15/will-gdpr-style-data-protection-law-work-for-india-pub-79113.

s'appuie sur des prévisions et des évaluations négatives faites par des groupes de réflexion européens sur le RGPD : cependant, sur huit sources, une seule a été publiée après la mise en œuvre effective du RGPD. Le ministère de la Justice du Royaume-Uni et le Centre européen d'économie politique internationale (ECIPE), un groupe de réflexion habituellement favorable au libre-échange et contre la réglementation, sont les principales sources de cette étude entre 2012 et 2014. Jusqu'à présent, ces sombres prévisions (baisse du PIB due au RGPD, baisse des flux de données en provenance et à destination des États-Unis) ne se sont pas concrétisées.

Mais une critique persiste. Les PME ont généralement plus de difficultés à se conformer au règlement, or elles constituent l'écrasante majorité du tissu économique indien et sont plutôt réticentes à financer des délégués à la conformité des données. Se conformer à une législation de type RGPD semble donc difficile en Inde. Le projet de loi a exempté les petites entreprises de la plupart des obligations, mais les conditions d'exemption sont difficiles à remplir : réaliser un chiffre d'affaires inférieur à 200 000 roupies indiennes[105], ne pas collecter les données de plus de 100 personnes concernées, ne pas les collecter dans le but de les divulguer à d'autres entités, et surtout, traiter les données manuellement. Elles concernent donc essentiellement le secteur informel de l'économie indienne.

Alors que cette évaluation spécifique souligne les similitudes avec le RGPD et critique une partie de cette approche, les commentaires de la Commission européenne se concentrent plutôt sur les ambiguïtés et les lacunes du projet de loi. Les autorités publiques peuvent exempter les sous-traitants des obligations sans autre justification que « toute

[105] L'équivalent de 2 500 euros.

loi adoptée par le Parlement ou l'Assemblée législative d'un État ». Le gouvernement central peut donner des directives à l'autorité de protection des données « dans l'intérêt de la souveraineté et de l'intégrité de l'Inde, de la sécurité de l'État, des relations amicales avec des États étrangers et de l'ordre public ». Le traitement de données à des fins répressives et de renseignement national n'est soumis qu'à des exigences très générales. Les personnes physiques et les entreprises ont peu de possibilités de recours contre les décisions des DPO pour autant que celles-ci ont été prises « de bonne foi ». Le droit d'accéder à ses propres données se limite à « un bref résumé ».

Plus que le simple PDPB : autres législations et projets de loi

Les textes précédant le PDPB dans le domaine de la protection des données sont les sections 43-A et 72-A du *The Information Technology (Amendement) Act* de 2008, qui prévoyait une indemnisation en cas de négligence dans le traitement de données ou de renseignements personnels sensibles (*Sensitive Personal Data or Information,* SPDI), et des sanctions en cas de divulgation de renseignements personnels. La définition de ces SPDI a été précisée par le règlement *IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules* de 2011. Cependant, le projet de loi PDPB élargit le champ des données personnelles sensibles par rapport au texte précédent, le règlement *IT Rules* de 2011, pour inclure les identifiants officiels, des renseignements sur la vie sexuelle d'une personne, des données génétiques, le statut transgenre ou intersexué, la caste ou la tribu. Ce règlement exige également des politiques de confidentialité, alors que ce point n'est pas très clair dans le PDPB, lequel se contente de mentionner la nécessité des

avis.

En outre, il existe certaines réglementations sectorielles concernant la collecte et le traitement des données. Par exemple, la Banque de réserve de l'Inde (*Reserve Bank of India,* RBI) a la compétence d'une autorité réglementaire pour les données financières et a publié des règles de traitement des données pour ce secteur. En 2018, le ministère indien de la Santé et des Affaires sociales a déposé un projet de loi, le *Digital Information Security in Healthcare Act (DISHA),* qui définit, comme son nom l'indique, les règles de collecte et de traitement des données dans le secteur de la santé. Ce projet de loi sera abordé plus en détail dans une section suivante.

Comme le DISHA, un certain nombre d'autres projets de loi incluent la confidentialité des données d'une manière ou d'une autre. Le règlement *Draft Information Technology [Intermediaries Guidelines (Amendment) Rules]* de 2018 s'applique à toute personne qui, au nom d'une autre personne, reçoit, conserve ou transmet un message électronique ou fournit un service en rapport avec ce message. Ils doivent publier des règles, des règlements, une politique de confidentialité et des conditions d'utilisation pour informer les utilisateurs des restrictions d'accès ou d'utilisation des ressources d'un intermédiaire. Un autre texte en préparation, le projet de loi *National E-Commerce Bill,* permettra au gouvernement indien d'accéder à un code source et à des algorithmes, tout en interdisant le partage de données sensibles de tiers, même avec leur consentement[106].

[106] Données indiennes pour le développement de l'Inde, « Draft National E-Commerce Policy », 23 février 2019, https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf

De bas en haut, une mer d'applications

En général, le contrôle des applications est sommaire. Le marché en ligne indien est submergé d'applications chinoises et américaines. TikTok, l'application chinoise de partage de vidéos qui est très populaire dans tout le pays, déclare expressément qu'elle « ne peut pas garantir la sécurité des informations transmises par l'intermédiaire de la plateforme » et a été impliquée dans le partage social d'attaques physiques contre des personnes en milieu rural. Un article de presse indique que « 20 applications vidéo chinoises dominent le réseau de divertissement mobile des villes de deuxième et troisième catégories, principalement grâce à des vidéos émoustillantes, des notifications suggestives, un humour osé et un contenu obscène »[107].

Les applications chinoises ne sont pas les seules à profiter d'un manque de réglementation en matière de respect de la vie privée. Les politiques de confidentialité de Google Pay et de WhatsApp Pay en Inde, bien que cette dernière ne soit pas encore lancée, déclarent qu'elles partagent des données avec des tiers, tout comme PayTM et PhonePe (appartenant à Flipkart)[108]. Twitter et d'autres réseaux sociaux lancent parfois leurs innovations en Inde, parce que l'environnement réglementaire y est moins contraignant. Face à

[107] Economic Times Online, « Are RSS's Fears about Tik Tok True? Here's What You Should Know », *The Economic Times,* 19 février 2019, economictimes.indiatimes.com/articleshow/68066972.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

[108] « WhatsApp Legal Info », *WhatsApp,* 5 février 2018, https://www.whatsapp.com/legal?doc=payments-in-privacy-policy&version=20180205.

et

Shrutika Verma, Mihir Dalal, « WhatsApp May Be Sharing Your Payments Data with Facebook », *Livemint,* 10 avril 2018, https://www.livemint.com/Industry/VmupcMWS2ZbVssXuIInP2J/WhatsApp-may-be-sharing-your-payments-data-with-Facebook.html.

l'inquiétude grandissante au sujet de la sécurité des données des applications chinoises et de celles des GAFA américains, tant à l'intérieur du pays qu'à l'échelle mondiale, l'Inde semble se tourner vers des instruments politiques pour trouver sa voie à travers les différents régimes de protection des données de ces pays.

Flux transfrontaliers de données et souveraineté des données

La localisation des données est l'un de ces outils. L'effort législatif en faveur de la localisation des données au nom de la souveraineté et de la sécurité est souvent considéré comme un soutien à l'industrie et aux entreprises locales. Le projet de PDPB comporte tout un chapitre sur le transfert transfrontalier des données qui est très clair à ce sujet. Une copie de toutes les données à caractère personnel qui relèvent de ce projet de loi doit être conservée en Inde. Quant aux données à caractère personnel « critique » (catégorie à définir par le gouvernement central), elles doivent être conservées exclusivement en Inde. En ce qui concerne le transfert transfrontalier de ce type de données, le projet de loi prescrit un environnement similaire à celui du RGPD, c'est-à-dire des outils de transfert basés sur l'adéquation. Autre exemple d'instinct nativiste, le projet de politique en matière de commerce électronique évoqué plus haut est intitulé « Les données de l'Inde pour le développement de l'Inde ». Il exige que toutes les données soient conservées dans des centres de données et fermes de serveurs en Inde et donne trois ans aux entreprises pour se mettre en conformité.

Sur le plan international, la plus grande controverse porte en effet sur la localisation des données, une question essentiellement

économique, mais qui peut également avoir des conséquences sur la sécurité et la confidentialité des données. Cette décision traduit une préoccupation économique générale et un angle sécuritaire plus marqué. De façon plus discutable, Mukesh Ambani, qui a déjà profité de l'offensive du gouvernement en faveur d'un réseau mobile universel, s'est élevé contre le « colonialisme des données » et a exhorté au « transfert du contrôle et de la propriété des données indiennes en Inde, en d'autres termes, à redonner la richesse indienne aux Indiens »[109]. En avril 2018, la Banque de réserve de l'Inde a ordonné aux entreprises de conserver leurs données financières en Inde afin de garantir un accès complet à ces données à l'autorité de contrôle. Elle ne leur a laissé que six mois pour la mise en œuvre, une démarche qu'elle a réitérée récemment, en juin 2019, après la demande de réexamen du gouvernement[110]. La Commission européenne critique l'ensemble de cette politique en estimant qu'elle entrave la libre circulation des données, qu'elle n'améliore pas la sécurité des données et qu'il s'agit avant tout d'une forme de protectionnisme. Elle relève également un paradoxe, puisque l'Inde « est déjà un leader mondial dans le secteur du traitement des données »[111], et évoque le risque de représailles d'autres pays. Les milieux d'affaires critiquent plus souvent le coût de l'investissement

[109] Mahesh Langa, « Mukesh Ambani Urges Modi to Take Steps against Data Colonisation by Global Corporations », *The Hindu,* 18 janvier 2019, https://www.thehindu.com/news/national/mukesh-ambani-urges-modi-to-take-steps-against-data-colonisation/article26025076.ece.

[110] PTI, « RBI to Examine Concerns over Data Localisation Rule: Government », *The Economic Times,* 18 juin 2019, https://economictimes.indiatimes.com/news/economy/policy/rbi-to-review-data-storage-rules-for-payment-firms-government/articleshow/69838249.cms?from=mdr.

[111] Bruno Gencarelli, « Submission on Draft Personal Data Protection Bill of India 2018 by the Directorate-General for Justice & Consumers to the Ministry of Electronics and Information Technology (MeitY) », *Service européen pour l'action extérieure,* 29 septembre 2018, https://eeas.europa.eu/delegations/india/53963/submission-draft-personal-data-protection-bill-india-2018-directorate-general-justice_en.

dans des serveurs de données gigantesques dans des conditions climatiques défavorables, et notamment la ponction qu'il représenterait sur l'approvisionnement onéreux en électricité de l'Inde.

« Big Government, Big Data »

Outre la question de la souveraineté des données, il y a celle des pouvoirs excessifs de l'État. En fait, l'un des principaux problèmes du PDPB, également souligné par la Commission européenne dans ses commentaires sur le projet de loi, est le pouvoir qu'il confère au gouvernement central pour préciser certaines des clauses essentielles. Le gouvernement peut décider des conditions d'emploi et de financement de l'autorité de protection des données (articles 50, 56 et 57) et du tribunal d'appel (articles 79-82), et donner sa propre définition des données critiques (article 40.1). Pour que l'autorité soit indépendante, il convient qu'elle dispose d'une autonomie, au moins sur les questions financières. Il est problématique qu'un texte juridique de 62 pages laisse autant de questions indéterminées. Le projet de directive sur les intermédiaires affiche la même tendance. Selon l'article 3(5), « Lorsqu'une ordonnance légale l'exige, l'intermédiaire doit fournir, dans un délai de 72 heures à compter de la communication, les renseignements ou l'assistance demandés par un organisme gouvernemental… » sous des conditions spécifiques[112].

[112] Ministry of Electronics and Information Technology, « Comments on the (Draft) Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018 », 24 décembre 2018, p.3, https://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf.

Ces dernières années, les militants de la protection de la vie privée en Inde ont exprimé un certain nombre de préoccupations au sujet des actions du gouvernement, à commencer par l'affaire de la carte Aadhaar précédemment évoquée. Des efforts ont été récemment déployés pour rationaliser les données numériques collectées par l'intermédiaire d'Aadhaar (qui sont considérées comme des données à caractère personnel sensible dans le cadre du régime proposé), d'abord sous la forme d'une authentification basée sur Aadhaar et de services basés sur Aadhaar dans le cadre de l'obligation de connaître son client, et maintenant sous la forme d'un pool d'interfaces de programmation d'applications ouvertes appelé India Stack[113]. Les cas d'actions gouvernementales touchant à la liberté sur Internet sont également nombreux. WhatsApp est mis sous pression pour identifier et arrêter la diffusion massive de messages qui concernent souvent des *fake news* ou qui encouragent la violence : l'entreprise affirme que cela violerait sa promesse de cryptage. Quant à Facebook, qui compte 260 millions d'utilisateurs en Inde, il a supprimé en 2015 la plus grande quantité de contenu (sur l'ensemble de ses services) jamais supprimée dans le monde à la demande du gouvernement indien[114]. Paytm, le porte-monnaie électronique le plus populaire du pays, a également remis aux autorités des données sur une manifestation de violence publique[115].

[113] « FAQs - IndiaStack », *IndiaStack,* 2016, https://indiastack.org/faq/.

[114] Christina Medici Scolaro, « Facebook Blocks More Content Here than in Any Other Country », *CNBC,* 13 novembre 2015, https://www.cnbc.com/2015/11/13/facebook-blocks-more-content-here-than-any-other-country.html.

[115] Madhulika Srikumar, « This Isn't Just About Paytm – Laws on Government Access to Data Need to Change », *The Wire,* 28 mai 2018, https://thewire.in/law/paytm-data-theft-cobrapost-sting.

Vers le modèle numérique chinois

La voie politique prise par l'Inde est incertaine. Modi en personne a courtisé les plus grandes entreprises américaines lors d'une visite dans la Silicon Valley et a lancé un appel pour aider l'Inde à devenir une puissance Internet[116]. Sous l'influence de l'arrêt de la Cour suprême de 2017, la future loi sur la protection des données s'est résolument orientée vers une législation de type RGPD, la principale différence étant le manque de recours juridique pour les personnes physiques. Mais d'autres législations vont dans une tout autre direction, celle de la Chine, en privilégiant la sécurité nationale sur la libre circulation des données. Ce n'est pas complètement le cas en ce qui concerne la localisation des données : si les exigences sont proches de celles édictées par la Chine, il n'y a pas les restrictions strictes en matière de transfert transfrontalier des données qui sont en place dans le cas chinois. Mais le droit de l'État d'obtenir des données personnelles par le biais des opérateurs est presque aussi illimité qu'en Chine, et la responsabilité incombe explicitement aux intermédiaires (sociétés de télécommunication ou plateformes de réseaux sociaux).

Le projet de directive sur les intermédiaires illustre ce point. Il est fondé sur un précédent règlement datant de 2011, dont il conserve une large part, notamment sur le contenu qui « menace l'unité, l'intégrité, la défense, la sécurité ou la souveraineté de l'Inde, les relations amicales avec des États étrangers, l'ordre public, ou qui incite à la réalisation d'une infraction identifiable, qui empêche toute

[116] Vindu Goel, « Narendra Modi, Indian Premier, Courts Silicon Valley to Try to Ease Nation's Poverty », *The New York Times,* 27 septembre 2015, https://www.nytimes.com/2015/09/28/technology/narendra-modi-prime-minister-of-india-visits-silicon-valley.html?action=click&module=RelatedCoverage&pgtype=Article&region=Footer.

enquête sur une infraction ou qui insulte une autre nation »[117]. La santé publique, la sécurité et les infrastructures critiques ont été ajoutées à la liste. Ce projet est fortement soutenu par Mukesh Ambani, le propriétaire du géant des télécommunications Jio, alors que de grandes entreprises étrangères comme Microsoft et Google s'en plaignent. Microsoft, dont le directeur général Satya Nadella, né à Hyderabad, est une icône du monde des affaires en Inde, a déclaré que filtrer l'ensemble du contenu demandé par le gouvernement constituerait non seulement une violation de la vie privée et de la liberté d'expression, mais représenterait également un tel défi que « le coût de toute tentative de mise en conformité serait prohibitif »[118]. À l'origine, le projet de politique nationale en matière de commerce électronique prévoyait d'inclure la localisation des données de commerce électronique, une disposition qui n'a été supprimée qu'après les remarques du secteur. La décision d'inclure cette disposition dans le PDPB appartient désormais au ministère indien de l'Électronique et des Technologies de l'information (MeitY)[119].

[117] Ministry of Electronics and Information Technology, « Comments on the (Draft) Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018 », 24 décembre 2018, p. 2, https://meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122018.pdf.

[118] Vindu Goel, « India Proposes Chinese-Style Internet Censorship », *The New York Times,* 14 février 2019, https://www.nytimes.com/2019/02/14/technology/india-internet-censorship.html.

[119] Anandita Singh Mankotia, « MeitY May Not Include E-Commerce Data in Privacy Bill », *The Economic Times,* 29 août 2019, https://economictimes.indiatimes.com/news/economy/policy/meity-may-not-include-e-commerce-data-in-privacy-bill/articleshow/70884990.cms?from=mdr.

Les limites d'une comparaison entre l'UE et l'Inde

Les objections de la Commission européenne doivent être nuancées. Le projet de loi indien sur la protection des données est la loi d'une fédération jouissant d'une pleine souveraineté, ce qui n'est pas le cas de l'UE. Par conséquent, le RGPD n'aborde ni la sécurité nationale ni l'ordre public, mais il prévoit des exceptions dans de nombreux domaines « d'intérêt public ». Il est vrai que le RGPD a prévu des mécanismes de recours et d'examen élaborés au niveau de l'État, ou au niveau de l'UE dans les affaires impliquant plusieurs pays. Mais les domaines dans lesquels l'UE n'est pas compétente sont laissés de côté. Une fois ce constat effectué et les exemptions prévues dans le règlement européen prises en compte, le projet de loi indien sur la protection des données semble moins éloigné du RGPD.

Il n'en demeure pas moins que les droits conférés par le projet de PDPB au gouvernement sont exprimés dans des termes à la fois vagues et généraux, ce qui rend assez difficile le recours d'une personne physique à une action en réparation. L'accès du gouvernement aux données privées est largement autorisé par un arrêt de la Cour suprême de 1996[120] qui portait sur des écoutes téléphoniques. Il est même facilité par un système de contrôle surchargé malgré l'existence de procédures judiciaires appropriées[121].

Les différences les plus importantes sont ailleurs. Alors que l'Europe a une politique limitée de soutien aux entreprises numériques,

[120] Cour suprême de l'Inde, People's Union Of Civil Liberties ... vs Union Of India (Uoi) And ANR. (18 décembre 1996).

[121] Zubin Dash, « Do Our Wiretapping Laws Adequately Protect the Right to Privacy? », *Economic and Political Weekly* 53, n° 6, 28 novembre 2018, 7–8, https://www.epw.in/engage/article/can-government-continue-unhindered-wiretapping-without-flouting-right-privacy.

principalement par le biais de subventions, le gouvernement indien est proactif : les programmes Digital India, Startup India, Skill India et le fonds India Innovation répondent tous à cet objectif. L'Inde a pris exemple sur les politiques industrielles et technologiques de la Chine, ce qui se manifeste dans plusieurs domaines : les énormes facilités accordées à Mukesh Ambani, grand partisan de Narendra Modi lors de la création de Jio[122] ; une incitation à la numérisation des données dans de vastes secteurs du gouvernement, généralement à partir de la plateforme initiale Aadhaar. Ayant pour but de créer un système national d'identification, Aadhaar, qui est basé sur un scan de l'iris et des empreintes digitales, a franchi la barre du milliard d'utilisateurs enregistrés en avril 2016. Nandan Nilekani, le fondateur d'Infosys et premier président de l'UIDAI *(Unique Identification Authority of India)* a alors lancé à grand renfort de publicité une « opportunité de capitalisation boursière de 600 milliards de dollars » pour étendre son utilisation aux systèmes de paiement[123]. Le recours aux techniques biométriques est particulièrement agressif. Les nouveaux systèmes de paiement incluent des fonctions de reconnaissance du pouce : « votre pouce est votre banque », a expliqué le premier ministre.

Rappelons que la plupart des textes juridiques examinés dans le cas indien ne sont pas encore approuvés par le Parlement, lequel déterminera l'issue du régime indien de protection des données. La législation indienne est donc prise en étau entre les acteurs internationaux et nationaux du marché du Web, une constitution et

[122] Simon Mundy, « India: The Creation of a Mobile Phone Juggernaut », *Financial Times,* octobre 2018, https://www.ft.com/content/4297df22-bcfa-11e8-94b2-17176fbf93f5.

[123] Nandan Nilekani, « India Financial Sectors », *Crédit Suisse,* 29 juin 2016, https://research-doc.credit-suisse.com/docView?language=ENG&format=PDF&document_id=1062747711&source_id=emcsplus&serialid=Wm0zJuKszkmbCwRYV7h

ses juges qui se sont montrés protecteurs du droit à la vie privée, et un gouvernement qui envisage la question sous l'angle de la modernisation et l'efficacité de la gouvernance. Les questions de confidentialité et de contrôle souverain des données sont en première ligne face à la libre circulation des données. Il reste à voir dans quelle direction l'Inde choisira d'aller. L'indétermination du statut de l'Inde est bien décrite dans une étude comparative qui classe le pays comme proche des États de surveillance, tels que la Chine ou la Russie, mais note pourtant que la législation à venir pourrait renverser une bonne partie de la situation, si elle était effectivement mise en œuvre[124].

[124] Paul Bischoff, « Surveillance States: Which Countries Best Protect Privacy of Their Citizens? - Comparitech », *Comparitech.Com,* 15 octobre 2019, https://www.comparitech.com/blog/vpn-privacy/surveillance-states/.

V

LA CHINE, L'ÉTAT-SURVEILLANCE

Avec la Chine, nous entrons dans un tout autre monde. Il existe des points communs entre le contrôle gouvernemental chinois et certaines dispositions actuellement envisagées par le gouvernement Modi en Inde, mais aucune ressemblance avec un règlement de type RPGD, à l'exception de certaines figures de rhétorique. Le numéro un chinois, Xi Jinping, souligne régulièrement, avec des accents presque messianiques, l'importance de placer la Chine à l'avant-garde des développements numérique et de l'intelligence artificielle : elle « pourvoira à l'amélioration constante de la qualité de vie du peuple »[125]. Sous sa gouverne, plusieurs facteurs convergent pour produire les effets d'échelle les plus importants et les plus intégrés au monde. Cependant, la caractéristique la plus importante est antérieure au mandat de Xi : l'Internet chinois fonctionne dans la pratique comme un intranet. Il n'y a aucun opérateur étranger de télécommunications. Les données de la Chine vers la Chine ne quittent jamais le pays. Le trafic extérieur passe uniquement par quelques points de contrôle qui peuvent être fermés[126]. Incontestablement, cette situation est totalement différente du Web indien fortement intégré. La Russie s'est inspirée du modèle de pare-feu de la Chine[127].

[125] Xi Jinping, « Message de Xi Jinping au premier sommet de la construction numérique en Chine 满足人民日益增长的美好生活 », 22 mars 2018.

[126] Catalin Cimpanu, « Oracle: China's Internet Is Designed More like an Intranet », *ZDNet,* 30 juillet 2019, https://www.zdnet.com/article/oracle-chinas-internet-is-designed-more-like-an-intranet/.

[127] Andrew Roth, « Russia's Great Firewall: Is It Meant to Keep Information in – or Out? », *The Guardian,* 28 avril 2019, https://www.theguardian.com/technology/2019/apr/28/russia-great-firewall-sovereign-internet-bill-keeping-information-in-or-out.

