



4.0 Les mutations clés en perspective

Au-delà des thèmes transversaux, il y a un certain nombre de mutations qui ont été identifiées lors des ateliers. Leur impact varie selon la situation géographique et le domaine d'activité. Cependant, elles ont toutes été considérées comme étant significatives lors de nombreuses discussions. Les mutations sont illustrées dans le graphique ci-dessous et sont énumérées ci-après :

1. Culture des données et culture numérique : une perspective éclairée sur les données, leur mode d'acquisition et d'utilisation augmente le niveau de confiance du public, permet de dissiper les malentendus et améliore le processus de prise de décision.

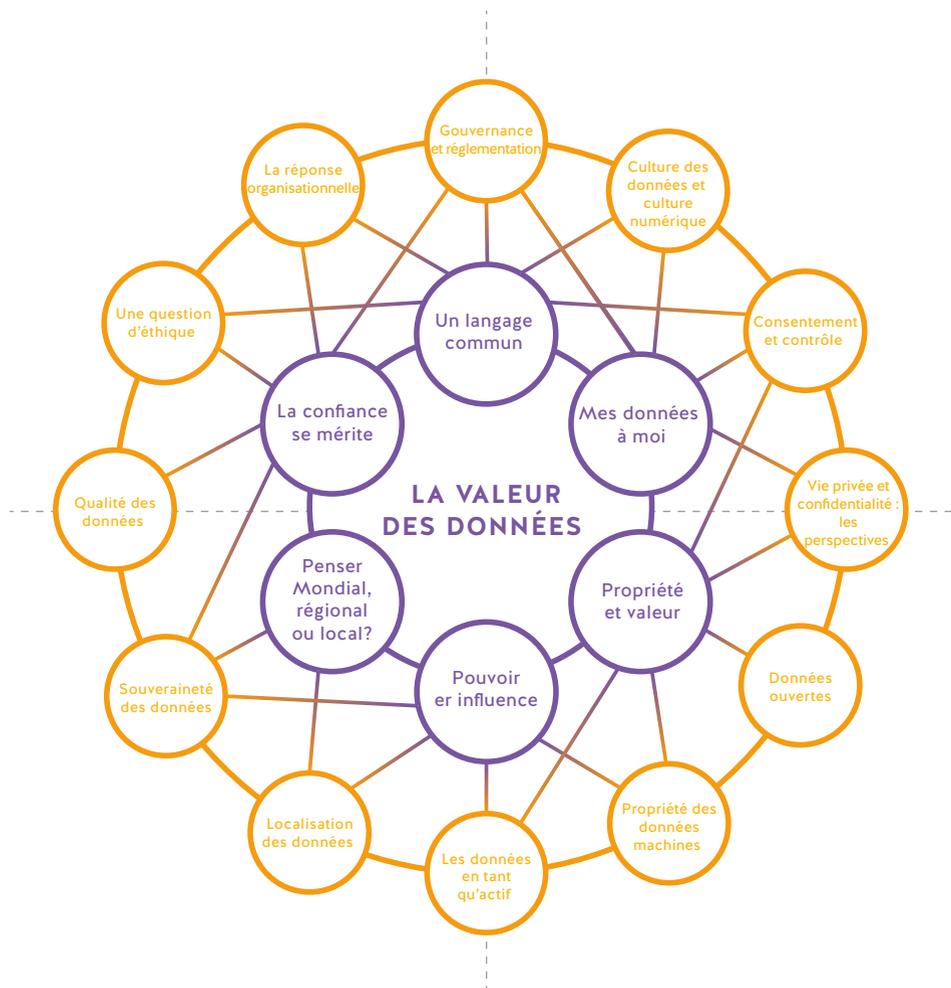
2. Perspectives en matière de confidentialité et de vie privée : il y a une forte conviction chez certains, liée au droit à la confidentialité des données. D'autres cependant, pensent que dans une ère de sécurité exacerbée, il s'agit d'un concept paradoxal et dépassé.

3. Consentement et contrôle : si le consentement éclairé n'est pas une option viable en tant que condition préalable à l'exploitation des données, il faudrait alors repenser notre perception de la finalité première poursuivie à travers le consentement, ainsi nous pourrions identifier une nouvelle approche.

4. Données ouvertes : la dynamique autour des données ouvertes est freinée par la privatisation des données publiques et les préoccupations sécuritaires croissantes. Cela va limiter durablement le potentiel des données.

5. Propriété des données machine : les discussions autour des droits de propriété liés à l'internet des objets (IdO) se font de plus en plus passionnées. Des enjeux liés aux droits, au contrôle et à l'exploitation des données poussent de nombreux secteurs d'activité à emprunter des voies différentes.

6. Les données en tant qu'actifs : les organisations sont tenues de justifier les données qu'elles possèdent et celles auxquelles elles ont accès. Elles doivent soumettre des rapports sur leurs portefeuilles de données et sont passibles d'impôts sur ces actifs.



7. Localisation des données : les pays estiment qu'il est judicieux de posséder des copies des données sur les citoyens et des données machine dans des centres régionaux. Les gouvernements et les entreprises cherchent à accéder aux données détenues par des compagnies étrangères.

8. Souveraineté des données : de plus en plus de gouvernements voient le contrôle des données nationales comme un moyen de protéger les droits des citoyens, de développer l'économie et de maintenir un sens de l'identité culturelle.

9. Qualité des données: alors que nous recherchons une vision plus claire, des préoccupations liées aux biais, aux données de faible qualité ou aux fausses nouvelles se font plus pressantes. Nettoyer et valider les données est un enjeu sur les plans social, politique et commercial.

10. Une question d'éthique : l'utilisation éthique des données pose problème, nous essayons toutefois de nous accorder sur une approche mondiale. Les acteurs des différents secteurs d'activité établissent leurs propres normes et tentent de s'aligner sur des principes communs.

11. La réponse organisationnelle : la gestion des données requiert une approche des affaires, digne du 21^{ème} siècle, et non une approche obsolète du 19^{ème} siècle. Le numérique est en passe de devenir la norme, nous sommes en train de dépasser progressivement les principes axés sur des produits physiques.

12. Gouvernance et réglementation : les préoccupations croissantes autour de l'utilisation des données influencent l'opinion publique. Les décideurs politiques souhaitent une approche mieux concertée à la réglementation, à la gouvernance et à l'obligation réditionnelle.

4.1 Culture des données et culture numérique



Une perspective éclairée sur les données, et la façon dont elles sont acquises et utilisées, augmente la confiance du public, permet de dissiper les malentendus et facilite la prise de décisions.

Contexte

À une époque où une pléthore de technologies est en train de remplacer les capacités humaines, beaucoup de participants à nos ateliers estiment qu'il est urgent d'assurer une meilleure compréhension publique, politique et organisationnelle de la valeur et de l'utilisation des données. Les régulateurs doivent être mieux informés, les travailleurs ont besoin de meilleures compétences techniques, et les citoyens doivent être équipés pour gérer leur empreinte numérique afin de mieux s'engager dans les services publics et de se protéger contre d'éventuels abus. Comment aborder cette question et contrer ce qui est considéré comme une fracture numérique qui ne cesse de s'élargir ? Cette problématique a suscité dix-neuf discussions distinctes sur la culture numérique au cours du projet sur la valeur future des données.

Trois perspectives différentes sur la culture des données ont été débattues lors de ces discussions :

- **Maturité réglementaire** : Y a-t-il une compréhension suffisante des enjeux chez les décideurs pour gérer avec succès la transition vers les technologies numériques et l'impact des technologies numériques ? Les régulateurs peuvent-ils mieux soutenir la culture numérique ?

Dans l'ensemble, il a été reconnu que la réglementation sera probablement toujours à la traîne par rapport à la technologie, et donc afin d'être aussi bien préparés que possible pour la transition prévue vers un environnement de travail plus automatisé, une collaboration plus étroite entre les entreprises et les décideurs est essentielle. A Lagos, Nairobi et Bangkok en particulier, on s'inquiète de ce que, sans une meilleure compréhension technique, les décideurs aient du mal à vraiment comprendre et gérer les changements économiques et sociaux à venir. Pour promouvoir cette option, qui fait l'objet d'une forte adhésion, l'idée d'une plus grande collaboration entre les régulateurs nationaux a été suggérée. Plusieurs participants ont proposé



qu'un organisme mondial, ou plus probablement régional, établisse un cadre éducatif, des normes claires d'apprentissage du numérique et fournisse un espace de partage des meilleures pratiques.

La plupart des participants à nos ateliers estiment qu'une meilleure compréhension du potentiel des données pour stimuler la croissance économique, façonnera ce que nous apprenons et comment nous apprenons. À Londres, il a été observé que l'enseignement d'éléments fondamentaux de la logique et du raisonnement et la mise en place d'un modèle de base pour la formation des adultes au numérique est une priorité pour un certain nombre de gouvernements.²⁷ En effet, un point de vue communément admis est que, la culture numérique est si importante qu'une formation élémentaire en codage fera bientôt partie du programme scolaire commun, au même titre que les mathématiques et les langues. À Madrid, la recommandation est qu'à côté des compétences pratiques, une meilleure compréhension de l'éthique, du contrôle et de la confidentialité soit assurée. Les participants ont observé que la génération des *Millennials* sera probablement la première à bénéficier des changements de politique, et compte tenu de cela, nous pourrions faire face à un fossé générationnel, car il y aura des personnes qui seront incapables de s'adapter aux changements technologiques à venir. Les gouvernements devront s'y préparer.

- **Travailleurs actifs** : notre économie, notre société et nos ressources humaines disposent-elles des compétences et atouts nécessaires à l'ère numérique ? Avons-nous besoin de former ou de mettre à niveau les travailleurs afin qu'ils puissent participer activement à l'économie numérique ?

Avoir et maintenir les bonnes compétences est essentiel pour faire face aux changements technologiques.²⁸ Comme la technologie est très adaptable, la capacité des machines à identifier

les modèles et tendances et à surpasser les humains en matière de reconnaissance d'images devrait fortement affecter les employés, qu'ils soient hautement qualifiés ou peu formés. En conséquence, les travailleurs de demain, y compris l'élite la plus instruite, pourraient avoir besoin de s'assurer que les compétences qu'ils apprennent viennent compléter celles qui sont facilement reproduites par les machines, et rester flexibles et ouverts à l'apprentissage de nouvelles compétences.²⁹ De nombreux participants ont estimé qu'il n'y a pas suffisamment de sensibilisation du public à la rapidité avec laquelle le changement s'impose à nous, et qu'en conséquence les nouvelles compétences qui seront bientôt nécessaires sont peu comprises ou mal connues.

Un certain nombre d'entreprises ont déjà leurs propres plateformes d'apprentissage pour tenir le personnel à jour ; IBM, par exemple, dispose d'une Académie de l'IA qui recommande des cours à partir d'un programme d'études fourni par Coursera. Cependant, certains estiment que, bien qu'utile, cette forme de « mise à niveau » ne fera qu'accroître le fossé entre ceux qui sont déjà dans l'élite professionnelle et ceux qui ont moins d'opportunités. Le véritable besoin, ont-ils fait valoir, est une « requalification » de la main-d'œuvre au sens large. Le manque de culture numérique pourrait impliquer que les travailleurs non qualifiés se retrouvent complètement exclus du monde du travail, car leurs fonctions peuvent être exécutées plus efficacement et de manière plus rentable par les machines. Dans ce sens, l'idée que les entreprises s'impliquent plus activement dans les programmes de formation, a été largement soutenue.

- **Citoyens éclairés** : Comment s'assurer que les citoyens peuvent comprendre et gérer les avantages et les risques de l'utilisation et du partage des données ? Comment l'éducation peut-elle les aider à naviguer sur Internet et sur les plateformes numériques et à s'engager dans les médias sociaux ?

À Madrid, Copenhague, San Francisco et Singapour, il a été estimé que la priorité de tout programme public de culture numérique ne devrait pas être de permettre aux individus de maîtriser une compétence particulière ou de devenir compétents dans une certaine plate-forme technologique, mais plutôt de les équiper pour prospérer dans une société de plus en plus numérique. Enseigner aux citoyens à gérer leur ombre numérique et les aider à mieux comprendre comment se protéger contre la fraude, devrait, selon eux, être une priorité nationale.

Ce que nous ont dit les participants

La fracture numérique

De Washington DC à Tokyo, de Bangkok à Sydney et de Manille à Johannesburg, des inquiétudes ont été soulevées au sujet de ceux qui n'auront pas accès à l'éducation numérique. A Tokyo, la perspective est que « *le fossé entre les personnes numériquement compétentes et les personnes qui ne maîtrisent pas le numérique représentera un énorme défi et sera lourd de conséquences s'il n'est pas résorbé* ». ³⁰ De même, à Washington DC, les participants nous ont dit que « *dans 10 ans, la société sera plus compétente sur le plan numérique, dans l'ensemble, mais l'adaptation sera inégale, en partie, en raison de la motivation du public, mais aussi à cause du manque d'opportunités. Par conséquent, la menace d'une augmentation des inégalités demeure une forte possibilité* ». ³¹ Il y a déjà un écart important à combler en matière de formation numérique. Un certain nombre de pays que nous avons visités ne peuvent toujours pas garantir ne serait-ce qu'une éducation de base pour tous leurs citoyens. Cela a été observé à Pretoria, où les participants ont souligné que, bien qu'il existe un énorme besoin d'éducation au numérique, la priorité dans certains domaines devrait être de commencer par le déploiement et l'intégration des programmes de développement de la petite enfance. Ce n'est qu'une fois que les enfants savent lire et écrire, que l'éducation numérique peut être abordée, « *un*

ordinateur, c'est juste une boîte si vous ne savez pas comment l'utiliser ». En Inde, il a été observé que la technologie peut également aider à atteindre ceux qui étaient auparavant coupés de l'éducation, et qu'il faudrait de nouvelles initiatives pour introduire des programmes mobiles de formation.

Une approche globale

La plupart des acteurs s'accordent sur le fait qu'il est nécessaire d'établir des normes mondiales communes : « *nous avons besoin d'une réglementation harmonisée* », ou du moins, des meilleures pratiques en matière de culture des données, mais on ne s'attend guère à ce que cela se produise de sitôt. Certains pensent que les choses se mettront en place spontanément avec le temps. ³² D'abord articulé à Bangkok, puis repris dans d'autres marchés, l'hypothèse que « *nous finirons par comprendre les exigences éducatives nécessaires pour faire face à un monde axé sur les données, et continuer à construire des plates-formes d'éducation éthique qui seront accessibles à tous* » a été avancée. Tout le monde ne partage pas ce point de vue. Certains pensent plutôt qu'il sera difficile pour les citoyens de vraiment comprendre comment gérer au mieux leurs propres données personnelles sans qu'il y ait des changements dans la façon dont les données personnelles sont gérées de manière globale. Ils ont plaidé en faveur d'une réglementation qui clarifie les modalités d'utilisation des données personnelles.

« Il doit y avoir différents points d'entrée à l'éducation numérique, à la fois par le biais des écoles et aussi à travers la formation continue pour ceux qui retournent dans le système éducatif »

Atelier de Copenhague

La passivité des entreprises

A Washington DC, les participants estiment que « *nous devons trouver des moyens de connecter les gens à la culture des données, de façon concrète. Les entreprises doivent aussi comprendre cela, et les Big Tech en particulier, devraient prendre leur part de responsabilité. Si l'on n'adopte pas une approche universelle de cette problématique, il y a un risque que les inégalités augmentent* ». A Copenhague, les participants ont souligné qu'il doit y avoir différents points d'entrée à l'éducation numérique, à la fois par le biais des écoles et aussi à travers la formation continue pour ceux qui retournent dans le système éducatif. « *Pour remédier à cette situation, la future politique devrait permettre l'apprentissage tout au long de la vie (en proposant plus de compétences techniques, interdisciplinaires, de meilleures méthodologies de recherche et de meilleurs réseaux), puis une intégration plus complète des connaissances numériques multidisciplinaires.* » Le fait de ne pas s'attaquer au problème risque de provoquer le scénario douloureux d'une hausse du chômage combinée à des pénuries de compétences.

A Bogota, compte tenu du fait que les emplois de l'avenir seront différents, on estime qu'il en sera de même de nos besoins éducatifs. Étant donné que la technologie remplacera probablement bon nombre des emplois traditionnels, au lieu de se concentrer sur les réalisations purement académiques, ils ont recommandé qu'il y ait également un accent sur les compétences dont nous aurons besoin pour travailler dans le futur : « *la façon dont nous éduquons nos enfants devra changer pour s'adapter aux besoins d'une société plus technique où les compétences telles que la collaboration, et des qualités plus douces telles que l'intégrité et la compassion, et pas seulement de meilleures compétences en mathématiques et en codage, auront une plus grande valeur. Jusqu'à présent, cet aspect n'est pas assez bien compris dans le secteur public, de sorte qu'il est difficile pour les organismes de réglementation d'élaborer des politiques appropriées qui offriront des avantages à long terme.* »

A Dakar, les perspectives sont optimistes. Ils estiment qu'avec le bon type de soutien politique, l'investissement dans la culture des données offre aux économies africaines l'occasion de rattraper les pays comme la Chine, la Corée et Singapour, qui ont déjà eu beaucoup de succès dans l'innovation en matière de données. « *Nous devons être prêts à construire une génération numériquement compétente. Nos jeunes devraient commencer à apprendre à coder. Ils doivent apprendre à travailler numériquement et plus efficacement* ». Cette perspective a été reprise à Lagos. L'urgence du développement est telle qu'ils estiment que la priorité devrait être « d'enseigner aux Nigériens comment accéder à Internet, l'explorer et y naviguer. L'éducation à la sécurité est moins importante » . Inversement, à Washington DC, on craint que les décideurs ne considèrent pas actuellement la culture numérique comme une priorité : « *promouvoir une dynamique de renforcement de la culture du numérique ne serait pas de trop, car cela démontrerait comment le numérique peut être un moteur de changement social.* »

Une affaire de génération

Pour l'avenir, certains ont suggéré qu'une plus grande culture numérique viendra tout simplement avec le temps. « *La dernière génération est intrinsèquement plus sophistiquée. Elle comprend implicitement une société axée sur les données et sait comment se protéger. De même, la prochaine génération de décideurs sera plus sophistiquée* ». ³³ Cependant, à Madrid, on a estimé que, bien que techniquement compétents, les jeunes peuvent ne pas avoir la maturité émotionnelle pour faire face aux implications sociales des nouvelles technologies. Pour remédier à cette situation, les participants ont suggéré que « *les jeunes fassent preuve de maturité émotionnelle avant d'être autorisés à intervenir dans des sites de média sociaux* ». ³⁴ Ils ont également affirmé que l'éducation du public devrait par conséquent, mettre l'accent sur la philosophie, la théorie critique, l'éthique et l'anthropologie, afin de fournir aux étudiants les compétences nécessaires pour participer à un nouveau contrat social.

Vérité et illusion

La provenance et l'authenticité des données sont des préoccupations majeures qui ont été abordées lors de nos discussions, et le débat visant à déterminer les acteurs responsables et comptables, garants de la véracité et de l'exactitudes des données a été en bonne place dans nos échanges. Certains ont affirmé que la confusion dans ce domaine menace déjà les valeurs démocratiques et la confiance dans le gouvernement, qu'il faudrait donc sensibiliser le public à ce sujet. Les initiatives pour y remédier comprennent des programmes de formation numérique, la création d'espaces sûrs en ligne, et un moyen controversé, actuellement en vigueur en Ouganda, la taxation de l'utilisation des médias sociaux. En effet, lors de l'atelier de Nairobi, cette mesure fiscale a été considérée comme un moyen de limiter la liberté d'expression.³⁵ L'atelier de Madrid a proposé « *un étiquetage plus clair et de meilleures conditions, pour aider les gens à comprendre comment leurs données personnelles sont utilisées et gérées. Nous pourrions même envisager d'étiqueter le contenu en utilisant des systèmes à code couleur, comme cela se fait dans les secteurs de l'alimentation et de l'énergie* ». Les participants de Singapour étaient d'accord en principe avec cette option, mais ont souligné que « *l'étiquetage aidera certes à déterminer où se trouve la vérité, et peut-être que l'estampillage des informations d'actualité permettra d'identifier les chaînes responsables. Cependant, tout cela dépendra du maintien de la confiance du public dans les médias établis* ».

Prise de conscience et compréhension

On espère qu'une plus forte culture des données se traduira par un plus grand engagement du public en ligne, ce qui donnera aux citoyens un meilleur accès à une gamme de services publics, notamment liés à la santé et aux soins sociaux, à l'éducation et aux transports. À Santiago, on a également fait valoir qu'une plus grande transparence, une plus grande responsabilisation et sensibilisation du public

à l'importance des données et à l'utilisation des données par le gouvernement agiront comme un moyen de surveiller le comportement des entreprises, en particulier en ce qui concerne l'utilisation de l'IA. « *Lorsque le public est plus impliqué, la redevabilité devient « horizontale » plutôt que verticale* ». Au fur et à mesure que la prise de conscience augmentera, il sera possible de « *surveiller le surveillant* » et de « *comprendre les enjeux de manière critique* », ainsi les grandes organisations de toutes sortes se verront obligées de modérer leurs actions et d'être plus sensibles à ce qui est considéré comme acceptable, tant en ligne qu'hors ligne.