La politique de long terme de l'État en faveur de toutes les industries numériques

A l'intérieur de cette sphère fermée, des programmes à long terme et des subventions colossales ont permis de créer une infrastructure de téléphonie mobile 4G : au dernier décompte, il existait 1,56 milliard d'abonnements de téléphonie mobile, soit plus d'un par personne[128]. Cette politique de développement domine également le trafic Internet, ce qui crée des possibilités d'utilisation partout et à tout moment. Le système rétrograde de paiement en espèces et le système bancaire étatique de la Chine ont été balayés par le plus grand système de paiement mobile au monde. En 2018, les plateformes de paiement mobile ont enregistré le chiffre stupéfiant de 60 milliards de transactions pour un montant revendiqué de 277 000 milliards de yuan, avec un taux de croissance explosif de 37 %[129]. En Chine, les paiements électroniques représentent déjà 25 % des échanges commerciaux, contre 11 % actuellement aux États-Unis. Le taux d'utilisation en Europe varie considérablement d'un État membre à l'autre. L'utilisation universelle des codes QR scannés, y compris pour donner de l'argent aux mendiants et utiliser du papier hygiénique dans les lieux publics, a également contribué à ce résultat. De plus, ces codes garantissent un enregistrement des données dans un format transférable unique. La concentration du secteur numérique en Chine est telle que deux opérateurs de télécommunications, China Mobile et China Unicom, dominent l'ensemble du marché de la téléphonie mobile, tandis que deux

[128] Yu Xiaoming, « Govt to Further Boost Advanced Manufacturing, Innovation and Competitiveness », *Chinadaily.com.cn,* 5 mars 2019, http://www.chinadaily.com.cn/a/201903/05/WS5c7e0b0fa3106c65c34ecdb1.html.

[129] Banque populaire de Chine, « Overall Situation of the Payment System in 2018 2018 年支付体系运行总体情况 », 20 mars 2019, p. 4, http://www.gov.cn/xinwen/2019-03/20/content_5375401.htm.

plateformes, Alipay et WeChat Pay, règnent sur 90 % du secteur des paiements mobiles.

Cette concentration est également importante dans tous les secteurs. Alibaba, qui compte parmi les dix plus grandes entreprises mondiales, n'est plus la plateforme de commerce électronique qui a fait sa réputation. C'est un écosystème de plateformes[130] composé de huit sociétés de commerce de gros et de détail (nationales et mondiales), cinq sociétés de médias et de divertissement, deux sociétés financières (520 millions de clients), dont Alipay et une plateforme de prêt aux petites et moyennes entreprises, une plateforme de navigation et de livraison ainsi qu'un moteur *life search* qui fournit des services de proximité pour la vie quotidienne (cinéma, restaurant,...), une plateforme logistique et une activité d'assurance santé en démarrage qui devrait tirer parti d'un très faible taux de pénétration de ce type de produit en Chine. Ainsi, Alibaba collecte en temps réel d'énormes quantités de données cédées indifféremment par les utilisateurs et les entreprises, données qui concernent la plupart de leurs activités quotidiennes. Son rival Tencent présente un taux de pénétration du marché similaire grâce à l'expansion horizontale de sa plateforme de messagerie WeChat, qui compte aussi entre 100 et 200 millions d'utilisateurs internationaux. Dans l'ensemble, le soutien de l'État chinois aux politiques Internet+ a grandement favorisé ceux que l'on appelle les « BAT » (Baidu, Alibaba et Tencent) en leur accordant, sur leur marché respectif, un quasi-monopole sur les données provenant des recherches sur le Web, des transactions en ligne et des médias sociaux. Cela va de pair avec une coopération très étroite avec les administrations publiques : une grande partie des données publiques est privatisée, mais le gouvernement dispose,

[130] Ming Zeng, « Everything Alibaba Does Differently — and Better », *Harvard Business Review,* 21 août 2018, https://hbr.org/2018/09/alibaba-and-the-future-of-business.

comme nous le verrons, d'un accès illimité à ces données. Il est intéressant de noter que les « BAT » sont en fait des sociétés holding basées aux îles Caïmans, qui dépendent des contrats avec leurs filiales basées en Chine pour toucher des dividendes.

Le problème de l'interdépendance technologique

Il ne faut pas considérer que le fait de posséder des *big data* signifie qu'elles sont utilisées de manière efficace, que ce soit en termes d'analyse ou de produits sur mesure. L'avancée réelle de la Chine dans le domaine de l'analyse est vivement contestée. Si certains experts comme Kaifu Lee[131] vantent les prouesses de la Chine alors qu'ils ont des intérêts personnels en jeu, des signes ponctuels indiquent que même les plus grandes plateformes peuvent dépendre de logiciels conçus en Amérique ou ailleurs. Alibaba, par exemple, a conclu un partenariat avec Salesforce, le leader américain des solutions de gestion de la relation client (*Customer Relationship Management* CRM), portant sur la fourniture de technologies basées sur le *cloud* à ses propres clients. L'entreprise a signé un partenariat similaire avec l'assureur européen AXA portant sur la fourniture de produits d'assurance sur mesure à ses clients e-commerce, aux PME chinoises ainsi qu'aux voyageurs utilisant Alipay en dehors de la Chine[132].

Cependant, l'exemple d'Alibaba, entreprise qui n'hésite pas à conclure des accords avec des concurrents potentiels sur son territoire et à

[131] Kai-Fu Lee, *AI Superpowers: China, Silicon Valley and the New World Order,* Boston: Houghton Mifflin Harcourt, 2018.

[132] AXA, « AXA, Alibaba et Ant Financial Services annoncent un partenariat stratégique mondial | AXA », *AXA.com,* 29 juillet 2016, https://www.axa.com/en/newsroom/press-releases/axa-alibaba-ant-financial-services-announce-global-strategic-partnership.

l'étranger, est à double tranchant. Alibaba se présente comme le « fournisseur exclusif » de Salesforce pour la Grande Chine, même si l'entreprise reconnaît la puissance des solutions CRM de Salesforce[133]. Elle a développé une application capable de « traiter le règlement d'un sinistre au titre de l'assurance automobile en quelques secondes tout en évaluant les dommages extérieurs du véhicule et en affichant les informations sur ces dommages aux utilisateurs, notamment où réparer le véhicule »[134]. Elle développe des applications de santé qui combinent des outils de diagnostic avec la recherche d'offres de prix pour remplir leurs ordonnances, des systèmes de paiement pour les patients des hôpitaux publics, qui permettent également à l'entreprise de proposer un deuxième avis médical ou de faire des propositions d'ordonnance, et enfin un outil de diagnostic et de paiement intégré. Elle fournit une technologie *blockchain* pour gérer les dossiers et ordonnances des patients au-delà des frontières provinciales[135].

Des oligopoles de données

Ce portrait met en évidence une différence majeure entre Alibaba ou d'autres géants numériques chinois et leurs concurrents internationaux : leurs activités, et donc leurs ressources de données, recoupent de nombreux secteurs. La question du transfert de données à des tiers, qui revêt une telle importance dans la conception des règles de confidentialité américaines, européennes ou indiennes, importe moins

[133] Tom Brennan, « Alibaba Now Exclusive Provider of Salesforce CRM in Greater China », *Alibaba Cloud Community,* 25 juillet 2019, https://www.alibabacloud.com/blog/alibaba-now-exclusive-provider-of-salesforce-crm-in-greater-china_595141.

[134] The Digital Insurer, « Alibaba - The Digital Insurer », *The Digital Insurer,* 10 novembre 2018, https://www.the-digital-insurer.com/cif-alibaba/.

[135] Michael O'Dwyer, « Alibaba - The Digital Insurer », *The Digital Insurer,* Non daté, https://www.the-digital-insurer.com/cif-alibaba/.

dans le cas chinois, où quelques plateformes constituent un oligopole de données. Néanmoins, comme nous allons le voir, ces plateformes ne négligent pas les recettes provenant de la revente à des tiers. WeChat, avec 1,1 milliard d'utilisateurs en Chine, 900 millions pour son système de paiement et 100 millions pour ses produits financiers, en est un autre exemple. Aucune plateforme non chinoise ne peut se targuer d'une telle omniprésence et d'un tel éventail de services. Il n'est pas surprenant que Mark Zuckerberg, le fondateur et principal actionnaire de Facebook, parle de passer d'un modèle fondé sur la publicité (avec de nombreux utilisateurs tiers ou consommateurs de données de l'entreprise), à d'autres services « comprenant les appels téléphoniques, les conversations vidéo, les groupes, les « stories », les entreprises, les paiements, le commerce et, à terme, une plateforme pour toutes sortes d'autres services privés »[136]. De la même manière, Google étend ses services de paiement et investit dans l'IA et les services de *cloud* dans le secteur de la santé.

Avant même d'aborder la question de la Chine sous l'angle de l'État de surveillance massive et de ses armes numériques, le fait est que ses plateformes techniquement privées agrègent plus de données personnelles que dans n'importe quelle autre pays. Alibaba, Tencent et Huawei sont les principaux acteurs de la construction d'une banque nationale de données intégrée pour le crédit social appliqué aux entreprises. La Chine ne se limite pas à ces plateformes. Une multitude de *start-up* s'y sont développées dans de nouveaux secteurs, celui de la reconnaissance faciale étant le plus connu. La question de la protection de la vie privée devrait être primordiale. Les grands chefs d'entreprise du secteur numérique ont des positions

[136] Li Yuan, « Mark Zuckerberg Wants Facebook to Emulate WeChat. Can It? », *The New York Times,* 7 mars 2019, https://www.nytimes.com/2019/03/07/technology/facebook-zuckerberg-wechat.html#click=https://t.co/q1vhufRaCi.

différentes à cet égard. Pour reprendre les propos de Jack Ma, le fondateur d'Alibaba : « l'Europe n'a pas de grande société Internet, parce qu'elle a beaucoup trop de systèmes juridiques (…) Internet n'en est encore qu'à ses débuts, et nous parlons déjà de la question de la protection de la vie privée et de la sécurité. Croyez-moi, nous serons capables de résoudre le problème, et si ce n'est pas le cas, nos enfants le feront »[137]. Pony Ma, le fondateur de Tencent, est plus prudent : « Les données ne peuvent pas être agrégées sans règles. Les données relatives à la communication, aux échanges sociaux et au comportement des consommateurs ne doivent pas être agrégées, car les conséquences seraient catastrophiques »[138]. Il a appelé à la mise en place de règles unifiées protégeant la confidentialité des données des internautes lors des deux sessions parlementaires chinoises de mars 2019[139].

La réglementation concerne avant tout la sécurité des données

Mais le débat général sur la vie privée est davantage axé sur la sécurité des données et le besoin général de réglementation que sur la protection de la vie privée. En tout état de cause, le contrôle est

[137] Sina.cn, « Ma Yu: The Combination of the Internet of Things and Big Data is the Future 马云：物联网和大数据的结合才是未来 », *Sina.cn,* 10 septembre 2017, https://tech.sina.cn/it/2017-09-10/detail-ifykuffc4789377.d.html?cre=tianyi&mod=wtech&loc=1&r=25&doct=0&rfunc=0&tj=none&tr=25&vt=4&pos=18.

[138] Zhang Chao, « Ma Huateng Answers : Tencent Does Not Dream. Social Exchange, Communication « Data Should Not Be Aggregated without Rules马化腾回应‘腾讯没有梦想’：社交、通信‘数据不能任意打通 », *Shidai Caijing,* 9 novembre 2018, https://tfcaijing.com/article/page/8a9eaf0566e21b6e0166f3e81bb11c44.

[139] Xinhua, « Ma Huateng: Collection of Private Information Through Big Data Should Not Be Too Complete 马化腾：大数据收集隐私信息不宜太全 », *Xinhuanet.com,* 4 mars 2017, http://www.xinhuanet.com//politics/2017-03/04/c_1120566998.htm.

dispersé entre des autorités multiples et différentes : le ministère de la Sécurité publique, la *State Administration for Market Regulation* (SAMR), la *Cyberspace Administration of China* (CAC) et au moins neuf autres entités gouvernementales sont impliquées dans des activités de réglementation nationales. Quelques experts réclament une approche globale de type RGPD afin de « mettre en place un service d'application de la loi unifié à guichet unique chargé de la protection des données personnelles »[140] tout en prévoyant des sanctions en cas de violations. Bien entendu, les experts et les sources officielles s'en donnent à cœur joie lorsqu'il s'agit de souligner les atteintes à la vie privée qui se produisent ailleurs. Dans un article sur le statut de la Chine en tant que puissance dans le domaine du *big data,* le *People's Daily* relève que les fuites de données à caractère personnel sont en augmentation à l'échelle internationale. Plus inquiétant encore, il note que 96,6 % des applications Android installées en Chine cherchent à accéder à des données personnelles et que 25,3 % d'entre elles ont un accès transfrontalier à ces données personnelles[141].

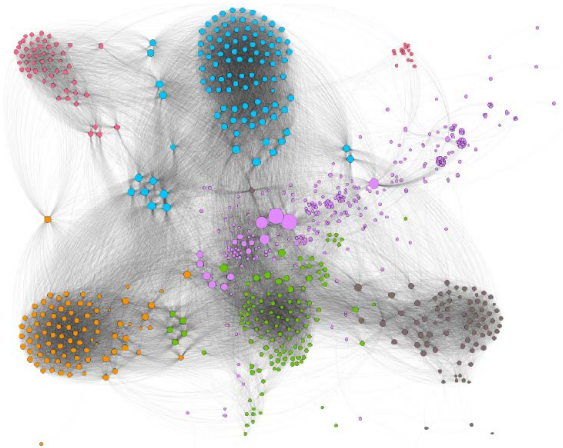
Des tiers se servent des oligopoles de données

Une étude détaillée, réalisée en coopération avec Microsoft et des chercheurs internationaux, approfondit cette question. Sur les principales plateformes chinoises donnant accès à des applications

[140] Cui Xiankang, Han Wei et Ren Qiuyu, « Proposed Guidelines Highlight China's Fragmented Protection of Online Privacy - Caixin Global », *Caixinglobal.com,* 9 mai 2019, https://www.caixinglobal.com/2019-05-09/proposed-guidelines-highlight-chinas-fragmented-protection-of-online-privacy-101413683.html.

[141] Liu Miao, « China's Big Data Is Not Only About 'Data Size' 中国大数据，不只‘数据大’ », *People's Daily Overseas* Edition, 9 juillet 2018, http://www.gov.cn/shuju/2018-07/09/content_5304898.htm.

tierces (Baidu, Tencent et Wandoujia), d'autres applications sont largement diffusées en arrière-plan sans que les utilisateurs ne se rendent compte qu'ils les ont utilisées auparavant. Chaque application lance en moyenne 76 autres applications. Sur un total de 800 applications fonctionnant sur 1 520 appareils (principalement des smartphones), 27,1 % de l'énergie est consommée par ces lancements non détectés. Ces applications forment des groupements comme le montre la figure ci-dessous pour Wandoujia :



Source: Mengwei Xu et al., "AppHolmes: Detecting and Characterizing App Collusion among Third-Party Android Markets," *Microsoft Research,* 3 avril 2017, p. 148, https://www.microsoft.com/en-us/research/publication/appholmes-detecting-characterizing-app-collusion-among-third-party-android-markets/.

Ces applications en arrière-plan requièrent souvent des autorisations sensibles mettant en danger les données personnelles. Ironiquement, une partie du problème réside dans le blocage du moteur de recherche Google sur l'internet chinois : les applications utilisent le service « push » sur Android (un autre produit de Google…) pour compenser cette lacune[142].

Selon une enquête réalisée par l'association des consommateurs chinois en 2018, 85,2 % des personnes interrogées ont subi une forme de fuite de données, mais un tiers d'entre elles ont décidé « d'accepter ce coup du sort »[143].

Les start-up en première ligne de la surveillance

Enfin, l'oligopole des BAT sur les données n'empêche pas la Chine de s'enorgueillir d'une scène vivante et bien soutenue pour les start-up. On peut certes soutenir que c'est aussi une bulle spéculative: 27 start-up se concentrent sur l'IA. Mais de nouveaux concurrents voient le jour. ByteDance est désormais la start-up la plus valorisée au monde. Elle possède TikTok (la version internationale de Douyin en Chine), une application de partage de vidéos en *lip-synching* extrêmement populaire auprès des enfants et des adolescents dans le monde entier, comme nous l'avons vu précédemment dans le chapitre sur l'Inde. Elle détourne une partie du trafic d'Alibaba et Tencent. C'est une bonne

[142] Mengwei Xu et al., « AppHolmes: Detecting and Characterizing App Collusion among Third-Party Android Markets », *Microsoft Research,* 3 avril 2017, https://www.microsoft.com/en-us/research/publication/appholmes-detecting-characterizing-app-collusion-among-third-party-android-markets/.

[143] Cqn.com.cn, « China Consumers Association released 'Investigation Report on the Personal Information Disclosure of Apps' 中消协发布《App个人信息泄露情况调查报告》 », *Cqn.com.cn*, 29 août 2018, http://www.cqn.com.cn/pp/content/2018-08/29/content_6213791.htm.

illustration de ce qui est en train de devenir le *splinternet*, c'est-à-dire un internet cloisonné. Ses politiques de confidentialité diffèrent en effet selon le marché. En revanche, certaines plateformes américaines ont annoncé qu'elles appliqueraient systématiquement les règles du RGPD, et pas seulement en Europe. Les utilisateurs européens relevant du RGPD, ainsi que les utilisateurs indiens, ont la possibilité d'accéder à leurs données à caractère personnel de TikTok s'ils le souhaitent. Ce n'était pas le cas aux États-Unis avant février 2019, et les données pouvaient être transférées vers des serveurs en Chine. En réalité, il n'y a rien d'inhabituel en ce qui concerne le transfert international de données, si ce n'est qu'il s'agit de données très personnelles collectées à l'âge le plus sensible, qu'elles permettent une identification personnelle et sont conservées *ad vitam æternam* en Chine[144].

Beaucoup d'autres entreprises en Chine développent des applications d'IA, qui fonctionnent par exemple par reconnaissance faciale et ont une multitude de fonctions de surveillance, pas seulement pour l'État. Hanwang, une entreprise créée en 2014, fournit des services de reconnaissance faciale et biométrique, de reconnaissance optique des humeurs ainsi que des services de surveillance de la qualité de l'air et des purificateurs d'air. Une de ses applications fonctionnant avec des caméras Hikvision propose aux écoles un « système de surveillance de classe » qui surveille l'attitude de chaque élève individuellement avant de lui attribuer une note hebdomadaire. C'est l'une des conséquences quotidiennes du plan de développement de l'intelligence artificielle nouvelle génération du gouvernement (NGAIDP). Ce plan vise à intégrer l'IA dans pratiquement tous les aspects de la vie, y compris la médecine, le droit, les transports, la protection de l'environnement et ce qu'il appelle

[144] David Carroll, « TikTok Might Be a Chinese Cambridge Analytica-Scale Privacy Threat », *Quartz,* 7 mai 2019, https://qz.com/1613020/tiktok-might-be-a-chinese-cambridge-analytica-scale-privacy-threat/.

une « éducation intelligente »[145]. L'omniprésence des caméras de surveillance, dont le nombre était estimé à 176 millions en 2017 et qui devrait atteindre 626 millions d'ici à 2020[146], constitue un grand avantage pour la collecte de données. Elles sont utilisées partout en Chine[147]. Ce n'est là que la conséquence sociétale dans la vie quotidienne d'une vision qui comprend la mise en œuvre sinistre de programmes d'intelligence artificielle et de reconnaissance faciale contre l'ensemble de la population du Xinjiang[148]. Dans un exemple exposé par inadvertance, l'un de ces systèmes recueillait chaque jour des informations individuelles détaillées sur 2,56 millions de personnes dans le Xinjiang, à l'aide de caméras de surveillance[149]. De manière fascinante, le Xinjiang a été désigné par le Ministère des Technologies de l'Information comme le centre de « projets pilotes » pour l'intégration du *big data* et l'intelligence artificielle en 2020[150].

[145] Xue Yujie, « Camera Above the Classroom », *Sixth Tone,* 26 mars 2019, https://www.sixthtone.com/news/1003759/camera-above-the-classroom.

[146] D'après des statistiques largement citées recueillies par Statista en 2017.
Source : Statista Research Department, « China: Surveillance Camera Installation 2017-2020 », *Statista,* 2019, https://www.statista.com/statistics/879198/china-number-of-installed-surveillance-cameras/.

[147] Pour divers exemples, voir : Julie Zaugg, « En Chine, la vie sous l'œil inquisiteur des caméras », *Les Échos,* 7 mars 2019, https://www.lesechos.fr/tech-medias/hightech/en-chine-la-vie-sous-loeil-des-cameras-997774.

[148] HRW, « China's Algorithms of Repression Reverse Engineering a Xinjiang Police Mass Surveillance App », *Humans Right Watch,* 1er mai 2019, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance.

[149] Catalin Cimpanu, « Chinese Company Leaves Muslim-Tracking Facial Recognition Database Exposed Online », *Zdnet.com,* 17 février 2019, https://www.zdnet.com/google-amp/article/chinese-company-leaves-muslim-tracking-facial-recognition-database-exposed-online/?__twitter_impression=true.

[150] Ministère de l'Industrie et des Technologies de l'Information de la Chine, « Notice of the Ministry of Industry and Information Technology of China, on Applying to the Big Data Pilot Project in 2020工业和信息化部办公厅关于组织开展2020年大数据产业发展试点示范项目申报工作的通知, » 6 novembre 2019, http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757022/c7517097/content.html, cité par *EastisRed* (Passe Muraille) n° 38, 18 novembre 2019, https://eastisred.fr/passe-muraille-n38-semaine-du-11-novembre/

Le crédit social chinois : une hydre plus grande que nature

Depuis 2014, aucune innovation en matière de contrôle n'a suscité autant de commentaires que le « système de crédit social » mis en place par la Chine[151]. Cela tient en partie au fait qu'il a été officiellement présenté en Chine comme un moyen d'accroître la confiance en appliquant un système de récompense et de sanctions. On fait rarement allusion en Chine au fait qu'il s'agit d'une imitation évidente des techniques de notation largement utilisées dans les économies de marché : aux États-Unis, par exemple, une cote de crédit est obligatoire non seulement pour obtenir une carte de crédit, un prêt ou une assurance, mais aussi pour louer un bien. Les incursions dans la vie privée ne sont pas seulement l'apanage de la Chine. Aux États-Unis, de gigantesques bases de données accessibles au public fournissent des renseignements sur tout le monde, y compris les contraventions de circulation, et permettent par exemple de localiser les délinquants sexuels connus dans votre quartier.

De plus, la Chine a une longue histoire en matière de surveillance collective : le système de surveillance des familles *(baojia)* à l'époque impériale était un système de surveillance mutuelle. Dans un contexte léniniste-maoïste, l'ensemble de la population a été classée dans une quarantaine de catégories, selon un mélange de critères d'origine de classe, de statut personnel et de comportement, du bon au mauvais, du rouge au noir. Le Parti communiste chinois a toujours eu un système de *dang'an* (dossiers contenant toutes sortes de renseignements cédés ou collectés) sur chacun de ses 90 millions de membres (en 2018).

[151] 社会信用体系 *(shehui xinyong tixi)*.

À l'inverse, à la base, là où l'État a toujours manqué de présence, la question de la confiance a toujours été primordiale. Par nécessité, la Chine était une société fondée sur les relations *(guanxi)* parce que c'était un moyen de surmonter la méfiance. En l'absence d'un système d'identification fiable à l'échelle de la nation, la pratique des noms multiples et des disparitions volontaires était également très fréquente.

Dans ce contexte, la cote de crédit social réinstaure la confiance sans avoir besoin de relations spéciales, ce qui est généralement bien accueilli par la population. Celle-ci apprécie l'ordre public et la discipline dans un contexte traditionnel d'individualisme et de manque de fiabilité.

La décision en 2014 de construire un système de crédit social d'ici à 2020 associe plusieurs expériences locales dans l'objectif global d'une « amélioration par le marché de l'ordre économique et social »[152]. La particularité de l'ordre politique chinois réside dans cette seule phrase : le marché sert l'ordre public, et il est donc difficile de distinguer les initiatives publiques et privées, et par exemple la notation du crédit à la consommation d'une catégorisation plus générale, avec des récompenses pour un bon comportement ou la punition pour un mauvais comportement dans d'autres domaines.

Pourtant, à ce stade, il n'est pas certain que tous les systèmes de crédit social, ni même la majorité d'entre eux seront intégrés dans

[152] Conseil d'Etat de la République populaire de Chine, « Significant Improvement in Economic and Social Order "Notice of the State Council on Printing and Distributing the Outline of the Construction of the Social Credit System (2014-2020) 经济社会秩序显著好转 "国务院关于印发社会信用体系建设规划纲要（2014—2020年）的通知" », *www.gov.cn*, 14 juin 2014, http://www.gov.cn/zhengce/content/2014-06/27/content_8913.htm

un système national unique. De nombreuses voix s'élèvent contre cela. De plus, classer, conserver et protéger les données représenterait un énorme exploit technologique, peut-être au-delà de tout besoin réel. Pour autant, les principaux systèmes existants sont à la fois impressionnants et inquiétants. Certaines initiatives locales ou pilotes sont effrayantes et présentent des défis plus importants pour la protection de la vie privée.