Enjeux pour la valeur des données

Aucune des problématiques mises en évidence par nos recherches : la nécessité pour les décideurs et les organismes de réglementation de mieux appréhender les nouvelles technologies et leurs enjeux, pour les travailleurs d'améliorer leurs compétences numériques, et pour les citoyens de mieux comprendre les conséquences potentielles de la manière dont leurs données sont collectées et utilisées, ne peut avoir une solution miracle. Elles nécessitent un certain temps d'évolution et de maturation. Mais la reconnaissance de plus en plus large de leur importance représente un pas en avant. Le triple programme d'amélioration de la culture numérique représente un plan d'action et d'amélioration notable. Il s'agit d'un préalable nécessaire à une économie saine, axée sur les données, qui elles-mêmes constituent un fondement essentiel du fonctionnement efficace de l'économie, tout comme la lecture, l'écriture et l'arithmétique constituaient des fondements essentiels de l'ère industrielle.

4.2 Culture, gouvernance et vie privée



Les différences de culture et de mode de gouvernance impliquent des attitudes différentes à l'égard de la notion de vie privée. Certains sont convaincus du droit à la confidentialité des données, d'autres pensent qu'il s'agit d'un concept paradoxal et dépassé.

Contexte

Une plus grande disponibilité et un meilleur accès aux données ont modifié les attitudes à l'égard de la confidentialité et de la sécurité des données. Nos ateliers ont révélé une diversité d'opinions à ce sujet, en fonction de la géographie, la culture et l'âge. Il y a un large éventail de points de vue sur la définition de la vie privée en tant que telle. Quels sont les enjeux ? Craint-on un « fouinage » inconséquent et injustifié ? Voudrait-on garder secrètes des informations potentiellement embarrassantes ? Nos libertés civiles seraient-elles menacées ? S'agit-il du risque que quelqu'un utilise nos informations privées pour nous nuire ou nuire à quelqu'un d'autre ? Lors de nos échanges, des tendances se sont clairement dégagées séparant ceux qui estiment que la protection de la vie privée est un droit

humain durement conquis et qu'il faut le protéger et ceux qui soutiennent que, dans ce monde axé sur les données, garantir la vie privée est irréaliste et peut même compromettre la sécurité nationale.

Les institutions européennes telles que l'UE et internationales telles que l'ONU, ainsi que plusieurs gouvernements, croient fermement en la vie privée, en tant que droit humain. Mais tout le monde ne partage pas cet avis. Les conversations menées à Abuja, Dakar, Tokyo, Jakarta et Singapour ont révélé une certaine ambivalence sur la question. Dans les deux ateliers organisés aux États-Unis, il y a eu un soutien à la « doctrine des tiers » (Third Party Doctrine), qui a longtemps régi la loi sur la vie privée et qui dispose qu'il ne peut y avoir aucune attente de confidentialité sur les données qui sont partagées avec un tiers. À Shanghai, on nous a dit que, bien que les perceptions soient en train d'évoluer, la vie privée n'est pas considérée comme importante en Chine. En effet, il n'y a pas de traduction directe en mandarin de l'expression « vie privée », le mot yinsi, qui en est la traduction approximative, est principalement associé au secret et à une santé mentale déficiente.



Comme pour un grand nombre de nos discussions, l'établissement d'un consensus a été compliqué par un manque de clarté au niveau du langage et par les implications de la notion de protection de la vie privée dans la pratique. Le concept est abstrait et touche de multiples questions, y compris les implications pour la sécurité nationale, la protection des mineurs, les réflexions sur les barrières légitimes fixées à ceux qui ont accès aux données et à ceux qui en profitent, et sur de nombreux domaines très spécifiques, tels que les données de l'IdO ou la reconnaissance faciale. En outre, les généralisations sont inutiles parce que la vie privée est définie par son contexte. Cela ne signifie pas le secret absolu, puisque nous partageons des informations sensibles avec les médecins, les amis, la famille, mais lorsque nous révélons des informations dans un contexte, nous ne nous attendons pas à ce qu'elles nous surprennent dans une toute autre situation.

Chez les défenseurs de la vie privée, il y a un paradoxe de plus en plus marqué entre protection de la vie privée et personnalisation des services. Alors que nous voulons avoir des produits et des services qui sont adaptés à nos besoins et à nos activités, nous insistons également pour que nos données restent privées, partagées uniquement quand nous le voulons et seulement avec les acteurs que nous choisissons. Certaines personnes, celles qui ne soutiennent pas forcément la protection de la vie privée, estiment que la notion de « vie privée » est un anachronisme, un concept qui s'est insensiblement dilué dans le cours des événements et qui n'avait peut-être pas beaucoup d'importance au départ. D'autres le considèrent comme d'une importance cruciale, définissant la forme et l'avenir de toute l'ère de l'Internet. Bien que les récentes atteintes à la protection des données et les manchettes qui en découlent aient sensibilisé le public à ce sujet, cela n'a pas encore eu d'influence notable sur les comportements. Ainsi, les décideurs sont confrontés à un dilemme : devraient-ils légiférer sur la base de la façon dont les citoyens se comportent réellement en ligne, appliquer un ensemble d'archétypes idéalisés, ou suggérer comment ils devraient

se comporter ? D'après nos ateliers, à mesure que la prise de conscience de la quantité de nos données personnelles qui sont échangées en ligne se précisera, on saura plus précisément quels sont les informations que les gens sont réellement prêts à partager et avec qui, en échange d'un meilleur service ou d'une meilleure qualité de vie.

À ce jour, le programme de protection de la vie privée est axé sur l'exploitation des données à caractère personnel, c'est-à-dire la collecte, l'utilisation et l'extraction de la valeur des données par les entreprises. Cependant, la collecte et l'utilisation des données par les gouvernements est une activité en plein essor d'autant plus que la prise de décisions axées sur les données, y compris l'IA est adoptée de plus en plus largement. Pour les gouvernements, à condition que les bons freins et contrepoids soient en place, il y a d'énormes avantages. Cela peut aider à combler les déficits financiers et les besoins d'investissement visant à améliorer les soins de santé, les systèmes de transport et les services publics, par exemple. La mutation est si prégnante que certains des participants à nos ateliers ont estimé que les démocraties devront recueillir des données non seulement pour l'amélioration des services publics, mais aussi pour rester compétitives. Si l'Occident promulgue des lois trop strictes sur la protection de la vie privée, il disposera de moins de données, une matière première clé pour l'intelligence artificielle, et par conséquent, se mettra dans une position désavantageuse par rapport à la Chine, où la surveillance devient omniprésente.

Dans certains cas, les différences juridiques en matière de protection des données personnelles constituent un obstacle commercial inattendu et limitent l'innovation. L'entrée en vigueur récente du RGPD dans l'UE, a été en partie, prévue pour répondre à cette situation. Il n'est pas aisé de se conformer à ce règlement. Cependant, il est clair que, pour la première fois, les lourdes amendes et les dénonciations publiques de non-conformité donnent aux régulateurs une allure plus terrifiante

qu'elle n'a pu l'être par le passé et fait peser sur les entreprises une obligation encore plus impérieuse de renforcer le contrôle des processus numériques pour mieux canaliser les flux de données.³⁶ De nombreux régulateurs sont désireux d'apprendre des succès et des échecs du RGPD, et sont en train d'observer sa mise en œuvre avec intérêt.

Changement générationnel

Quel que soit le point de vue, aujourd'hui, les attitudes vis-à-vis de la vie privée en ligne évoluent pendant que la génération cadette, qui n'a pas connu la vie avant l'Internet, est en train de murir. Cela ne signifie pas qu'il y aura une harmonie. Encore une fois, nous avons constaté des divergences d'opinion sur les perspectives en matière de vie privée, alors que le monde lutte pour trouver un équilibre entre la vie privée, le confort et la sécurité. À Londres, il a été suggéré qu'en raison de la nature quasi obligatoire des services de données inédits et attrayants, il y a de fortes chances que la protection de la vie privée, telle que nous la connaissons, même en Europe, ne soit plus une préoccupation. A l'atelier de Johannesburg les participants ont adopté l'approche inverse, faisant valoir que l'évolution de la culture numérique chez les citoyens et les États conduira à une meilleure compréhension des conséquences négatives du partage excessif de données, et donc les sensibilités au sujet de la vie privée pourraient s'exacerber. Il y avait aussi des divergences quant à la façon de gérer cela³⁷. Certains voient que les solutions techniques telles que le cryptage garantiront le maintien du droit à la vie privée, mais d'autres préconisent une plus grande transparence afin que les individus soient mieux informés et, par conséquent, mieux en mesure de contrôler la façon dont leurs données sont utilisées.

Une approche mondiale ?

Le grand défi qui nous attend est de savoir si la protection de la vie privée peut être abordée par le biais d'accords mondiaux. Il est généralement reconnu qu'il y a un besoin à ce niveau. Alors que les différentes régions cherchent toutes à faire progresser la réglementation des données en s'inspirant de l'APEC et du RGPD, l'émergence d'un cadre mondial de protection de la vie privée est défendue par ceux qui recherchent un meilleur contrôle et une plus grande transparence. Le Forum économique mondial n'est qu'une des nombreuses organisations qui tentent de développer une approche internationale, collaborative et globale.³⁸ Les principaux domaines d'intérêt sont une réelle transparence, le renforcement de la responsabilisation et de l'autonomisation des personnes. L'inventeur du Web, Sir Tim Berners Lee, travaille également sur la question. Il préconise un nouveau « Contrat pour le Web », qui vise à protéger les droits et libertés des personnes. Il stipule que les gouvernements doivent s'assurer que leurs citoyens ont accès à l'ensemble de l'Internet, tout le temps, et que leur vie privée est respectée, afin qu'ils puissent être en ligne « librement, en toute sécurité, et sans crainte ». Comme Sir Berners Lee l'observe lui-même, « aucun groupe ne devrait s'isoler pour le faire, toutes les contributions seront appréciées ».

Inévitablement, tous les pays ou même les départements n'évoluent pas à la même vitesse et dans la même direction, de sorte qu'il est probable que la réglementation régionale se poursuive pendant un certain temps. En Amérique, par exemple, la Constitution des États-Unis ne contient aucune protection explicite de la vie privée, de sorte que le pouvoir judiciaire a cherché des moyens de relier les protections constitutionnelles existantes avec les questions de protection de la vie privée de l'époque, telles que la protection du quatrième amendement contre les perquisitions et les saisies abusives. Malgré les appels d'un parterre de PDG pour une meilleure législation politique, les États-fédéraux américains sont à la traîne par rapport à d'autres régions. Cette question pourrait être abordée si

d'autres États suivent l'exemple donné par la récente Loi sur la protection des données personnelles des consommateurs de Californie (California Consumer Privacy Act - CCPA). Cependant, l'envie de changement pourrait être faible. La vie privée n'a pas été considérée comme une priorité lors des discussions de nos ateliers de San Francisco et de Washington DC. Cela est constaté en dépit des contributions de chercheurs tels que Pew qui soutiennent que les américains se soucient bien des problèmes liés à la vie privée, c'est qu'ils ne savent pas comment y faire face.³⁹

La Chine et l'Inde, qui ont chacun plus d'internautes que l'Europe ou l'Amérique ont de citoyens, ont des approches divergentes et contradictoires de la vie privée. Fait intéressant, l'Inde, l'un des pays les plus peuplés du monde, a adopté une approche quelque peu contradictoire à l'égard de la législation sur la protection des données personnels. Le pays a récemment annoncé un projet de loi sur la protection des données. Les entreprises et le gouvernement devront généralement respecter des principes juridiques similaires à ceux de l'UE, et comme pour le RGPD, cette loi s'appliquerait à toutes les entités, partout dans le monde, qui traitent les données des Indiens. En même temps, il est également favorable à la localisation des données et exige que les données des Indiens restent à l'intérieur des frontières nationales. Des règles inspirées de la politique chinoise sont également prévues pour étendre les pouvoirs de surveillance de l'État. En Mars 2019, le gouvernement a mis en place un projet de politique de commerce électronique, faisant valoir que les données personnelles des Indiens devraient être traitées comme un actif « national ».⁴⁰

En Chine, bien que jusqu'en 2018, la loi n'ait pas défini les éléments à considérer comme des données personnelles, les obligations en matière de sécurité ainsi que les responsabilités sont en train de se préciser en raison de l'inquiétude du public concernant l'impact du vol de données, et de l'ambition des entreprises chinoises telles que TenCent et Alibaba

de conquérir les marchés occidentaux. Ces objectifs viennent se mettre en travers des activités de surveillance chères au gouvernement chinois et ont suscité le resserrement des règles de protection des données pour les entreprises tout en facilitant pour le gouvernement la captures des informations privées.

Compte tenu de ces enjeux complexes, il n'est pas surprenant que certains pensent que les entreprises considèrent ces problématiques de confidentialité comme un avantage concurrentiel. La campagne de marketing 2019 d'Apple lancée au CES de Las Vegas, comprend un argument majeur en matière de protection de la vie privée : « Ce qui se passe dans votre iPhone, reste dans votre iPhone ». Récemment, Facebook a promis que le contenu de tous les messages sera crypté, sur toutes ses plateformes.

« Les Nigériens ne sont pas rassurés sur les questions de vie privée, c'est la raison pour laquelle beaucoup se protègent en ayant un alias en ligne, cela les aide à se prémunir contre des groupes de pression et de la surveillance du gouvernement ».

Atelier d'Abuja

Ce que nous ont dit les participants

La fracture numérique

Nos ateliers ont révélé que les attitudes nationales à l'égard de la protection de la vie privée varient selon les niveaux de confiance. A Tokyo, on nous a dit que *« les gens sont prêts à échanger des informations sur eux-mêmes pour une vie meilleure. Au pire, cela leur est égal. Comme nous partageons toujours plus de données, dans dix ans, les préoccupations au sujet de la vie privée vont s'estomper davantage »*.

À Jakarta, on nous dit que *« l'Indonésie est un pays où les gens sont très partageurs, et même sur le plan culturel, les Indonésiens ont tendance à « surpartager »* ». En Afrique, les réactions étaient similaires. A Dakar, par exemple, on a observé *« qu'en Europe, la vie privée est une grande préoccupation. Il y a des raisons historiques à cela. Nous sommes une société plus ouverte »*. En revanche, à Lagos, les participants nous ont dit que *« les Nigériens ne sont pas rassurés sur les questions de vie privée, c'est la raison pour laquelle beaucoup se protègent en ayant un alias en ligne, cela les aide à se prémunir contre des groupes de pression et de la surveillance du gouvernement »*.

Certains suggèrent que le concept de vie privée est en train de perdre de son attrait. A Londres, une suggestion a été que *« l'augmentation massive des données permettra une personnalisation massive. Il n'y aura plus de vie privée, en raison de la nature impérieuse des services disponibles, lorsqu'on y renonce »*. Il a également été souligné qu'il faudra du temps pour que cela devienne culturellement acceptable. *« Le changement sera plus lent que prévu. La technologie des données est à l'apogée de son cycle de vie (hype cycle). Un certain réalisme autour de ses limites finira par émerger »* A Manille, il a été observé que ce genre de démonstration de force

par les entreprises et les nantis pourrait *« conduire à une période d'austérité en matière de données. La façon dont nous gérons la protection de la vie privée à l'ère numérique sera donc un déterminant clé de la valeur future des données »*.

Quel que soit le point de vue, aujourd'hui, les attitudes vis-à-vis de la vie privée en ligne évoluent pendant que la génération cadette, qui n'a pas connu la vie avant l'Internet, est en train de murir. Encore une fois, nous avons constaté des divergences d'opinion sur les perspectives en matière de vie privée. À Londres, il a été suggéré, qu'en raison de la nature quasi obligatoire des services fournis, la vie privée, telle que nous la connaissons deviendra une problématique dépassée. Il y a de fortes chances que *« les données de tous deviennent la propriété de chacun »*. A Bangalore, on ne partage pas ce point de vue, on estime plutôt que *« la protection de la vie privée deviendra une problématique publique. La surveillance exercée par les Etats sera de plus en plus préoccupante et l'on s'interrogera sur les moyens de minimiser les méfaits de l'accès des gouvernements à « toutes » les données »*.

« La façon dont nous gérons la protection de la vie privée à l'ère numérique sera donc un déterminant clé de la valeur future des données »

Atelier de Manille

Choix en matière de réglementation

Il y a d'innombrables avantages à partager les données notamment pour comprendre les mécanismes des déficits financiers et les besoins en investissements destinés aux systèmes de transport et aux services publics. Mais le danger d'une surveillance excessive inquiète encore beaucoup de monde. Bien que la technologie soit souple, sans les limites et contrepois appropriés, il est encore possible de faire du mal en se servant des données. A Dakar, les participants ont suggéré « *qu'il y ait des règles claires sur les données à collecter sur les finalités recherchées. Il faut que l'on soit en mesure de protéger les personnes vulnérables* ». Par exemple, bien que les responsables des forces de l'ordre puissent utiliser l'IA pour identifier les criminels, cela peut aussi signifier qu'ils (ou d'autres) sont en mesure d'écouter les citoyens ordinaires. Les gouvernements chinois et américain sont en train de mettre en place la reconnaissance faciale pour « tracer » leurs citoyens. Certains considèrent qu'ils vont un peu trop loin.⁴¹ Beaucoup de participants sont en faveur de l'introduction de nouveaux principes convenus à l'échelle mondiale, qui à leur avis, seront nécessaires pour assurer un consensus sur le degré de surveillance raisonnable. A Jakarta, l'idée est que « *si nous possédons ou conservons des données, nous ne pouvons pas fuir nos responsabilités, mais nous avons besoin d'un cadre mondial pour les données* ».

Le grand défi qui nous attend est de savoir si la protection de la vie privée peut être abordée par le biais d'accords mondiaux. Il est généralement admis que ces accords sont nécessaires. À Londres, on constate « *qu'aujourd'hui, nous avons un ensemble disparate de mesures législatives sur la confidentialité des données, mais les flux de données circulent à l'échelle mondiale. Nous avons besoin de principes mondiaux de la protection de la vie privée* ». Alors que les différentes régions cherchent toutes à faire progresser la réglementation des données,

l'émergence d'un cadre mondial de protection de la vie privée est défendue par ceux qui recherchent un meilleur contrôle et une plus grande transparence. A Bangalore, il a été noté que « *la création d'un conseil mondial des données pourrait faciliter les négociations internationales. Actuellement, il y a peu de consensus autour de la souveraineté des données, les différences culturelles autour de la vie privée en sont un exemple* ». Mais qui, ou plutôt quelle organisation, sera digne de confiance et capable de prendre l'initiative sur ce point ? Comme l'ont montré les tentatives de gouvernance d'Internet, la création d'une entité supranationale est une mission difficile, en raison d'impératifs politiques contradictoires et d'intérêts commerciaux concurrents.

Beaucoup de participants à nos ateliers croient que le RGPD a établi la norme que d'autres devraient suivre.⁴² À Mexico, on estime « *qu'il y a déjà des normes mondiales, et certains pays agissent déjà à l'échelle transnationale. Le RGPD a un impact qui va au-delà des frontières européennes* ». Le Nigéria, est l'un des nombreux pays où l'on constate que « *le RGPD va changer le paysage des données et inspirer de nouvelles normes. Il offre un modèle pour la législation locale, et a mis en évidence certaines des questions clés autour des données qui ne sont pas encore une priorité au Nigéria, mais qui vont prendre de l'importance au cours des dix prochaines années* ».

Dans toute l'Australie, l'Asie, l'Afrique et l'Amérique du Sud, nous avons entendu de façon cohérente et récurrente l'idée qu'un « *RGPD-lite* » serait le raccourci qui suffirait à couvrir l'essentiel localement et internationalement. De même, à Jakarta, la perspective était « *qu'il y aura une alternative asiatique au RGPD, axée sur l'éthique et les principes asiatiques* ». Ceux-ci peuvent, par exemple, être moins axés sur l'individu. Dans toute l'Afrique, il y avait également un intérêt à développer une réglementation pertinente au niveau local. A Lagos, une des idées

avancées est d'y aller progressivement : « *le secteur privé va faire pression sur le gouvernement pour s'assurer qu'il y a une législation claire autour de la responsabilité, et exiger la création d'une politique nigériane de protection des données qui reflète les mêmes principes que ceux énoncés dans le RGPD* ».

Enjeux pour la valeur des données

Le consensus sur les niveaux appropriés de protection de la vie privée est encore hors de portée, et les points de vue actuels sont souvent orientés par la culture. Cependant, avec l'adaptation et l'adoption de cadres communs pour plusieurs régions différentes, on pourrait atteindre une certaine harmonie. Bien que beaucoup de gens estiment que la protection de la vie privée ne sera plus une préoccupation dans le long terme, la majorité pense que pour la prochaine décennie, en particulier pour les multinationales et de nombreux gouvernements plus démocratiques, cela continuera d'être une préoccupation primordiale. La protection de la vie privée étant également présentée comme un avantage concurrentiel et utilisée comme un mécanisme pour renforcer la confiance et la crédibilité, plusieurs entreprises tentent de l'utiliser comme facteur de différenciation.⁴³



« Il y aura une alternative asiatique au RGPD, axée sur l'éthique et les principes asiatiques ».

Atelier de Jakarta

4.3 Consentement et contrôle



Concrètement, il est impossible de s'appuyer sur le consentement éclairé pour régler la question du traitement des données personnelles. Reconsidérer les finalités recherchées lors de sa mise en place pourrait mener à une nouvelle approche de cette problématique.

Contexte

La collecte, le partage et la vente des données personnelles constituent le gagne-pain de nombreuses entreprises en ligne, ces tâches constituent également une source importante de revenus. Le grand public ne prend conscience que progressivement de cette situation, et maintenant, certains commencent à se demander s'ils sont à l'aise avec ce modèle, surtout à la lumière des révélations de l'utilisation abusive des données qui ont eu lieu au cours de notre période de recherche.

Nos discussions ont confirmé que plusieurs dilemmes doivent être reconnus lorsque l'on parle de consentement éclairé. Le premier concerne la tension persistante entre les données collectées pour être utilisées à des « fins commerciales » et les données requises pour les « opérations ». Certains ont estimé que seules les données qui seraient bénéfiques pour l'utilisateur devraient être collectées et traitées, tout en reconnaissant que cela limiterait nécessairement les fonctionnalités des services et la capacité de création de valeur au profit des usagers. Le deuxième dilemme est la reconnaissance de la nécessité de concilier les demandes de produits et services personnalisés, avec les impératifs de la confidentialité des données. Compte tenu de cela, les participants à nos ateliers sont fermement convaincus que les données personnelles devraient être considérées comme un bien personnel ou commercial et qu'à ce titre, les clients devraient avoir accès à suffisamment d'informations pour pouvoir décider en toute connaissance de cause, jusqu'où ils sont prêts à aller pour échanger leurs données contre des produits et services.



Il est toutefois difficile de mettre cela en œuvre. Des textes trop longs inscrits en petits caractères en guise de conditions générales d'utilisation peuvent s'avérer rébarbatifs, non seulement c'est difficile à comprendre mais la quantité d'informations personnelles collectées peut se révéler choquante. Les prestataires de services craignent que la révélation de l'ampleur des données collectées et monétisées, puissent mettre leur modèle économique en péril si les consommateurs finissent par rechigner à partager leurs données. En conséquence, certains participants estiment qu'au lieu de tenter de pallier les inconvénients du « consentement éclairé », l'on ferait mieux d'identifier de nouveaux moyens de permettre aux personnes de garder le contrôle de leurs données personnelles. On peut envisager par exemple une réglementation plus rigoureuse du secteur, une intervention plus forte du gouvernement ou l'introduction d'intermédiaires qui pourraient mieux défendre les intérêts des consommateurs et contrôler l'accès aux données personnelles, en fonction de conditions préalablement convenues. La manière de trouver le bon équilibre entre ces solutions a fait l'objet de discussions lors de 11 ateliers du Projet sur la Valeur future des données.

De nombreux participants à nos ateliers ont soutenu que, même si l'intention est louable, le processus actuel d'obtention du consentement est inadapté. Le Règlement général sur la protection des données (RGPD) de l'Union européenne stipule que le consentement éclairé doit être donné librement, être spécifique, éclairé et sans ambiguïté, mais cela est très difficile à réaliser. L'approche actuelle est de demander aux usagers de cocher une case sur le site pour confirmer qu'ils ont lu et accepté le contrat qui permet aux fournisseurs de services de recueillir, partager, ou commercialiser leurs données personnelles, en échange de divers services en ligne. Ce n'est pas pratique, car la majorité des clients sont peu enclins à passer du temps à lire ces petits caractères. En effet, ils trouvent irritant d'être constamment invités à le faire. En conséquence, la plupart d'entre eux n'a qu'une appréciation confuse des conséquences potentielles de la divulgation

d'informations personnels. Nous ne savons quand, comment ni pourquoi nos données vont être recueillies, ni avec qui elles seront échangées ou partagées.⁴⁴ En toute honnêteté, s'attendre à ce que les fournisseurs soient en mesure d'articuler les nuances du consentement sous une forme digeste n'est pas réaliste non plus. Si les entreprises ont des politiques de confidentialité courtes et simples, on leur reproche de ne pas fournir suffisamment de détails, à l'inverse, si elles sont trop longues, personne ne les lira.

Enfin, le consentement ne fonctionne que lorsque les clients ont la possibilité d'utiliser un service alternatif. Compte tenu de la taille et de l'ampleur des principales plates-formes numériques, certains affirment que le consentement, éclairé ou non, est un exercice inutile, car les utilisateurs se sentent obligés d'utiliser le service, et doivent accepter les conditions générales, tout simplement parce qu'il n'y a pas d'alternative satisfaisante. L'Autorité allemande de la concurrence a récemment condamné Facebook sur ces questions de consentement et de monopole. Facebook a fait appel de la décision.

Il n'y a pas que les fournisseurs de services qui recueillent de l'information. Les gouvernements sont également confrontés au dilemme des limites à respecter pour concilier la collecte de données d'intérêt public, avec le respect des libertés individuelles telles que la vie privée. Par exemple, une ville intelligente administrée ou commandée par un conseil local a la possibilité de recueillir une grande partie des données personnelles sur les citoyens dans le cadre de leur vie quotidienne, avec la promesse de fournir de meilleurs services publics et une interaction plus efficace en ligne, avec le gouvernement et les autorités locales. Mais à quel moment cela devient-il intrusif ? En outre, la gestion du consentement éclairé sera encore plus compliquée avec l'émergence de nouvelles technologies telles que la reconnaissance faciale, l'Internet des objets, l'informatique quantique et l'intelligence artificielle, sans parler de l'existence de modèles de tarification de plus en plus complexes, tels que le groupage de différents produits et services.

Tout cela suggère la nécessité de trouver d'autres moyens de s'assurer que ceux qui fournissent des données peuvent exercer un meilleur contrôle sur l'endroit et la manière dont elles sont utilisées. Les solutions possibles discutées au cours de nos ateliers comprennent : une culture numérique plus élargie, une réglementation accrue, l'introduction de gestionnaires de données ou d'entrepôts de données personnelles qui représenteraient les individus, et éventuellement une contrepartie pécuniaire offertes aux utilisateurs par les prestataires de services en échange de l'accès à leurs données.

Ce que nous ont dit les participants

À Bangalore, la conversation a commencé par une discussion sur la taxonomie des données. « *Le consentement doit être défini d'une autre manière. La légitimité et le caractère raisonnable doivent être clairement exprimés* ». Cela a été repris à Singapour, où l'opinion est qu'il y a des « *conflits entre ce que les consommateurs considèrent comme la propriété et le consentement, et ce que les entreprises considèrent comme un accès. Cela montre qu'il est nécessaire de définir plus clairement les notions, en explicitant les nouveaux termes. Nous n'avons pas un référentiel clair* ». Un récent rapport de l'Université de Southampton confirme ce besoin de clarté. « Ce ne serait pas un luxe, étant donné le rythme des changements dans le domaine des NTIC et la multitude de finalités pour lesquelles les données pourraient être mises à profit ».⁴⁵

A San Francisco, les participants ont observé que même s'il y a des avantages à court terme à assurer plus de transparence autour de l'utilisation des données personnelles par les prestataires de services, à plus long terme, il y a des modèles économiques et des pressions réglementaires qui pourraient pousser les organisations à insister sur une plus grande sensibilisation du public au consentement. Toutefois, « *la technique a une longueur d'avance sur*

la réglementation et c'est là que réside le pourquoi du comment de l'introduction des méthodes peu orthodoxes ». Les participants ont également fait remarquer que même si une culture numérique plus prégnante « *renforcerait le pouvoir de contrôle des usagers* », la disponibilité des informations requises ne conduirait pas nécessairement à la prise de décisions éclairées chez les usagers : « *nous ne sommes pas sûrs que la population entière saura gérer les questions liées au consentement, malgré l'amélioration de la culture numérique* ». Ils ont ainsi estimé qu'il faudrait plus d'innovation pour permettre aux usagers de s'impliquer dans le contrôle de l'utilisation des données tout en veillant à ce que les produits et les services soient conçus en intégrant les paramètres de consentement. Une des solutions proposées est d'adapter la technologie en incluant des petites brèves explicatives et des modalités de sélection simples et ergonomiques pour paramétrer les options de confidentialités.⁴⁶ Les participants ont également suggéré que les données ne soient partagées que si elles offrent de la valeur à la personne auprès de laquelle elles sont récoltées, mais ont reconnu que, si les entreprises en ligne sont obligées de limiter la collecte de données à celles qui présentent des avantages spécifiques pour leurs utilisateurs, des changements importants dans les modèles d'affaires actuels pourraient s'ensuivre.

« Il y a des conflits entre ce que les consommateurs considèrent comme la propriété et le consentement, et ce que les entreprises considèrent comme un accès. Cela montre qu'il est nécessaire de définir plus clairement les notions, en explicitant les nouveaux termes. Nous n'avons pas un référentiel clair ».

Atelier de Singapour

A Madrid, on estime que le consentement éclairé devrait être abandonné au profit de l'établissement de normes de comportement convenues ; « ... *ce dont nous avons besoin, c'est d'un ensemble clair de principes* ». Cette vision est partagée à Jakarta où l'on a affirmé que les entreprises plutôt que les personnes physiques devraient supporter le poids de la gestion des données personnelles. « *Nous sommes lassés par ces histoires de consentement. Les organisations doivent soulager les usagers de cette responsabilité et mettre le fardeau plutôt sur le dos des entreprises qui seront chargées de s'assurer qu'il n'y ait pas de préjudices* ». Les participants de Hong Kong suggèrent que les régulateurs et les entreprises mettent en place un partenariat et que l'implication des parties prenantes et la collaboration sont les approches les plus raisonnables, même si ce processus va prendre du temps. Toutefois, la crainte réside dans le fait que si les débats autour du choix du responsable qui dirigera un tel processus ne sont pas résolus, « *le secteur privé va s'auto-réguler et élaborer une formule passe-partout qui ne garantira pas une plateforme égalitaire* ». ⁴⁷

Certains participants pensent que la réglementation gouvernementale est le seul moyen efficace de résoudre le problème. Ils estiment que le RGPD de l'Union européenne a ouvert la voie à de nouvelles possibilités pour les décideurs politiques dans d'autres marchés et que ce règlement « *met la barre plus haute pour la transparence à l'échelle mondiale* ». ⁴⁸ Au Nigéria, on a affirmé que le « *RGPD va inspirer de nouvelles normes* » et à Santiago, on a affirmé que « *le Chili observera ce qui se fait de bon ou de mauvais dans les autres pays pour sa propre gouverne* ». A San Francisco, les participants sont généralement en faveur d'une réglementation renforcée, d'ailleurs une nouvelle loi qui entrera en vigueur en 2020, la CCPA, imposera aux entreprises basées en Californie des règles plus strictes de

protection des données, notamment en donnant aux consommateurs de cet Etat plus d'accès et de pouvoir sur la façon dont leurs données sont utilisées et en prévoyant des amendes en cas de non-respect des dispositions. A Johannesburg, on estime que le renforcement de la réglementation est l'approche la plus plausible car elle est portée « *par la pression des consommateurs et par une demande de plus en plus pressante de transparence* ». Un des moteurs de cette approche sera l'augmentation du niveau de culture numérique qui « *va réveiller les consommateurs et les amener à se soucier de l'usage de leurs données personnelles* ».

D'autres modèles ont également été discutés. A Toronto, au lieu de plaider pour le consentement éclairé, qui à leur avis, est impossible à exercer, on estime qu'il serait plus pratique de reconnaître que les données personnelles sont une matière première nécessaire aux prestataires de services, et qu'à ce titre, les personnes physiques devraient recevoir une compensation pour leur utilisation. Ils ont donc suggéré qu'un « *dividende des données* », soit versé à tous les citoyens par les prestataires de services en échange de leur autorisation à accéder, collecter et monétiser leurs données. Cela signifierait que les citoyens pourraient être remboursés chaque année pour l'utilisation de leurs données par les entreprises qui ont l'intention d'en profiter. Ce modèle est similaire à celui mis en œuvre par les compagnies pétrolières, qui versent un dividende aux citoyens de l'Alaska pour l'extraction des ressources pétrolières de cet État.

« Nous sommes lassés par ces histoires de consentement. Les organisations doivent soulager les usagers de cette responsabilité et mettre le fardeau plutôt sur le dos des entreprises qui seront chargées de s'assurer qu'il n'y ait pas de préjudices »

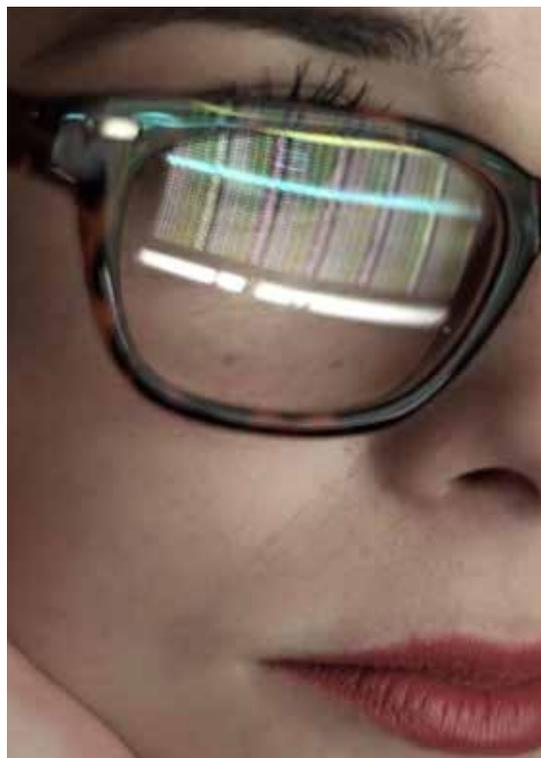
Atelier de Jakarta

Certains participants de Londres, Tokyo, Singapour et Johannesburg ont proposé qu'au lieu de forcer les consommateurs à prendre des décisions qu'ils sont tout simplement incapables d'assumer, une plus grande attention devrait être portée sur le rôle des gestionnaires de données qui, en tant que tiers de confiance, pourraient mieux représenter les droits des consommateurs et permettre « *le partage sélectif et contextuel des données dans des situations appropriés et pour les bonnes raisons* ». Cela donnerait aux consommateurs un plus grand contrôle des principes autour desquels leurs données peuvent être mobilisées, mais leur épargnerait la corvée d'avoir à vérifier cela chaque fois qu'ils s'inscrivent à un nouveau service. La réglementation, selon eux, serait plus adéquate si elle mettait l'accent sur le partage responsable plutôt que sur un regain de transparence.

Enjeux pour la valeur des données

Le concept de « consentement » a révélé une ligne de faille qui expose les hypothèses qui sont au cœur de l'élaboration des politiques et de la réglementation, allant jusqu'aux mythes juridiques qui constituent un fondement du droit des contrats : l'hypothèse que tous les contrats sont conclus entre des parties libres et égales qui sont pleinement informées de la nature et des conséquences de ce qu'ils acceptent (et derrière cela, l'hypothèse que les êtres humains sont d'abord et avant tout des décideurs « rationnels » toujours prêts à faire des choix « rationnels »).

La grande question est de savoir ce qui peut remplacer le consentement éclairé, et dans le même temps, quelles réformes apporter à son fonctionnement. De nombreuses suggestions alternatives plus pratiques, plus réalistes et plus viables ont été faites, y compris l'introduction de nouveaux intermédiaires, des tiers de confiance. Les progrès sur ce front seront stratégiques, si l'on doit maintenir des relations sûres, efficaces et de confiance entre les organisations et les citoyens.



« Si les débats autour du choix du responsable qui dirigera un tel processus ne sont pas résolus, le secteur privé va s'auto-réguler et élaborer une formule passe-partout qui ne garantira pas une plateforme égalitaire »

Ateliers de Hong Kong

4.4 Données ouvertes



La dynamique autour des données ouvertes est freinée par la privatisation des données publiques et les préoccupations croissantes liées à la sécurité. Cela limite le potentiel des données à servir à l'ensemble de la société.

Contexte

Les données ouvertes ou *Open data* reposent sur le principe qu'un large éventail d'informations souvent financées par l'État devraient être gratuitement accessibles à quiconque souhaiterait en faire usage. Sa popularité repose sur l'hypothèse que, tant que les garanties correctes sont en place, il peut rendre les gouvernements plus transparents, responsables et efficaces, tout en permettant aux entreprises d'utiliser les données pour créer des produits et services innovants et utiles.⁴⁹

Il existe différents types de données ouvertes :

- Les données mises à disposition par les gouvernements et d'autres institutions à des fins de transparence ;

- Les données mises à disposition par n'importe quelle organisation pour permettre l'innovation, souvent par des entreprises privées pour créer de nouveaux services payants, l'Open banking avec une législation de grande portée telle que le PSD2 en est un bon exemple ;
- Les données ayant pour but de donner le contrôle aux citoyens et aux communautés pour encourager leur sentiment d'appartenance et leur gestion autonome.

Une foule d'organismes internationaux, dont la Banque mondiale,⁵⁰ l'OCDE,⁵¹ l'UE⁵² et de nombreuses agences des Nations Unies,⁵³ soutiennent tous le mouvement Open Data. Pour suivre le mouvement, Open Data Barometer et Global Open Data Index, organismes chargés d'évaluer la situation des données ouvertes, cherchent tous à mettre en évidence les pays et les gouvernements les plus ouverts.^{54 55 56}



L'ouverture de vastes domaines publics numériques, allant des cartes aux composés chimiques, est le moteur d'une pléthore d'innovations, beaucoup ayant des effets sociaux et économiques positifs, comme CityMapper et OpenStreetMap, qui aident les gens à planifier leurs itinéraires en intégrant des données pour tous les modes de transport urbains.