Un système crée par la banque centrale chinoise en 2015 avec huit entités, dont le Sesame Credit (développé par Ant Financial, une filiale d'Alibaba) et Tencent Credit Information Co., regroupe les données comportementales et des achats en ligne, d'organismes publics et de commerçants pour générer une notation instantanée des individus. Les notations comportent des critères de stabilité, le comportement du site Web et les fréquentations (relations sociales par exemple). En 2015, Sesame Credit a noté à elle seule 300 millions de personnes et 37 millions de petites entreprises[153]. Les données de cote de crédit sont utilisées par d'autres sociétés de notation, par exemple l'application de rencontre BaiHe pour évaluer un(e) partenaire. Un « jeu » permet à des amis de rivaliser pour leur cote de crédit. De nombreux systèmes de crédit social utilisent également des données provenant de ces grands systèmes nationaux.

Mais la montée en puissance ne s'arrête pas là. Un site web national et public, Credit China, agrège les données de 44 services centraux, 22 plateformes provinciales et 122 institutions sociales. Toutes sortes de données allant de la fiscalité à la protection

[153] Ant Financial, « Ant Financial Unveils China's First Credit-Scoring System Using Online Data », *Ant Financial,* 28 janvier 2015, https://www.alibabagroup.com/en/news/press_pdf/p150128.pdf.

de l'environnement, en passant par les aliments et les médicaments, sont partagées en même temps que les listes de personnes « noires » ou « rouges ». Pour lutter contre la « léthargie » bureaucratique consistant par exemple à ne pas tenir compte de ces données, les entreprises tierces peuvent y accéder moyennant paiement. Une entreprise, BaiHang Credit, a été créée avec une participation de 35 % de l'État – la *National Internet Finance Association of China* – et de 8 % pour chacune des entreprises pilotes, en principe privées, à l'origine du crédit social. On obtient ainsi à la fois une notation privée et un partage public-privé des données qui révèle une fois encore le caractère unique de la Chine.

La conséquence publique la plus connue de ce réseau intégré est la capacité, à partir des données disponibles auprès du Centre national de crédit public, de refuser certains services : fin 2018, 17,5 millions de voyages en avion et 5,5 millions de trajets en train ont été refusés. Selon le *People's Daily,* il existait également des listes noires pour les terrains de golf, les hôtels et appartements haut de gamme, les écoles privées et les produits financiers[154]. Dans un cas extrême, un tribunal de la province du Shandong a ordonné en 2017 aux compagnies de téléphone d'introduire des messages automatiques de mise en garde dans les appels reçus de personnes non fiables[155]. À l'autre extrémité du spectre, les bonnes notes de comportement social, récompensant notamment

[154] Xue Yuan, « The Release of 2018 Annual Report on the Credit Blacklist 2018年失信黑名单年度分析报告发布 », *www.gov.cn,* 19 février 2019, http://www.gov.cn/fuwu/2019-02/19/content_5366674.htm.

[155] BBC News in Chinese, « From Portfolio to Credit Score, Is China on the Way to an "Orwellian" Monitoring Society从档案袋到信用评分 中国是否正走向‘奥威尔式’监控社会 », *BBC News in Chinese,* 17 octobre 2018, https://www.bbc.com/zhongwen/simp/chinese-news-45886126.

les actions d'utilité sociale et la fiabilité générale, permettent d'obtenir des réductions sur de nombreux services. Cela peut aller jusqu'à un accès prioritaire aux hôpitaux. Les cotes de crédit social peuvent déterminer l'accès des citoyens aux services publics, à l'aide sociale, aux admissions scolaires, à l'emploi, aux promotions professionnelles et aux activités commerciales. Ces programmes concerneraient moins de 10 % de la population classée dans les catégories rouge ou noire. Mais la recette du maoïsme traditionnel a toujours été d'opposer de larges majorités à des minorités ciblées et de récompenser une minorité de « militants ». Le même système de récompense et de sanction est appliqué aux entreprises, qui sont également notées en fonction de leurs politiques « pour créer un environnement commercial et légal plus réglementaire, équitable, transparent et prévisible »[156]. Par exemple, un retard de paiement vous placera sur la liste noire, et l'entreprise et son représentant légal seront tous deux confrontés à des « obstacles ».

La diversité des expériences et des systèmes en place a suscité des débats sur leurs limites : le crédit social doit-il être fondé sur des critères juridiques explicites ou doit-il s'étendre à des jugements moraux définis en termes flous ? Le droit à l'oubli et, plus concrètement encore, la manière de rétablir son crédit, notamment en cas d'erreur, font l'objet de discussions. La question de la « propagation des rumeurs », souvent synonyme de critique des autorités, est également très répandue. Certains experts appellent

[156] Luo Pan, « Ministry of Commerce: The Construction of the Corporate Social Credit System Will Not Adopt the So-Called Suppression Measures商务部：企业社会信用体系建设不会采取所谓打压措施 », *Chinanews.com,* 29 août 2019, https://www.chinanews.com/gn/2019/08-29/8941547.shtml.

à une réglementation nationale du crédit social. Au printemps 2019, le système n'était plus qu'une « priorité de classe 3 » lors de la session de l'Assemblée Nationale Populaire, c'est-à-dire qu'il pourrait ne pas être unifié dans un avenir proche[157].

Un débat public réduit sur la protection de la vie privée

Compte tenu des politiques de « crédit social » mises en place à grande échelle dans toute la Chine, on peut considérer le cas du Xinjiang comme une expérience qui peut être dupliquée ailleurs. Mais il y a peu de débats publics en Chine sur ces aspects, et il n'y a pas non plus beaucoup d'experts qui écrivent sur des aspects plus larges du droit à la vie privée. Les débats existants concernent des affaires qui ont lieu ailleurs, généralement en Amérique ou dans des entreprises américaines. Nous avons déjà évoqué le cas d'Android. Les dirigeants de Huawei à l'étranger vantent à l'occasion les mérites du RGPD. C'est une composante de la communication de l'entreprise qui est totalement absente en Chine[158]. Une discussion sur la protection de la vie privée dans un magazine s'adressant aux consommateurs s'articule autour de Facebook et d'un expert de l'Université de Georgetown[159], une autre dans un journal scientifique

[157] Zhang Yuzhe et Han Wei, « In Depth: China's Burgeoning Social Credit System Stirs Controversy - Caixin Global », *Caixinglobal.com,* 1er avril 2019, https://www.caixinglobal.com/2019-04-01/in-depth-chinas-burgeoning-social-credit-system-stirs-controversy-101399430.html.

[158] Joy Tan, « Transparency and Privacy Go Hand in Hand », *Linkedin.com,* 25 novembre 2018, https://www.linkedin.com/pulse/transparency-privacy-go-hand-joy-tan/.

[159] « Facial Recognition, Privacy Protection and the Scientific Challenges, 刷脸，隐私保护与科技的博弈 », *Consumer Daily* 126 (Juillet 2015).

populaire tourne également autour de Facebook et de Deepmind[160]. Il semble que les publications en République populaire de Chine ne parviennent pas à trouver d'exemples tirés de leur propre industrie numérique et de ses pratiques.

Il existe toutefois une exception concernant la collecte de données à des fins commerciales. En 2017, une ONG de défense des consommateurs de la province du Jiangsu, soutenue par le gouvernement, a ouvert une enquête contre 27 applications « espionnes » qui récupèraient les données personnelles des consommateurs. Elle a ensuite engagé des poursuites contre Baidu, la seule entreprise parmi les 27 qui n'avait pas retiré cette fonctionnalité. L'affaire a été portée devant les tribunaux. Baidu a fait marche arrière et mis jour son application. L'ONG a ensuite retiré son action en justice[161]. Comme nous le verrons, il peut y avoir des tensions entre les organismes de réglementation et les entreprises commerciales.

Pourtant, il y a beaucoup plus de discussions pertinentes sur les données personnelles lorsque celle-ci s'inscrivent dans le contexte de la sécurité des données, qu'il soit question de fraude et de mauvais usage des données ou de sécurité nationale.

[160] Fang Lingsheng, « Identification Systems: The End of Personal Privacy 识别系统：个人隐私终结者 »,*World Science*, mars 2015, p. 30-37.

[161] Zhang Jie, « Consumer Rights Group Withdraws Complaint against Baidu », *Chinadaily.com.cn,* 15 mars 2018, http://www.chinadaily.com.cn/a/201803/15/WS5aaa1535a3106e7dcc141dda.html.

Cadre réglementaire de la Chine numérique

La réglementation chinoise de plus en plus importante en matière de cybersécurité et de protection des données constitue un cas d'application du triangle qui nous est devenu familier entre trois objectifs : l'efficacité, qui implique ici un développement plus rapide de l'IA et des applications de *big data* ; la protection des données personnelles, largement perçue en Chine comme empêchant l'utilisation abusive des données par des acteurs privés ; et la question prioritaire de la sécurité nationale, aspect le plus connu à l'étranger. Ces objectifs se retrouvent dans l'élaboration d'un dédale de règlements divers. Deux difficultés majeures limitent l'interprétation : il est difficile de hiérarchiser les lois, les règlements et les normes car une grande partie des directives « informelles » s'avèrent en réalité assez contraignantes. Et comme toujours avec les textes juridiques chinois, les ambiguïtés abondent et leur mise en œuvre est extrêmement variable.

Malgré tout, le corpus en cours d'élaboration est impressionnant. Après une série de mesures administratives prises en 2000 pour réguler l'Internet, la loi chinoise de 2017 sur la cybersécurité est devenue le texte de référence. Cette loi penche en faveur de « la garantie de la cybersécurité, la sauvegarde de la souveraineté dans le cyberespace, la sécurité nationale et l'intérêt public », même si elle concerne également les droits découlant de la loi pour les individus et les organisations. Elle oblige les opérateurs de réseau à apporter leur soutien à tous les organes de sécurité qui assurent la sécurité nationale et enquêtent sur les activités criminelles « conformément à la loi ». Elle demande également à tous les opérateurs de « contribuer volontairement » à la sécurité des « infrastructures critiques » au sens large : « services publics de

communication et d'information, électricité, trafic, ressources en eau, finances, service public, administration en ligne et autres ». L'inclusion du terme « autres » en tant que clause dérogatoire permettant toute extension est un phénomène très fréquent dans le droit public chinois, du Code pénal à ces règles relatives à la cybercriminalité. Leur but est essentiellement de laisser les autorités libres d'utiliser leur propre définition en fonction des circonstances. Les données « critiques », là encore définies de manière très générale et vague, doivent être conservées en Chine, une disposition qui a suscité des critiques de la part des entreprises et opérateurs étrangers en Chine. Les opérateurs doivent réussir des examens périodiques de sécurité. La loi oblige également tous les utilisateurs à indiquer leur véritable nom. Le gouvernement peut « prendre des mesures temporaires concernant les réseaux de communication dans une région spécialement désignée, comme la limitation des communications » : un *black-out* qui a été appliqué à divers reprises au Xinjiang.

La loi sur la cybersécurité et la protection des données personnelles

En principe, la loi protège les utilisateurs : les opérateurs de réseau « doivent strictement préserver la confidentialité des informations qu'ils collectent sur les utilisateurs » et les utilisateurs ont un droit conditionnel à l'effacement ou à la rectification de leurs données à caractère personnel si elles n'ont pas été collectées légalement ou si elles sont erronées. Elle définit les « informations personnelles »[162] comme « toutes sortes d'informations, enregistrées sous forme

[162] 个人信息 *(geren xinyi)*.

électronique ou par d'autres moyens, qui prises isolément ou conjointement avec d'autres informations sont suffisantes pour déterminer l'identité d'une personne physique, notamment les noms complets, dates de naissance, numéros d'identification nationaux, informations biométriques personnelles, adresses, numéros de téléphone, etc. de personnes physiques ».

En l'état actuel des choses, la loi chinoise sur la cybersécurité présente des caractéristiques communes avec le « projet indien de directives sur les intermédiaires » de 2018 : l'introduction de la notion de données « critiques », la mention ambigüe de dispositions « conformes à la loi ». En plus d'inclure des exceptions dans « d'autres » situations, elle limite au territoire chinois le stockage de toutes les données critiques. Les restrictions imposées par l'Inde ont une portée moins large. Toutefois, la possibilité de suspendre complètement les communications n'est plus une disposition propre à la Chine. Les services de données Internet mobile ont parfois été suspendus au Cachemire et dans d'autres parties de l'Inde en vertu de l'article 144 du Code pénal indien concernant les rassemblements illégaux.

Dans les termes définis par notre triangle, la loi chinoise de 2017 sur la cybersécurité est très orientée vers les droits de l'État, les obligations des opérateurs privés, laissant quelques droits conditionnels et génériques pour les personnes physiques.

Le dédale réglementaire en fabrication

Cette loi a été accompagnée ou suivie d'une série de lois, de règlements et de normes : on peut dénombrer à ce jour six systèmes dans différents domaines (la protection des données étant l'un d'eux) et plus de dix nouvelles « normes » : ils s'ajoutent aux 240 normes existantes établies depuis 2010 en matière de « technologie de sécurité de l'information »[163]. Dans notre domaine de référence, ils concernent les transferts transfrontaliers de données, les services de renseignements nationaux et le contre-espionnage. De nombreuses autres réglementations sectorielles existent et s'appliquent notamment à la finance, la banque, le commerce électronique et la protection des consommateurs. Le flou et les ambiguïtés abondent, y compris dans certains cas sur le fait de savoir si les règles sont obligatoires ou de simples directives. Cela s'explique aussi en partie par le système juridique particulier de la Chine, où les règles sont rédigées chemin faisant, puis éventuellement réécrites ou modifiées.

La plupart de ces règles vont dans le sens d'un contrôle accru de l'État. Les règles transfrontalières interdisent la copie externe de données dans de nombreux champs qui vont jusqu'aux habituelles « autres circonstances pouvant affecter la sécurité nationale ainsi que les intérêts sociétaux et publics ». Le projet de loi le plus récent sur les transferts transfrontaliers de données n'exige plus d'évaluation officielle pour les entreprises ayant plus de 1 000 gigas de données ou employant plus 500 000 personnes, mais il responsabilise davantage toutes les entreprises, qui doivent conserver leurs données numériques pendant cinq ans. L'évaluation des risques reste

[163] Elles sont gérées par le *China National Information Security Standards Technical Committee* (CNISSTC), et publiées exclusivement en chinois sur son site Web à l'adresse suivante https://www.tc260.org.cn/

également très générale et ouverte. Les médias, le commerce électronique, le paiement électronique, les moteurs de recherche, les courriels, les blogs, le *cloud computing*, les systèmes d'entreprise et le *big data* font désormais partie des infrastructures. L'article 7 de la loi chinoise de 2018 sur le renseignement national, largement cité dans le débat international sur Huawei, stipule que chaque « organisation ou citoyen doit soutenir, aider et coopérer au travail de renseignement national conformément à la loi et préserver la confidentialité du travail de renseignement national dont il ou elle a connaissance ». Sans surprise, les lois de contre-espionnage chinoises comportent des obligations similaires, mais la version de 2017 franchit deux étapes supplémentaires. Elle s'applique en effet aux personnes en Chine et à l'étranger, lorsqu'elles sont liées à l'espionnage, à des actes tels que « la fabrication ou la déformation de faits, la publication ou la diffusion de mots ou d'informations mettant en danger la sécurité de l'État, ou la fabrication, distribution ou publication de produits audiovisuels ou autres publications mettant en danger la sécurité de l'État ».

La spécification de 2018 sur la sécurité des informations personnelles : un tournant décisif

Pour les particuliers comme pour les entreprises, le nouveau règlement le plus important est celui de 2018 sur la technologie de sécurité de l'information, la *Personal Information Security Specification (PIS)* [164].Il convient de faire deux réserves importantes: en tant que

[164] National Information Security Standardization Technical Committee, « Information Security Technology – Personal Information Security Specification 信息安全技术个人信息安全规范 », *National Information Security Standardization Technical Committee,* 1er mai 2018, https://www.tc260.org.cn/upload/2018-01-24/1516799764389090333.pdf

« spécification » ou « norme » *(guifan)*, ce n'est pas une loi, mais elle est souvent considérée comme telle par les autorités. D'autre part, elle a déjà été modifiée et est constamment complétée par de nouvelles réglementations spécifiques[165], notamment par un nouveau projet de texte sur la gestion de la sécurité des données qui semble aller plus loin dans les obligations imposées aux entreprises en matière de protection des données à caractère personnel[166]. Cela étant, il est important de noter que la spécification PIS s'inspire largement du RGPD dans la forme, mais qu'elle diffère par certains aspects clés. Les rédacteurs de la spécification PIS ont extrait « l'essence » des documents disponibles (lignes directrices de l'OCDE sur la protection de la vie privée, lignes directrices de l'APEC (Coopération économique pour l'Asie-Pacifique) sur la protection de la vie privée, RGPD, norme ISO correspondante, lois américaines, etc.) et les ont adapté au cas de la Chine[167]. Mais ils ont aussi clairement indiqué que, depuis le début, ils visaient une réglementation certes plus stricte qu'aux États-Unis, mais pas autant qu'en Europe[168].

[165] Yan Luo, « China Releases Draft Amendments to the Personal Information Protection Standard », *Inside Privacy,* 11 février 2019, https://www.insideprivacy.com/international/china/china-releases-draft-amendments-to-the-personal-information-protection-standard/.

[166] Les projets de mesures ont été publiés sur le site Web de la CAS.
Source : CAC, « Notice of the National Internet Information Office on Public Consultation on the "Data Security Management Measures (Draft for Comment)" 国家互联网信息办公室关于《数据安全管理办法（征求意见稿）》公开征求意见的通知 », *Cac.gov.cn,* 28 mai 2019, http://www.cac.gov.cn/2019-05/28/c_1124546022.htm.

[167] Sina Technology, « The story behind the issuing of 'Personal Information Security Specification' compromises of 33 experts made the Standard Possible《个人信息安全规范》出台记：33专家博弈炼就标准 », *Sina.com.cn,* 1er mai 2018, http://tech.sina.com.cn/i/2018-05-01/doc-ifzvpatr7140886.shtml.

[168] *Ibid.*

Les similitudes ont été décrites par un observateur externe[169], tandis que les divergences sont expliquées par l'un des experts ayant contribué à la rédaction du texte[170]. La spécification PIS détaille les obligations en matière de consentement de l'utilisateur, à commencer par la minimisation de la collecte de données et de leur utilisation secondaire, et impose des exigences sécuritaires aux opérateurs tiers. Elle crée une catégorie d'informations personnelles « sensibles », comprenant notamment les « numéros de carte d'identité, informations biométriques, numéros de compte bancaire, enregistrement et contenus des communications, informations sur les biens, informations de crédit, données de localisation, informations relatives au logement, données de santé et données physiologiques, données de transactions et informations personnelles (PI) sur les enfants âgés de 14 ans et moins », et exige leur anonymisation. Cette disposition, l'obligation pour les entreprises qui traitent de grandes quantités de données personnelles de nommer des délégués à la protection des données et la mise en place de sanctions ont amené certains à conclure que la spécification PIS s'inscrit dans la lignée du RGPD.

Bien que le « consentement » ne soit que l'un des six motifs légitimes du traitement licite des données dans l'article 6.1 du RGPD, l'article 41 de la loi chinoise sur la cybersécurité impose ce « consentement », mais prévoit une liste d'exceptions dans la spécification PIS. Les articles 5.4 et 8.5 énumèrent des exemptions relatives à la sécurité et à la défense nationales, à la sécurité publique, à la santé publique et aux intérêts publics importants, aux enquêtes criminelles, aux

[169] Samm Sacks, « China's Emerging Data Privacy System and GDPR », *Csis.org,* 9 mars 2018, https://www.csis.org/analysis/chinas-emerging-data-privacy-system-and-gdpr.

[170] Hong Yanqing, « Answers and explanations on five points regarding the Personal Information Security Certification 对《个人信息安全规范》五大重点关切的回应和解释 », *WeChat,* 5 février 2018, https://mp.weixin.qq.com/s/rSW-Ayu6zNXw87itYHcPYA.

poursuites pénales, aux procès criminels et à l'exécution d'un jugement, etc. ; la protection des principaux droits et intérêts légitimes, tels que la vie et les biens des personnes concernées ou d'autres personnes, et s'il est difficile d'obtenir le consentement de la personne concernée ; lorsque cela s'avère nécessaire pour maintenir le fonctionnement sûr et stable des produits ou des services fournis, par exemple pour détecter et traiter les dysfonctionnements des produits ou services ; lorsque cela s'avère nécessaire pour que le responsable du traitement, en tant qu'agence de presse, fasse des bulletins d'informations légaux ; lorsque cela s'avère nécessaire pour que le responsable du traitement, en tant qu'institut de recherche universitaire, effectue des recherches statistiques ou universitaires dans l'intérêt public, qu'il a également anonymisé les informations personnelles lorsqu'il communique ses recherches universitaires ou donne des résultats à l'extérieur ; et enfin « dans d'autres situations prévues par les lois et réglementations ». Détaillée et très large, cette liste d'exceptions de la réglementation chinoise semble pourtant laisser moins de marge de manœuvre que le RGPD. Une liste d'exceptions peut-elle rivaliser avec la flexibilité globale donnée par ce que l'on appelle les « intérêts légitimes » dans l'article 6.1 du RGPD ?

Le *Big State* en tant qu'arbitre entre particuliers et entreprises

Hong Yanqing prend le temps d'expliquer pourquoi c'est pourtant le cas, et comment la spécification PIS dispense du consentement des utilisateurs dans bien des situations. Pour le RGPD, la justification des « intérêts légitimes » impose aux entreprises de suivre chaque étape de sa procédure interne et d'être prêtes, en cas de demande,

à fournir la preuve de leurs « intérêts légitimes », ce qui rend les entreprises plus responsables. Hong décrit une exigence en matière de consentement beaucoup plus souple dans la spécification PIS que dans le RGPD[171]. La norme exige un consentement explicite lorsqu'il s'agit d'informations personnelles sensibles, mais seulement un consentement autorisé, un terme qui n'a pas été défini dans la norme, dans le cas des autres informations personnelles. Hong explique ensuite qu'en « utilisant le terme de « consentement autorisé », je veux dire que vous êtes encouragé à adopter le consentement explicite, mais si cela n'est pas réalisable, un consentement implicite peut suffire »[172]. La réglementation chinoise, souple et évolutive, est souvent expliquée par le contexte de l'exigence d'innovation et de l'efficacité économique. Une réglementation stricte sur les données à caractère personnel comme le RGPD ne conviendrait pas à la Chine compte tenu de sa capacité à protéger les données à caractère personnel et de la situation actuelle du secteur des données en termes de développement[173]. L'efficacité et l'intérêt des entreprises ont été pris en compte dans la spécification PIS, car l'équipe qui l'a rédigée était composée de 33 personnes, que l'on peut diviser en deux camps : les entreprises et les experts.

Le débat à ce sujet a été suffisamment important pour que la révision de 2019 de la loi sur la cybersécurité (actuellement en phase de

[171] Sina Technology, « The story behind the issuing of 'Personal Information Security Specification' compromises of 33 experts made the Standard Possible 《个人信息安全规范》出台记：33专家博弈炼就标准 », *Sina.com.cn*, 1er mai 2018, http://tech.sina.com.cn/i/2018-05-01/doc-ifzvpatr7140886.shtml.

[172] 洪延青, « Answers and explanations on five points regarding the Personal Information Security Certification 对《个人信息安全规范》五大重点关切的回应和解释 », *WeChat,* 5 février 2018, https://mp.weixin.qq.com/s/rSW-Ayu6zNXw87itYHcPYA.