Les données ouvertes contribuent également à l'économie. La Commission européenne estime que la valeur marchande des données ouvertes sera d'environ 285 milliards d'euros d'ici 2020. Les entreprises se joignent maintenant aux gouvernements et aux organismes publics pour mettre à disposition des ensembles de données pour un usage libre, souvent dans le cadre d'initiatives d'utilisation des données pour des bonnes causes (Data for good).⁵⁷

Dans certaines localités, la conscience du potentiel des données ouvertes reste faible et comme cela a été observé lors de l'atelier de Côte d'Ivoire, sensibiliser davantage sur cette question est considéré comme un « préalable à un partage plus élargi ». Par ailleurs, il y a des moments où le potentiel des données ouvertes est surestimé et certaines hypothèses relatives aux données ouvertes sont trompeuses. Il faut noter par exemple que :

- Ouvrir l'accès aux données ne produit pas systématiquement des avantages ;
- Toutes les informations ne peuvent pas ou ne devraient pas être rendues accessibles ;
- Tous les acteurs ne sont pas en mesure d'utiliser les données ouvertes. Bien que les données ouvertes soient publiées dans le but d'offrir un accès plus large, la réalité est que le nombre d'acteurs qui peuvent vraiment en faire usage est faible ; ils ont besoin d'infrastructures, de compétences hautement techniques, d'accès aux actifs techniques et de capitaux. Cela signifie que ceux qui exploitent ces données sont souvent des acteurs institutionnels et organisationnels établis et non des citoyens profanes.⁵⁸

- Les données ouvertes n'aboutissent pas automatiquement à un gouvernement ouvert. Comme le fait remarquer la Web Foundation, « la communauté continue de lutter pour démontrer l'impact positif des données ouvertes sur la bonne gouvernance »,^{59 60}

Un certain nombre d'études suggèrent que moins d'un tiers des données qui sont mises à disposition sont effectivement utilisées. Il y a de nombreuses raisons à cela, notamment un manque de compétences en matière de traitement des données parmi les fonctionnaires, les activistes et les journalistes⁶¹. En outre, pour être vraiment efficace, les données ouvertes doivent être accessibles et de haute qualité, et pas seulement disponibles en grande quantité. Cependant, de nombreux ensembles de données qui ont été publiés ont été élaborés à des fins administratives et ne sont pas structurés de manière à être facilement triés, analysés et associés à d'autres données.⁶² Jusqu'à présent, il n'existe pas de définition commune de ce qui caractérise des données ouvertes de « bonne qualité »⁶³, même si beaucoup sont extrêmement optimistes quant à son potentiel, la recherche de McKinsey suggère que des données ouvertes de meilleure qualité pourraient aider à débloquer une valeur économique annuelle de 3,2 à 5,4 trillions de dollars à l'échelle mondiale.⁶⁴

« Tant qu'il y a un accès à des données viables, on peut réaliser beaucoup de choses. Les données ouvertes sont de plus en plus reconnues comme un élément essentiel d'un gouvernement transparent et efficace »

Atelier d'Abidjan

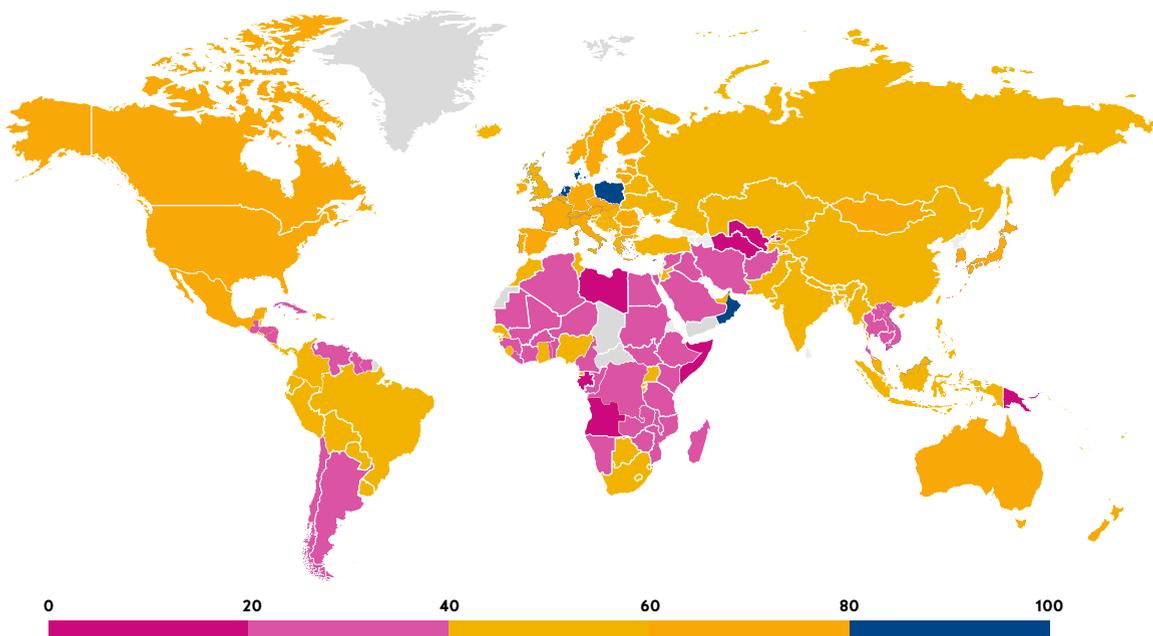
Ce que nous ont dit les participants

Au cours de nos discussions, nous avons constaté une opinion très favorable vis-à-vis des données ouvertes. En Europe et en Amérique du Nord, les données ouvertes sont considérées comme un enjeu clé pour l'avenir. Ailleurs, à travers l'Asie et l'Afrique, le principe a été également adopté. A Abidjan, par exemple, l'opinion est que « *tant qu'il y a un accès à des données viables, on peut réaliser beaucoup de choses. Les données ouvertes sont de plus en plus reconnues comme un élément essentiel d'un gouvernement transparent et efficace* ». Cependant, beaucoup de participants partagent le point de vue évoqué à Bangkok selon lequel, « *le secteur public ne comprend pas les avantages qui peuvent découler des données ouvertes* ».

Les obstacles et les contraintes ont également été admis. Les participants à l'atelier ont estimé que certains ensembles de données ouvertes ne

sont pas tenus à jour. Un participant de Bangkok a fait remarquer que, « *bien que les données du gouvernement soient accessibles, elles sont de piètre qualité et on ne sait pas très bien comment les utiliser pour générer un impact positif* ». Des interrogations subsistent quant à la prise en charge des coûts de l'amélioration des données ouvertes notamment leur exhaustivité, cohérence, pertinence et adéquation. Les participants de San Francisco ont formulé la question : « *qui va payer pour le nettoyage des données ?* » Alors que certains estiment que cette responsabilité incombe au gouvernement, d'autres proposent que ceux qui utilisent ces données paient une sorte de redevance pour contribuer à la prise en charge des coûts.⁶⁵

Un débat plus large et très houleux se tient autour de la « privatisation » des données ouvertes. Nous avons entendu des opinions sans équivoque sur la façon dont les données ouvertes sont compromises par des positions agressives en matière de propriété intellectuelle dans certains endroits.



Quatre problématiques clés ont été mises en évidence au cours de nos discussions :

- **Propriété intellectuelle** : comme on l'a souligné à Toronto, certains organismes publics tels que l'Ordinance Survey du Royaume Uni et Canada Post, ont passé de nombreuses années à renforcer leur expertise et leurs connaissances et exercent des droits d'auteur sur des ensembles de données clés. Comme la génération de ces données a été financée à l'origine par l'État, beaucoup estiment que ce cloisonnement est contraire à l'intérêt national. D'autres y voient une protection légitime de leurs investissements antérieurs.
- **Licences** : étant donné que les données de valeur commerciale sont regroupées en « données dérivées » et que de nouvelles formes de valeur sont identifiées, il y a un manque de clarté sur l'opportunité et la manière de partager cette valeur. Cela pourrait se faire notamment par le biais de l'octroi de licences, de nouveaux droits d'auteur et de brevets. Les applications de cartographie telles que Waze dépendent des données ouvertes, mais leur modèle économique, qui est basé sur la publicité ciblée hyper localisée, implique la collecte et la monétisation des informations personnelles.⁶⁶ À Toronto, on a estimé « *qu'il s'agit d'un conflit évident entre l'ambition revendiquée et la réalité du modèle économique* ». Un autre exemple est le reconditionnement et la revente par des entreprises privées des données sur les horaires des trains publics.
- **Privatisation de l'information publique** : de nouvelles sources commerciales de valeur sont créées à partir d'informations publiques, académiques et gouvernementales, et sont ensuite utilisées dans des activités privées. Lors des discussions menées à Singapour, des exemples tels que « *la privatisation par Uber de l'expertise de Carnegie Mellon en matière de véhicules autonomes* », à travers le recrutement de nombreux universitaires de premier plan pour profiter de leur

savoir-faire⁶⁷ ou encore les tentatives d'obtention de brevets sur des plantes présentes dans la nature il y a une dizaine d'années par Monsanto. On peut également citer quantités de démarches comparables entreprises plus récemment par des sociétés comme Facebook, Microsoft et Amazon.⁶⁸ Les tactiques comprennent l'attraction de professeurs d'université en leur proposant jusqu'à 10 fois leurs salaire universitaire, la mobilisation de ressources informatiques étendues et la promesse de limiter la bureaucratie.⁶⁹ À l'avenir, si davantage d'informations publiques sont ouvertes, on craint que les entreprises privées n'exploitent davantage cette aubaine par le biais de mécanismes de propriété intellectuelle. Ce n'est pas une préoccupation nouvelle. La question s'est posée il y a quinze ans, lorsque les informations publiées à partir du projet de génome humain financé avec des fonds publics a été « privatisé » par des entreprises comme Incyte Genomics, qui en 2005, avait breveté 2 000 gènes humains.⁷⁰ Plusieurs participants pensent que, dans un monde où la paternité des oeuvres en ligne est de plus en plus collective et collaborative, et où les brevets protègent les modèles économiques numériques autant que la technologie, la finalité originelle de la réglementation de la propriété intellectuelle se délite. Les ensembles de données ouvertes, affirment-ils, ne devraient pas faire l'objet de brevets ni d'autres formes de propriété intellectuelle, comme le droit d'auteur.

- **Privatisation des organismes publics** : Enfin, il est également prouvé que certains gouvernements « mettent » des biens publics, y compris la propriété intellectuelle qui leur est associée et des données publiques qui devraient rester ouvertes, entre les mains des entreprises privées. La privatisation potentielle d'organismes gouvernementaux, tels que le Cadastre du Royaume-Uni (Land Registry) et l'entité chargée du contrôle aérien aux États-Unis, constituent deux épreuves en cours.⁷¹ Les observateurs croient qu'il pourrait y en avoir beaucoup d'autres à l'échelle mondiale,

particulièrement en ce qui concerne les informations liées à l'environnement et aux ressources.

Il y a cependant des problématiques juridiques sur la façon de partager les données anonymes des gouvernements et des entreprises d'une manière sûre et éthique, dans un contexte de méfiance de la part du public. Certains estiment que les défenseurs des données ouvertes ont été peut-être trop naïfs dans leur quête, le scandale autour de Cambridge Analytica l'a clairement montré. Comme cela a été observé lors d'un atelier au Danemark⁷²: « *nous voulons laisser la carotte sous le nez du lapin mais nous ne voulons pas qu'il le mange* ». Il s'agit certainement d'un processus d'apprentissage. Les fiduciaires de données, entités juridiques distinctes conçues pour aider les organisations à extraire de la valeur des données anonymisées, sont un moyen de limiter les risques et d'apaiser les préoccupations quant à la façon dont les données sensibles sont détenues par des tiers. Ils permettent également aux citoyens de devenir fiduciaires, et donc d'avoir leur mot à dire dans la façon dont leurs données anonymes sont utilisées.

D'autres problèmes ont été identifiés autour de la frontière parfois floue entre les données ouvertes et les données personnelles. L'utilisation de données ouvertes peut notamment augmenter la probabilité de la mise en évidence de caractéristiques identifiables. Des chercheurs de l'Université catholique de Louvain (UC Louvain) et de l'Imperial College de Londres ont construit un modèle pour estimer à quel point il serait facile de désanonymiser n'importe quel ensemble de données. Un ensemble de données ayant 15 attributs démographiques, par exemple, « rendrait 99,98 % des habitants du Massachusetts uniques »,⁷³ Cette problématique a été abordée à Toronto, où l'on craint que les données agrégées détenues par le Gouvernement sur les services de santé et les services sociaux puissent, par exemple, être utilisées en association aux données recueillies pendant que les individus se déplacent dans les

réseaux de transport et dans les espaces urbains, pour pouvoir les réidentifier, et que les conclusions qui en résultent puissent être utilisées sans le consentement explicite des personnes concernées. Afin de minimiser ce risque, des niveaux d'accès et de contrôle appropriés doivent être établis.⁷⁴ Il devrait être possible de fournir l'accès à des données plutôt élémentaires, telles que les données démographiques à haute résolution aux organisations humanitaires présentes dans une zone de conflit, par exemple, mais pas aux parties en conflit, telles que les forces gouvernementales et les forces « rebelles » qui pourraient les utiliser pour causer encore plus de dommages. La question ici est de savoir quelle est la personne ou l'organisation est la mieux équipée pour attribuer les droits d'accès et les personnes habilitées.

« Une réglementation plus rigoureuse est nécessaire, avec des dispositions pour encadrer l'agrégation et l'anonymisation des données. Si cela est impossible, alors l'utilisation de ce type de données devrait être uniquement réservée aux chercheurs qui adhèrent à des normes plus strictes d'utilisation des données que celles qui sont généralement appliquées dans leur secteur d'activité ».

Atelier de Copenhague

Enjeux pour la valeur des données

Il semble qu'à l'avenir, il y aura une exigence de clarté toujours plus pressante au sujet de la nature des données à libérer, dans quel but et par qui. Différents types d'informations impliquent différents usages. Beaucoup de participants à nos ateliers ont reconnu que les objectifs poursuivis lors de l'utilisation des données ainsi que les méthodes de stockage devraient être examinés par les experts en cyber sécurité. Des rapports réguliers sur la transparence, identifiant les acteurs habilités à accéder aux informations contribueraient à réduire considérablement les risques.

« Qui va payer pour le nettoyage des données ? »

Atelier de San Francisco

A Copenhague, on a proposé de définir l'utilisation libre de données commerciales sensibles ou non sensibles

- Pour les données **commerciales**, lorsque les entreprises privées et les entités publiques apportent des informations, un objectif commun peut motiver l'ouverture des données. « *le partage des données liées aux tests cliniques afin d'optimiser les avantages de l'élaboration de médicaments est une illustration pertinente* ».
- Des dispositions réglementaires supplémentaires peuvent s'avérer nécessaires pour les données **personnelles** et les données **sensibles** lorsque la confidentialité et la sécurité sont indispensables. « *Une réglementation plus rigoureuse est nécessaire, avec des dispositions pour encadrer l'agrégation et l'anonymisation des données. Si cela est impossible, alors l'utilisation de ce type de données devrait être uniquement réservée aux chercheurs qui adhèrent à des normes plus strictes d'utilisation des données que celles qui sont généralement appliquées dans leur secteur d'activité* ».

Enfin, pour la plupart des ensembles de données **non sensibles** et des ensembles de données publiques, il sera essentiel d'améliorer leur accessibilité, renforcer la sensibilisation du public et la culture numérique.



4.5 Propriété des données machine



Le débat autour des droits de propriété des données issues de l'Internet des objets (IdO) fait fureur. Des enjeux liés au titre, au contrôle, à l'utilisation des données poussent les acteurs des différents secteurs d'activité à emprunter des voies distinctes.

Contexte

Jusqu'ici, l'attention était plutôt portée sur les données personnelles. Mais à l'avenir l'attention pourrait aller vers les quantités de plus en plus importantes d'informations générées par les machines. On estime qu'en 2020, il y aura plus de 50 milliards d'objets connectés.

Les données de machine à machine (M2M) et les données issues des objets connectés augmentent à un rythme effréné avec un énorme impact sur nos vies et sur le fonctionnement de la société. Tandis que de nombreux capteurs transmettent des

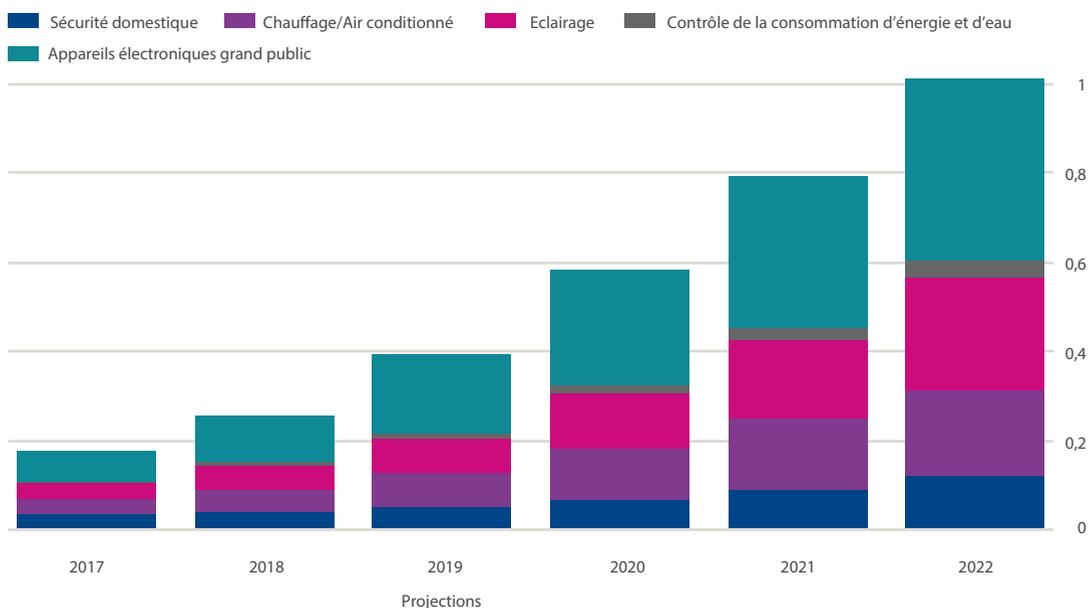
données, certains appareils connectés fonctionnent comme des aspirateurs numériques, avalant toutes sortes d'informations susceptibles d'être analysées par d'autres et partagées à l'infini. Sans même un clic, les données les plus vitales comme les plus banales circulent à travers les chaînes logistiques, entre les voitures, les bâtiments, etc. En effet, la trajectoire de croissance de ce type de technologie est tellement rapide que certains pensent qu'en 2030, chaque appareil aura systématiquement un capteur intégré et une connexion internet.⁷⁵ Les projections concernant le nombre d'objets connectés en activité varient. Selon Intel, d'ici à 2030, il y aura 20 milliards d'objets connectés.⁷⁶ Cisco les estime à environ 500 milliards.⁷⁷ La Chine générera bientôt 20% de l'ensemble de ses données à partir d'appareils connectés.⁷⁸ EMC prédit que l'IdO nécessitera bientôt près de 40 trillions de gigabytes d'espace de stockage tandis que IDC estime que 175 zettabytes de données seront stockées d'ici 2025.⁷⁹



Pour autant, il n'y a pas de principes aboutis autour de la valeur des données extraites, mais l'impact financier potentiel de l'IdO est considérable. Bain prédit que d'ici 2020, les applications IdO B2B vont générer 300 milliards de dollars par an.⁸⁰ Une estimation prévoit qu'une augmentation de 10% de connexions M2M générera plus de 2 milliards de dollars aux Etats-Unis dans les dix prochaines années.⁸¹ PwC prévoit 6 trillions de dollars en investissements rien qu'aux Etats-Unis.⁸² Quels que soient les chiffres au final, une chose est claire, comme le mentionnent les participants à l'atelier de Francfort, la problématique de la propriété des données issues de l'IdO est en passe de « devenir un enjeu crucial ».⁸³

Propriété des données machine, une période d'incertitude

La vraie question à poser est de savoir si les données issues de l'IdO auront plus de valeur si elles sont propriétaires, ou ouvertes à tous. Il n'est certainement pas facile d'optimiser les opportunités offertes par l'IdO. Un réel problème réside dans le fait que dans de nombreux secteurs, il n'y a pas d'approche conventionnelle à la propriété des données machine et de nombreuses zones d'ombre subsistent en ce qui concerne le contrôle, les avantages et l'accès. Alors que pour le débat complexe des données personnelles, les progrès ont été constants, pour les données machine il n'y a pas d'orientation marquée notamment pour déterminer si la propriété doit être liée au fabricant de l'appareil ou à son utilisateur.



SOURCE: IHS Markit

Emergence des données machine : augmentation des appareils IdO (2017 - 2022)

Dans le secteur agricole du 21^{ème} siècle, qui est de plus en plus automatisé, par exemple, les agriculteurs peuvent posséder ou non les données produites par les équipements utilisés dans leurs exploitations. Le fabricant d'équipements agricoles a souvent le droit de récolter les données et de les utiliser au sein d'un système plus large.⁸⁴ Les données fonctionnent de la même manière que la chaîne de valeur alimentaire, comme lorsque le blé est récolté, transformé en farine et intégré à la fabrication du pain qui est vendu au consommateur final. Comme cela a été suggéré lors d'un autre débat facilité par Future Agenda sur le futur de l'utilisation des terres, « *pour un hamburger dont la chaîne d'approvisionnement a été tracée, le débat sur la propriété des données sources issues de la vache, de l'agriculteur, de l'unité de transformation de la viande ou de McDonalds, est un exemple tout simple pour lequel les perceptions sont divergentes* ». La chaîne d'approvisionnement de McDonalds est réputée efficace et collaborative, mais avec des millions d'exploitations impliquées, déterminer la propriété des données n'est pas si simple.⁸⁵

Dans le secteur automobile, on note un certain enthousiasme à propos du déploiement de nouveaux véhicules de plus en plus autonomes, toutes générant et partageant d'énormes quantités de données. Toyota estime que le volume de données échangées entre les véhicules et le Cloud atteindra 10 exabytes (10¹⁸) par mois vers 2025.⁸⁶ De nombreux propriétaires ou locataires de voiture peuvent penser que les données produites par cette dernière et donc une part considérable de la valeur générée, leur appartient ou devrait leur appartenir. Mais les autres acteurs du secteur ont une autre opinion et les réactions peuvent varier en fonction de la nature des données.⁸⁷ Par exemple, les données de localisation, vitesse, destination, température extérieure, émissions, pourraient être accessibles et exploitables par tous, tandis que les informations plus spécifiques portant notamment sur l'état des routes, les niveaux de carburant, le niveau de fatigue du conducteur, l'état des freins et

des pneus, voire même les données relatives aux accidents, pourraient être maintenues par plusieurs parties impliquées notamment les constructeurs automobiles, les compagnies d'assurances, les réparateurs automobiles, les agences publiques, les marques de carburants. « *Très peu de données automobiles, à l'exception des informations détaillées sur la performance des moteurs devraient être propriétaires. Les données en soi, ont une valeur très limitée, l'impact provient plutôt de ce que l'on obtient en les exploitant* ».⁸⁸

D'après nos discussions et compte tenu de toute l'activité, l'investissement et l'élaboration de stratégies par un groupe de gouvernements et d'entreprises clés, pour l'heure, il n'y a pas de réponse universelle à la question de la propriété des données machine. Plusieurs parties prenantes ayant des intérêts particuliers sont toutefois prêtes à trouver un terrain d'entente, voire conclure un protocole mondial, mais cela pourrait prendre des années avant qu'il ait des progrès notoires. Pour nombres d'acteurs en tout cas, avoir plus de visibilité sur les critères de propriété des données machine et de légitimité des acteurs habilités à les analyser et à y ajouter de la valeur, est une priorité majeure.