[173] Hu Wenhua et Kong Huafeng, « The Impact of EU General Data Protection Regulation on China and Its Response », *Computer Applications and Software* 35, n° 11, novembre 2018.

commentaires) aille dans deux directions : ajouter une exemption « lorsqu'elle est liée à l'obligation des responsables du traitement des données personnelles d'appliquer les lois et règlements » de l'État ; mais supprimer l'exemption de consentement « lorsque cela s'avère nécessaire pour signer et exécuter un contrat conformément à la demande de la personne concernée ». Hors ces situations, les obligations des entreprises se trouvent renforcées en matière de protection des données. En d'autres termes, dans notre triangle cité plus haut, le troisième point, à savoir les intérêts ultimes de l'État dans la collecte de données à grande échelle, est une fois de plus le grand gagnant. Mais la protection des données à caractère personnel l'emporte parfois aux dépens des entreprises qui sont chargées de sa mise en œuvre. L'État chinois peut admettre de protéger les personnes physiques en tant que consommateurs contre les intérêts commerciaux prédateurs, bien qu'il ne le fasse pas contre lui-même.

On ne peut terminer cette tentative de description sans livrer deux conclusions provisoires. Premièrement, pas grand-chose ne contraint le Léviathan, c'est-à-dire l'État-surveillance. Deuxièmement, une abondance de règles, souvent modifiées, complétées ou réécrites, coexiste avec des ambiguïtés persistantes à plusieurs niveaux : la distinction entre règles impératives et orientations suggérées est ténue. La loi peut donc être appliquée de manière restrictive, ou tout aussi bien s'étendre arbitrairement à d'« autres » catégories. L'absence de dispositions concernant les moyens de mise en œuvre suggère que la loi sert principalement à titre dissuasif. L'obligation pour les entreprises qui traitent beaucoup de données à caractère personnel d'employer des délégués à la protection des données a même été réduite : dans la loi de 2017 sur la cybersécurité, le seuil pour cette obligation était de 500 000 personnes concernées. Il est passé à

un million dans le projet de révision de 2019. Bien que le RGPD et la réglementation naissante de l'Inde aient leurs limites, aucun des deux n'approche de la conjonction de trous noirs et du dédale réglementaire dans le cas chinois.

VI

FOCUS : LA CONFIDENTIALITÉ DES DONNÉES DE SANTÉ

Le traitement des données numériques, les analyses de *big data* et maintenant l'intelligence artificielle sont autant d'éléments qui présentent un potentiel énorme pour améliorer les soins de santé. Les outils de diagnostic rapide, les outils prédictifs, les appareils portables, l'interprétation des images, le *machine learning*, la télémédecine et l'analyse des facteurs génétiques ou comportementaux sont des technologies très prometteuses pour ce secteur. Cette révolution est aussi fondamentale que la découverte des vaccins ou des antibiotiques en leur temps. Cependant, il ne faut pas sous-estimer l'investissement et la réorganisation des données existantes qui seront nécessaires pour tenir ces promesses : un acteur clef comme Deepmind, avec sa division santé à la pointe de la recherche (aujourd'hui intégrée à Google Health), enregistre d'importants déficits. Les *big data* liées à la santé représentaient 153 exaoctets en 2013. Elles devraient atteindre 2 314 exaoctets d'ici à 2020[174]. Parmi les applications récentes, on peut citer la détection et le diagnostic de tumeurs du poumon, le scanner oculaire et le glaucome, les lésions rénales aiguës, mais également les corrélations statistiques effectuées à partir de bases de données volumineuses, par exemple le lien entre la consommation d'alcool et l'apparition de la maladie d'Alzheimer. Les dossiers médicaux électroniques (DME) font gagner du temps et donc aussi de l'argent. Mais pour cela, les professionnels

[174] Research and Markets, « Global Big Data in Healthcare Market: Analysis and Forecast, 2017-2025 (Focus on Components and Services, Applications, Competitive Landscape and Country Analysis) », *Researchandmarkets.Com,* mars 2018, https://www.researchandmarkets.com/research/wbhh4n/11_45_bn_big?w=5.

de santé doivent disposer d'outils simples qui leur permettent de saisir les données requises : l'ergonomie est souvent oubliée, surtout dans les systèmes publics décentralisés. Il est frappant de constater que les innovations numériques révolutionnent à la fois la recherche médicale avancée et la prévention des maladies, mais aussi la médecine de terrain.

La mise en œuvre du *big data* et de l'IA comporte également son lot de menaces : les aspects prédictifs peuvent avoir des applications redoutables pour l'assurance maladie et l'assurance-vie, et plus généralement pour la confidentialité de l'état de santé d'une personne. Alors que l'assurance et le crédit financier reposaient sur la mise en commun des risques, la mise à disposition de données médicales et d'outils prédictifs, au-delà des questionnaires de santé déjà répandus, pourrait individualiser les profils de risque au point où l'assurance en perdrait tout son sens. Les données de santé ne sont utiles que si elles peuvent être partagées entre les professionnels de santé concernés, les chercheurs en médecine, mais aussi, par nécessité, avec les organismes d'assurance publics ou privés qui prennent en charge les coûts des traitements médicaux. Les risques de piratage informatique et autres failles de sécurité sont importants, surtout en cas de stockage décentralisé des données. En raison du manque d'informations accessibles au public et de la crainte que les données soient divulguées aux banques, aux assurances, aux employeurs et même aux proches, les patients sont parfois réticents à l'idée de transmettre leurs données. Les premiers concernés sont les sites en ligne d'informations médicales d'ordre général, car ils sont souvent les premiers à vendre les données de leurs visiteurs et à refuser la mise en place d'un processus de notification et de

consentement facile[175]. Dans ce qui est un cas classique de bataille entre l'épée et le bouclier, les nombreuses limites des techniques d'anonymisation et de pseudonymisation ont déjà été mentionnées[176]. Cela amène également à chercher une nouvelle solution, sous la forme de données simulées, dont il sera question dans la section suivante.

Pour le RGPD, les données de santé relèvent de la clause d'intérêt public

De quelle manière nos cas d'étude, à savoir l'Europe, l'Inde et la Chine, abordent-ils la réglementation des données relatives à la santé et les questions de respect de la vie privée ? Comme nous le verrons, beaucoup de choses sont encore en gestation. La santé est peut-être le secteur numérique par excellence pour lequel des règles spécifiques sont nécessaires, et où différents objectifs doivent être conciliés : protection des données personnelles sensibles, recherche médicale, amélioration des prestations de soins de santé et exigences financières en période d'envolée des coûts médicaux.

Pour l'UE, l'approche du RGPD est très générique, même si son article 9 reconnaît la santé comme une catégorie particulière de données à caractère personnel. Il inclut les « données à caractère personnel relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne »

[175] Martin Untersinger, « Données personnelles : les mauvaises pratiques des sites de santé », *Le Monde.fr,* 4 septembre 2019, https://www.lemonde.fr/economie/article/2019/09/04/donnees-personnelles-les-mauvaises-pratiques-des-sites-de-sante_5506226_3234.html.

[176] Cf. page 43.

(article 4). Les États membres peuvent imposer de nouvelles limites au traitement des « données génétiques, des données biométriques ou des données concernant la santé ». Mais les données de santé illustrent parfaitement le cas où le traitement « pour des motifs d'intérêt public » est autorisé sans le consentement de la personne concernée (considérant 54), à l'exclusion d'autres finalités pour des tiers, tels que les employeurs ou les compagnies d'assurance et les banques. Cette exemption de consentement pour des raisons d'intérêt public ou légitime est très large : elle couvre l'état de santé, y compris la morbidité, le handicap et leurs déterminants, les besoins en matière de soins de santé, les ressources consacrées aux soins de santé, la fourniture de soins de santé, les dépenses de santé et leur financement, ainsi que les causes de mortalité. Cette exemption couvre également le droit à l'effacement.

Toutefois, les assurances publiques et privées sont traitées différemment : le traitement est autorisé « pour assurer la qualité et l'efficience des procédures de règlement des demandes de prestations et de services dans le régime d'assurance-maladie » (considérant 52), même sans consentement (considérant 54). Mais de tels traitements de données concernant la santé « ne devraient pas aboutir à ce que des données à caractère personnel soient traitées à d'autres fins par des tiers, tels que des employeurs ou les compagnies d'assurance et les banques ». Il est intéressant de noter que l'efficience est reconnue comme une nécessité pour les systèmes de santé publics, mais aucun cas particulier ne semble être prévu pour une assurance maladie privée dans le contexte plus large des entreprises privées. Fait intéressant, des chercheurs chinois ont examiné l'impact financier du RGPD pour les hôpitaux, entre son adoption en 2016 et les premiers mois de sa mise en œuvre en 2018. L'étude met l'accent sur les coûts de mise en conformité,

mais relève également l'écart grandissant entre les hôpitaux qui sont en mesure de fournir des services de santé numériques (considérés comme plus efficients) et ceux qui ne disposent pas des ressources financières et humaines suffisantes. Elle conclut qu'à plus long terme, seuls les premiers survivront dans un environnement ouvert. La conformité est donc un moyen d'atteindre un meilleur niveau de performance[177].

Plutôt générique sur la protection des données de santé, le RGPD laisse une grande marge de manœuvre aux États membres pour décider de leurs propres règles, parce qu'ils relèvent de la catégorie exemptée de « l'intérêt public ». Cependant, en légiférant sur ces catégories exemptées, les États membres sont autorisés à aller au-delà du champ d'application du RGPD, et non en deçà. Le rapport multipartite de la Commission européenne évaluant la première année d'application du RGPD note à plusieurs reprises que des interprétations ou règles nationales différentes posent encore problème dans le secteur de la santé. Pour les assurances, les règles de dispense du consentement explicite varient d'un pays à l'autre. Les entreprises pharmaceutiques notent que l'interprétation des garanties nécessaires au traitement des données de recherche peut encore varier d'un pays à l'autre. Dans le domaine de la santé, « l'application des clauses spécifiques du RGPD par les États membres a créé des obstacles considérables pour les entreprises ayant des activités transfrontalières »[178].

[177] Bocong Yuan et Jiannan Li, « The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation », *International Journal of Environmental Research and Public Health* 16, n° 6, 25 mars 2019 : 1070, https://doi.org/10.3390/ijerph16061070.

[178] Multistakeholder Expert Group, « Contribution from the Multistakeholder Expert Group to the Stock-Taking Exercise of June 2019 on One Year of GDPF Application », *Commission européenne,* 13 juin 2019, p.22, https://ec.europa.eu/commission/sites/beta-political/files/report_from_multistakeholder_expert_group_on_gdpr_application.pdf.

La France comme étude de cas

Il est intéressant d'examiner le cas de la France, parce que celui-ci combine des traits contradictoires. Depuis 1945 et la création d'un système national d'assurance (qui est également un organisme de contrôle et un acheteur public de médicaments, de matériels et d'équipements médicaux), il existe un suivi et un enregistrement quasi universels des actes médicaux et des dépenses liées à la santé. Le système national d'information inter-régimes unique (SNIIRAM), une base de données des demandes de remboursement et des remboursements pseudonymisés, a été créé en 1999 et réorganisé en un système national des données de santé (SNDS) encore plus vaste en 2017. Il regroupe plusieurs autres bases de données des hôpitaux sur les causes de décès. Ce système est souvent considéré comme unique par les sources françaises, en raison de sa portée dans le temps et de son caractère inclusif. En réalité, il est loin d'être unique aujourd'hui, car l'agrégation des ressources de données de santé, leur numérisation et leur traitement homogène se répandent dans tous les pays. Dans les faits, les restrictions d'utilisation mises en place par la loi française, les silos de données dans les différentes institutions et les contraintes d'utilisation risquent de placer la France, et plus particulièrement la recherche médicale et pharmaceutique, dans une position désavantageuse. Cependant, les banques de données existantes ont également attiré l'attention de l'organisme de contrôle français responsable du RGPD sur les atteintes involontaires à la vie privée : la pseudonymisation insuffisante et la faible protection des terminaux locaux ont été critiquées.

La première loi « Informatique et Libertés » (1978) interdisait le traitement des données de santé (sans les définir) avec d'importantes exceptions : les traitements de données nécessaires à la médecine

préventive, au diagnostic médical, à la fourniture de soins ou de traitements ou à la gestion des services de santé assurés par un membre d'une profession médicale ; les traitements statistiques effectués par l'Institut national de la statistique et des études économiques (INSEE) ; les traitements de données nécessaires à la recherche médicale. La loi française relative à la protection des données personnelles (2018) limite le traitement des données biométriques, génétiques et de santé à des fins d'intérêt public. Une ordonnance publique de décembre 2018 donne une définition plus détaillée des limites au traitement des données personnelles (y compris les données de santé et autres données sensibles, telles que la religion ou l'orientation sexuelle). Mais elle introduit également des exceptions extrêmement larges. L'article 5 de l'ordonnance énumère six cas pouvant faire l'objet d'une exception, dont l'un comprend « les traitements effectués par les autorités publiques dans l'exécution de leurs missions, si le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant ». Un législateur chinois n'aurait pas pu l'écrire de façon plus alambiquée et ambiguë.

Le système souffre de carences bien connues, qui concernent en partie le processus mais aussi les limitations dues à sa finalité. Comme les données ont été collectées à des fins de remboursement, leur contenu médical se limite souvent à de brèves catégorisations. À l'instar d'autres pays, les informations médicales réelles sont à la fois cloisonnées et souvent conservées sous une forme non numérique ou sous une forme numérique non normalisée. Rendre ces données interopérables, au-delà de l'échange individuel de données médicales

concernant des personnes isolées, est une tâche énorme. La généralisation des dossiers médicaux partagés (DMP) individuels et la création d'un service de *cloud* hébergeant ces données extrêmement sensibles est une étape dans cette direction. Pour le moment, le DMP est davantage un fichier d'information qu'un format de données unique, ce qui limite son utilisation plus large. Aujourd'hui, 6 millions de personnes sont enregistrées dans le système national de dossiers médicaux partagés ; or le système des hôpitaux parisiens compte à lui seul 10 millions de patients, un écart qui montre combien il est difficile de combiner les informations dans une banque de données unique ou coordonnée[179]. Selon toute vraisemblance, la mise en place d'un hébergement unique devrait conduire à la normalisation du format à l'avenir. En cas d'épidémie, cette normalisation permettra d'intervenir plus rapidement. Il est frappant de constater qu'à l'heure actuelle, Amazon ou Google sont en mesure de cartographier les épidémies de grippe plus rapidement et plus précisément que n'importe quel service de médecine ou d'épidémiologie, en se référant aux recherches ou commandes de médicaments en vente libre[180].

Une autre difficulté tient aux conditions d'accès à ces données, lesquelles varient selon qu'il s'agit de professionnels de santé ou de sociétés commerciales, médicales ou d'assurance. Cette restriction semble bienvenue. Mais pour tous, il est actuellement nécessaire de justifier l'accès par une finalité unique et clairement définie : or, cela va à l'encontre de l'objectif d'identification des facteurs par le biais de l'IA, un processus qui s'apparente davantage à une pêche aux indices dont on ne peut connaître à l'avance les résultats.

[179] Solveig Godeluck, « Les hôpitaux de Paris ont ouvert près de 10 millions de dossiers patients », *Les Échos,* 28 octobre 2019.

[180] Ali Alessa et Miad Faezipour, « A Review of Influenza Detection and Prediction through Social Networking Sites », *Theoretical Biology and Medical Modelling* 15, n° 1, 1er février 2018, https://doi.org/10.1186/s12976-017-0074-5

L'exigence d'une finalité unique et précise découle de la réticence culturelle à transmettre ses données vitales. Le *privacy paradox* fonctionne très bien pour dissiper cette réticence dans la vie quotidienne des consommateurs. Mais dans le cas des données de santé, où il est plus difficile pour la personne qui livre ses données privées de comprendre le retour immédiat et à court terme, ce paradoxe est moins efficace. Une meilleure information sur l'utilisation des données pourrait venir à bout de ce préjugé. Il est clair qu'il faut rassurer et informer.

À l'heure actuelle, les entreprises pharmaceutiques françaises se plaignent, non sans raison, d'être obligées de se tourner vers d'autres bases de données. Les États-Unis disposent d'énormes ressources de données de santé, ce qui donne lieu à ce que l'on pourrait appeler une course aux armements entre les nouvelles lois locales sur la protection de la vie privée et les entreprises de marketing. Predilytics, du groupe Welltok, affirme être en mesure de « révéler le risque avec un impact au niveau individuel »[181] pour 274 millions de personnes enregistrées. Kaiser Permanente est à la fois l'assureur et le fournisseur de soins de santé de 12 millions de personnes. Elle agrège ses données en conséquence[182]. LiveRamp, la société qui a succédé à Acxiom[183] et que nous avons déjà mentionnée, s'associe à HealthVerity pour « relier les données de santé des patients et leur comportement numérique ». « Les points de contact tout au long du parcours du patient peuvent être reliés entre eux, depuis les impressions de la campagne publicitaire et les consultations du site de la marque

[181] Welltok, « Analytic Services - Welltok - Optimizing Health, Maximizing Rewards », *Welltok,* 2019, https://www.welltok.com/analytic_services/.

[182] Kaiser Permanente, « Kaiser Permanente 2018 Annual Report », *Kaiserpermanente.org,* 2018, https://healthy.kaiserpermanente.org/static/health/annual_reports/kp_annualreport_2018/?kp_shortcut_referrer=kp.org/annualreport.

[183] Voir Introduction, p. 11.

jusqu'aux visites chez le médecin et le contenu des ordonnances »[184]. Très prochainement, grâce à un partenariat avec « la plus grande chaîne de supermarchés des États-Unis », on pourra également « relier les chariots de courses des patients à leurs données de soins de santé et explorer l'impact réel de leur régime alimentaire, de leur consommation de tabac et d'alcool, de leurs achats de produits en vente libre ou même de l'insécurité alimentaire sur leur parcours »[185]. Stimuler la publicité numérique des sociétés du secteur de la santé et du secteur pharmaceutique reste un objectif prioritaire de l'entreprise, car le secteur ne représente actuellement « que 2,8 % des dépenses totales de publicité numérique aux États-Unis ».

La Chine est également attractive. Elle a rejoint en 2017 un organisme international qui définit des spécifications de qualité. Elle a facilité l'accès des sociétés étrangères aux bases de données locales. Les projets de *big data* et de recherche dans le domaine de la santé se multiplient. Sanofi, par exemple, mène des essais sur le diabète et les maladies immunologiques à Chengdu[186]. Mais la délocalisation des sources de données de santé n'est pas la panacée. Les données vitales et autres données de santé varient d'une population à l'autre. L'autorisation de mise sur le marché d'un nouveau médicament à des fins commerciales ne peut pas être fondée sur des essais effectués

[184] HealthVerity, « HealthVerity and LiveRamp Develop Privacy-Centric Linkage between Patient Healthcare Data and Digital Behavior », *Prnewswire.com,* 15 octobre 2019, https://www.prnewswire.com/news-releases/healthverity-and-liveramp-develop-privacy-centric-linkage-between-patient-healthcare-data-and-digital-behavior-300938656.html.

[185] HealthVerity, « Grocery Data: The Missing Ingredient in The Patient Journey », *Healthverity.com*, 15 octobre 2019, https://info.healthverity.com/healthverity-8451-webinar.

[186] Takada Noriyuki, « China's Big Data Draws Big Pharma », *Nikkei Asian Review,* 1er août 2019, https://asia.nikkei.com/Business/Pharmaceuticals/China-s-big-data-draws-Big-Pharma2.

dans un autre pays sur une population différente. Pour cette seule raison médicale et pour des raisons de concurrence internationale entre sociétés pharmaceutiques et prestataires de soins de santé, y compris sur les outils d'analyse, la France devrait continuer à faciliter l'accès à et l'utilisation de ses grandes bases de données de santé, tout en se protégeant des excès mentionnés ci-dessus.

La législation exigeante de l'Inde en cours de préparation

Actuellement, le cadre juridique indien régissant les données de santé numériques se résume à une référence dans la section relative aux données personnelles de la loi de 2000 sur les technologies de l'information. Elle impose la protection des données sensibles et empêche toute divulgation illicite. Toutefois, cette disposition ne s'applique qu'aux « personnes morales », à l'exclusion des hôpitaux publics. L'autre règle existante est une norme de 2016 relative aux dossiers de santé électroniques (*Electronic Health Record Standards,* EHRS)[187] qui a été publiée par le Ministère de la santé et du bien-être de la famille (MoHFW). Elle énonce les normes techniques, administratives et physiques concernant la collecte et la conservation des données. Le champ d'application n'est pas clair, pas plus que les délais d'accès aux dossiers des patients. Les informations d'identification uniques telles que les URL et les adresses IP ne sont pas répertoriées comme des informations sensibles. L'EHRS concerne davantage la standardisation des dossiers numériques que la protection des données. Un code d'éthique pour les médecins reste

[187] The Ministry of Health and Family Welfare of India, « Electronic Health Record (EHR) Standards Version 2016 for India », 2016, https://mohfw.gov.in/sites/default/files/17739294021483341357.pdf.

vague dans ses prescriptions. En Inde, aucune loi n'oblige les hôpitaux à divulguer les atteintes aux règles de sécurité. Par contraste, la loi américaine *Health Insurance Portability and Accountability Act* (HIPAA) de 1996[188] exige qu'un hôpital divulgue toute atteinte à la sécurité des données ayant touché plus de 500 patients. Le RGPD contient également des dispositions strictes en cas de violations[189]. L'absence d'une réglementation appropriée est également soulignée dans la controverse sur l'usage étendu du numéro d'identification unique Aadhaar et de sa vulnérabilité.

La situation devrait très probablement changer de manière conséquente. D'une part, la politique nationale de santé (2017) comprend des plans ambitieux en faveur de la numérisation et de l'intégration nationale des données de santé, notamment des registres de santé nationaux, des réseaux de plateformes et d'échange, des connexions par fibres optiques et l'utilisation généralisée des tablettes et des smartphones. Les applications dans ce domaine sont en plein essor. D'autre part, l'Inde est sur le point d'adopter un projet de loi sur la sécurité de l'information numérique dans les soins de santé, le *Digital Information Security in Healthcare Act* (DISHA), proposé par le ministère de la Santé le 11 mars 2018[190]. La période de consultation des parties prenantes a pris fin le 21 avril 2019 et un projet de loi est en cours de finalisation : même si le gouvernement s'est désormais engagé, le processus avec la Lok Sabha (chambre

[188] Office for Civil Rights, « Breach Notification Rule », *HHS.gov,* 14 septembre 2009, https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

[189] Akhil Deo, « Without Data Security and Privacy Laws, Medical Records in India Are Highly Vulnerable », *The Wire,* 27 janvier 2017, https://thewire.in/law/without-data-security-and-privacy-laws-medical-records-in-india-are-highly-vulnerable.

[190] The Ministry of Health and Family Welfare of India, « Government of India Ministry of Health & Family Welfare (EHealth Section) », 2018, https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf.

basse du Parlement) pourrait encore changer le résultat, comme c'est le cas pour de nombreux projets de loi.

Pour le moment, le DISHA est une proposition radicale et globale[191] en matière de protection de la confidentialité des données de santé qui va beaucoup plus loin que l'autre projet de loi numérique majeure du gouvernement Modi en cours de préparation, la *Personal Data Protection Bill* (PDPB)[192]. Le consentement individuel est primordial, les exceptions spécifiées étant beaucoup plus restrictives que celles prévues par le projet de loi PDPB en général, ou par le RGPD sur cette question. Le déni de service est impossible. La loi renforce également le droit à l'effacement. L'accès du gouvernement aux données de santé est limité à des fins strictement sanitaires. « Les compagnies d'assurance ne doivent pas insister pour accéder aux données de santé numériques des personnes qui cherchent à souscrire des polices d'assurance santé ou pendant le traitement d'une demande de règlement : l'accès aux données numériques détenues par l'établissement clinique spécifique auquel la demande se rapporte n'est autorisé que sous réserve du consentement des utilisateurs » (article 29.5). Les sociétés pharmaceutiques n'ont pas accès aux données de santé numériques individuelles, même pour la recherche. Une autorité nationale de santé électronique (NEHA) doit être créée et la loi contient désormais des dispositions prévoyant des sanctions en cas d'infractions.

[191] Singh Madhur, « India to Be First to Protect Health Data of Citizens with Iron-Clad Law? », *Business Standard,* 31 mai 2018, https://www.business-standard.com/article/economy-policy/india-to-be-first-to-protect-health-data-of-citizens-with-iron-clad-law-118053100126_1.html.

[192] Ikigai Law, « DISHA and the Draft Personal Data Protection Bill, 2018: Looking at the Future of Governance of Health Data in India », *Ikigai Law,* 25 février 2019, https://www.ikigailaw.com/disha-and-the-draft-personal-data-protection-bill-2018-looking-at-the-future-of-governance-of-health-data-in-india/#acceptLicense.

Le projet de loi DISHA peut encore se heurter aux prochaines conclusions du comité Srikrishna sur la protection des données personnelles, et ses dispositions les plus radicales font l'objet de critiques professionnelles[193]. L'effort réglementaire ne s'arrête pas là. Le gouvernement de l'Union en est actuellement à la dernière étape avec la Rajya Sabha (chambre haute du Parlement) d'un projet de loi de 2019 sur les technologies ADN (utilisation et application) qui réglemente et limite l'utilisation de l'empreinte génétique aux actions civiles en recherche de paternité et au traitement consenti des données génétiques pour tous les crimes et délits soumis au Code pénal indien, les crimes et délits passibles de plus de 7 ans d'emprisonnement ne nécessitant pas de consentement[194].

Dans l'ensemble, la façon dont l'Inde traite les questions de protection des données et de respect de la vie privée dans le secteur de la santé semble unique. Une offensive très forte en faveur d'outils numériques coordonnés et intégrés coexiste avec ce qui promet d'être une politique de confidentialité rigoureuse, qui dépasse les exigences du RGDP de plusieurs manières. Jusque-là, alors que les soins de santé à la base pourraient être améliorés par la poursuite de la numérisation, la recherche pharmaceutique, qu'elle soit menée par des entreprises étrangères ou indiennes, semble être moins prioritaire aux yeux du gouvernement indien. Le DISHA contraste avec la tendance générale à privilégier l'innovation et les exigences de l'État aux dépens de la protection de la vie privée, comme en témoignent le PDPB et les nombreuses politiques numériques.

[193] Pour un exemple de ces critiques, voir : Rahul Matthan, « A New Direction for Data Privacy in Healthcare », *Livemint.Com,* 11 avril 2018, https://www.livemint.com/Opinion/3LK0TR6zdXmelkaJuTUnnJ/A-new-direction-for-data-privacy-in-healthcare.html.

[194] Ministry of Science and Technology and Earth Sciences of India, « The DNA Technology (Use and Application) Regulation Bill », 8 juillet 2019, https://www.prsindia.org/billtrack/dna-technology-use-and-application-regulation-bill-2019.

La Chine utilise les données de santé comme une ressource

En Chine, les données de santé sont explicitement considérées comme une ressource au service de l'État développemental. L'incitation à utiliser les données de santé s'inscrit dans le cadre de la stratégie *Internet Plus* proposée par le Premier ministre Li Keqiang en 2015. Cette stratégie vise à stimuler le développement et à augmenter la valeur économique de certaines industries traditionnelles par l'utilisation d'Internet. L'expression « permettre aux gens de moins courir et laisser les données courir plus » est largement utilisée pour expliquer le concept d'*Internet Plus*. Sans surprise, les *Guiding Opinions on Promoting and Regulating the Application and Development of Big Data in Health and Medical Care*, publiées par le Conseil d'État chinois en 2016, décrivent le *big data* sanitaire et médical comme une ressource fondamentale et stratégique de l'État. Ces lignes directrices émergent dans le contexte de la promotion de nouveaux secteurs d'activité et de mesures pour favoriser une croissance économique plus forte[195]. Elles insistent ensuite sur la nécessité de mieux utiliser le gouvernement, de mieux concevoir « l'intégration, le partage et l'application ouverte du *big data* dans le domaine de la santé et des soins médicaux » et « d'apporter un soutien fort à la construction d'une Chine saine, à l'achèvement de l'édification générale d'une société modérément prospère et à la réalisation du rêve de grande renaissance de la nation chinoise ».

[195] General Office of the State Council of the People's Republic of China, « Guiding Opinions on Promoting and Regulating the Application and Development of Big Data in Health and Medical Care 国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见 », 2016, http://www.gov.cn/zhengce/content/2016-06/24/content_5085091.htm.

Avec l'appui du gouvernement et les pressions en faveur de l'intégration, du partage et de l'application ouverte du *big data* dans le domaine de la santé et des soins médicaux, les efforts portent leurs fruits. Si l'on prend l'exemple de la province du Guangdong, 3 112 établissements médicaux et de santé ont mis leurs données en commun. La banque nationale de données électroniques sur la santé au niveau provincial contient des informations sur 80 millions de résidents permanents[196].

Une présentation détaillée des politiques de la Chine en matière de données numériques indique que « bien que la protection de la vie privée soit un sujet extrêmement important pour le *big data* dans le domaine de la santé et de la médecine, il n'existe aucune loi ou directive spécifiques à ce sujet en Chine »[197]. En effet, la loi de 2017 sur la cybersécurité ne mentionne pas le mot « santé ». La spécification PIS a inclus le terme « informations médicales » dans la définition des informations personnelles sensibles, mais sans aller plus loin. Cependant, trois projets de loi sur les soins de santé de base et la promotion de la santé ont été publiés pour consultation publique depuis 2017. L'un d'entre eux aborde la question de la confidentialité des informations médicales à l'article 90 (dans le troisième projet, pour consultation publique jusqu'au 26 septembre 2019) de la manière suivante : « L'État protège la vie privée lorsqu'il s'agit de la santé des citoyens et assure la sécurité des informations personnelles sur la santé. Aucune organisation ni personne n'a le droit d'acquérir, d'utiliser ou de divulguer des informations personnelles sur la santé d'un citoyen

[196] Health Commission of Guangdong Province, « Guangdong Health Case Letter », *Gd.Gov.Cn,* 19 juin 2019, http://wsjkw.gd.gov.cn/zwgk_bmwj/content/post_2516919.html.

[197] Luxia Zhang et al., « Big Data and Medical Research in China », *BMJ Medical Research,* 5 février 2018, j5910, https://doi.org/10.1136/bmj.j5910.

sauf si exigé par la loi, des règlements administratifs ou avec le consentement de la personne »[198].

En avril 2018, le bureau général du Conseil d'État a publié les *Opinions of the General Office of the State Council on Promoting the Development of Internet Plus Health Care*[199] sans jamais mentionner la protection des données personnelles. Ils ont été suivis par la publication en septembre 2018 de *Measures for the Administration of Internet Diagnosis and Treatment,* de *Measures for the Administration of Internet Hospitals* et de *Specifications for the Administration of Remote Medical Services,* toutes trois mises en œuvre à titre expérimental[200]. Ces trois derniers documents font une mention générale de la « protection de la vie privée », sans détailler les moyens concrets pour y parvenir. Néanmoins, ils abordent tous la question de la coopération avec les institutions tierces et soulignent la nécessité d'un accord précisant les responsabilités de toutes les parties dans différents domaines, y compris en matière de protection de la vie privée. Par conséquent, la présentation détaillée que nous avons cité au paragraphe précédent n'est pas exacte dans sa conclusion. Mais il est probable que le commentaire de ses auteurs traduise la distance qui sépare le droit et la pratique.

[198] National People's Congress, « Basic Healthcare and Health Promotion Law (draft) 中华人民共和国基本医疗卫生与健康促进法(草案) », 2019, https://npcobserver.files.wordpress.com/2019/08/basic-healthcare-and-health-promotion-law-3rd-draft.pdf

[199] General Office of the State Council of the People's Republic of China « Opinions of the General Office of the State Council on Promoting the Development of Internet plus Health Care 国务院办公厅关于促进“互联网+医疗健康”发展的意见 », 2019.

[200] The National Health Commission of the People's Republic of China, « About the Issuing of the Measures for the Administration of Internet Diagnosis and Treatment (trial implementation), etc. 关于印发互联网诊疗管理办法（试行）等3个文件的通知 », 2018, http://www.cac.gov.cn/2018-09/14/c_1123431844.htm

Jusqu'à présent, les *Administrative Measures on the Standards, Security and Service of National Health and Medical Big Data (For Trial Implementation)* sont la réglementation la plus concrète sur la protection des données de santé[201]. Elles ont été publiées en juillet 2018 par la Commission nationale de la santé, et abordent la question de la collecte des données, de la conservation des données, de la fourniture de services, de l'utilisation et du partage de données[202]. En ce qui concerne plus particulièrement le partage des données, « la Commission nationale de santé est chargée d'établir un mécanisme de partage ouvert des *big data* relatives aux soins de santé, de coordonner la construction d'un système de catalogue de ressources et d'un système d'échange de données, et de renforcer le service et la gestion du cycle de vie des *big data* relatives aux soins de santé ». L'objectif est orienté vers la construction de ressources de données de santé partagées, mais les règles ne précisent guère la notion de protection des données de santé au-delà des généralités déjà présentes dans la spécification PIS.

La Chine a tout mis en œuvre pour collecter, agréger et utiliser toutes les données de santé disponibles dans le secteur des soins de santé et dans l'industrie pharmaceutique. L'Inde envisage au contraire une loi très restrictive, même si ses ultimes développements méritent d'être scrutés. Aux États-Unis, l'interdépendance entre l'assurance

[201] The National Health Commission of the People's Republic of China, « Administrative Measures on the Standards, Security and Service of National Health and Medical Big Data (For Trial Implementation) 关于印发国家健康医疗大数据标准、安全和服务管理办法（试行）的通知 », 2018, http://www.cac.gov.cn/2018-09/15/c_1123432498.htm

[202] The National Health and Family Planning Commission of the People's Republic of China, « Explaining the Administrative Measures on the Standards, Security and Service of National Health and Medical Big Data (For Trial Implementation) 国家健康医疗大数据标准、安全和服务管理办法（试行）》解读 », 14 septembre 2018, http://www.cbdio.com/BigData/2018-09/14/content_5834771.htm

privée et les soins de santé est troublante, mais c'est aussi là que les développements de l'IA et des *big data* sont les plus prometteurs : c'est un champ de bataille au Royaume-Uni, en raison de la base importante de son *National Health Service*. Le cas français doit nous rappeler que le *big data* utilisable n'est pas si facile à déployer sur des systèmes étendus et décentralisés. À condition de définir clairement ce que les compagnies d'assurance peuvent utiliser et ce à quoi elles peuvent avoir accès (y compris avec le consentement des personnes concernées), l'amélioration du champs, de l'accessibilité et de la qualité des données médicales, génétiques et comportementales doit être un objectif prioritaire de santé publique.

VII

CONCILIER LE RESPECT DE LA VIE PRIVÉE, L'INNOVATION ET L'INTÉRÊT PUBLIC

Sur les processus et les méthodes de protection des données à caractère personnel, le contraste entre les approches européenne et américaine existe, mais il ne doit pas être exagéré. Le RGPD ressemble certes à un jardin à la française bien ordonné, et la réglementation américaine à un labyrinthe, mais nous devrions aller au-delà des apparences. On pourrait toujours invoquer l'adage « Qui veut trop embrasser mal étreint » contre le RGPD ainsi que de nombreuses autres directives de l'UE. Sundar Pichai, le PDG de Google, met en garde contre une approche générale et plaide en faveur d'une réglementation sectorielle de l'IA « au lieu de se précipiter dans une voie qui empêche l'innovation et la recherche »[203].

Les pourvois devant la Cour de justice de l'Union européenne (CJUE) créeront des précédents, et dans une certaine mesure, ils produiront des effets similaires à ceux de la jurisprudence aux États-Unis. Des exemples récents le montrent, comme celui de l'arrêt rendu le 1er octobre 2019 par la CJUE sur les règles spécifiques relatives au consentement de l'utilisateur aux cookies[204].

Pour ce qui est des exceptions relatives à l'intérêt public, l'écart entre les États-Unis et l'Europe risque également de se resserrer, ce qui pourrait être une mauvaise nouvelle pour les citoyens européens.

[203] Tim Bradshaw, « Google Chief Sundar Pichai Warns against Rushing into AI Regulation », *Financial Times,* 20 septembre 2019, https://www.ft.com/content/b16e6ee8-dbb2-11e9-8f9b-77216ebe1f17.

[204] CJUE, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Planet49 GmbH (1er octobre 2019).

En matière de récupération des données, nous avons déjà souligné les similitudes entre l'analyse de marché (ou « capitalisme de surveillance » comme certains l'appellent) et la surveillance étatique. Mais il existe aussi des risques d'un abus des exceptions relatives à l'intérêt public, que ce soit par une interprétation biaisée de la loi ou par des pratiques illégales. La description glaçante faite par Edward Snowden[205] des programmes de surveillance de masse créés après le 11 septembre et la façon dont ceux-ci ont contourné les protections constitutionnelles devrait être méditée, qu'on le considère comme un lanceur d'alerte ou comme un traître. Les polémiques autour de l'identification biométrique ne sont pas réservées au programme indien Aadhaar. La France vient par exemple de décréter un processus de reconnaissance faciale unique permettant de vérifier l'identité des titulaires de passeport ainsi que des étrangers qui déposent une demande de résidence et qui contactent les services publics[206]. À mesure que les Européens rattraperont leur retard dans les programmes d'analyse des *big data* et les programmes d'IA, les questions se multiplieront.

À partir de l'examen de ce que font les partenaires et les concurrents de l'Europe, qui vont parfois au-delà du RGPD mais qui le plus souvent mettent la barre plus bas, et les moyens d'améliorer et de réviser le RGPD, nous formulons quelques propositions de politique publique, tant positives que négatives, présentées ci-dessous.

---

[205] Edward Snowden, *Permanent Record,* New York : Macmillan, 2019.

[206] Pour une critique de l'autorité de contrôle française, voir :
Source : CNIL, « Délibération N° 2018-342 Portant Avis Sur Un Projet de Décret Autorisant La Création d'un Traitement Automatisé Permettant d'authentifier Une Identité Numérique Par Voie Électronique Dénommé "Application de Lecture de l'identité d'un Citoyen En Mobilité" (ALICEM) et Modifiant Le Code de l'entrée et Du Séjour Des Étrangers et Du Droit d'asile (Demande d'avis N° 18008244) », 18 octobre 2018.

Des règles ambitieuses mais génériques

De manière explicite, le RGPD est un « règlement général », un terme qui n'était pas utilisé auparavant pour désigner les règlements de l'UE, ce qui soulève la question des lignes directrices explicatives (quelques-unes ont vu le jour) et des réglementations sectorielles (aucune à ce jour). **Des règles ambitieuses mais génériques laissent une marge d'interprétation et contiennent des lacunes, y compris de grands espaces pour les exceptions.** Nous arrivons au paradoxe de l'article 23, sobrement intitulé « Limitations ». Il prévoit que l'État peut accéder aux données des citoyens par une suspension des obligations de l'État et des droits des citoyens dans certains cas.

Mais aussi, **plus les exigences de conformité sont rigoureuses et générales, plus il est probable qu'elles ne seront pas mises en œuvre.** Nous rencontrons tous des exemples de non-conformité flagrante, à commencer par des sites sur lesquels, dans la pratique, il est impossible de faire un choix quant à la confidentialité de ses données. De leur côté, les entreprises numériques et les représentants du monde des affaires, qui sont désormais des responsables du traitement ou des sous-traitants, attirent l'attention sur plusieurs facteurs : le coût de la mise en conformité, en particulier pour les petites entreprises ; la question des ressources humaines (des délégués à la protection des données formés par exemple). Ils soulignent régulièrement que le langage même du RGPD met l'accent sur des objectifs très différents et difficiles à concilier. **Les entreprises font face à une absence d'aide opérationnelle et ont besoin de beaucoup de conseils pour se conformer au règlement.** Les responsables du traitement et les sous-traitants sont investis d'une grande responsabilité quant à l'interprétation.

Le travers de l'*opt-out* par défaut

L'approche par « l'avis de notification et de consentement » est sans doute l'aspect le plus populaire du RGPD, parce qu'on dit que cet avis permet à l'individu de reprendre le contrôle de ses données à caractère personnel. Or avoir plus de contrôle semble plus satisfaisant. En réalité, **une approche maximaliste présente des inconvénients et semble explosive.**

Une option négative par défaut (à moins que l'utilisateur ne prenne une mesure positive ou *opt-in*, aucune donnée ou métadonnée ne peut être récupérée) ou une option globale de non-suivi réduiraient considérablement l'utilisation personnalisée de la plupart des sites et applications, qui reposent sur des requêtes et des échanges de données. Selon le RGPD, l'accès aux données ne peut pas être subordonné à un consentement à l'extraction des données. Le choix rationnel d'un individu est en effet d'obtenir le produit tout en refusant de livrer l'information. Mais si de nombreux utilisateurs s'attendent à naviguer gratuitement sur le web, au détriment des autres utilisateurs qui continuent de donner leur consentement préalable *(opt-in)*, cela risque de détruire l'économie d'Internet, qui repose sur sa mise à disposition gratuite *en échange de données personnelles.* C'est tout aussi injuste que la situation actuelle, où le niveau de conformité très inégal des sites et des entreprises donne un avantage concurrentiel aux fraudeurs sur ceux qui appliquent le RGPD à la lettre. **Au niveau macroéconomique, cela met le système en faillite et aboutit au même résultat que l'option entièrement négative par défaut. Quelqu'un doit payer, d'une façon ou d'une autre, ou nous reviendrons à l'ère pré-Internet. L'Internet serait-il le même si tous les services et toutes les informations étaient payants ?** Il s'agit d'un changement fondamental qui peut ne pas être accepté

par les particuliers en tant que consommateurs, contrairement aux citoyens revendiquant le droit à la vie privée. Un groupe de réflexion français adepte de l'économie libérale a proposé d'inverser la proposition : les particuliers étant propriétaires de leurs données à caractère personnel, ils pourraient les vendre aux plateformes numériques. De toute évidence, cette proposition se heurterait immédiatement à de nombreux problèmes, par exemple l'utilisation des données par des tiers ou une utilisation non prévue. Mais elle a le mérite de mettre fin à l'hypocrisie sur les relations entre les internautes et les fournisseurs d'Internet[207].

Le paradoxe de la protection de la vie privée *(privacy paradox)*

Face aux conséquences insoutenables du choix rationnel des individus, nous devrions envisager ce que les experts en protection de la vie privée appellent le *privacy paradox*[208], mais que l'on pourrait également qualifier « d'hypocrisie de la confiance ». Le besoin, le désir et la convoitise, pas nécessairement dans cet ordre, l'emportent sur le principe de précaution dans la psyché individuelle. Dans un environnement numérique, nous renonçons constamment à notre vie privée à d'autres fins utiles ou agréables. Ce que l'on pourrait qualifier de *speed googling* va certainement à l'encontre de la lecture des avis de confidentialité. Ce n'est qu'un tout petit exemple dans un monde rempli de compromis entre confort et protection des données.

---

[207] Isabelle Landreau et al., « Mes data sont à moi - pour une patrimonialité des données personnelles », *Génération Libre,* janvier 2018, https://www.generationlibre.eu/wp-content/uploads/2018/01/2018-01-generationlibre-patrimonialite-des-donnees.pdf.

[208] Voir partie II. Qu'est-ce que le respect de la vie privée et comment le garantir ?, Politiques de confidentialité, avis de notification et de consentement, page 51.

La disparition prochaine de l'argent liquide (qui est déjà une réalité dans des pays aussi divers que la Chine ou la Suède) est un parfait exemple, conduisant à l'hypocrisie de la confiance. La Chine était autrefois la société la plus éprise d'argent liquide, en partie pour son anonymat, en partie parce qu'il est l'instrument d'échange symbolique entre les personnes, y compris les défunts. Aujourd'hui, même les transactions en espèces les plus infimes pourraient être remplacées par des paiements électroniques. **Une société sans argent liquide est une société transparente, qui annule complètement l'anonymat que l'argent liquide conférait aux transactions.** Ainsi, après le billet de cent dollars, la cryptomonnaie, le bitcoin par exemple, est devenue la nouvelle monnaie anonyme de choix et le restera aussi longtemps qu'elle sera un moyen d'échange privé. La Chine a donc décidé de devenir le premier émetteur public au monde d'une monnaie numérique, que l'on ne peut plus appeler cryptomonnaie. Cette monnaie aiderait probablement la Chine à échapper à l'emprise du dollar sur les transactions internationales. Mais la banque centrale a déjà annoncé qu'elle « marquerait » la monnaie pour retrouver la trace des personnes qui l'utilisent. « *La monnaie numérique de la banque centrale peut circuler aussi facilement que de l'argent liquide (…) en même temps, elle peut permettre un anonymat contrôlable* », selon Mu Changchun, directeur adjoint de la division des paiements et des règlements de la Banque populaire de Chine (PBOC)[209].

[209] Dexin Guo, « 'Digital Renminbi' Is Revealed '数字人民币' 初露真容 », *Xinhua,* 21 août 2019, http://www.xinhuanet.com/fortune/2019-08/21/c_1124900323.htm.

Différences entre les États membres

Les différences d'interprétation se reflètent à travers la diversité des adaptations dans le droit national des États membre[210]. **C'est l'âge de consentement qui est le plus souvent mentionné comme un problème.** Il existe également **d'énormes différences entre les capacités d'application des États membres,** et probablement une volonté d'aller de l'avant fluctuante selon les pays. Une étude portant sur 17 États membres de l'UE ainsi que sur la Croatie (mais qui ne couvre pas des pays comme la France, les Pays-Bas ou le Royaume-Uni) révèle que les autorités de contrôle polonaise et espagnole disposent des ressources humaines les plus importantes (environ 250 personnes) et que celles des 12 autres pays comptent moins de 50 personnes[211].

La sécurité nationale n'étant pas une compétence de l'UE, les États membres peuvent préciser eux-mêmes ce qui constitue (ou ne constitue pas) l'élargissement de la portée des dérogations. *Quis custodiet ipsos custodes[212]?*

Les décisions relatives à l'interprétation du RGPD peuvent suivre différents processus : si la question a des implications transfrontalières et si la personne physique ou l'entité morale concernée a un établissement au sein d'un État membre de l'UE, l'autorité de contrôle

[210] Pour un examen des adaptations nationales après huit mois d'application, voir cette étude portant sur dix États membres :
Source : Karen Mc Cullagh, Olivia Tambou et Sam Bourton, *National Adaptations of the GDPR*, Luxemburg : Collection Open Access Book, Blogdroiteuropeen, février 2019.

[211] EDPB, « First Overview on the Implementation of the GDPR and the Roles and Means of the National Supervisory Authorities », 8 mars 2019, https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf.

[212] « Mais qui gardera ces gardiens ? »

de cet État membre jouera un rôle prépondérant dans l'examen du cas. Sa décision sera dès lors valable dans toute l'UE : c'est l'approche du guichet unique. **Mais le processus ne s'applique pas si le plaignant n'est pas basé à l'intérieur de l'UE ou si le lieu où les décisions sont prises ne coïncide pas avec son établissement légal.** Il peut donc y avoir 28 décisions. Même cette disposition a sa propre exception : dans les cas « urgents », toute autorité de contrôle peut prendre une décision qui aura trois mois de validité. Nous aurions pu espérer un processus plus simple et plus clair.

Trois affaires récentes, qui en l'occurrence impliquent toutes Google, illustrent bien la complexité de la situation. Sur la question de l'enregistrement de conversations privées par le personnel de Google dans le but d'améliorer les performances de la reconnaissance vocale, le commissaire à la protection des données de Hambourg a pu prendre des mesures, même si l'établissement principal de Google est en Irlande[213]. Une décision importante de la CJUE établit que le droit de l'Union européenne (le RGPD) n'impose pas la mise en œuvre d'une obligation de déréférencement dans les moteurs de recherche au-delà des frontières de l'UE[214]. Mais une juridiction d'un État membre peut effectivement imposer le déréférencement sur toutes les versions d'un moteur de recherche « à la lumière des normes nationales » et en examinant l'équilibre entre le droit à la vie privée et la liberté de l'information. En d'autres termes, les juridictions nationales peuvent aller au-delà du RPGD dans leur propre pratique juridique, mais pas en deçà, à condition qu'un

[213] The Hamburg Commissioner for Data Protection and Freedom of Information, « Press Release. Speech Assistance Systems Put to the Test - Data Protection Authority Opens Administrative Proceedings against Google », 1er août 2019, https://datenschutz-hamburg.de/assets/pdf/2019-08-01_press-release-Google_Assistant.pdf.

[214] CJEU, « Google LLC, successor in law to Google Inc. vs Commission nationale de l'informatique et des libertés (CNIL) » (24 septembre 2019).