« La réalisation d'analyses de pointe permettrait de maximiser la valeur qui serait potentiellement extraite des données et de fournir un champ d'intervention plus équitable à l'endroit des PME »

Atelier de Jakarta

Ce que nous ont dit les participants

Comme mentionné précédemment, beaucoup de gens croient que les données ne devraient pas être soumises à la législation sur la propriété. Cependant, en Occident, le propriétaire des données est souvent considéré comme l'organisation qui détient le titre légal de l'appareil qui a enregistré ou généré les données, qu'il s'agisse d'un lampadaire, d'un tracteur, d'une sonnette, ou d'un train à grande vitesse. Tant qu'il n'y a pas d'autre accord en vigueur, il est probable que la seule entité qui ait le droit d'utiliser ou de disposer de ces données soit celle qui les a effectivement produites en premier lieu. Ainsi, le titre de données est comme un titre de propriété. Cependant, comme nous l'avons souligné dans nos conversations parallèles sur la valeur des données automobiles, « *l'organisation qui a la possession d'une machine n'en est pas nécessairement propriétaire; les choses peuvent devenir assez incertaines lorsque, par exemple, l'équipement est loué par une organisation à une autre* ». ⁸⁹ Comme la location est aujourd'hui l'approche privilégiée dans de nombreux secteurs, de l'agriculture aux transports en passant par la santé et la gestion des bâtiments, ce postulat reste d'actualité.

Certains experts estiment que celui qui génère les données en est le propriétaire, et que ces données peuvent être vendues. Mais d'autres suggèrent que dans les écosystèmes de plus en plus complexes avec des chaînes d'approvisionnement décentralisées et des réseaux qui opèrent maintenant dans de nombreux secteurs, la source des données peut concerner plusieurs parties, ainsi qu'un nombre important de personnes impliquées dans la livraison des produits et qui pensent eux aussi, posséder les données. Il n'est donc pas surprenant que plusieurs participants de Tokyo aient estimé que « *nous avons besoin d'une réflexion fondamentale sur les caractéristiques définissant le propriétaire des données* ». En fait, « *il n'y a pas de lois générales sur la propriété de l'information, en dehors de certaines*

dispositions réglementaires portant sur des secteurs verticaux ».

Les participants à l'atelier estiment qu'à l'avenir, le changement le plus important se produira dans deux principaux domaines : le rôle de l'IA et l'accès aux analyses de données.

- A Francfort, certains pensent que les « données seront de plus en plus générées et exploitées par des machines, sans jamais être touchées par des humains ». « *Les machines vont prendre des décisions automatisées au fur et à mesure que les rapport M2M et l'IA vont s'imposer* » et la transition du contrôle se fera vers les algorithmes ou leurs propriétaires. Une proposition a été faite dans ce sens à San Francisco, disant en substance, « *nous ferons appel à la réglementation des algorithmes pour gérer des données machines qui échappent à la gouvernance humaine* ». Ainsi, au fur et à mesure que les machines vont créer et exploiter de nouvelles données, l'IA sera peut-être nécessaire pour les réguler et c'est à ce niveau que se posent les problèmes de propriété et de valeur. Une autre opinion exprimée au Japon suggère « *qu'à l'avenir, les métadonnées seront générées par l'IA* » et « *la question de la propriété des métadonnées se posera* ».
- À Jakarta, de nombreux participants estiment que les nouvelles capacités d'analyse de données de l'Internet des objets devraient être rendues plus accessibles à l'industrie au sens large au lieu d'être la chasse gardée des grandes entreprises de technologie. « *La réalisation d'analyses de pointe permettrait de maximiser la valeur qui serait potentiellement extraite des données et de fournir un champ d'intervention plus équitable à l'endroit des PME* ». En effet, plusieurs participants pensent que, s'il n'est pas correctement réglementé, ce déséquilibre des capacités entre ces quelques dirigeants et la masse de l'industrie, pourrait conduire à des inégalités importantes autant au sein d'un même

secteur que sur le plan national. Un point de vue connexe exprimé en Allemagne est qu'au cours de la prochaine décennie, « *les entreprises de taille moyenne vont peiner, pendant que les grandes entreprises seront plus à l'aise parce qu'elles disposeront de plus de ressources et de données* ».

Plus généralement, on a observé un consensus à Stockholm autour de l'idée que nous devons aller vers une compréhension plus « *hétérogène de l'IdO* », et si possible exiger une forme « *d'assurance qualité pour les données de l'IdO* ».

Enjeux pour la valeur des données

Dans un domaine où les statistiques quotidiennes se comptent par trillions, on voit que la propriété des données machine pose déjà problème. Compte tenu de cette incertitude concernant notamment les prérogatives des différents acteurs dans des contextes spécifiques, certains s'étonnent de ce que tant d'entreprises et de fonds de capital-risque soient en train d'investir massivement dans les villes intelligentes, les voitures connectées et le commerce numérique tandis que le public dans sa majorité estime que la valeur potentielle des données machine constitue un élément essentiel de la logique commerciale. Toutefois, en dépit de la confusion ambiante, l'intérêt des villes, des gouvernements, de la société en général ne fera que croître. La source, la propriété et l'accès aux données machine est un débat crucial pour beaucoup de secteurs d'activité. Indubitablement, la valeur de ces données et leur intérêt, en fonction des acteurs, seront décisifs.



« Les données seront de plus en plus générées et exploitées par des machines, sans jamais être touchées par des humains »

Atelier de Francfort

4.6 Les données en tant qu'actifs



Les organisations sont tenues de rendre compte des données qu'elles possèdent ou auxquelles elles ont accès. Elles doivent déclarer leur portefeuille de données et s'acquitter des impôts sur les données.

Contexte

Il est reconnu que les données sont un atout précieux pour les organisations qui en collectent. Jusqu'ici, les entreprises axées sur les données ont eu du mal à adhérer aux concepts économiques ou aux mécanismes fiscaux classiques. Une entreprise prospère disposant de nombreux actifs corporels a évidemment un « capital » substantiel. Mais devrait-on considérer les données comme un actif ou même comme un « capital » surtout si les données détenues par l'entreprise sont des données personnelles ou des données machine qui ne sont pas la propriété de l'organisation en question. D'autre part, quelle est la valeur qui est taxée ?

Si les données sont officiellement reconnues comme des actifs d'entreprise, d'importants enjeux organisationnels, industriels et commerciaux pourraient émerger. Comme cela a été formulé pour la première fois à l'atelier de Jakarta, si la valeur future d'une entreprise comprend la valeur des données qu'elle possède, gère, analyse ou consulte, alors la manière dont les entreprises axées sur les données sont évaluées et peut être taxées va changer. Les données seraient évaluées en tant qu'actifs. Les enjeux potentiels d'une telle mesure pour les affaires, la croissance économique, l'évaluation du PIB sont considérables.



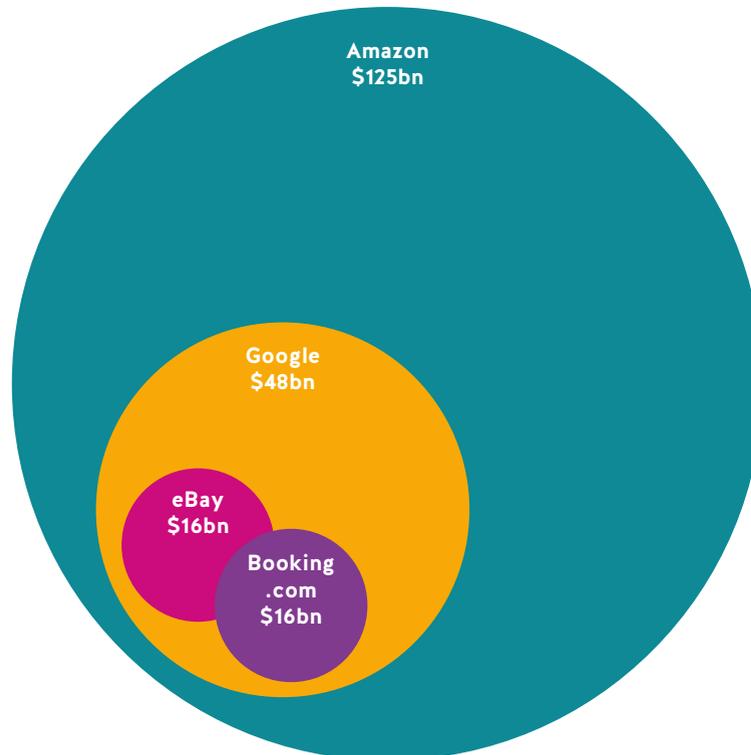
Les données en tant qu'actifs

De nombreux experts ont affirmé que si les données venaient à être considérées comme un actif distinct, elles seront suivies et tracées de manière plus rigoureuse et seront éventuellement réglementées. Un nombre croissant de chercheurs étudient ce scénario.⁹⁰ Si les données sont officiellement reconnues comme un actif commercial, les entreprises devront certainement justifier plus précisément des données qu'elles contrôlent ou utilisent. Toute grande entité, qu'il s'agisse d'une entreprise, d'un gouvernement ou d'une ONG, pourrait se voir obligée de déclarer la valeur de ses actifs de données de manière régulière. Cela pourrait impliquer une évaluation comptable formelle

de certains ensembles de données mais aussi l'évaluation de la valeur générée par ces actifs.

Le défi fondamental ici est de savoir comment évaluer les données d'une entité de telle sorte qu'elles soient comparables à la valeur de celles d'une autre entité, ou à un autre référentiel d'ordre général. Les flux de données ne sont pas une marchandise : chaque circuit d'information est unique, en termes de ponctualité et d'exhaustivité. Cette nature hétéroclite fait qu'il est difficile de définir un ensemble spécifique de données et de le tarifier afin de déterminer sa valeur.

SOURCE: <https://www.imf.org/en/News/Seminars/Conferences/2018/04/06/6th-statistics-forum>



Qui possède quoi ? : Valeur estimative des données (2017)

Bien que l'attention de nombreuses entreprises et gouvernements soit actuellement portée sur les données personnelles, différents secteurs sont en train de d'essayer d'établir une méthode consensuelle d'évaluation des ensembles de données spécifiques à leur domaine. Les acteurs du secteur pétrolier par exemple, commencent à s'aligner sur l'analyse sismique qui est utilisée pour cartographier les réserves. Dans le secteur automobile, des initiatives sont menées pour trouver une méthode d'évaluation des données générées par les véhicules autonomes connectés. En outre, la valeur des données IdO des villes intelligentes commence à attirer l'attention. Les gouvernements sont en train de prendre conscience de la valeur de leurs actifs de données et essaient de mettre en place des normes communes. En 2018, par exemple, une commission spéciale du Parlement britannique⁹¹ suggérerait que la valeur des données agrégées de l'ensemble de données patients du NHS pourrait être estimée à 10 milliards de livres sterling.⁹² Le Gouvernement britannique est en train d'examiner les possibilités.

Pour apporter de la rigueur dans cette démarche, le FMI, entre autres organisations, tente de contribuer à la définition d'une approche d'évaluation des ensembles de données. Lors d'une conférence en novembre 2018, des chercheurs ont expliqué pourquoi l'impact des données doit être prise en compte dans l'évaluation de la valeur de l'économie. Dans un article, les données d'Amazon ont été estimées à 125 milliards de dollars avec une croissance annuelle de 35%. Ainsi les données représentent 16% de la valeur marchande de cette société.⁹³ Les données de Google ont été estimées à 48 milliards de dollars au moment de la publication de l'article.⁹⁴

Certains estiment que ceux qui détiennent des ensembles de données sont déjà en train de planifier l'évaluation de leur valeur. Pour ceux qui souhaitent acheter des informations dans le dark web, par exemple, la valeur relative des données personnelles de santé représente près de dix fois

celle des informations relatives à la carte bancaire d'un individu.⁹⁵ Experian, pour ne pas la nommer, a expliqué en détail quelles sont les pièces de données personnelles communément vendues et dans quel but elles sont achetées.⁹⁶ Le Financial Times propose également un évaluateur automatique de données personnelles.⁹⁷ De façon plus légitime, un groupe de banques d'investissement, d'économistes et de consultants sont en train de faire leur propre analyse des principales sociétés de technologie afin de mieux les noter et de faire des projections sur la valeur de leurs futurs actifs.⁹⁸

Les données en tant que passif

Si les données sont considérées comme un actif, alors elles peuvent aussi devenir un passif. Il faut naturellement les stocker et les maintenir, ce qui dans les deux cas, engendre des coûts. Les entreprises devront prendre cela en compte. Les comptables devront toujours équilibrer les livres comptables et calculer les capitaux propres issus des données, donc il sera important d'avoir un passif de données à compenser par des actifs de données. Après tout, les actifs procurent des avantages économiques ultérieurs, alors que les passifs représentent une obligation ou un risque ultérieur. Le fait de stocker certains types de données, par exemple, peut faire baisser la confiance des usagers et par conséquent, ces données peuvent devenir un passif. Cela peut aussi vouloir dire que le coût de la sécurisation des données sera plus élevé que le coût associé à sa perte. Les experts en sécurité des données avancent qu'il vaudrait mieux considérer la grande quantité de données détenues par les organisations comme un passif car la valeur qu'elles peuvent en extraire est très faible comparée aux coûts liés à leur protection contre le vol et les abus ou aux coûts associés à leur vol ou perte lorsque ces risques viennent à se réaliser.

Certains marchés comme celui du Royaume-Uni condamnent déjà les entreprises qui ne protègent pas les données qu'elles détiennent à des amendes

salées. Ce risque, ajouté à l'ingéniosité de la dernière génération de pirates informatiques implique que de plus en plus, les entreprises vont devoir effectuer des provisions pour risques et charges, spécifiquement pour les données. Une conséquence inattendue pourrait être l'essoufflement de l'innovation car les barrières à l'entrée sur les marchés seraient trop élevées.

Fiscalité numérique

L'idée que les gouvernements pourraient (et devraient) exiger une taxe sur les activités numériques d'une organisation est controversée aux États-Unis, mais plus largement acceptée ailleurs. La Commission européenne a proposé une taxe dite taxe sur les services numériques, à un taux de 3 %, sur les activités locales des grandes entreprises de technologie telles que Google, Facebook et Apple.⁹⁹ Le Royaume-Uni a créé un précédent en annonçant son intention d'introduire une taxe sur les services numériques d'ici 2020, afin que les multinationales « ayant des activités rentables au Royaume Uni contribuent une juste part d'impôts »,¹⁰⁰ D'autres États membres de l'UE ont présenté des propositions au niveau national. Récemment, l'OCDE a également annoncé son objectif de convenir de règles similaires à l'échéance 2020.¹⁰¹ À ce jour, toutes les approches concernent uniquement l'imposition des revenus des activités des entreprises.

Taxes sur les données

Pour l'heure, les discussions ne portent pas sur l'imposition des données, mais sur les revenus associés au numérique. Toutefois, il se pourrait que l'on soit au début d'un processus qui pourrait aboutir à une taxe plus importante visant également les données. Comme le font plusieurs pays européens et certains états tels que l'état fédéral de la Colombie-Britannique au Canada, qui appliquent un impôt annuel sur la fortune personnelle, basé sur la valeur marchande des actifs détenus à titre individuel par les contribuables, si les données d'une entreprise ont une valeur convenue, alors, soutient-on, les gouvernements pourraient exiger un impôt annuel sur les actifs de données en plus de l'impôt sur les bénéfices des sociétés ou l'intégrer à ce dernier.

Pour les organisations, il y a un net inconvénient à la création d'une taxe sur les données. Beaucoup estiment qu'elle pourrait étouffer l'innovation, car l'information serait bridée afin de minimiser les coûts. Par ailleurs, certains estiment que d'un point de vue social, la taxation pourrait être un levier puissant qui sonnerait le glas du « hold-up » des données que l'on a observé ces dernières années. Selon eux, si on en arrive là, c'est simplement le signe que le secteur des données arrive à maturité et qu'il se produit un rééquilibrage du pouvoir et de l'argent.¹⁰² Pour chaque optique envisagée, les chercheurs examinent les implications plus larges de la création de valeur supplémentaire et l'impact sur le PIB national et mondial, si les recettes numériques, les taxes sur les données et d'autres actifs de données sont inclus dans les calculs. Comme l'a déclaré un participant à un atelier aux États-Unis, « lorsque l'on associera le capital données et la fiscalité numérique, les choses deviendront réellement intéressantes ».

Ce que nous ont dit les participants

Les actifs de données

Les participants ont été généralement d'accord sur le fait « *qu'une approche commune de certification des données en vue de leur évaluation viendrait des citoyens à travers une dynamique sectorielle, régionale ou communautaire plutôt que d'une initiative mondiale pilotée par les dirigeants* »¹⁰³ La manière de « *justifier la valeur attribuée à quelque chose qui ne nous appartient pas* » est une autre question qui a été débattue à Hong Kong. A San Francisco, on est d'avis qu'il est préférable que la tâche soit confiée à une instance dirigeante indépendante afin de garantir la transparence et la crédibilité. Cette idée a été explorée à Toronto où l'on a proposé « *qu'un cadre commun consensuel soit créé (par secteur d'activité)* ». Beaucoup de participants à travers le monde ont approuvé cette proposition. Toutefois, il n'y avait pas de consensus sur le choix de l'entité qui pourrait porter cette initiative.

Les passifs de données

En Europe, la législation qui régit la notion de passif raisonne dans une logique de biens palpables, de ce fait, l'on s'est souvent demandé, lors des échanges, si ce raisonnement juridique serait adapté et pourrait être appliqué aux produits de bases de données.¹⁰⁴ A Sydney, l'idée d'étendre la notion de passif de données à celle de négligence de données a été évoquée. L'un des postulats avancés dans cette veine, est « *qu'il existe une responsabilité de partager et d'utiliser les données pour le bien commun* », tandis qu'un autre est en substance que « *le fait de ne pas utiliser les données de manière appropriée au profit du privé et du public devrait être considéré comme une négligence* ».

Le capital données

Une autre idée évoquée pour la première fois à Sydney et soutenue par Londres, San Francisco et Toronto est de considérer les données comme le septième capital dans le modèle multi-capital qui sous-tend actuellement le reporting intégré. Certaines organisations ont déjà commencé à inclure leur capital social, environnemental, naturel et humain dans leurs déclarations annuelles, au-delà des déclarations sur leur impact financier.¹⁰⁵ Guidés par des sociétés comme AXA, Puma et Unilever, un parterre de grandes entreprises, qui ne cesse de s'agrandir, s'implique dans ce débat et prévoit de faire des déclarations sur les différents impacts de leurs résultats opérationnels. Ces entreprises testent et adoptent conjointement des approches normalisées pour évaluer et déclarer l'impact et la valeur de ce qu'elles considèrent comme reflétant la gammes complètes de leurs activités. L'inclusion du capital données dans ce mix serait une initiative qui arriverait à point nommé. A Manille, les participants ont le sentiment que « *si l'on avait un système plus formel pour évaluer la valeur des données en tant que capital, on pourrait mieux les utiliser, puisque « le mode d'emploi » serait intégré au système et pris en compte dans la valeur même des données* ».

Certains sont en désaccord avec ces principes et soulignent que, contrairement aux autres actifs incorporels tels que la R&D (ex : les brevets) qui pourraient se déprécier au fil du temps, l'agrégation et le croisement de données peut générer une nouvelle valeur et dans ce sens, le capital données pourrait croître bien plus rapidement que les six autres formes de capital et fausser les projections relatives à l'impact d'une organisation. Certains pensent que les données sont déjà prises en compte dans la R&D. A Londres, on estime que « *la déclaration du capital données se fait déjà, surtout dans l'évaluation de la R&D, et notamment sous forme de propriété intellectuelle* ». A Toronto, l'observation suivante a été faite : « *c'est comme*

le capital de la propriété intellectuelle mais dans un sens plus large ». Cependant, à San Francisco, cette perception a été remise en question: « *peut-on considérer les données en elles-mêmes comme de la propriété intellectuelle, ou faut-il en faire quelque chose pour qu'une valeur leur soit attribuée ?* » Si l'on peut la considérer comme relevant intrinsèquement de la propriété intellectuelle, alors, une valeur corporelle distincte relative au capital données, au moins en termes comptables, devra être créée.