« équilibre » des différents droits ait été examiné. Dans une autre affaire en attente d'un arrêt de la CJUE, la CNIL a décidé que si le processus de décision d'une entreprise dans le cadre du RGPD fait d'elle un « responsable du traitement » et qu'elle est située dans un État membre différent de celui où elle est établie, l'affaire peut être tranchée par l'autorité de contrôle de cet autre pays. Étant donné la difficulté à localiser l'activité et le processus de décision, identifier le lieu réel où se prennent les décisions de l'entreprise s'avérera litigieux et, en tout état de cause, va à l'encontre de la simplicité de la disposition du guichet unique. La décision « pourrait finalement se révéler préjudiciable à une mise en œuvre effective du RGPD à l'échelle de l'Union européenne (notamment à l'uniformité d'application et la sécurité juridique) à plus long terme »[215].

Le fait que Google, dont le siège social européen est situé en Irlande mais qui a des intérêts beaucoup plus importants dans d'autres États membres, ait souvent été un cas test n'est pas un hasard. On observe une tendance à plus de souveraineté sur les données numériques et les ressources fiscales, et donc à la détermination du domicile en fonction du marché. Cependant, cette tendance est contestée, et l'indécision nuira à la perspective d'un marché numérique unifié et à toute entreprise qui gère des données au-delà des frontières en général. **Changer radicalement de siège social, de lieu de production, de point de vente ou de lieu de décision, que ce soit pour des raisons réglementaires ou fiscales, est une entreprise internationale de grande envergure.** Mélanger simultanément les deux approches revient à faire rouler certains véhicules du côté droit de la route et les autres du côté gauche…

[215] Lokke Moerel, « CNIL's Decision Fining Google Violates One-Stop-Shop », *SSRN,* 19 février 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3337478.

La frontière technologique évolue rapidement

La technologie est une frontière en évolution rapide, où les règles existantes ne permettent pas d'anticiper quoi que ce soit, si ce n'est en termes et objectifs très généraux. Il est impossible d'arrêter le mouvement, à moins de décider de contrôler radicalement l'innovation. Nos concurrents envisageraient-ils de telles mesures ? C'est peu probable si l'on en juge par les cas chinois, indiens et américains. Les enjeux vont au-delà de la « Convention de Genève » que certains ont appelée de leurs vœux. Pour la protection de la vie privée et des données, comme pour la cybersécurité et les négociations sur la maîtrise des armements en général, des accords internationaux sont certes souhaitables, mais ils doivent faire l'objet d'une vérification rigoureuse. Dans le domaine de la cybersécurité comme dans celui de la maîtrise des armements, la dissuasion est souvent apparue comme l'option complémentaire ou l'alternative à des accords. Une telle option n'existe pas pour le droit à la vie privée. **Ce n'est qu'en ouvrant ou en fermant notre marché numérique que nous pouvons espérer influencer le comportement d'acteurs dont le socle se situe en dehors de celui-ci.**

Nous devons savoir que parfois, « on ignore ce qu'on ne sait pas » *(there are unknown unknowns)*. Il est impossible de prédire quel type de données se révéleront personnelles, sensibles ou critiques. La situation de l'IA rappelle l'ironie d'une récente campagne d'affichage publicitaire d'une société d'épargne : « Les robots ne peuvent pas vous prendre votre travail si vous êtes déjà à la retraite »[216] : le message implicite est que tous ceux qui ne sont pas

[216] Les robots sont bien entendu le résultat de l'intelligence artificielle. Cette campagne d'affichage de Prudential en 2019 a fait, à juste titre, du bruit sur le Web. Parmi de nombreux sites Web : Source : r/ABoringDystopia, « Automation Can't Take Your Job If You Don't Have One. », *Reddit,* 29 janvier 2016, https://www.reddit.com/r/ABoringDystopia/comments/bci7pz/automation_cant_take_your_job_if_you_dont_have_one/.

à la retraite sont à la merci des robots. Voici quelques exemples, bien que par définition, ils concernent des cas qui se sont déjà concrétisés : des banques de données ADN, telles que 23andme ou Ancestor.com, sont en train de révolutionner les enquêtes criminelles en réidentifiant l'ADN anonyme de parents éloignés (cousins au troisième ou quatrième degré), comme ce fut le cas en 2018 pour le tristement célèbre « tueur du Golden State » en Californie. Une banque de donnée génétique de 2 millions de personnes est suffisante pour identifier 90 % de la population américaine[217]. Lenddo, une entreprise technologique basée à Singapour, scrute le comportement social et mobile en ligne (par exemple, le niveau de chargement de la batterie d'un smartphone) pour déterminer la probabilité qu'un emprunteur rembourse ses prêts[218]. Les plateformes de streaming pour chaînes de télévision gardent désormais la trace des émissions regardées par les téléspectateurs et monétisent ces informations par le biais de la publicité comportementale[219]. L'analyse des données des réseaux sociaux complétée par des techniques d'intégration et de fusion permet d'identifier les comportements probables des individus bien mieux que n'importe quelle autre technique disponible auparavant.

Les technologies *blockchain* créent un problème supplémentaire pour l'un des aspects de la protection de la vie privée : le droit à

[217] Yaniv Erlich et al., « Identity Inference of Genomic Data Using Long-Range Familial Searches », *Science* 362, n° 6415, 11 octobre 2018 : 690–94, https://doi.org/10.1126/science.aau4832.

[218] Hope King, « This Startup Uses Battery Life to Determine Credit Scores », *CNNMoney,* 24 août 2016, https://money.cnn.com/2016/08/24/technology/lenddo-smartphone-battery-loan/index.html.

[219] Hooman Mohajeri Moghaddam et al., « Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices », *Freedom-to-tinker.com,* 18 septembre 2019, https://freedom-to-tinker.com/2019/09/18/watching-you-watch-the-tracking-ecosystem-of-over-the-top-tv-streaming-devices/.

l'effacement. Dans les *blockchains,* tous les participants peuvent consulter les données enregistrées ; plusieurs copies de la *blockchain* coexistent sur différents ordinateurs ; une fois les données enregistrées, elles ne peuvent être ni modifiées ni supprimées ; les décisions sont prises par consensus entre les participants, sans arbitre central. Des mesures de précaution, telles que le cryptage et la pseudonymisation, sont absolument nécessaires[220]. Mais malgré cela, la CNIL et la *Financial Conduct Authority* (FCA), l'autorité de contrôle britannique, mettent actuellement en garde contre l'utilisation des *blockchains*[221].

Collecte et utilisation

Ce qu'il est plus réaliste de réglementer, c'est l'utilisation des données collectées et leur interprétation, à condition qu'il existe bel et bien un État de droit, notamment un droit légal de vérification et de recours des individus. En un sens, cela a toujours existé dans les procédures judiciaires : une personne ne peut être condamnée devant un tribunal sur la base de preuves recueillies illégalement. Le premier obstacle à l'utilisation aveugle des algorithmes est l'interdiction des décisions individuelles fondées exclusivement sur un traitement automatisé. L'article 22 du RGPD a énoncé cette interdiction tout en prévoyant des exceptions très larges. Là encore, le droit de l'État membre peut introduire des garanties supplémentaires. Dans le cas de la France, le changement du processus d'admission à l'enseignement supérieur, pour passer d'un algorithme entièrement automatisé

[220] CNIL, « Blockchain and the GDPR: Solutions for a Responsible Use of the Blockchain in the Context of Personal Data », *Cnil.fr*, 6 novembre 2018, https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data.

[221] Andrew Solomon, « Block Chain: Is the GDPR Out of Date Already? », *Lexology.com,* 30 août 2017, https://www.lexology.com/library/detail.aspx?g=d4c0481a-c678-4748-80cb-4ab917e66207.

(Admission Post-Bac ou APB) à un algorithme nécessitant une intervention humaine et offrant certaines possibilités de demander des explications sur la décision prise (Parcoursup), illustre bien ce point. **Il faudrait édicter le même genre de limitation pour la conduite (ou le vol) autonome : en fin de compte, le principe de responsabilité exige de pouvoir identifier l'action et la responsabilité humaines.** C'est l'une des réponses à la question posée par un récent rapport sur l'IA : « Existe-t-il des domaines où le jugement humain, aussi faillible soit-il, n'a pas vocation à être remplacé par la machine ? »[222].

Le deuxième obstacle consiste à **exiger un système de contre-pouvoirs dans la mise en œuvre de décisions défavorables fondées sur des preuves numériques.** Une législation adoptée sous le coup de l'émotion, à la suite d'une attaque terroriste, réduira souvent les garanties. Les attentats de Lashkar-e-Taiba à Mumbai (2008) ou les actes terroristes commis en France (2015) ont dans les deux cas conduit à de nouvelles lois antiterroristes laissant peu de possibilités de contrôle judiciaire, pour ne pas dire aucune. Dans le cas français, elles comprennent de « vastes pouvoirs de procéder à des perquisitions informatiques ainsi que la possibilité de bloquer des sites web qui auraient fait l'apologie du terrorisme, sans aucune autorisation judiciaire préalable »[223]. Une nouvelle loi relative au renseignement adoptée en 2015 est en attente d'une décision de la Cour européenne des droits de l'homme quant à sa légalité[224]. Il faudrait examiner

[222] Cédric Villani, « Synthèse. Donner un sens à l'Intelligence artificielle », mars 2018, https://www.aiforhumanity.fr/pdfs/MissionVillani_Summary_ENG.pdf

[223] David Sullivan, « The Consequences of Legislating Cyberlaw After Terrorist Attacks »?, *Just Security,* 9 avril 2019, https://www.justsecurity.org/63560/the-consequences-of-legislating-cyberlaw-after-terrorist-attacks/.

[224] Assemblée nationale et Sénat, « Loi N° 2015-912 du 24 juillet 2015 relative au renseignement (1) », https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030931899&categorieLien=id

très attentivement toutes les exceptions qui contournent la nécessité d'un contrôle judiciaire ou qui fondent une action négative sur des critères prédictifs plutôt que sur des preuves réelles. Dans des cas plus anodins mais importants sur le plan économique comme l'assurance, des critères sont nécessaires pour limiter l'individualisation des clients, en compensant la nécessité de dissuader les comportements à risque par la nature collective de l'assurance.

Pas de vie privée dans votre voiture

Les enjeux de la conduite autonome vont au-delà du respect de la vie privée. La sécurité est l'un d'eux. Personne ne considérerait les boîtes noires des avions comme une atteinte à la vie privée des pilotes, et personne ne remettrait en question l'existence des disques d'enregistrement des temps de conduite dans les camions commerciaux. Les conducteurs installent régulièrement des caméras de tableau de bord censées filmer les circonstances d'un accident et permettre d'établir les responsabilités ou de garantir de meilleurs tarifs d'assurance. D'autres innovations limitent la vie privée : suivi GPS, applications de conduite, péages. Au fil de ses améliorations, la conduite autonome soulèvera des questions colossales liées aux décisions automatisées et aux responsabilités, qui sont différentes de la question de la protection de la vie privée et des données. Le piratage informatique est une vive préoccupation à la fois pour la sécurité et pour la protection de la vie privée.

Mais d'autres développements, dont certains sont difficiles à prévoir, créeront de nouveaux types de problèmes liés à la protection de la vie privée, et de ce point de vue, les systèmes permettant la conduite automatisée peuvent différer considérablement. En termes simples, il existe deux méthodes opposées : l'une est une voiture robotisée et dotée de multiples capteurs qui trouve son chemin et

évite les obstacles. C'est la voie empruntée par les Américains, fondée sur la notion d'individus libres. La dépendance à des appareils de type GPS n'est pas plus grande qu'avec la génération de voitures précédente. Même dans ce type de solution, les voitures peuvent devenir des ordinateurs, comme c'est le cas pour les questions de maintenance : elles conservent un enregistrement de toutes les activités précédentes. Il sera probablement laissé en place au moment de la revente : une Tesla conserve la trace de toutes les actions de conduite depuis sa mise en circulation.

L'autre approche consiste à considérer la voiture comme un smartphone sur roues, un appareil émetteur et récepteur doté d'un système de réseau. Cela signifie au minimum des routes numérisées, et la Chine pousse déjà dans cette direction. L'amélioration de la gestion du trafic, à partir d'applications comme Waze par exemple, suit également cette voie. Ce choix augmente bien sûr aussi la possibilité d'un contrôle à distance. Mais les choses peuvent aller plus loin : des capteurs d'haleine peuvent déjà empêcher un conducteur en état d'ébriété de démarrer son moteur. La capacité à reconnaître si un piéton est handicapé, s'il est ivre ou s'il traverse en dehors des passages piétons s'améliorera si ses informations personnelles sont déjà dans le système. La première génération de dispositifs autonomes concerne principalement la sécurité passive. La deuxième génération pourrait être plus proactive et inquisitrice. Là encore, le compromis entre protection de la vie privée et sécurité réapparaît.

Avec ce bond en avant, une voiture devient une collection d'équipements reliés à l'Internet des Objets. Les données sont partagées avec de nombreux tiers. **Les fabricants, les assureurs, les gestionnaires de trafic et les prestataires de covoiturage peuvent être co-responsables de ce traitement, déterminant conjointement les moyens et les objectifs du traitement de certaines données à caractère personnel.**

La souveraineté et le *splinternet*

La souveraineté des données entretient une relation difficile avec la protection des données. Les États qui s'efforcent d'aller vers la souveraineté des données veulent en réalité exercer davantage de contrôle sur ce qu'ils appellent « leurs données ». Cela va souvent de pair avec une indifférence pour la *digital privacy* et une lutte contre les instruments susceptibles de protéger les données et communications personnelles des particuliers : *clouds* inaccessibles, applications de chiffrement et de messagerie, VPN, etc. Il faut également reconnaître honnêtement que la frontière avec les exigences légitimes de toute société de droit est poreuse, et que ce phénomène s'inscrit donc dans un continuum avec les discussions sur l'ordre public, la sécurité nationale et « l'intérêt général ». Les attitudes peuvent également varier selon les catégories de données : par exemple, nous avons vu qu'un projet de loi sur les données de santé en Inde est plus protecteur du droit à la vie privée que les lois américaines ou le cadre européen global. Les différentes attitudes à l'égard de la souveraineté des données et de la *digital privacy* conduisent à la fragmentation de l'Internet et créent un « splinternet », qui pourrait soit prendre la forme de groupements partageant la même vision soit suivre des divisions nationales fondées sur la souveraineté numérique.

La première approche est envisageable pour des États partageant la même vision et souscrivant à des valeurs communes à l'État de droit et surtout à un certain degré de contrôle mutuel. Le RGPD européen et les accords d'adéquation qui en résultent avec des pays tiers reposent tout autant sur la libre circulation des données que sur la protection des données ou de la vie privée. Le Japon a également lancé l'initiative *Data Free Flow with Trust* (DFFT) au

sommet du G20 à Osaka en juin 2019. Cette initiative vise à définir la gouvernance mondiale des données, et plus encore à éviter un souverainisme digital (et en particulier le modèle du grand pare-feu chinois…), plutôt que de réglementer la confidentialité des données : elle n'a rencontré qu'un succès limité jusqu'à présent, l'Inde, l'Indonésie et l'Afrique du Sud par exemple ayant refusé de signer une déclaration commune. Les lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel (1980, révisées en 2013) soulignent la nécessité d'une convergence progressive. La Coopération économique pour l'Asie-Pacifique (APEC) a également publié un *Digital Privacy Framework* (2005, révisé en 2015) inspiré des lignes directrices de l'OCDE.

La deuxième approche, consistant à donner la priorité à la souveraineté numérique et à fragmenter l'Internet mondial, est beaucoup plus probable dans les cas où l'État l'emporte sur la loi et où la méfiance envers les autres États est la norme. Par exemple, la Russie et la Chine se ressemblent beaucoup dans leurs conceptions de la souveraineté, de la surveillance et du cybermilitantisme à l'étranger. Mais c'est précisément pour ces raisons que l'on se demande comment ils pourraient constituer un environnement commun de données à l'intérieur duquel la libre circulation prévaudrait. Tout comme ce sera le cas à long terme pour les économies de marché par opposition aux politiques étatiques, **les sociétés appliquant l'État de droit peuvent avoir le dessus, car elles sont mieux équipées pour échanger des *big data* avec un certain degré de sécurité. Mais elles se demanderont s'il est sage d'autoriser des plateformes provenant d'environnements fermés comme la Chine ou la Russie de « braconner » sur leurs marchés de données libres.**

Vers un réseau Internet mondial dual

Un Internet dual est la meilleure alternative au *WorldWideWeb* unique. À supposer qu'une fragmentation du monde numérique soit inévitable, et même souhaitée par les représentants d'États avec une sphère Internet et une sphère de données fermées, les exigences en matière de protection des données personnelles et de la vie privée favorisent une solution à deux mondes, l'un appliquant des règles intérieures et transfrontalières équivalentes, l'autre se fragmentant selon des frontières nationales et étatiques de contrôle. Dans le monde réel, les choix ne sont pas aussi tranchés : les différents États auront des exigences différentes pour certaines catégories de données. D'autre part, la confiance ne peut se construire au détriment de la vérification, même avec les partenaires les plus proches. Reconnaissons donc que les **« décisions » d'adéquation pour la libre circulation des données devront tenir compte de l' objectif stratégique d'éviter l'isolement.**

Lorsqu'on réfléchit aux règles et à la mise en œuvre de la protection des données à caractère personnel et de la vie privée, il convient d'anticiper les problèmes au-delà des frontières de l'UE. Il y a de nombreuses raisons à cela. L'une réside dans les débats sur la souveraineté et la fragmentation numérique. Une deuxième raison est que les concepts et les expériences dans ce domaine évoluent et sont partagés. Même s'ils ont une philosophie générale cohérente comme point de départ de principe, les Européens ont tendance à surestimer le rôle qu'ils ont joué dans l'origine de la réflexion sur ces questions. Nous ne cessons de rencontrer des affaires, des débats, des exemples législatifs et surtout des techniques de protection des données (et des remises en cause de ces techniques) qui trouvent leur origine aux États-Unis. On ne se rend pas

suffisamment compte que, malgré la forte influence normative qu'exerce le RGPD, **de nombreuses solutions et outils de protection des données trouvent leur origine aux États-Unis.**

La présente étude n'a pas pour objectif d'examiner les implications financières et institutionnelles de ces choix technologiques pour l'innovation européenne. L'Europe recèle une partie des talents qui sont souvent captés par les entreprises possédant un avantage concurrentiel. Mais il est clair que la recherche de solutions optimales exige **une ouverture d'esprit et une coopération transatlantique avec tous les partenaires partageant la même vision et confrontés aux mêmes problèmes.** Par-dessus tout, l'État de droit est le dénominateur commun, au-delà de la stricte intégration des données qui existe entre ces partenaires. Et nous ne devrions pas présumer que l'**État de droit est garanti sans vérification et sans institutions indépendantes, en d'autres termes, sans contre-pouvoirs.**

Notre étude sur l'Inde et la Chine indique également qu'une lutte mondiale entre les modèles de gouvernance numérique pourrait bien être en cours, comme c'est le cas pour d'autres enjeux internationaux. Le triangle formé par le respect de la vie privée, l'efficacité et la sécurité a différentes solutions. Comme c'est le cas pour les flux commerciaux et financiers, l'Europe ne peut être conçue comme un univers numérique fermé. Au-delà de la coopération transatlantique et des compromis sur ces questions, **la volonté de créer des normes devrait être contrebalancée par la nécessité de rester attractif.** On peut faire une analogie entre le choix des « décisions d'adéquation » de l'Europe (en réalité des accords d'adéquation) et le choix des accords de libre échange. Ces derniers se déclinent sous différentes formes qui vont d'accords commerciaux de surface à des accords commerciaux approfondis. La tendance de la dernière décennie a

penché vers des traités de plus en plus complets intégrant l'investissement et l'arbitrage, les services, la propriété intellectuelle et les normes[225] : jusqu'à ce que la tendance se renverse avec le fiasco du partenariat transatlantique de commerce et d'investissement (TIPP) et des premiers projets de partenariat transpacifique (TPP). Dans le cadre des décisions d'adéquation, des choix similaires devront être faits, entre des critères exigeants et exhaustifs nécessitant des ajustements forts et permanents de la part des partenaires et des accords plus limités de partage de données. Le *Privacy Shield* UE-États-Unis, même s'il est controversé, en est le meilleur exemple.

Action *ex ante* ou *ex post*

Ni le cadre de l'avis de notification et de consentement, ni l'approche fondée sur la confiance et le *privacy by design*, ni le cadre réglementaire *ex ante* ne peuvent être rejetés au motif qu'ils sont limités. Ils servent l'objectif de protection de la vie privée et des données. Mais la **réglementation doit aussi s'appuyer sur une action *ex post,* voie qui mène aux sanctions ou aux poursuites en responsabilité civile.** Les deux voies ne sont pas les mêmes, bien qu'elles puissent être combinées : la jurisprudence et les poursuites en responsabilité civile sont les voies empruntées habituellement aux États-Unis, mais les organismes de réglementation peuvent imposer des amendes très lourdes aux entreprises en infraction. En revanche, la tradition européenne repose sur des dispositions explicites en matière de sanctions plutôt que sur des procédures contentieuses.

[225] Edith Laget et al., « Deep Trade Agreements and Global Value Chains », *World Bank Group,* juin 2018, http://documents.worldbank.org/curated/en/356541529933295649/Deep-trade-agreements-and-global-value-chains.

Dans les deux cas, les chiffres comptent. Lorsqu'une approche coopérative de la réglementation laisse aussi la possibilité de réponses *ex post,* les sanctions doivent être classées par niveau : les sanctions sévères ont un effet dissuasif sur les contrevenants les plus importants ou les plus notoires. Le principal problème de cette approche est que la technologie numérique évolue, et par conséquent, que le volume et le nombre d'infractions peuvent prendre une ampleur énorme compte tenu du public concerné. **Or, les organismes de réglementation, les tribunaux et les autorités chargées de l'application de la loi ne changent pas d'échelle.** Et comme le grand public perçoit bon nombre des infractions comme une simple piqûre, voire ne les perçoit pas du tout, le nombre de plaintes ne reflète pas l'ampleur du problème. **Les recours collectifs *(class action)* sont nécessaires dans ce domaine.** Il faut également savoir si les données ont été recueillies illégalement, à quelle fin elles ont pu être utilisées et quel est le lien entre le préjudice subi et l'utilisation de ces données par une autre partie. Ces considérations sont importantes, car les **sanctions peuvent être soit proportionnelles à une infraction considérée comme tel, soit égales au montant réel du préjudice infligé.** Ceci est plus difficile à évaluer dans les affaires numériques.

Aux États-Unis, la *Federal Trade Commission* (FTC) dispose d'un grand pouvoir dissuasif et elle est très rarement contestée devant les tribunaux par les entreprises ciblées. Mais elle a utilisé ce pouvoir avec parcimonie dans le passé, en adoptant une approche progressive dans les affaires touchant à la vie privée. Elle opte souvent pour des accords négociés ou des « décrets consentis » *(consent decrees)* avec les entreprises de technologie numérique comme Facebook, Google, Microsoft, Twitter, Snapchat et Oracle[226], ce qui revient à

[226] William McGeveran, « Friending the Privacy Regulators », *Arizona Law Review* 58, n° 4 (2016): 959–1026, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820683.

placer l'entreprise concernée en liberté surveillée pendant une période pouvant aller jusqu'à 20 ans. Les récidives peuvent avoir des conséquences plus importantes : jusqu'à 16 000 dollars d'amende par infraction, un montant multiplié par des milliers ou des millions de cas. Jusqu'à récemment, les sanctions pour violation des règles de protection de la vie privée n'avaient jamais atteint le niveau des amendes infligées pour des pratiques anti-concurrentielles. Google a été condamné à une amende une première fois en 2011, puis à nouveau en 2012 pour la même infraction, et a dû payer 22,5 millions de dollars la deuxième fois. Ce montant a été considéré comme élevé à l'époque. Il est désormais éclipsé par l'amende de 5 milliards de dollars infligée le 24 juillet 2019 à Facebook (soit 9 % du chiffre d'affaires de Facebook en 2018) pour des pratiques trompeuses en matière de confidentialité qui étaient en partie liées à l'affaire Cambridge Analytica. De toute évidence, on assiste à un changement d'échelle, et les questions de protection de la vie privée sont désormais au même niveau que les affaires liées à la concurrence.