Les taxes sur les données

Alors que de nombreuses entreprises soutiennent activement un accord mondial sur l'imposition des données (par le biais de l'OCDE), quelques entreprises américaines ainsi que des leaders politiques s'opposent fermement à ce mouvement. A l'atelier de San Francisco, les participants ont en majorité estimé que « *les gouvernements tentent de trouver le moyen de faire des données une nouvelle source de revenus et cela n'est pas juste* » et que « *l'Union européenne n'est pas en train de taxer les données mais plutôt les activités commerciales des entreprises numériques dans le but de supprimer des échappatoires fiscales* ». D'autres participants estiment que ces initiatives offrent un prétexte aux autres pays qui vont leur emboîter le pas.¹⁰⁶

En Afrique du Sud, les participants considèrent globalement que « *les gouvernements africains n'ont pas la capacité de taxer l'économie numérique, ils ne parviennent pas encore à taxer le secteur pétrolier correctement* ». Certains ont exprimé des doutes quant à la capacité des régulateurs à gérer ce problème. « *...les gouvernements (africains) feront face à de nombreux obstacles s'ils souhaitent taxer les transactions numériques. Il faudrait une meilleure compréhension de la filière des données, c'est-à-dire, lorsque des données sont générées, la valeur qu'elles produisent et qui en profite* ». Les participants ont noté par ailleurs que, même si en théorie les médias sociaux sont déjà taxés dans certaines localités, la raison pour laquelle les Ougandais doivent payer l'équivalent de cinq centimes chaque jour pour se connecter à chacun de leurs réseaux sociaux préférés, quel qu'il soit, est plutôt la réduction de leur liberté d'expression et non une meilleure répartition des revenus.¹⁰⁷ A Jakarta, on a plutôt le sentiment « *qu'il s'agit d'une affaire qui relève de la politique et qui est gérée par le ministre des finances, cela dépend de la manière dont il souhaite lever des fonds* ».

« Il faudrait une meilleure compréhension de la filière des données, c'est-à-dire, lorsque des données sont générées, la valeur qu'elles produisent et qui en profite ».

Enjeux pour la valeur des données

Bien que plusieurs acteurs de l'économie numérique n'aient pas l'idée que les données soient considérées comme un actif, beaucoup d'autres acteurs notamment les gouvernements, les organismes intergouvernementaux, les cabinets de conseils aimeraient bien voir le concept se concrétiser. Pour le moment, les mécanismes ne sont pas forcément cohérents mais si un secteur d'activité ou une région arrive à rassembler autour des principes fondamentaux, une grande vague de changement soufflera sur l'économie. Le défi est de créer un cadre réglementaire propice à la concurrence tout en poussant les organisations ayant l'information comme atout névralgique, à endosser les responsabilités liées aux données qui sont entre leurs mains.

Lors des discussions initiales, les supputations récurrentes au sujet de la valeur des données d'Amazon ou de Google et de leur poids financier montrent qu'actuellement ces éléments ne sont pas intégrés de façon évidente. Si au cours des dix prochaines années, les analystes et les économistes aboutissent à une compréhension commune de la problématique, le fait de considérer les données comme un actif pourrait être un des moteurs les plus puissants de la perception de la valeur des données et pourrait même déterminer le comportement des organisations en termes de redevabilité.



« Un cadre commun consensuel devrait être créé (par secteur d'activité) »

Atelier de Toronto

4.7 Localisation des données



Les états trouvent leur compte dans la conservation de copies des données de tous leurs citoyens ainsi que des données machines dans des centres de données régionaux. Mais dans le même temps, états et entreprises locales souhaitent accéder aux données détenues par des entreprises étrangères.

Contexte

La localisation des données vise à garantir qu'une copie de toutes les données générées à l'échelle nationale reste stockée et accessible dans le pays d'origine. Il s'agit de limiter les flux de données transfrontaliers soit en obligeant les entreprises à conserver les données dans une certaine juridiction, soit en imposant des exigences supplémentaires avant qu'elles ne puissent être transférées à l'étranger. Les objectifs derrière ces restrictions sont variés et incluent la protection de la vie privée, la cybersécurité, le maintien de l'ordre public, la répression, la fiscalité et le développement économique.

La localisation des données connaît un succès auprès du public dans un certain nombre de pays. Dans les pays asiatiques fortement peuplés tels que la Chine et l'Inde, beaucoup de gens pensent que le fait de restreindre l'accès aux données nationales facilitera la croissance économique au niveau local et permettra de consolider le pouvoir politique. Cela implique la mise en place de mesures d'adaptation inédites. En Inde par exemple, en 2018, la banque centrale indienne (Reserve Bank of India) a interdit aux entreprises d'envoyer des données financières à l'étranger, par ailleurs, un projet de politique du Gouvernement envisage d'interdire le transfert international de données générées par les utilisateurs indiens de sites de e-commerce. Le nombre de restrictions de flux de données transfrontaliers a triplé au cours des dix dernières années, on en comptait 80 au moment de la rédaction du présent rapport.¹⁰⁸

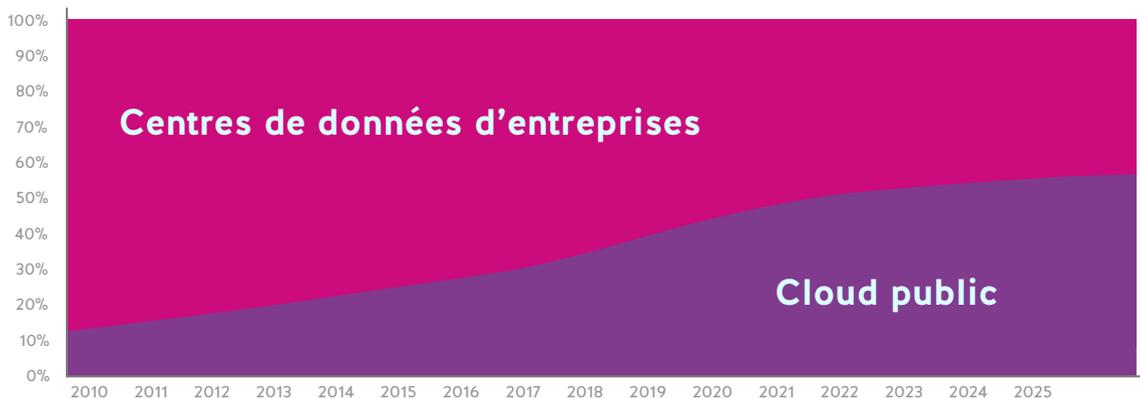


Les détracteurs de la localisation des données estiment pour leur part que cela va plutôt réduire la croissance qu'autre chose. Les cabinets de conseil tels que Deloitte estiment que la localisation a des conséquences négatives sur l'économie.¹⁰⁹ Les défenseurs de la libre circulation des données estiment que les législations locales contreviennent aux principes de libre-échange en rajoutant des contraintes financières lourdes pour les entreprises notamment avec les surcoûts liées à la construction, l'exploitation et la maintenance de centres de données dans plusieurs pays ainsi que la création et la mise à jour d'ensembles de données séparées, même s'il s'agit de bases de données miroirs. De leur côté, il est clair qu'ajouter à cela la corvée de devoir solliciter plusieurs approbations réglementaires pour intervenir sur un marché ou pour se conformer aux règles spécifiques d'un secteur d'activité, va réduire les opportunités.¹¹⁰ Les détracteurs de la localisation pensent, au final, que c'est une mesure contreproductive pour les économies émergentes, elle limite la croissance économique et aura des impacts négatifs sur le développement social.

Ce que nous ont dit les participants

Lors de nos discussions, les défenseurs de la localisation des données ont porté leurs observations sur trois principaux domaines :

- 1. Le développement économique :** encourager les investissements et le développement des centres de données nationaux attractifs et associables à l'investissement direct étranger.
- 2. Les écosystèmes technologiques :** maintenir la croissance des centres locaux d'expertise et d'accès aux données pour promouvoir l'innovation et la croissance des entreprises régionales.
- 3. L'accès aux marchés :** grâce à la réglementation qui serait utilisée comme un levier politique, les multinationales pourraient céder le contrôle des ensembles de données en échange de leur accès aux marchés.



Source: Data Age 2025, sponsorisé par Seagate avec les données de l'IDC Global DataSphere, novembre 2018

Données mondiales : Données stockées dans des clouds publics et centres de données d'entreprises

Développement économique

Dans ce domaine, le fil d'ariane de nos échanges était la problématique de la limitation, à ce jour, des profits de la monétisation des données et de la valeur des données aux seules multinationales, même si l'on a observé une hausse du PIB mondial. A Hong Kong, l'opinion généralement exprimée est « *qu'il y a des entreprises dont les bénéficiaires excèdent le PIB de plusieurs pays et qui détiennent un pouvoir extraordinaire. Ce pouvoir concentré dans le secteur privé et qui n'est pas comptable face aux processus démocratiques, cela peut être très dangereux* ». On a eu le sentiment lors de certains ateliers que les participants, dont certains sont des décideurs politiques, veulent rompre avec cet ordre des choses. A Bangalore, par exemple, l'opinion est que les « *entreprises ne respectent pas les gouvernements lorsqu'elles n'ont pas de personnel présent physiquement dans les pays* ». L'homme le plus riche de l'Inde qui est le Président directeur général de Reliance Group a affirmé que « *les données de l'Inde doivent être contrôlées et détenues par le peuple indien et non par des entreprises et surtout pas des multinationales* ». ¹¹¹ Le Gouvernement est séduit par une telle politique et espère atténuer le pouvoir des grandes entreprises étrangères et stimuler les industries locales à travers une législation visant la localisation des données. La Chine est en train d'adopter une approche similaire et d'autres pays sont en train d'observer tout cela avec intérêt. Lors de notre atelier de Jakarta, des participants ont souligné « *qu'il y a un risque d'élargissement du fossé numérique...en conséquence, le rôle du gouvernement en ce qui concerne la gestion des données doit consister à adopter une approche transformatrice* ».

Toutefois, à Sydney, on a fait remarquer que la législation relative à la localisation des données n'est vraiment intéressante que pour les pays à forte démographie. « Quelques méga pays comme l'Inde peuvent mettre en place leur propre système indépendant mais la plupart des pays qui ne sont pas dans ce cas savent qu'ils n'ont pas une influence assez forte pour limiter le partage des données ».

Ecosystèmes technologiques

Un autre argument en faveur de la localisation est que cette dernière peut stimuler le secteur technologique local. C'est l'opinion partagée à Nairobi, où les participants pensent que cela va « *encourager l'innovation technologique à l'échelle locale* » et « *faciliter l'élaboration et l'orientation d'une législation en faveur de l'augmentation de la consommation de services informatiques et technologiques, comme un aiguillon, capable de déclencher une dynamique de multiplication des centres de données* ». ¹¹² En toute logique, cela devrait pouvoir se faire puisqu'il faudra de toute manière construire plus de centres de données, localement. Toutefois, certains ont considéré qu'une dynamique de création de centres de données risque d'être d'une efficacité limitée car les coûts de stockage dans le pays sont relativement onéreux et il y aura une perte d'opportunité en ce qui concerne le traitement des données étrangères. Ils ont également fait noter que de plus en plus, les chaînes d'approvisionnement de biens sont dotées de flux de données qui circulent dans les deux sens, entre le fabricant et le consommateur. La croissance sera alors restreinte si les données ne peuvent pas être agrégées à l'échelle internationale. ¹¹³ A Manille, à la lumière des différentes contributions, on a estimé que la législation en vigueur en matière de protection des données est assez solide et fournit des dispositifs de contrôle opérationnels pour prévenir d'éventuels abus lors de l'utilisation des données. Par conséquent, au lieu de fermer la porte aux données, il vaudrait mieux positionner le pays comme « *un pôle d'excellence pour le traitement de données provenant d'autres régions ou états* ».

En Inde, la législation en faveur de la localisation des données est en train de créer progressivement une jurisprudence, soutenue par une puissante union entre les leaders du secteur de la technologie, l'Etat, les politiques, sans compter la Reserve Bank of India.^{114 115 116} Les finalités escomptées portent sur la sécurité nationale, le développement économique et le désir de construire des écosystèmes innovants axés sur la technologie. Les multinationales, y compris les entreprises indiennes comme TCS, Infosys et Wipro qui évoluent au sein de cadres conventionnels internationaux, pensent toutefois que cette politique manque de vision.¹¹⁷ A Bangalore, une vision diagnostique évoquée lors des échanges est « *qu'un nouveau compromis peut être consenti, inspiré de normes internationales...cependant, on pourrait toucher le fond avant de réémerger car pour le moment, il n'y a pas de consensus autour de la localisation des données* ».

Accès aux marchés

Avec son Grand pare-feu, la Chine, réussit à contrôler son propre internet. Bien que dans d'autres pays, ils sont nombreux à apprécier le principe d'une politique sectorielle de localisation des données qui serait appliquée à la santé, aux services financiers, certains voient de nombreuses contradictions dans la loi de cybersécurité de la Chine qui est entrée en vigueur en juin 2017 et a été pleinement appliquée au début de l'année 2019.¹¹⁸ Certaines mesures controversées vont affecter les transferts de données personnelles en dehors du pays et empêcher les entreprises qui ne veulent pas respecter ces dispositions de mener des activités dans le pays.¹¹⁹

Une question importante est le niveau d'accès du Gouvernement chinois aux données stockées à l'intérieur de son territoire. Le service cloud de Microsoft Azure en Chine affirme se trouver dans un centre de données installé chez un tiers indépendant

et que l'infrastructure d'AWS est privée. Cependant peu de participants à nos discussions croient que ces données ne sont pas accessibles par l'Etat chinois. Apple, en revanche, a choisi d'utiliser le service de Guizhou-Cloud (GCBD), un centre de données public. Cela a été remis en question lors de l'atelier de Bangkok où l'on s'est montré sceptique vis à vis de l'authenticité de la position d'Apple en matière de vie privé et de confidentialité. En Occident, Apple s'est positionné comme une organisation qui défend le droit à la vie privée en tant que droit civique.¹²⁰ Toutefois, ceux avec qui nous avons échangé, surtout en Asie, pensent que ces principes ont été dilués en échange d'un accès au marché chinois, qui est un marché substantiel.¹²¹ Sans doute, le sentiment qui règne à Bangkok est « *qu'Apple a flanché* ». Par ailleurs, des préoccupations ont été exprimées quant à l'indépendance des entreprises internationales chinoises de technologie qui stockent des données étrangères dans leurs serveurs. Beaucoup pensent qu'elles sont également obligées de donner au Gouvernement l'accès à leurs registres.¹²²

A Hong Kong, la perspective est que « *nous sommes en train d'éprouver des difficultés d'ordre culturel lorsque nous envisageons la gestion de l'Internet dans l'avenir. Quels seraient les implications de la victoire du modèle chinois ? Et que se passerait-il si la Chine exportait ses valeurs dans le monde ?* » Alors que cette bataille culturelle bat son plein, les participants se sont demandé si l'on pourrait se retrouver face à un scénario où il y aurait un ensemble de normes pour l'internet en Occident et un autre pour des territoires clés de l'Asie.

« Les divergences en matière de données sont l'un des symptômes d'un grand conflit systémique...qui est important, parce que plus la Chine va grandir, plus elle sera imitée par d'autres peuples »

Enjeux pour la valeur des données

Dans certains pays, notamment au sein des Etats-Unis et de l'Union européenne, on commence à se mobiliser contre la législation en faveur de la localisation des données. A Washington DC, cette dynamique a été intégrée à celle plus élargie du changement géopolitique. « *Les divergences en matière de données sont l'un des symptômes d'un grand conflit systémique...qui est important, parce que plus la Chine va grandir, plus elle sera imitée par d'autres peuples* ». Il y a également une dynamique forte en Asie du Sud-Est. En Thaïlande et aux Philippines, qui ont des législations distinctes en matière de confidentialité des données, qui pourraient être appliquées en matière de localisation des données dans une certaine mesure, on est plutôt en faveur de l'élaboration de cadres de confidentialité qui protègent les consommateurs, tout en permettant la circulation des données à travers les frontières.¹²³

Certains mettent l'engouement pour une réglementation en faveur de la localisation sur le compte d'un manque d'expertise chez les décideurs politiques. A Bangkok, on a proposé que « *le niveau de connaissance des fonctionnaires en matière de données soient améliorées, de même que leur compréhension de leurs avantages potentiels* ». A Bangalore, on pense « *qu'il y aura un renforcement de la localisation des données à travers le monde mais qu'en même temps on notera une insatisfaction croissante chez les consommateurs qui se plaindront d'un internet plus lent et de nouvelles contraintes sur la vente de biens et la prestation de services. Les investisseurs préféreront peut-être aller voir ailleurs* ».

Dans une logique anti-localisation, Singapour essaie d'inverser la tendance, estimant que ceux qui insistent pour confiner les données au niveau local font peser une menace sur la croissance de l'économie numérique dans la région. Le Directeur de la banque centrale nationale a récemment partagé son point de vue sur le sujet : « si les données ne peuvent pas franchir les frontières, alors l'économie numérique non plus, et cela nous appauvrirait ». De

plus, « *une bonne partie des mesures de localisation des données dans le monde sont dues à des notions malavisées de cybersécurité ou de confidentialité ou pire encore, à des réflexes vieillots de protectionnisme* ».¹²⁴

La localisation des données est un concept qui se trouve piégé dans la dynamique antimondialiste et l'on prend de plus en plus conscience du fossé entre ceux qui produisent les données et ceux qui en profitent. Il n'y a pas si longtemps, les multinationales avaient les coudées franches grâce à l'absence de réglementation, mais maintenant, c'est différent, beaucoup d'entre elles estiment que malgré les coûts et les contraintes supplémentaires, si elles veulent tenir le coup dans les marchés émergents à forte démographie et à forte croissance, elles auront besoin d'un environnement réglementaire stable et cohérent. Une proposition avancée pour la première fois à Bangalore, qui est de « *créer un Conseil mondial des données qui pourrait faciliter les négociations internationales* » a remporté une large adhésion.

En perspective, même s'il y a des avantages à élaborer des principes internationaux, les motifs de discordes entre pays sont si nombreux qu'il serait illusoire de penser que cela pourrait se concrétiser rapidement. Alors que les multinationales et les entités inter-gouvernementales se mobilisent contre la localisation, dans un monde où le patriotisme et le nationalisme gagnent du terrain, ils devront peut-être bien prendre des mesures plus vigoureuses pour répondre aux préoccupations réelles et profondes, liées aux sensibilités culturelles, à la croissance économique et à la sécurité nationale.

4.8 Souveraineté des données



De plus en plus de gouvernements considèrent le contrôle des données nationales comme un moyen de protéger les droits des citoyens, de développer l'économie et de maintenir un sentiment d'identité culturelle.

Contexte

A l'époque des balbutiements d'Internet, les données circulaient librement à travers les frontières, naturellement, et faute de réglementation. La technologie rendait ces échanges d'informations rapides, faciles et abordables et il n'y avait pas de règles, réglementations ou préoccupations publiques poussant à remettre tout cela en question. Les grandes entreprises internationales ont particulièrement joui de cette situation. Mais de nos jours, la situation est toute autre. Ce système est de plus en plus contesté.

La montée du sentiment nationaliste, les inquiétudes persistantes concernant la confidentialité et la sécurité des données, la détermination de certains à imposer le « capitalisme de la surveillance » et l'exigence que les citoyens et les économies locales puissent avoir leur part du gâteau sont des phénomènes qui contribuent à une tendance mondiale visant à restreindre ou mettre un terme à la circulation des données au-delà des frontières nationales. Aujourd'hui, plus de 60 pays sont en train de mettre en œuvre des politiques poursuivant cet objectif. Des débats animés se tiennent entre les gouvernements nationaux, régionaux et le secteur privé afin d'orienter la réglementation de la souveraineté des données dans les Amériques, en Europe et en Asie-Pacifique.¹²⁵ Des pays aussi différents que la Russie, l'Allemagne, la France, l'Indonésie et le Vietnam ont décidé que les données de leurs citoyens seront stockées dans des serveurs physiques au sein des frontières physiques de leur pays. Aux Etats-Unis, certaines agences fédérales souhaitent que leurs données soient exclusivement stockées à l'intérieur



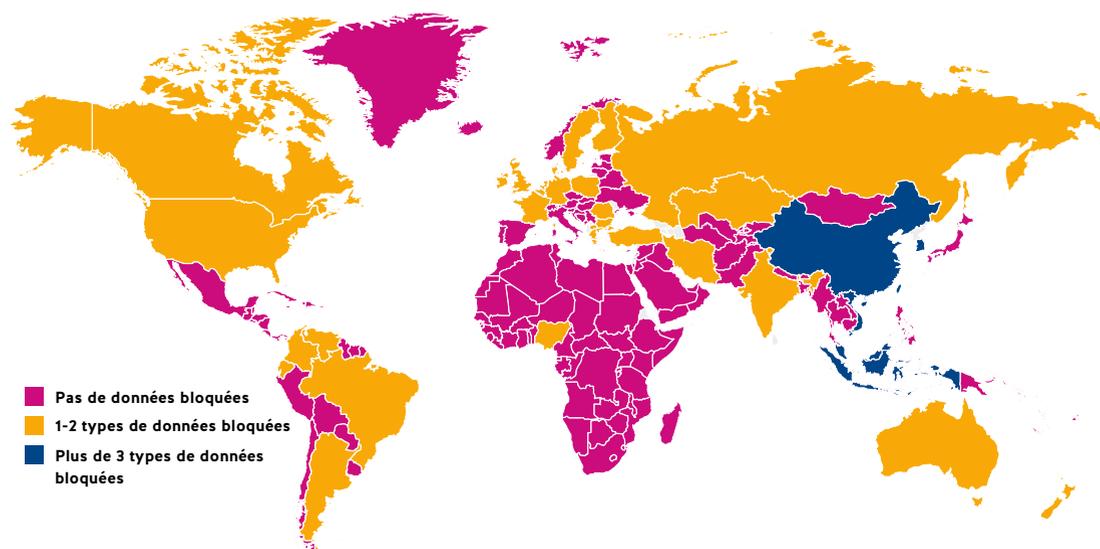
des frontières nationales. L'Australie a clairement défini un cadre légal pour les données médicales. Le Règlement général sur la protection des données (RGPD) de l'Union européenne restreint les transferts de données personnelles de provenance européenne par les organisations, vers tout autre pays, si elles ne sont pas en conformité avec les dispositions pertinentes de la législation en matière de protection des données.

Ceux qui s'opposent à cette tendance avancent l'idée que la libre circulation des données est fondamentale pour l'économie physique et numérique et constitue un ressort vital pour l'innovation. Par conséquent, le développement continu de l'économie numérique et l'augmentation de la productivité dans les industries traditionnelles dépendent de la capacité à transférer des données y compris les données personnelles des consommateurs au sein d'un pays et au-delà, pour une analyse, un traitement et un stockage efficaces. De plus, la liberté de mouvoir

des données personnelles sans restriction entre pays a des retombées positives, non seulement pour les organisations, mais également pour les citoyens et les pays. Cela est particulièrement vrai pour les pays dirigés par des gouvernements autoritaires où pèsent des atteintes à la liberté d'expression.

Mais alors, pourquoi défendrait-on autant la souveraineté des données ? Lors de nos discussions, trois raisons fondamentales justifiant l'attrait pour cette idée ont été identifiées :

1. La sécurité nationale
2. La surveillance des citoyens
3. L'impérialisme des données



Pays bloquant la circulation mondiale des données (2017)

Ce que nous ont dit les participants

Sécurité nationale

En Inde, les participants ont fait remarquer que dans le futur, « *les acteurs clés seront ceux qui sont riches en données et non ceux qui sont riches en argent, la quantité et la disponibilité des données plutôt que le poids économique du pays, définiront les traités multilatéraux et l'ampleur de la souveraineté en matière de données* ». Nombre de nos interlocuteurs partagent cet avis et de nombreuses discussions ont été menées sur la protection des données nationales sensibles de tous ordres, surtout dans ce contexte d'évolution technologique du secteur des données qui facilite toujours davantage le partage transfrontalier des données. Dans ce sens, les techniques de surveillance des Etats-Unis et de la Chine ont fait l'objet d'un débat intense. Notre atelier a envisagé les façons dont les pays pourraient renforcer leur sécurité numérique en restreignant la circulation transfrontalière des données et en investissant dans l'hébergement dématérialisé (Cloud Computing).¹²⁶ Un certain nombre de gouvernements dont le Brésil, l'Inde et l'Union européenne ont déjà tenté d'investir ce terrain.¹²⁷ Ailleurs, notamment à Singapour, Jakarta et Hong Kong, les conversations mettent en évidence le besoin des états de maintenir le contrôle des données de leurs citoyens pour des raisons de sécurité nationale. Le problème qui se pose à Jakarta est qu'actuellement, « *les courriels du Gouvernement, des entreprises et des particuliers sont très dépendants des plateformes occidentales* ». Toutefois, des dispositions réglementaires sont en cours d'élaboration pour faire face à ce problème.

A Singapour, où la confiance au Gouvernement est grande, beaucoup de participants sont convaincus de l'importance de la souveraineté des données pour garantir la sécurité nationale, surtout en ce qui

concerne le partage des données médicales : « *bien que pour l'instant, il n'y ait pas d'indication pertinente sur l'ampleur de l'impact que pourrait exercer le partage des données patients sur la sécurité publique...actuellement, nos loisrestreignent le partage de données personnelles (y compris les données médicales) au-delà des frontières nationales* ».

Surveillance des citoyens

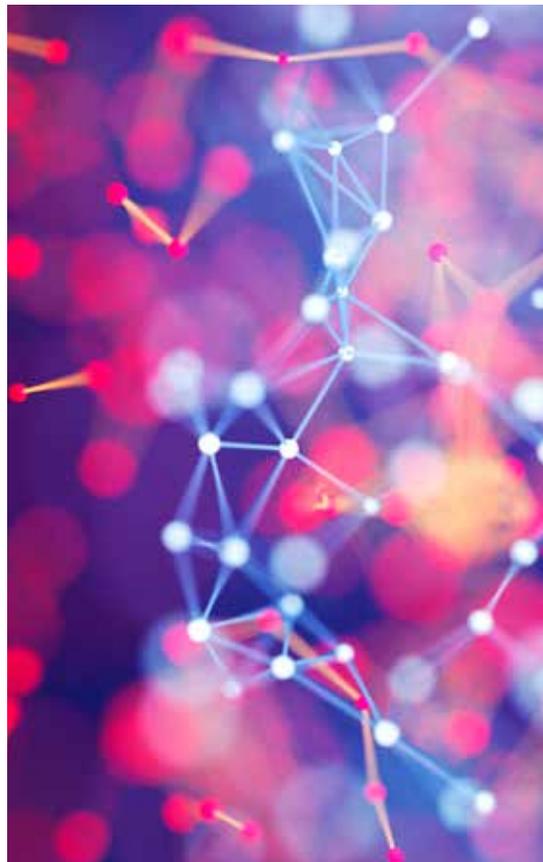
Certains participants estiment que la surveillance de plus en plus soutenue exercée par l'Etat est indispensable pour la sécurité nationale, tout en reconnaissant qu'elle peut attenter aux droits individuels. A Pretoria, les participants ont reconnu la nécessité d'adopter une approche nuancée en faveur d'un exercice équilibré de la sécurité nationale, laissant la liberté de partager et de consulter les données personnelles. Une des questions posées est la suivante : « *comment devons-nous gérer la législation sur les communications personnelles au nom de la sécurité nationale, surtout dans les états fragiles et non démocratiques de l'Afrique ?* » Les participants se sont également interrogés sur la valeur de la souveraineté des données dans des pays où la confiance en l'Etat est faible ou inexistante et ont fait remarquer que « *s'il y a un « paralysie internationale », il n'y aura pas de moyen de protester en dehors d'Internet, les données peuvent être utilisées là où la loi ne peut pas agir* ».

« Les acteurs clés seront ceux qui sont riches en données et non ceux qui sont riches en argent, la quantité et la disponibilité des données plutôt que le poids économique du pays, définiront les traités multilatéraux et l'ampleur de la souveraineté en matière de données ».

Atelier de Bangalore

A Singapour, il a été noté que « *la question fondamentale est de savoir comment établir une hiérarchie des droits entre individus, citoyens, entreprises et gouvernements* ». En Chine, garder le contrôle de toutes les données produites par les citoyens permet au Gouvernement de produire sa propre notation sociale et de maintenir son contrôle sur la population. Une note a été attribuée à chaque citoyen en fonction de son « historique comportemental », et ceux dont la note est faible, subissent des restrictions d'accès aux services et de liberté de voyager, pouvant aller jusqu'à l'annulation du passeport. Ce niveau de surveillance s'étend à tous les aspects de la vie du citoyen. A Shanghai, nous avons entendu dire que « *toutes les données médicales chinoises devront être stockées dans les serveurs de l'une des trois entreprises chinoises plébiscitées par le Gouvernement, d'ici à 2020* ». Lors d'une autre discussion en Chine, nous avons été informés de l'augmentation des hôpitaux sur Internet qui sont en train de consolider des millions de dossiers patients et qui permettent l'identification massive des personnes ayant des caractéristiques spécifiques représentant un intérêt.

Le Gouvernement russe exige également un accès plus poussé aux données personnelles de ses citoyens. En effet, le Président Putin a récemment introduit une loi sur la « souveraineté numérique » qui, en théorie, permettra au Kremlin de censurer ou de couper l'Internet dans le pays. En pratique, cela pourrait être difficile à concrétiser car les fournisseurs d'accès Internet russes disposent de serveurs à l'étranger et le Gouvernement russe aurait besoin de la coopération de l'Occident pour y parvenir. Jusqu'ici, Facebook et Google résistent à la demande de la Russie de révéler l'identité de leurs utilisateurs. Mais la pression ne cesse de s'intensifier pour qu'ils se conforment à la loi.



« La question fondamentale est de savoir comment établir une hiérarchie des droits entre individus, citoyens, entreprises et gouvernements »

Atelier de Singapour

Impérialisme des données

Partout dans le monde, nous avons entendu les préoccupations des participants concernant le fait que les multinationales, surtout américaines, ont bâti des empires en traitant les données comme une ressource naturelle que l'on peut extraire et exploiter sans une compensation équitable pour ceux qui les ont générées.

A Madrid, on était entièrement d'accord que « *les services occidentaux dominants, conçus par des ingénieurs occidentaux, reflétant des valeurs occidentales et élaborés à partir de données occidentales seront de plus en plus perçus comme une imposture impérialiste, inconséquente ou inadaptée dans des régions culturelles différentes* ». Ailleurs, on a observé un rejet généralisé de ce qui est perçu comme la cupidité de l'Occident. Lors des échanges à Nairobi et à Johannesburg, l'intérêt a été porté sur le moyen de s'assurer que les données africaines ne seront pas exploitées par les entreprises internationales comme des ressources naturelles. L'Afrique du Sud, par exemple, a restreint le partage d'échantillons sanguins avec les entreprises basées aux Etats-Unis, telles que ancestry.com et 23andme, pour le profilage génétique, parce que « *nous ne voulons pas que les données africaines « bon marché » soient monétisées par d'autres* ». A Nairobi, les participants ont exploré les possibilités offertes pour protéger la culture africaine. La législation sur la souveraineté des données devrait, à leur avis, assurer « *qu'à l'avenir, nous respectons les origines des données sur les cultures africaines et que nous les monétisons nous-mêmes* ». ¹²⁸ Ils ont également envisagé des moyens de protéger les données africaines, en élaborant « *des réglementations (nationales) appropriées et en installant la transparence des données pour mettre en œuvre cette monétisation* ». Ces dispositions devraient prévoir « *des modèles de valeurs partagées et des cadres de communication et de restitution clairs* ».

A Dakar, on a plaidé pour « *l'utilisation de la valeur des données dans l'intérêt national et non pour le seul bénéfice des entreprises internationales* ». Des opinions similaires ont été exprimées à Abuja.

« *L'Afrique a besoin de politiques plus précises sur les données, savoir ce qui est collecté, pourquoi et par qui* ». A Abidjan, des participants ont proposé une coopération renforcée entre états africains : « *alors que les préoccupations liées à la sécurité vont croissantes, et que l'assurance des développeurs africains s'affermir, les ivoiriens souhaitent de plus en plus contrôler les données qu'ils produisent et être moins dépendants des états occidentaux* ».

A Johannesburg, où la réglementation visant l'application de la loi de protection des informations personnelles, POPI, est entrée en vigueur en décembre 2018, on a le sentiment qu'une approche régionale visant la protection des données des citoyens devrait être élaborée afin de dynamiser l'économie locale. Les étudiants de Pretoria partagent cet avis et proposent que « *L'Afrique crée ses propres serveurs et ses propres systèmes* » et plaident pour la « *décolonisation des données* », afin que *L'Afrique puisse prendre le contrôle des données qui sont générées sur le continent* ». Et si les gouvernements sont prêts à investir, beaucoup de participants encouragent fortement « *le développement de média et de contenus régionaux spécifiques, en utilisant les données africaines afin que cela soit plus adapté au marché local, ce qui ferait baisser le coût des services et améliorerait l'offre faite aux consommateurs* ».

« Les services occidentaux dominants, conçus par des ingénieurs occidentaux, reflétant des valeurs occidentales et élaborés à partir de données occidentales seront de plus en plus perçus comme une imposture impérialiste, inconséquente ou inadaptée dans des régions culturelles différentes »

Atelier de Madrid

Certaines préoccupations liées à une éventuelle instrumentalisation de la demande de « souveraineté » par les états-nations autoritaires pour atteindre leurs propres visées totalitaristes au lieu de protéger leurs citoyens de l'intrusion et de l'exploitation étrangère, ont été exprimées. Pour limiter ce risque, les participants de Johannesburg estiment que même si les états imposent une législation en matière de souveraineté des données, il faudrait des « indicateurs de dignité des données » convenus à l'échelle internationale, qui permettent la supervision et l'utilisation des données comme un bien commun, tout en préservant « *la dignité des citoyens* ». A leur avis, cela aurait l'avantage de limiter d'éventuels abus de pouvoir. Si la clarté n'est pas établie, ils craignent que la liberté d'expression soit restreinte et que le protectionnisme « *étouffe l'innovation* » et « *suscite le doute quant à la capacité des données à engendrer le bien, sans compter la menace d'une corruption commerciale et administrative généralisée* ».

Les participants à l'atelier de Sydney ont été plutôt favorables aux motivations de la souveraineté des données : « *vous préférerez sans doute être manipulés par votre propre gouvernement plutôt que par un autre* » a-t-on fait noter. Toutefois, de nombreux participants étaient d'avis « *que les effets résident dans la nature des données en question : Singapour exerce un contrôle rigoureux des données médicales, mais reste ouvert pour ce qui concerne les données commerciales. En Australie, nous maintenons la souveraineté des données relatives aux services financiers* ». Ce que l'on peut retenir en analysant ces échanges, c'est que « *seuls quelques méga-pays seraient en mesure de créer leur propre écosystème, mais la plupart des pays savent qu'ils ne pourront pas se permettre de renoncer au partage des données* ».

Ailleurs, même si l'on a reconnu que la souveraineté des données peut avoir un impact, lors des ateliers en Europe et aux Etats-Unis, les participants étaient plutôt rares à croire que cette approche pourrait prendre de l'ampleur. A Londres, les échanges ont

eu lieu après nos ateliers en Afrique, les participants ont rejeté l'idée d'impérialisme des données qu'ils jugent infondée. Leur perspective est que « *la souveraineté des données n'est pas une bonne chose et que la circulation des données devrait être assurée* ». De même, lors des échanges à San Francisco, la souveraineté des données a été considérée comme une réaction excessive. Un participant a affirmé qu'il « *ne faudrait pas tirer sa poudre aux moineaux, la législation a 5 ans de retard sur la vraie vie* ». On a l'impression que pendant que les autres pays s'inquiètent de la souveraineté des données, « *aux Etats-Unis nous poursuivons notre chemin, nous nous concentrons davantage sur les moyens permettant de mieux exploiter les données* ». Une observation a été faite par ailleurs : « *on a le sentiment que les autres pays utilisent la souveraineté des données comme une excuse pour ne pas avancer* », et « *nous, nous avons des défis plus importants à relever* ».

« Singapour exerce un contrôle rigoureux des données médicales, mais reste ouvert pour ce qui concerne les données commerciales. En Australie, nous maintenons la souveraineté des données relatives aux services financiers »

Atelier de Sydney

Enjeux pour la valeur des données

La façon dont la souveraineté des données est perçue dépend d'un certain nombre de facteurs et de motivations. Il est plus facile de croire que la souveraineté des données est une « bonne chose » si les citoyens ont confiance en leur gouvernement et en sa capacité d'utiliser les données pour protéger leurs droits et promouvoir leurs intérêts nationaux. Cependant, dans les pays où le niveau de confiance au gouvernement est faible, la souveraineté des données pourrait être utilisée pour restreindre la liberté d'expression et le contact avec le monde extérieur. Auquel cas, nombreux sont ceux qui diraient que c'est « une mauvaise chose ».

La taille a également son importance. La Chine, la Russie et l'Inde sont des « grands » pays et sont naturellement dans une meilleure position pour utiliser la souveraineté des données à leur avantage, que les « petits » pays. Leur poids économique combiné est sans doute substantiel. De nombreuses entreprises de technologie occidentales reconnues sont tentées d'étendre leurs activités à ces marchés tous aussi tentants et aux marchés de l'Afrique, qui combinent les avantages d'une population jeune et d'une classe moyenne en croissance. Ces dernières s'opposent à l'idée de souveraineté des données. Si la dynamique de souveraineté se poursuit, une bonne partie des données qui seront générées à l'avenir pourrait être exclue de l'économie mondiale.

Il y a sans doute beaucoup à faire pour remédier aux préoccupations très concrètes relatives à la protection des données des citoyens, que nos interlocuteurs ont exprimé. Une plus grande confiance, une plus grande collaboration entre les nations est nécessaire. Sans cela, nous pouvons nous attendre à une action plus restrictive des états pour confiner les données. Si les choses se passent ainsi, la réaction au plaidoyer pour la souveraineté des données que nous avons observée à Londres et à San Francisco paraît quelque peu dénuée de sagesse, face à un paysage politique en constante évolution.

« Il ne faudrait pas tirer sa poudre aux moineaux, la législation a 5 ans de retard sur la vraie vie »

Atelier de San Francisco

4.9 Qualité des données



Plus nous cherchons à comprendre l'environnement des données, plus nous observons que les préoccupations liées aux données biaisées, aux données de qualité insatisfaisante ou à l'inexactitude des données augmentent. Nettoyer et valider les données de nature sociale, politique ou commerciale constitue un réel combat.

Contexte

Qu'il s'agisse de simples tâches administratives, de réflexions inédites, de prise de décision ou de mise en œuvre de décisions, si les données qui alimentent ces processus sont fausses, les résultats seront presque inévitablement insatisfaisants, inefficaces et potentiellement dangereux, avec des effets délétères.¹²⁹

Les données les plus précieuses doivent être de bonne qualité. Les organisations ne veulent certainement pas de données médiocres. Les

organisations qui maîtrisent parfaitement la façon dont leurs données sont mobilisées, indexées et stockées sont plus aptes à en assurer la qualité. Celles qui cherchent à combiner des informations de sources externes proposant divers degrés de qualité et de cohérence, ne sont pas à l'abri des mauvaises surprises. C'est la raison pour laquelle, « nettoyer » les données est un enjeu de taille. La question qui a préoccupé les participants à nos ateliers est de savoir si nous sommes réellement à la hauteur du défi lié aux répercussions des données de mauvaise qualité. Si la réponse est : « ça ne va pas trop », alors il faudrait se préparer à une débandade dans toutes sortes de domaines automatisés y compris les politiques, les investissements et même les décisions sociales. Imaginez des écarts de subventions publiques dues à des données de recensement inexactes, des enfants séparés de leur parents à tort à cause d'erreurs dans les algorithmes des services sociaux ou de manière plus prosaïque, la duperie des usagers des sites de rencontre en ligne.



Le défi

Lors de nos ateliers, nous avons distingué trois types de données de mauvaise qualité : les données insatisfaisantes, les données biaisées et les données inexactes.

- **Les données insatisfaisantes** sont incomplètes, obsolètes, non concordantes, mal traitées ou tout simplement fausses. Les causes sont diverses, allant des données saisies dans des colonnes inappropriées au données doublons en passant par les saisies incohérentes, les fautes d'orthographe, ainsi de suite.
- **Les données biaisées** correspondent davantage à des ensembles de données créées pour générer une image. Elles sont devenues particulièrement sensibles car les algorithmes

d'apprentissage machine sont basées sur ces ensembles de données pour faire des projections et prendre des décisions ; un ensemble de données biaisées peut refléter des biais qui existent déjà dans la société comme par exemple, le fait que les postes les plus intéressants sont occupés par des hommes blancs d'âge moyen. Il peut également refléter les valeurs des codeurs, les réponses à des questionnaires d'enquêtes qui ont été conçus avec un parti pris, ou provenir d'un problème de processus ou d'une conception comme par exemple, une déclaration dans une rubrique inappropriée, une sélection non aléatoire à l'échantillonnage, des erreurs de mesure systématiques.

- **Les fausses données** ont été fomentées délibérément pour induire en erreur – même si elles peuvent paraître d'excellente qualité et proviennent de sources vérifiées. Il s'agit



également d'un point hautement sensible, quand des fausses informations sont délibérément partagées dans les média sociaux. Elles peuvent aussi être générées lorsque les personnes communiquent délibérément des fausses données parce qu'elles n'ont pas confiance aux organisations avec lesquelles elles partagent ces données.