En Europe, une seule amende (celle de la CNIL contre Google) a dépassé la barre du million d'euros la première année. Il y a eu un autre cas au Danemark depuis, mais ironiquement, c'est le Royaume-Uni s'apprêtant à quitter l'UE, qui est passé à la vitesse supérieure en infligeant deux amendes de respectivement 99 et 283 millions d'euros, dans les deux cas pour des infractions touchant un grand nombre de particuliers.

Les poursuites en responsabilité civile, ou ce qu'un expert inspiré appelle « l'Internet des *torts* » *(internet of torts)* sont l'alternative aux sanctions. Le modèle est évidemment fondé sur la conception américaine en matière de protection de la vie privée axée sur le consommateur, et s'applique de plus en plus aux atteintes à la

sécurité des données émanant d'un fiduciaire de données, en d'autres termes, du gardien ou de l'exploitant des données. Le raisonnement est simple : **un fiduciaire de données (ou n'importe quelle entreprise) devrait prendre les précautions nécessaires si leur coût est inférieur au dommage résultant d'une violation, pondérées par la probabilité du dommage**[227]. Ce modèle est celui de la formule de Hand, qui a été utilisée pour la première fois en 1943 pour évaluer les dommages et la responsabilité dans l'affaire du naufrage d'une barge en 1943[228]. Elle procède d'une reconnaissance économique : les entreprises font des analyses coût/prix. Dans la pratique, la formule est plus difficile à appliquer. Elle l'est d'autant plus lorsqu'il s'agit d'évaluer le préjudice virtuel, moral ou de réputation susceptible de découler d'une atteinte à la vie privée.

Conclusion

Une grande partie de notre vie privée a disparu pour toujours, ou aussi longtemps que durera l'ère numérique. Tant que nos voisins eux-mêmes ne disposent pas (encore) de l'IA et d'algorithmes sophistiqués, il reste utile de réglementer la collecte et le traitement des données personnelles. Il y a de fortes chances que les entités les plus grandes et les plus sophistiquées, qu'il s'agisse de plateformes, d'entreprises numériques ou d'États bien dotés, contournent certaines de ces règles au moins une partie du temps, soit par des interprétations restrictives, soit en saturant les capacités

[227] Rebecca Crootof, « The Internet of Torts », *Duke Law Journal* 69, 26 février 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3342499.

[228] L'affaire U.S. vs Carroll Towing Co. est apparemment enseignée dans tous les cours de droit. United States v. Carroll Towing Co., 159 F.2d 169 (2d Cir. 1947), *Justia Law* (US Court of Appeals for the Second Circuit 1949), https://law.justia.com/cases/federal/appellate-courts/F2/159/169/1565896/

de mise en œuvre, soit tout simplement parce que les règles existantes ne couvrent pas les nouvelles catégories de données collectées et leur interprétation.

Ce qui précède n'est qu'un aperçu des problèmes pratiques et éthiques auxquels nous ferons face à l'ère numérique et de l'IA. Notre tour d'horizon s'est concentré sur la réglementation existante ou prévue, sur le présent ou l'avenir proche, et il présente déjà des lacunes flagrantes. Presque toutes les règles établies jusqu'à présent, de l'approche *top-down* de la Chine à l'approche cartésienne de l'Europe, sans oublier le *mix* indien, ne semblent aborder que les questions actuellement les plus importantes, telles que la protection de l'État ou de l'intérêt public, la sensibilisation et le consentement des utilisateurs ou la réglementation du traitement des données électroniques. Mais il faut le répéter, l'innovation et la technologie vont plus vite.

Ce qui suit est donc **une courte liste de propositions visant à améliorer ces règles.** Tracer la voie pour l'IA et concevoir le mélange d'incitations et de garde-fous dont elle aura besoin pour rester relativement inoffensive serait un travail d'une autre envergure. Cela requiert d'abord l'intervention de spécialistes de l'informatique qui comprennent ses potentialités et les processus à l'œuvre. Nous nous contenterons de formuler des propositions pour l'époque actuelle, telles qu'elles émergent du domaine que nous avons pu étudier.

Proposition 1 : Renforcer le contrôle, l'application et l'adaptabilité du RGPD

La première proposition découle d'un problème commun à toute législation européenne : **une règle ne saurait être meilleure que sa mise en œuvre réelle.**

Avec 28 autorités nationales de contrôle dont les niveaux de ressources diffèrent considérablement, cette proposition n'est pas facile. La conformité des décisions nationales avec le RGPD sera probablement mise à l'épreuve par des pourvois tels que celui qui est en cours devant la CJUE et qui concerne une loi sur la diffamation[229]. À travers ces recours, la question du guichet unique sera également mise à l'épreuve, parce que les autorités de contrôle affirment leur propre rôle. On peut soupçonner que les instances réglementaires les plus faibles seront plus laxistes, et donc plus souvent choisies comme centre d'activité des entreprises numériques.

Comme elle le fait actuellement dans plusieurs affaires, la CJUE reconnaît que, dans bien des cas, le RGPD n'établit pas le mécanisme de guichet unique. Le règlement distingue l'établissement officiel d'une entreprise de son centre réel de prise de décision et de contrôle. Par définition, la décision de la CJUE au sujet du RGPD dans sa rédaction actuelle est juridiquement fondée. Mais de là découle une

[229] Dans cette affaire, une dirigeante du parti autrichien des Verts visée par des commentaires diffamatoires (en vertu de la loi autrichienne) sur Facebook demande à la CJUE d'ordonner la suppression de ce commentaire et de commentaires identiques à l'échelle mondiale. Cette affaire renvoie également à la question du traitement automatisé

proposition : **un RGPD révisé devrait éviter les restrictions nuisant à un processus de décision unitaire.** Ce processus est fondamental pour qu'un marché unique du numérique voie le jour à l'avenir. Il a des implications importantes : **il faudrait définir des lignes directrices concernant les ressources budgétaires et humaines allouées par chaque État membre à son autorité de contrôle, en tenant compte de la taille du pays, mais également de la densité des acteurs numériques.** Il est intéressant de noter que l'Irlande, qui est un lieu d'établissement fréquent des entreprises numériques, au-delà de ce que sa taille justifierait, a pris les devants aussi bien dans l'application du RGPD que dans les décisions qu'elle a rendues. Une exigence de ressources supplémentaires ne lui poserait pas trop de problèmes.

Les rapports de la Commission européenne et du comité multipartite évaluant la première année d'application du RGPD soulignent tous deux le faible niveau des sanctions infligées jusque-là (comme nous l'avons vu, c'est l'autorité de contrôle du Royaume-Uni qui est passée à la vitesse supérieure au cours des derniers mois). Il est peut-être trop tôt pour en juger, car il subsiste des ambiguïtés et des malentendus possibles dans la mise en œuvre du RGPD. Des lignes directrices sont en cours de publication : il y aura un dilemme opposant la complexité et la mise en œuvre. **Il est difficile de mettre à jour et de remanier les réglementations en permanence si l'on veut que ces règles soient appliquées de façon universelle.** Tout comme la mise en péril du mécanisme de guichet unique affaiblirait le RGPD dans son ensemble, **les propositions nouvelles doivent mettre en priorité l'accent sur la clarté, la simplicité et la facilité de la mise en œuvre.** Elles ne suffiront pas à relever les défis fondamentaux posés par les technologies futures, mais le soutien du public en faveur du RGPD diminuera s'il n'est pas perçu comme efficace à court terme sur des questions visibles de tous.

Proposition 2 : Rendre les politiques de confidentialité plus lisibles et ergonomiques

Certaines des améliorations nécessaires sont évidentes. Ni le RGPD ni les lignes directrices qui en découlent ne font grand cas de l'expérience utilisateur (UX) lorsqu'ils visent l'objectif premier du RGPD : permettre aux particuliers de reprendre le contrôle de leurs données personnelles.

a. **Standardiser les formulaires d'avis de notification et de consentement qui apparaissent à l'écran.** Tout utilisateur actuel découvre rapidement que certains de ces formulaires sont plus ergonomiques et utilisables que d'autres. D'autres sont complexifiées par des étapes intermédiaires telles que la lecture de politiques de confidentialité provenant de différentes sources. Dans des cas extrêmes mais fréquents, il n'y a aucune possibilité de décider. Il s'agit plutôt d'une information d'*opt-in*.

b. **Les demandes de collecte de données en un ou plusieurs points doivent par défaut être d'*opt-out***, l'absence de réponse doit signifier *opt-out*, par exemple. En l'état actuel des choses, le considérant 32 du RGPD exige une action positive claire en faveur de l'*opt-in*, mais les cases d'*opt-in* cochées par défaut ne suffisent pas. Le fait de fermer ou d'ignorer une fenêtre ne doit pas constituer un tel signe.

c. Utilisation d'icônes ou de signes semi-alphabétiques : c'est d'ailleurs incontournable dans d'autres pays, où le taux d'analphabétisme est élevé. Tout comme les panneaux de signalisation routière sont normalisés et mémorisés, **la mise en place d'un code de conduite numérique atténuera le problème**

des politiques de confidentialité longues et formulées en des termes difficiles à comprendre.

d. **Applications d'IA facilitant le respect de la vie privée :** certaines applications permettent de lire et d'analyser les politiques de confidentialité. Il serait utile pour le public que ces applications soient examinées et éventuellement approuvées ou notées, et que les résultats soient publiés. Voici des exemples de ce type d'applications : *Guard*[230], une application neuronale qui analyse et évalue les conditions de confidentialité de sites connus ; *Terms of service; Didn't read (ToS; DR)*[231] , qui classe et évalue les sections en petits caractères des politiques de confidentialité de A à E (de la plus protectrice à la moins protectrice). Elle a été créée en faisant appel à la production participative et est évaluée par les utilisateurs.

Au-delà de ces exemples, **l'aide aux utilisateurs en matière de protection de la vie privée est un domaine de recherche qui devrait désormais être financé par les fonds publics de l'Union européenne.** Le projet *Personalized Privacy Assistant* de l'Université Carnegie Mellon[232], financé par la Defense Advanced Research Projects Agency (DARPA), l'U.S. Air Force, la National Science Foundation, Google et Yahoo, en est un équivalent américain. Ce projet est également membre d'un consortium plus vaste appelé *The Usable Privacy Project*[233].

---

[230] « Discover the Hidden Secrets in Privacy Policies | Guard », *Guard,* https://useguard.com.

[231] « Terms of Service; Didn't Read », *Tosdr,* https://tosdr.org/classification.html.

[232] « Personalized Privacy Assistant Project », *Privacyassistant.org* (Carnegie Mellon University, 2018), https://www.privacyassistant.org.

[233] « The Usable Privacy Policy Project », *Usableprivacy.org,* 2019, https://www.usableprivacy.org.

Proposition 3 : Assurer le respect effectif de la vie privée dès la conception *(privacy by design)*

a. Le RGPD a explicitement reconnu la *privacy by design* dans ses considérants 78 et 108 ainsi qu'à l'article 25. La *privacy by design* intègre les principes de minimisation des données, de limitation des finalités, de conservation et d'intégration du respect de la vie privée dès la première étape du cycle de vie d'un développement. Aucune ligne directrice officielle n'a été publiée mais le Contrôleur européen de la protection des données (CEPD) a rendu un avis en mai 2018[234]. Il prend acte de certaines recherches décrites ci-dessus et formule des recommandations, parmi lesquelles : garantir que **l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) dispose des ressources nécessaires pour encourager la recherche et l'interaction avec les entreprises privées ; multiplier les mesures d'incitation et expliciter les obligations, y compris les responsabilités légales » ; favoriser « la mise en place d'un inventaire et d'un observatoire de l'état des connaissances » de l'ingénierie de la vie privée » ; et publier des conseils à l'intention des contrôleurs de données.**

Ces suggestions de l'ENISA sont excellentes, mais elles sont formulées sous forme d'espoirs et non de prescriptions. La vérité est qu'une part écrasante des recherches sur le respect de la vie privée dès la conception, que ce soit dans le domaine des sciences sociales ou de l'innovation numérique, provient des États-Unis et est souvent menée dans le cadre de programmes associant une aide fédérale, des entreprises privées et des établissements

[234] « Avis préliminaire sur le respect de la vie privée dès la conception », *Contrôleur européen de la protection des données,* 31 mai 2018, https://edps.europa.eu/sites/edp/files/publication/18-05-31_preliminary_opinion_on_privacy_by_design_fr.pdf.

scientifiques. Une remarquable étude du Service de recherche du Parlement européen (EPRS) a débouché sur un rapport relatif à la responsabilité et la transparence des systèmes algorithmiques. Ce rapport indépendant, dont la recommandation la plus importante est d'encourager et de protéger les lanceurs d'alerte à l'intérieur des organisations, comprend 576 notes en fin de texte : elles proviennent essentiellement de la littérature américaine disponible[235].

b. Il est donc nécessaire de **renforcer la recherche et les liens entre les législateurs, les entreprises et la communauté scientifique** au-delà du niveau recommandé par l'Avis du CEPD. Les entreprises et les conseillers responsables de la conformité aux règles louent unanimement les vertus du concept de *privacy by design,* mais ils ne savent pas comment le mettre en œuvre. Assurément, il existe une tension au sein de chaque entreprise entre les objectifs commerciaux et la protection de la vie privée. Par eux-mêmes, les délégués à la protection des données ne sont peut-être pas assez influents pour garantir un juste équilibre entre ces objectifs. Le RGPD souligne l'importance des analyses d'impact internes relatives à la protection des données comme processus formel permettant d'identifier les risques ainsi que les mesures de contrôle et d'atténuation appropriées. Leur portée est plus restreinte que la *privacy by design*, et dans ce domaine, il existe en effet une ligne directrice antérieure du groupe de travail sur l'Article 29 qui a précédé l'EDPB[236]. Les compagnies d'assurance sont peut-être

[235] « A Governance Framework for Algorithmic Accountability and Transparency - Think Tank », *Service de recherche du Parlement européen,* avril 2019, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)624262.

[236] Commission européenne, « Lignes directrices sur l'analyse d'impact relative à la protection des données », 2017, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236.

les entreprises qui connaissent le mieux ce processus, puisqu'elles traitent des quantités énormes de données ayant des conséquences importantes pour la vie privée. La nécessité de lignes directrices et d'instructions de travail claires en matière de protection des données s'applique avant tout aux textes publics d'orientation : que ce soit dans le cadre de la prochaine directive « vie privée et communications électroniques » ou par le biais de nouvelles lignes directrices concernant le RGPD, c'est la manière la plus pragmatique de fournir aux entreprises, et en particulier à leurs délégués à la conformité des données, une feuille de route allant au-delà d'exigences abstraites.

Proposition 4 : Donner le droit effectif d'obtenir une explication dans le cadre du RGDP

a. Le considérant 71 prévoit que le public a le droit d'obtenir une explication quant aux décisions prises par un traitement automatisé. Les algorithmes sont comme des boîtes noires pour presque tous les utilisateurs. En ce qui concerne l'explication, le projet le plus important à ce jour est l'intelligence artificielle explicable *(Explainable Artificial Intelligence,* XAI), une initiative lancée en 2016 par la DARPA[237], l'agence même à l'origine d'ARPANET, le précurseur de l'Internet. Comme on pouvait s'y attendre, la majorité des objectifs et des programmes énoncés ne concernent pas le respect de la vie privée des utilisateurs. Le projet vise explicitement à améliorer l'efficacité du *deep learning* : « Les systèmes de *machine learning* auront la capacité d'expliquer leur logique, de caractériser leurs forces et leurs faiblesses, et de faire comprendre

[237] Matt Turek, « Explainable Artificial Intelligence », *Defense Advanced Research Projects Agency,* https://www.darpa.mil/program/explainable-artificial-intelligence.

leur comportement futur ». En ce sens, l'explicabilité publique aux utilisateurs individuels et sa mise en responsabilité ne sont qu'une retombée de ce programme. Plusieurs projets, tels que celui de la Texas A&M University sur la détection des *fake news,* ou de l'UC Berkeley sur les véhicules autonomes ou l'acquisition d'un « modèle mental raisonnablement précis des « politiques opératoires » des robots », et l'accent général mis sur l'aide à apporter aux utilisateurs pour qu'ils comprennent les principes des algorithmes qu'ils utilisent, ont des implications importantes pour l'explication des décisions aux individus.

L'application Credit Karma, qui permet de comprendre les cotes de crédit, est un exemple beaucoup plus terre-à-terre de l'explicabilité. D'autres outils ont été créés, tels que le score Match de Google sur Google Maps[238] ou Netflix Percent Match.

b. **Responsabilité des produits :** les garanties, l'obligation de ne pas porter tort, ont été une conséquence de la révolution industrielle. Dans la mesure où les données numériques concernent le commerce, et si nous admettons que nous n'en sommes plus au stade où les données personnelles ne peuvent pas être échangées, **c'est un bon modèle pour l'ère numérique également. Au lieu de nier le caractère commercial de nombreuses données personnelles, nous devrions adapter notre processus d'application à cette réalité.**

c. Le rapport de l'EPRS sur la responsabilité des algorithmes mentionné ci-dessus contient des suggestions politiques

[238] Mariella Moon, « Google Maps Can Predict How Much You'll like a Restaurant », *Engadget,* 31 juillet 2018, https://www.engadget.com/2018/07/31/google-maps-match-feature/.

intéressantes qui s'appliquent principalement au secteur public et à des exceptions fondées sur l'intérêt public. La première série de suggestions concerne la **sensibilisation par l'éducation, les organismes de surveillance et les lanceurs d'alertes**. Le rapport recommande des exceptions **permettant de rendre transparents *(reverse engineering)* les algorithmes lorsque l'intérêt public est en jeu.** Des affaires importantes allant de certains aspects de l'affaire Snowden à la mise en lumière des biais algorithmique par ProPublica[239] sont citées. On pourrait ajouter que l'ingénierie inverse a permis la découverte cruciale du logiciel utilisé par la Sécurité publique chinoise contre la population du Xinjiang[240]. Mais l'ingénierie inverse est souvent interdite par la loi ou exclue par les droits de propriété intellectuelle, et **il faudrait donc accorder des exemptions aux lanceurs d'alerte pour des motifs d'intérêt public.** On peut ajouter une autre proposition : **utiliser autant que possible le codage ouvert *(open source)* pour les logiciels intégrant des algorithmes.** La transparence est aussi devenue un facteur de cybersécurité, au contraire des millions de lignes de codage invérifiables. La tendance actuelle vers l'utilisation de codes *open source* associe davantage de cybersécurité à davantage de responsabilité dans la sphère publique. Pour vérifier l'innocuité des programmes, l'absence de logiciels malveillants ou d'extraits de code insérés dans le but de siphonner des données, des algorithmes et un codage *open source* sont nécessaires, sinon suffisants par eux-mêmes. En France, le rapport Villani sur l'IA a proposé **la création d'un groupe d'experts publics certifiés.**

[239] Julia Angwin, et al., « Machine Bias », *ProPublica,* 23 mai 2016, https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing.

[240] « China's Algorithms of Repression | Reverse Engineering a Xinjiang Police Mass Surveillance App », *Human Rights Watch,* 1er mai 2019, https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass-surveillance

Ceux-ci pourraient effectuer des audits d'algorithmes et de bases de données ainsi que des tests ; ils pourraient être sollicités dans le cadre d'une procédure judiciaire.

À l'inverse, **pour la transmission de données personnelles confidentielles ou sensibles, le cryptage de bout en bout est une proposition fréquente,** même s'il n'est pas totalement inviolable : il reste vulnérable aux deux extrémités, et l'informatique quantique pourrait prochainement sonner le glas des codes de cryptage sûrs. Le contre-argument est bien évidemment la nécessité de découvrir les activités criminelles et de les empêcher de s'enfoncer dans l'obscurité *(going dark)*. **Ces débats ne doivent pas être éludés, mais ils ne doivent pas non plus avoir lieu uniquement dans des situations de crise. L'objectif de respect de la vie privée recule alors devant celui de la sécurité.**

En résumé, l**a transparence est nécessaire pour les algorithmes publics qui permettent de prendre des décisions concernant des individus. Avec les logiciels libres, il est plus difficile de dissimuler des codes-espions et autres logiciels malveillants,** à condition qu'il y ait bien sûr un contrôle régulier. Cela s'applique aux programmes de collecte, d'interprétation et d'utilisation des données. *A contrario,* l'**opacité est nécessaire à la transmission et à la conservation de données privées, qu'elles appartiennent à des particuliers ou à des entreprises. Dans ce cas, le cryptage de bout en bout est une approche souhaitable.** Des exceptions dues à des considérations d'ordre public ne devraient être envisagées qu'avec prudence et l'indispensable présence d'un contrôle indépendant.

Proposition 5 : Créer la possibilité de recours en responsabilité et dommages[241]

L'Union européenne a eu l'habitude d'évaluer les sanctions antidumping selon la « règle du droit moindre » : les sanctions devaient être juste suffisantes pour compenser le préjudice réel causé par les marchandises sous-évaluées, au lieu d'être fondées sur le montant total du *dumping*[242]. Le caractère flagrant des pratiques de dumping des sociétés chinoises sur le marché de l'UE a suscité un débat sur les méthodes d'évaluation des sanctions antidumping. Les amendes énormes infligées dans d'autres domaines par les organismes de réglementation américains à des entreprises non américaines et le montant colossal des liquidités des géants informatiques de la Silicon Valley ont sans doute incité la Commission européenne à repenser le montant des amendes fondées sur des violations du droit de la concurrence. **Les pratiques juridiques et réglementaires européennes se trouvent dans une période de transition bienvenue entre ces deux approches. Ce phénomène fait partie d'une tendance plus large, mais s'applique également au domaine des violations de la vie privée.** Aux États-Unis, dans le cas de l'amende infligée à Facebook en 2019, la FTC a relevé avec fierté que cette amende était 20 fois supérieure au second montant jamais infligé à travers le monde pour atteinte à la vie privée et qu'un tribunal n'aurait probablement pas statué en faveur d'un

[241] *Tort and litigation* qui peut se traduire par des actions en responsabilité délictuelle et en contentieux

[242] François Godement, « China's Market Economy Status and the European Interest », *European Council on Foreign Relations,* 23 juin 2016, p. 7, https://www.ecfr.eu/page/-/ECFR_180_-_CHINA_MARKET_ECONOMY_STATUS_AND_THE_EUROPEAN_INTEREST_%28002%29.pdf.

tel changement d'échelle. Le montant de cette amende était perçu comme un signal lancé à toutes les entreprises[243].

L'autre action *ex post* est le recours en dommages. La formule de Hand, mentionnée précédemment, qui repose sur l'évaluation de la proportionnalité et tient compte de la taille de l'entreprise, est un bon début. Le rapport de l'EPRS contient de bonnes propositions tant sur la responsabilité des algorithmes que sur les contentieux. Il exhorte les **États membres à s'efforcer de faire preuve d'une plus grande responsabilité publique avec les algorithmes qu'ils utilisent pour prendre des décisions.** Des exemples existent, tels que la publication de la formule de calcul de l'impôt en France. Compte tenu des nouvelles techniques qui apparaissent, des consultations publiques et des analyses d'impact périodiques sont requises. La consolidation de données à caractère personnel provenant de sources et d'entreprises privées ayant conclu un marché public, ainsi que le traitement arithmétique et algorithmique effectué ultérieurement par ces organismes publics sur des données collectées à titre privé, devraient faire l'objet d'une attention particulière.

La même exigence de transparence totale **ne s'applique pas au secteur privé et aux entreprises privées, en partie parce qu'elle est difficile à mettre œuvre et aussi parce qu'elle peut aller à l'encontre des intérêts commerciaux des entreprises, les algorithmes étant une fonction vitale de celles-ci.** Sur ce point, le rapport va dans le sens américain sur la question essentielle des recours en responsabilité délictuelle et en dommages : **« il serait préférable**

[243] Lesley Fair, « FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making », *Federal Trade Commission,* 24 juillet 2019, https://www.ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history.

d'établir un cadre de responsabilité juridique qui permette aux prestataires de services d'accepter une plus grande responsabilité délictuelle en échange d'exigences réduites en matière de transparence et d'analyse de l'impact algorithmique »[244]. Enfin, le rapport s'intéresse aux initiatives mondiales, dans ce qu'il appelle la « quatrième révolution industrielle (…) : la course aux armements de l'IA. » Il propose d'adopter **« une position forte dans les négociations commerciales pour protéger la capacité réglementaire d'enquêter sur les systèmes algorithmiques et de tenir les parties responsables des violations des lois européennes et des droits de l'homme ».** Il propose de créer une Organisation Internationale de l'Intelligence Artificielle sur le modèle de l'Union internationale des télécommunications (UIT) existante. Cette proposition est le fruit de l'inspiration de quatre chercheurs, dont trois vivent et travaillent en Amérique et un au Royaume-Uni.

Nous soutenons fermement la proposition de l'EPRS visant à renforcer la responsabilité délictuelle *ex post* tout en limitant les nouvelles exigences imposées aux entreprises privées en matière de responsabilité algorithmique.

[244] « A Governance Framework for Algorithmic Accountability and Transparency - Think Tank », *Service de recherche du Parlement européen,* avril 2019, p. 73, http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_STU(2019)624262.

Proposition 6 : Introduire des réglementations sectorielles

Certains secteurs ont besoin d'une réglementation spécifique ou plus précise. Le secteur de la santé, les services financiers, les données de la police en font partie. Ce but est en partie atteint avec la directive de l'UE, également appelée directive « Police-Justice », qui a été adoptée en 2016, avant le RGPD[245]. En tant que directive, elle doit être transposée dans les lois des États membres, et elle est donc sujette à interprétation. Néanmoins, **des procédures sont en cours devant la CJUE concernant la légalité de la collecte et de la conservation à grande échelle de données de surveillance par la police et les services de renseignement.** Elles ont été introduites par le Royaume-Uni (à la suite d'une contestation de Privacy International) et par les hautes juridictions administratives françaises et belges (à la suite de poursuites d'ONG) afin de vérifier la légalité de leurs actions nationales. Des audiences approfondies sont en cours[246].

Dans d'autres secteurs, il y a les exemples du DISHA, le vaste projet de loi sur la réglementation des données de santé en cours de discussion en Inde, ou de la HIPAA, le *Health Insurance Accountability and Portability Act* américain de 1996 sur la responsabilité et la portabilité de l'assurance maladie. En ce qui concerne la protection des données dans le secteur financier, les États-Unis ont pris les devants dès 1999 dans le cadre d'une loi plus large sur la

[245] « Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 », *EUR-Lex,* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680.

[246] Bill Goodwin, « European Court to Decide on Legality of Bulk Phone and Internet Surveillance », *Bill Goodwin,* 13 septembre 2019, https://www.computerweekly.com/news/252470666/European-court-to-decide-on-legality-of-bulk-communications-surveillance.

modernisation de la finance, le *Gramm-Leach-Bliley Financial Modernization Act.* **Encourager l'adoption de règles sectorielles dans certains cas** ne signifie pas nécessairement que l'UE doive approuver l'extraordinaire dédale de réglementations État par État qui s'ensuit souvent aux États-Unis.

Proposition 7 : Créer des données de santé simulées pour améliorer l'anonymisation

Notre focus sur la protection des données de santé reflète une préoccupation universelle dans tous les systèmes. Dans la recherche de compromis ou des meilleures solutions, **les données de santé simulées apparaissent comme un moyen technologique de gérer les échecs de l'anonymisation et de la pseudonymisation.** Un exemple a été développé par Simulacrum, avec le soutien de grandes entreprises pharmaceutiques, pour gérer les données de patients atteints d'un cancer transmises par *Public Health England* (PHE). Cela est d'autant plus important que le *National Health Service* du Royaume-Uni a déjà été critiqué pour avoir transmis des données à Deepmind, c'est-à-dire en fin de compte à Google. Grâce à la nouvelle technique, les données sont d'abord anonymisées et regroupées en lots d'au moins 50 échantillons par PHE. Transférées à Simulacrum, les données sont ensuite synthétisées de manière à ne jamais reproduire un patient réel. **Cette couche supplémentaire concilie le besoin de recherche sur les *big data* et la garantie de confidentialité des données.** Elle mérite donc d'être étudiée et étendue. Inévitablement, le résultat ne peut être meilleur que l'algorithme utilisé, et certains détails et associations de données risquent d'être perdus dans le processus.

REMERCIEMENTS

Cette étude des débats sur le respect de la vie privée numérique doit beaucoup à la liberté précieuse accordée à l'auteur pour le temps de la recherche et pour son écriture. L'étude n'aurait pas non plus été possible sans l'aide de **Meeta Tarani**, stagiaire et chargée de mission, et **Viviana Zhu,** chargée d'étude, qui ont participé à la recherche et émis des observations précieuses durant la rédaction. A un moment ou un autre, **Gilles Babinet, Eric Chaney, Théodore Christakis, Mathieu Duchâtel, Marie-Anne Frison-Roche, Théophile Lenoir, Angèle Malâtre-Lansac, Laure Millet, Victor Poirier,** et **Stefan Soesanto** ont apporté des éclairages et proposé des perspectives utiles.

Personnes auditionnées

- **Andrea Carrera Mariscal**, Juriste Protection des Données Personnelles, Orange S.A.
- **Mathieu Coulaud**, Directeur Juridique, Microsoft France
- **Olivier Esper,** Responsable des Affaires Gouvernementales et de la Politique Publique, Google France
- **Christophe Fessart,** Délégué à la Protection des Données, Enedis
- **Clotilde Jolivet,** Directrice des Relations Gouvernementales France, Sanofi
- **Franck Perraudin,** Directeur Affaires Publiques Asie, Sanofi
- **Jean-Renaud Roy,** Directeur des Affaires Publiques, Microsoft France
- **Ralf Sauer,** Chef Adjoint de l'Unité Flux Internationaux et Protection des Données, DG Justice et Consommateurs, Commission Européenne
- **Fabien Venries,** Responsable de la Privacy et du Marketing Stream, Orange Group

Enfin, une relecture minutieuse a été effectuée par **Pierre Pinhas**, et cette étude vous a été présentée grâce à l'**équipe de communication** de l'Institut Montaigne.

Les opinions exprimées dans cette étude n'engagent ni les personnes précédemment citées ni les institutions qu'elles représentent.

LES PUBLICATIONS DE L'INSTITUT MONTAIGNE

- Transition énergétique: faisons jouer nos réseaux (décembre 2019)
- Religion au travail : croire au dialogue - Baromètre du Fait Religieux Entreprise 2019 (novembre 2019)
- Taxes de production : préservons les entreprises dans les territoires (octobre 2019)
- Médicaments innovants : prévenir pour mieux guérir (septembre 2019)
- Rénovation énergétique : chantier accessible à tous (juillet 2019)
- Agir pour la parité: performance à la clé (juillet 2019)
- Pour réussir la transition énergétique (juin 2019)
- Europe-Afrique : partenaires particuliers (juin 2019)
- Media polarization « à la française »? Comparing the French and American ecosystems (mai 2019)
- L'Europe et la 5G : le cas Huawei (partie 2, mai 2019)
- L'Europe et la 5G : passons la cinquième ! (partie 1, mai 2019)
- Système de santé : soyez consultés ! (avril 2019)
- Travailleurs des plateformes : liberté oui, protection aussi (avril 2019)
- Action publique : pourquoi faire compliqué quand on peut faire simple (mars 2019)
- La France en morceaux : baromètre des Territoires 2019 (février 2019)
- Énergie solaire en Afrique : un avenir rayonnant ? (février 2019)
- IA et emploi en santé : quoi de neuf docteur ? (janvier 2019)
- Cybermenace : avis de tempête (novembre 2018)
- Partenariat franco-britannique de défense et de sécurité : améliorer notre coopération (novembre 2018)
- Sauver le droit d'asile (octobre 2018)
- Industrie du futur, prêts, partez ! (septembre 2018)
- La fabrique de l'islamisme (septembre 2018)
- Protection sociale : une mise à jour vitale (mars 2018)
- Innovation en santé : soignons nos talents (mars 2018)
- Travail en prison : préparer (vraiment) l'après (février 2018)
- ETI : taille intermédiaire, gros potentiel (janvier 2018)
- Réforme de la formation professionnelle : allons jusqu'au bout ! (janvier 2018)
- Espace : l'Europe contre-attaque ? (décembre 2017)
- Justice : faites entrer le numérique (novembre 2017)
- Apprentissage : les trois clés d'une véritable transformation (octobre 2017)
- Prêts pour l'Afrique d'aujourd'hui ? (septembre 2017)
- Nouveau monde arabe, nouvelle « politique arabe » pour la France (août 2017)
- Enseignement supérieur et numérique : connectez-vous ! (juin 2017)
- Syrie : en finir avec une guerre sans fin (juin 2017)

- Énergie : priorité au climat ! (juin 2017)
- Quelle place pour la voiture demain ? (mai 2017)
- Sécurité nationale : quels moyens pour quelles priorités ? (avril 2017)
- Tourisme en France : cliquez ici pour rafraîchir (mars 2017)
- L'Europe dont nous avons besoin (mars 2017)
- Dernière chance pour le paritarisme de gestion (mars 2017)
- L'impossible État actionnaire ? (janvier 2017)
- Un capital emploi formation pour tous (janvier 2017)
- Économie circulaire, réconcilier croissance et environnement (novembre 2016)
- Traité transatlantique : pourquoi persévérer (octobre 2016)
- Un islam français est possible (septembre 2016)
- Refonder la sécurité nationale (septembre 2016)
- Bremain ou Brexit : Europe, prépare ton avenir ! (juin 2016)
- Réanimer le système de santé - Propositions pour 2017 (juin 2016)
- Nucléaire : l'heure des choix (juin 2016)
- Un autre droit du travail est possible (mai 2016)
- Les primaires pour les Nuls (avril 2016)
- Le numérique pour réussir dès l'école primaire (mars 2016)
- Retraites : pour une réforme durable (février 2016)
- Décentralisation : sortons de la confusion / Repenser l'action publique dans les territoires (janvier 2016)
- Terreur dans l'Hexagone (décembre 2015)
- Climat et entreprises : de la mobilisation à l'action / Sept propositions pour préparer l'après-COP21 (novembre 2015)
- Discriminations religieuses à l'embauche : une réalité (octobre 2015)
- Pour en finir avec le chômage (septembre 2015)
- Sauver le dialogue social (septembre 2015)
- Politique du logement : faire sauter les verrous (juillet 2015)
- Faire du bien vieillir un projet de société (juin 2015)
- Dépense publique : le temps de l'action (mai 2015)
- Apprentissage : un vaccin contre le chômage des jeunes (mai 2015)
- Big Data et objets connectés. Faire de la France un champion de la révolution numérique (avril 2015)
- Université : pour une nouvelle ambition (avril 2015)
- Rallumer la télévision : 10 propositions pour faire rayonner l'audiovisuel français (février 2015)
- Marché du travail : la grande fracture (février 2015)
- Concilier efficacité économique et démocratie : l'exemple mutualiste (décembre 2014)
- Résidences Seniors : une alternative à développer (décembre 2014)
- Business schools : rester des champions dans la compétition internationale (novembre 2014)

- Prévention des maladies psychiatriques : pour en finir avec le retard français (octobre 2014)
- Temps de travail : mettre fin aux blocages (octobre 2014)
- Réforme de la formation professionnelle : entre avancées, occasions manquées et pari financier (septembre 2014)
- Dix ans de politiques de diversité : quel bilan ? (septembre 2014)
- Et la confiance, bordel ? (août 2014)
- Gaz de schiste : comment avancer (juillet 2014)
- Pour une véritable politique publique du renseignement (juillet 2014)
- Rester le leader mondial du tourisme, un enjeu vital pour la France (juin 2014)
- 1 151 milliards d'euros de dépenses publiques : quels résultats ? (février 2014)
- Comment renforcer l'Europe politique (janvier 2014)
- Améliorer l'équité et l'efficacité de l'assurance-chômage (décembre 2013)
- Santé : faire le pari de l'innovation (décembre 2013)
- Afrique-France : mettre en œuvre le co-développement
  Contribution au XXVI[e] sommet Afrique-France (décembre 2013)
- Chômage : inverser la courbe (octobre 2013)
- Mettre la fiscalité au service de la croissance (septembre 2013)
- Vive le long terme ! Les entreprises familiales au service de la croissance et de l'emploi (septembre 2013)
- Habitat : pour une transition énergétique ambitieuse (septembre 2013)
- Commerce extérieur : refuser le déclin
  Propositions pour renforcer notre présence dans les échanges internationaux (juillet 2013)
- Pour des logements sobres en consommation d'énergie (juillet 2013)
- 10 propositions pour refonder le patronat (juin 2013)
- Accès aux soins : en finir avec la fracture territoriale (mai 2013)
- Nouvelle réglementation européenne des agences de notation : quels bénéfices attendre ? (avril 2013)
- Remettre la formation professionnelle au service de l'emploi et de la compétitivité (mars 2013)
- Faire vivre la promesse laïque (mars 2013)
- Pour un « New Deal » numérique (février 2013)
- Intérêt général : que peut l'entreprise ? (janvier 2013)
- Redonner sens et efficacité à la dépense publique
  15 propositions pour 60 milliards d'économies (décembre 2012)
- Les juges et l'économie : une défiance française ? (décembre 2012)
- Restaurer la compétitivité de l'économie française (novembre 2012)

- Faire de la transition énergétique un levier de compétitivité (novembre 2012)
- Réformer la mise en examen Un impératif pour renforcer l'État de droit (novembre 2012)
- Transport de voyageurs : comment réformer un modèle à bout de souffle ? (novembre 2012)
- Comment concilier régulation financière et croissance : 20 propositions (novembre 2012)
- Taxe professionnelle et finances locales : premier pas vers une réforme globale ? (septembre 2012)
- Remettre la notation financière à sa juste place (juillet 2012)
- Réformer par temps de crise (mai 2012)
- Insatisfaction au travail : sortir de l'exception française (avril 2012)
- Vademecum 2007 – 2012 : Objectif Croissance (mars 2012)
- Financement des entreprises : propositions pour la présidentielle (mars 2012)
- Une fiscalité au service de la « social compétitivité » (mars 2012)
- La France au miroir de l'Italie (février 2012)
- Pour des réseaux électriques intelligents (février 2012)
- Un CDI pour tous (novembre 2011)
- Repenser la politique familiale (octobre 2011)
- Formation professionnelle : pour en finir avec les réformes inabouties (octobre 2011)
- Banlieue de la République (septembre 2011)
- De la naissance à la croissance : comment développer nos PME (juin 2011)
- Reconstruire le dialogue social (juin 2011)
- Adapter la formation des ingénieurs à la mondialisation (février 2011)
- « Vous avez le droit de garder le silence… » Comment réformer la garde à vue (décembre 2010)
- Gone for Good? Partis pour de bon ? Les expatriés de l'enseignement supérieur français aux États-Unis (novembre 2010)
- 15 propositions pour l'emploi des jeunes et des seniors (septembre 2010)
- Afrique - France. Réinventer le co-développement (juin 2010)
- Vaincre l'échec à l'école primaire (avril 2010)
- Pour un Eurobond. Une stratégie coordonnée pour sortir de la crise (février 2010)
- Réforme des retraites : vers un big-bang ? (mai 2009)
- Mesurer la qualité des soins (février 2009)

- Ouvrir la politique à la diversité (janvier 2009)
- Engager le citoyen dans la vie associative (novembre 2008)
- Comment rendre la prison (enfin) utile (septembre 2008)
- Infrastructures de transport : lesquelles bâtir, comment les choisir ? (juillet 2008)
- HLM, parc privé
  Deux pistes pour que tous aient un toit (juin 2008)
- Comment communiquer la réforme (mai 2008)
- Après le Japon, la France…
  Faire du vieillissement un moteur de croissance (décembre 2007)
- Au nom de l'Islam… Quel dialogue avec les minorités musulmanes en Europe ? (septembre 2007)
- L'exemple inattendu des Vets
  Comment ressusciter un système public de santé (juin 2007)
- Vademecum 2007-2012
  Moderniser la France (mai 2007)
- Après Erasmus, Amicus
  Pour un service civique universel européen (avril 2007)
- Quelle politique de l'énergie pour l'Union européenne ? (mars 2007)
- Sortir de l'immobilité sociale à la française (novembre 2006)
- Avoir des leaders dans la compétition universitaire mondiale (octobre 2006)
- Comment sauver la presse quotidienne d'information (août 2006)
- Pourquoi nos PME ne grandissent pas (juillet 2006)
- Mondialisation : réconcilier la France avec la compétitivité (juin 2006)
- TVA, CSG, IR, cotisations…
  Comment financer la protection sociale (mai 2006)
- Pauvreté, exclusion : ce que peut faire l'entreprise (février 2006)
- Ouvrir les grandes écoles à la diversité (janvier 2006)
- Immobilier de l'État : quoi vendre, pourquoi, comment (décembre 2005)
- 15 pistes (parmi d'autres…) pour moderniser la sphère publique (novembre 2005)
- Ambition pour l'agriculture, libertés pour les agriculteurs (juillet 2005)
- Hôpital : le modèle invisible (juin 2005)
- Un Contrôleur général pour les Finances publiques (février 2005)
- Les oubliés de l'égalité des chances (janvier 2004 - Réédition septembre 2005)

Pour les publications antérieures se référer à notre site internet :
www.institutmontaigne.org

INSTITUT
MONTAIGNE

ABB FRANCE
ABBVIE
ACCURACY
ACTIVEO
ADIT
AIR FRANCE – KLM
AIR LIQUIDE
AIRBUS GROUP
ALLEN & OVERY
ALLIANZ
ALVAREZ & MARSAL FRANCE
AMAZON WEB SERVICES
ARCHERY STRATEGY CONSULTING
ARCHIMED
ARDIAN
ASTORG
ASTRAZENECA
A.T. KEARNEY
AUGUST DEBOUZY
AVRIL
AXA
BAKER & MCKENZIE
BANK OF AMERICA MERRILL LYNCH
BEARINGPOINT
BESSÉ
BNP PARIBAS
BOLLORÉ
BOUGARTCHEV MOYNE ASSOCIÉS
BOUYGUES
BRUNSWICK
CAISSE DES DÉPÔTS
CAPGEMINI
CAPITAL GROUP
CAREIT
CARREFOUR
CASINO
CHAÎNE THERMALE DU SOLEIL
CHUBB
CIS
CISCO SYSTEMS FRANCE
CMA CGM
CNP ASSURANCES
COHEN AMIR-ASLANI
COMPAGNIE PLASTIC OMNIUM
CONSEIL SUPÉRIEUR DU NOTARIAT
CORREZE & ZAMBEZE
CRÉDIT AGRICOLE
CRÉDIT FONCIER DE FRANCE
D'ANGELIN & CO. LTD
DASSAULT SYSTEMES
DE PARDIEU BROCAS MAFFEI
DENTSU AEGIS NETWORK
DRIVE INNOVATION INSIGHTS - DII
EDF
EDHEC BUSINESS SCHOOL
EDWARDS LIFESCIENCES FRANCE
ELSAN
ELSEVIER SCIENCES
ENEDIS
ENGIE
EQUANCY
ETHIQUE & DEVELOPPEMENT
EURAZEO
EUROGROUP CONSULTING
EUROSTAR
FIVES
FONCIÈRE INEA
GALILEO GLOBAL EDUCATION FRANCE
GETLINK
GIDE LOYRETTE NOUEL
GOOGLE
GRAS SAVOYE
GROUPAMA
GROUPE EDMOND DE ROTHSCHILD
GROUPE M6
GROUPE ORANGE
HAMEUR ET CIE
HENNER
HSBC FRANCE
IBM FRANCE
IFPASS
ING BANK FRANCE
INSEEC
INTERNATIONAL SOS
INTERPARFUMS
IONIS EDUCATION GROUP
ISRP
JEANTET & ASSOCIÉS
KANTAR
KATALYSE

SOUTIENNENT L'INSTITUT MONTAIGNE

INSTITUT
MONTAIGNE

KPMG S.A.
LA BANQUE POSTALE
LA PARISIENNE ASSURANCES
LAZARD FRÈRES
LINEDATA SERVICES
LIR
LIVANOVA
L'ORÉAL
LOXAM
LVMH - MOËT-HENNESSY - LOUIS VUITTON
M.CHARRAIRE
MACSF
MALAKOFF MÉDÉRIC
MAREMMA
MAZARS
MCKINSEY & COMPANY FRANCE
MÉDIA-PARTICIPATIONS
MEDIOBANCA
MERCER
MERIDIAM
MICHELIN
MICROSOFT FRANCE
MITSUBISHI FRANCE
NATIXIS
NEHS
NESTLÉ
NEXITY
OBEA
ODDO BHF
ONDRA PARTNERS
ONET
OPTIGESTION
ORANO
ORTEC GROUP
PAI PARTNERS
PRICEWATERHOUSECOOPERS
PRUDENTIA CAPITAL
RADIALL
RAISE
RAMSAY GÉNÉRALE DE SANTÉ
RANDSTAD
RATP
RELX GROUP
RENAULT
REXEL
RICOL LASTEYRIE CORPORATE FINANCE
RIVOLIER
ROCHE
ROLAND BERGER
ROTHSCHILD MARTIN MAUREL
SAFRAN
SANOFI
SCHNEIDER ELECTRIC
SERVIER
SGS
SIA PARTNERS
SIACI SAINT HONORÉ
SIEMENS
SIER CONSTRUCTEUR
SNCF
SNCF RÉSEAU
SODEXO
SOFINORD-ARMONIA
SOLVAY
SPRINKLR
STAN
SUEZ
SYSTEMIS
TALAN
TECNET PARTICIPATIONS SARL
TEREGA
THE BOSTON CONSULTING GROUP
TILDER
TOTAL
TRANSDEV
UBER
UBS FRANCE
UIPATH
VEOLIA
VINCI
VIVENDI
VOYAGEURS DU MONDE
WAVESTONE
WENDEL
WILLIS TOWERS WATSON
WORDAPPEAL

SOUTIENNENT L'INSTITUT MONTAIGNE

Imprimé en France
Dépôt légal : décembre 2019
ISSN : 1771-6756
Achevé d'imprimer en décembre 2019

INSTITUT
MONTAIGNE

COMITÉ DIRECTEUR

PRÉSIDENT

Henri de Castries

VICE-PRÉSIDENTS

David Azéma Associé, Perella Weinberg Partners
Jean-Dominique Senard Président, Renault
Emmanuelle Barbara *Senior Partner,* August Debouzy
Marguerite Bérard Directeur du pôle banque de détail en France, BNP Paribas
Jean-Pierre Clamadieu Président du Comité exécutif, Solvay
Olivier Duhamel Président, FNSP (Sciences Po)
Marwan Lahoud Associé, Tikehau Capital
Fleur Pellerin Fondatrice et CEO, Korelya Capital, ancienne ministre
Natalie Rastoin Directrice générale, Ogilvy France
René Ricol Associé fondateur, Ricol Lasteyrie Corporate Finance
Arnaud Vaissié Co-fondateur et Président-directeur général, International SOS
Florence Verzelen Directrice générale adjointe, Dassault Systèmes
Philippe Wahl Président-directeur général, Groupe La Poste

PRÉSIDENT D'HONNEUR

Claude Bébéar, Fondateur et Président d'honneur, AXA

INSTITUT
MONTAIGNE

IL N'EST DÉSIR PLUS NATUREL QUE LE DÉSIR DE CONNAISSANCE

Données personnelles comment gagner la bataille

« Les gentlemen ne lisent pas le courrier des autres ». En réalité, ils le font parfois, légalement ou subrepticement. Comment dès lors rétablir une forme de garantie de la vie privée ? Cette garantie est devenue une préoccupation omniprésente. Légalement, elle s'exprime au moyen de la protection des données personnelles, et occupe une place centrale dans les réglementations et les débats qui y ont trait.

Ce débat a deux matrices. L'une est aux États-Unis, où sont nés la notion de privacy et les premiers textes. L'autre est l'Europe, avec son règlement général sur la protection des données (RGPD), notre sujet principal. Mais les choix de l'Inde et de la Chine sur le respect de la vie privée numérique vont aussi influencer nos acteurs et déterminer si la libre circulation des données sera compatible avec nos principes.

Nous envisageons le secteur de la santé comme étude de cas. Les Européens doivent se préparer à des changements radicaux dans le domaine médical et pharmaceutique, parfois au détriment de leur préférence traditionnelle pour le respect de la vie privée. Enfin, cette étude se conclut par sept propositions afin d'améliorer le RGPD.

Institut Montaigne
59, rue La Boétie - 75008 Paris
Tél. +33 (0)1 53 89 05 60 – www.institutmontaigne.org

10 €
ISSN 1771-6764
Décembre 2019