L'ampleur et la portée de ces trois types de données ne font que croître. Elles peuvent rendre l'utilisation de certains ensembles de données difficile voire impossible et si les inexactitudes ne sont pas repérées corrigées et isolées, elles finissent par polluer les bonnes données et affecter les décisions qui en dépendent.

Gérer les données de qualité insatisfaisante

Déterminer si les informations sont exactes reste encore une tâche manuelle, fastidieuse et coûteuse même si l'IA et l'automatisation des tâches commencent à servir dans ce domaine. Cela explique pourquoi en 2018, la compagnie pharmaceutique mondiale Roche était prête à racheter pour 1,9 milliards de dollars, Flatiron Health, une start-up dont la spécialité est de nettoyer les données cliniques et plus particulièrement celles qui sont liées au cancer. La compétence qui a retenu l'attention de Roche ici, est la contribution humaine à l'extraction des données.¹³⁰

Beaucoup d'entreprises sont aux prises avec l'amélioration rapide et peu coûteuse de la qualité de leurs données. Certains se concentrent davantage sur la saisie des données, d'autres cherchent des moyens de corriger les erreurs. Une alternative serait d'utiliser uniquement les bonnes données et de se débarrasser des « mauvaises » mais dans cette approche, il est essentiel de définir clairement « les bonnes données. Du point de vue de la santé, par exemple, il y a une perspective émergente qui soutient que ce n'est pas parce qu'une donnée n'est pas de qualité médicale qu'elle n'a pas de valeur. La question est de savoir si l'information est appropriée.

Dans tous les cas, il s'agit d'un exercice fastidieux et coûteux, 80% du temps des spécialistes de données et consacré au nettoyage des données.¹³¹

Les données biaisées

La plupart des préoccupations liées aux données biaisées portent sur les ensembles de données utilisées pour entraîner et raffiner les algorithmes automatisés. A Washington DC, le cas du programme de recrutement d'Amazon a été débattu. Les modèles informatiques d'Amazon ont été entraînés à valider des candidatures, en observant des tendances dans les CV envoyés à l'entreprise sur une période de 10 ans. La plupart des candidatures étaient masculines, le reflet de la prédominance de la gente masculine dans le domaine des technologies. Le résultat était que le système d'apprentissage automatisé a conclu de lui-même que les candidats masculins étaient préférables. Il n'est pas garanti que d'autres méthodes de sélection de candidats se révèlent discriminatoires selon la même logique. En effet, les algorithmes d'Amazon semblaient aussi avoir un faible pour les hommes qui jouent à la crosse et qui s'appellent Jared.^{132 133} Amazon a depuis, abandonné le projet. C'est un bon exemple de la difficulté de gérer les biais. Etant donné que près de 55% des responsables des ressources humaines américains espèrent recourir à l'IA dans les cinq prochaines années, cette situation est extrêmement préoccupante rien que dans ce domaine somme toute restreint du recrutement.¹³⁴

« Il y a un cercle vicieux : les fausses données entraînent la méfiance et la méfiance entraînent les fausses déclarations ».

Atelier de Hong Kong

Un autre exemple évoqué lors de nos ateliers est que les algorithmes d'IA utilisés pour déterminer qui doit aller en prison perdent le nord, à cause de leur dépendance vis-à-vis des données historiques.¹³⁵ En 2016, les tribunaux américains ont adopté des outils d'évaluation de risques qui génèrent des notes sur la récidive. Les décisions sont prises par des algorithmes d'apprentissage machine qui utilisent des données historiques pour sélectionner des tendances associées au crime, en vue de produire un chiffre unique estimant la probabilité pour un prisonnier de récidiver. Un juge prend alors cette note en considération dans la décision relative à la réhabilitation du prisonnier ou à la durée de sa peine. Cela signifie que les populations qui ont été historiquement ciblées par la police telles que les communautés à faibles revenus et les minorités, risquent d'avoir des notes de récidive très élevées. Cela implique par conséquent que les algorithmes pourraient amplifier les biais préétablis et générer des données encore plus biaisées pour perpétuer le cycle. Puisque la plupart des algorithmes d'évaluation de risques sont propriétaires, il est impossible de remettre en question leurs décisions et de leur faire assumer leurs responsabilités.

Certains participants étaient préoccupés par le manque de diversité dans le secteur de la technologie et par l'impact que cela a sur l'évolution de l'IA. A l'échelle mondiale, seul 22 % des professionnels de l'IA sont des femmes. Plus les algorithmes déterminent les finalités sociales, plus les équipes de développement de logiciels doivent assurer la diversité, afin d'identifier les cas où les biais faussent les décisions. Bien qu'il y ait une demande de plus en plus forte de codeurs, inventeurs et investisseurs féminins pour que les technologies reflètent plus fidèlement la société, les améliorations prennent du temps à se faire sentir. Certains craignent qu'il y ait un effet-club, dont l'inconvénient serait qu'en constatant que leurs congénères sont peu nombreuses dans ce secteur, les femmes soient peu enclines à suivre

cette filière. Les employeurs ne peuvent pas à eux seuls défaire les discriminations liées au genre mais ils peuvent prendre des mesures de mitigation, par exemple, en proposant des parcours de formation techniques aux femmes en reconversion et en se montrant plus transparents en matière de rémunération et d'opportunités.

L'IA peut aider à mettre la vérité à jour à partir d'ensembles de données confuses et sera utilisée avec succès dans différentes applications. Toutefois, des risques y sont associés. Un sujet récurrent de conversation lors de nos ateliers a été la nécessité pour les entreprises d'établir un processus transparent de contrôle du comportement éthique de leurs systèmes d'IA. Cela pourrait inclure des normes communes pour l'entraînement des données, pour la conception d'algorithmes ainsi que des applications concrètes dans le monde réel. Une partie de la solution résiderait dans la réglementation, avec notamment des amendes lourdes en cas de non-respect des normes. En outre, des efforts concertés pour veiller à une prise de conscience chez le public des problèmes éventuels pourraient être envisagés.

« L'étiquetage permettra de déterminer la véracité des informations et peut être que l'estampillage de la source des informations d'actualité permettra au public d'identifier les chaînes responsables ».

Atelier de Mexico

Les fausses données

Les fausses nouvelles (fake news) sont devenues un sacré casse-tête autant pour les entreprises que pour les gouvernements. Il y a un marché de plus en plus conséquent pour l'exploitation de la vulnérabilité du monde numérique, et des acteurs fort malins et parfois sans scrupules se chargent de l'entretenir. Les fausses nouvelles peuvent être tellement sophistiquées que les identifier relèverait d'une gageure. Les activistes mettent la pression sur les gouvernements pour qu'ils mettent en place des règles plus sévères pour protéger davantage la société civile. Certains envisagent l'adoption de protocoles internationaux plus strictes comme celles qui restreignent la vente d'armes.

L'essentiel de ce débat dépasse le cadre du présent rapport, mais les fausses nouvelles ne constituent pas la seule forme de fausses données. Lors de nos échanges à Washington DC par exemple, il a été souligné que près de 20% des données du recensement des Etats-Unis seraient inexactes, principalement parce que les citoyens qui les déclarent redoutent la réaction du Gouvernement s'ils déclarent les vraies informations. Les agents chargés du recensement ne sont pas autorisés à effectuer des manœuvres de compensation ou à mitiger ce phénomène, même s'ils savent que 20% du contenu des ensembles de données clés est inexact. Dans cet exemple, les fausses déclarations sont essentiellement motivées par la crainte de l'intervention de l'Etat chez le public et chez certaines communautés. Souvent, ceux qui ont besoin de soutien, comme les pauvres, les nouveaux immigrants, les personnes âgées, déclarent sciemment de fausses informations sur leurs revenus, leur santé, leur âge. L'ironie est que sans les données de recensement qui permettent d'identifier les besoins, les décideurs politiques sont incapables de justifier leurs demandes de fonds supplémentaires pour appuyer ces mêmes personnes qui ne déclarent pas

les informations adéquates. Lorsque nous avons abordé le sujet quelques jours plus tard à Toronto, les participants ont reconnu que chez eux aussi, des problèmes statistiques similaires existent, mais que les agents au Canada sont autorisés à « corriger » les ensembles de données sur lesquels le problème est identifié afin d'éviter d'induire en erreur les politiques et les activités.

Ce n'est probablement pas grave de déclarer une fausse adresse électronique pour se connecter à un réseau wifi public ou pour acheter une paire de chaussures mais cela peut le devenir lorsqu'il y a des conséquences néfastes. Au Nigéria, le niveau de méfiance est tel que peu de gens déclarent des informations exactes ou des adresses emails correctes aux agences gouvernementales. Comme cela a été observé à Hong Kong, il y a un cercle vicieux : les fausses données entraînent la méfiance et la méfiance entraîne les fausses déclarations ». Le défi se pose réellement lorsque les données doivent être authentiques pour permettre d'identifier un individu, une machine ou un lieu. Le principe d'identité numérique est important à ce niveau, il a d'ailleurs été exploré en détail dans un autre projet de Future Agenda.¹³⁶

« Il faut faire attention à ne pas faire du mieux l'ennemi du bien. Ce n'est pas parce que des biais ont été identifiés que les données sont intrinsèquement mauvaises ».

Santiago workshop

Ce que nous ont dit les participants

Partout dans le monde, il y a une grande préoccupation au sujet de la provenance et de la fiabilité des informations présentées aux usagers des média sociaux et du rôle des algorithmes dans l'élaboration des informations. A Bangalore, « *on est de plus en plus préoccupé par la supervision et le contrôle des média sociaux, le but étant de limiter la manipulation des consommateurs par les entreprises et d'autres organisations* ». A Mexico City, on craint que « *la discrimination ne devienne un réel problème surtout quand la reconnaissance faciale deviendra plus courante* ». A Singapour, on est plutôt optimiste : « *l'IA sera plus sophistiquée et contribuera à détecter les fraudeurs, mais nous ne sommes pas sûr qu'elle sera assez rapide pour détecter les fausses nouvelles avant qu'elles ne soient publiées...L'étiquetage permettra de déterminer la véracité des informations et peut être que l'estampillage de la source des informations d'actualité permettra au public d'identifier les chaînes responsables* ».

De nombreux participants ont évoqué la confiance apparemment aveugle à l'égard des algorithmes et précisé que même les données nettoyées peuvent contenir des biais. A Madrid, plusieurs participants ont souligné que « *les données biaisées servent de plus en plus à effectuer des sélections automatisés* ». ¹³⁷ Au Canada, on a suggéré de gérer les biais en faisant de la « *sensibilisation sur les algorithmes et NON sur l'élimination des biais, parce que nous devons savoir pourquoi les données ont été élaborées* ».

A Santiago, on a proposé de s'interroger sur « *la possibilité de mesurer les biais* ». Est-il possible de développer un référentiel de la qualité ou un système d'alerte sur les données, indiquant si oui ou non les données sont exemptes de biais, modérément biaisées ou extrêmement compromises ? Cependant, à Hong Kong on pense « *qu'il faut faire attention à ne pas faire du mieux l'ennemi du bien* ».

Ce n'est pas parce que des biais ont été identifiés que les données sont intrinsèquement mauvaises ». Cela dit, au cours du même atelier, il a été reconnu « *qu'il y a un risque que les données biaisées soient intégrées aux programmes d'IA, ce qui va mener à une marginalisation perpétuelle de certains individus* ». Ce qui est sûr, c'est que, dans la mesure où l'apprentissage machine est rétrospective, plus on va s'appuyer sur lui, plus les biais risquent de s'enraciner.

Une des solutions proposées a été « *d'envisager l'élaboration de cadres réglementaires stricts qui requièrent des évaluations du potentiel de nuisance des données d'applications et de continuer à surveiller les nuisances effectives qui surviennent dans le monde réel* ». Certains participants de Hong Kong se sont demandé également « *s'il ne faudrait pas créer ou désigner une organisation internationale qui établisse des principes autour des biais* ». Toujours à Hong Kong, il a été précisé que « *l'enjeu est de déterminer quelle institution sera capable d'identifier et d'exclure les biais, ceux qui proviennent des données de base comme ceux qui sont constatés à l'issue des traitements. Faudra-t-il prendre en compte les faits avérés dans ce processus* ». En outre, « *il est difficile pour le moment de savoir si les résultats seront positifs ou négatifs. Il y a pleins d'exemples de biais en Chine, sur beaucoup de points, cela va des prêts hypothécaires au Sida en passant par les sanctions pénales, la diversité et l'inclusions sociales, et il est difficile de déterminer comment les personnes ont été catégorisées* ».

Une autre réflexion évoquée à Sydney est que « *les données biaisées pourraient être source d'inégalités* ». A Londres, dans une prospective à l'échéance 2030, certains participants sont du même avis et prédisent « *une augmentation de l'exclusion sociale à travers des biais intégrés à la source dans les processus automatisés, les réseaux et chez les concepteurs* ». Au Nigéria, il s'agit d'un problème à dimension plutôt sociétale puisque « *la corruption et la méfiance vis-à-vis du système est à la source de l'amorcellement* ».

de fausses données et de fausses nouvelles ». Les gens déclarent sciemment des fausses informations au Gouvernement et aux entreprises. Cela « *remet en cause la fiabilité de nos bases de données parce que les citoyens prennent le parti de ne pas déclarer les bonnes informations* ». Au-delà de l'éradication de la corruption, d'autres suggestions portaient sur une meilleure éducation du public pour combattre ce problème et sur la « *sensibilisation sur les avantages du partage des données fiables* ».

Perspectives

L'appréciation de cette problématique à Copenhague peut se résumer ainsi : « *au fond, nous devons avoir une vision objective de ce que sont les bonnes données, mais il est aussi essentiel de s'entendre sur ce qu'est « l'objectivité »...un des enjeux fondamentaux en perspective, est de savoir qui va en décider* ». Les participants ont reconnu que « *pour les recensements nationaux, on risque de traverser une période d'anarchie des données et de prédominance des fausses données avant que les choses ne changent* ».

Lors du dernier atelier à Santiago, les participants ont partagé ce sentiment et ont déclaré que « *d'ici à 2030, la réglementation actuelle devra être mise à jour. Les décideurs politiques doivent être formés sur ces questions et être au moins capables de s'entendre sur l'utilisation appropriée des algorithmes et d'identifier les données biaisées* ». Nous devons également réfléchir à la taxonomie et à la classification des algorithmes. « *Le défi sera d'étendre la protection juridique à tous les domaines de la vie, notamment à la grande diversité de situations qui pourraient induire des effets discriminatoires qui vont avoir un impact sur les personnes et sur les tiers* ».

Certains participants ont prôné la création d'une « *Organisation mondiale des données, qui peut établir des principes sur la qualité et les biais* ». ¹³⁸ Toutefois, contrôler la propagation des fausses données est une tâche plus délicate. Les fausses

données contaminent les ensembles de données fiables, faussent notre perspective et induisent progressivement en erreur sur les actions à mener.

Enjeux pour la valeur des données

Si nous comptons pouvoir utiliser nos données à l'avenir, même avant de songer à leur valeur pour la société ou l'économie, alors il faut qu'elles soient fiables. L'opinion des participants, qui ont évoqué cette problématique de la qualité lors de nos ateliers, est que la société n'est pas encore suffisamment consciente de son ampleur et de sa complexité. Une réelle transparence et des processus de reddition des comptes sont des solutions, mais la qualité des données de base est aussi importante. Cependant, accepter et gérer des données brutes contaminées associées à des données propres est une situation à laquelle beaucoup devront s'habituer. Dans la plupart des applications, quelques inexactitudes restent tolérables mais cela ne peut pas devenir la norme. Pensez aux données cliniques. Un consensus mondial sur les niveaux de pertinence requis serait utile dans ce cas, avec l'appui d'une institution qui peut établir des normes et jouer le rôle d'arbitre lorsqu'il y a des différends.

Il est clair que les organisations qui peuvent nettoyer les données efficacement, rapidement et avec précision apportent une valeur ajoutée et ces ensembles de données structurées et de haute qualité produiront une valeur supérieure. Les données devenant de plus en plus intégrées aux opérations de notre société et de notre économie, maintenir et garantir leur qualité est essentiel.

4.10 Une question d'éthique



L'utilisation éthique des données est une préoccupation importante mais il y a des initiatives collectives qui visent à créer une approche mondiale. Les secteurs d'activités établissent leurs propres normes et essaient de s'aligner sur des principes communs.

Contexte

Au début de la révolution des données, les acteurs les plus impliqués dans les données, notamment leur collecte et leur utilisation, avait très peu de recul sur les implications sociales de leurs activités. Cependant l'utilisation et le contrôle des données posent de nombreuses préoccupations d'ordre éthique. L'éthique porte sur les principes moraux qui orientent les actions et les comportements d'un individu. Cela ramène à la façon dont les personnes se traitent mutuellement : à l'intention d'un individu vis à vis d'un autre, qu'elle soit bienveillante, indifférente ou hostile et au comportement d'un

individu vis-à-vis d'un autre, qu'il soit nuisible ou bénéfique. Les participants à nos ateliers ont souvent fait remarquer que, dans la course aux données et aux opportunités qu'elles offrent, l'éthique a été parfois reléguée au second plan.

Gérer la complexité de l'éthique dans l'ère du *Big Data* peut se révéler délicat, parce que la législation est peu disante en la matière. Cependant, les gouvernements, les organisations basées sur les données, de même que la société civile reconnaissent que c'est un aspect important. Ils admettent également que le fait de ne pas traiter les préoccupations liées à l'éthique pourrait remettre en question la confiance du public en général et la confiance dans l'économie des données dans son ensemble.¹³⁹



Reconnaître la dimension éthique liée à la collecte et à l'utilisation des données est une chose. Se mettre d'accord sur un code éthique approprié en est une autre, compte tenu notamment :

- Des nombreuses utilisations possibles des données dans différents domaines (de la médecine à la finance, de l'administration de routine aux décisions relatives à l'habilitation, aux créances et aux bénéfices en passant par les applications d'IA visant à générer des orientations et des décisions de manière automatisée)
- Le nombre et la diversité des impacts potentiels de l'utilisation des données (qui comprennent notamment l'équité dans le partage des bénéfices financiers ou autres, l'ampleur et les implications d'une surveillance omniprésente ou l'émergence ou la hausse de la discrimination à cause d'une utilisation spécifique des données)
- La nature hétéroclite des principales parties prenantes (entreprises privées, gouvernements, chercheurs et académiciens, personnes physiques, citoyens comme consommateurs)
- Les différentes normes et valeurs adoptées par les cultures et les sociétés
- Les différents besoins, circonstances et priorités de ces cultures et sociétés

« C'est pour redorer leur image.

L'éthique ne peut pas l'emporter sur la tentation des marchés. La réalité c'est que les profits l'emportent sur l'éthique mondiale. »

Ce que nous ont dit les participants

D'après nos échanges, il n'y a pas de doute sur le fait que l'éthique est en train de devenir un élément clé du débat général sur les données. Le développement rapide et l'intérêt des médias pour l'IA amplifient la portée de cette problématique.¹⁴⁰ En 2008, Google, qui dispose des performances les plus avancées en matière d'IA, avait publié un cadre éthique porté par ces principes en matière d'IA, le premier de ces principes étant le bénéfice pour la société.¹⁴¹ Dans plusieurs ateliers, la nomination du premier Responsable de l'utilisation éthique et humaine de Salesforce a été évoquée et perçue comme le signal d'un changement plus profond.¹⁴² Salesforce est en train de déployer des efforts conséquents pour faire de l'utilisation éthique des données, un critère de différenciation. On ne sait pas très bien si cette démarche peut lui procurer un avantage compétitif à l'image du positionnement de certaines organisations vis-à-vis de la confidentialité. Cependant, on peut penser qu'une dynamique d'intervention est en train de s'amorcer car les entreprises mettent de plus en plus l'éthique des données en avant et la société dans son ensemble plaide pour une action dans ce sens. Parallèlement, beaucoup d'entreprises cherchent à se prémunir des risques en mettant en place des comités d'éthique chargés de superviser leurs activités.¹⁴³

L'éthique de la valeur des données et l'éthique de l'utilisation des données sont implicitement liées dans l'esprit de certains, toutefois les problématiques débattues lors de nos ateliers pesaient plutôt les rapports suivants :

- Ethique contre profit
- Différences culturelles
- Ethique et réglementation
- Respect des droits liés aux données
- Cadre flexible

Ethique contre profit

A Washington DC, on nous a rappelé que *« l'éthique c'est aussi comment on se comporte quand personne ne nous voit : ce n'est pas ce que l'on peut faire, c'est que l'on devrait faire »*. Ce n'est pas aussi facile. Même si les visées ne sont pas toujours contradictoires, les entreprises doivent parfois faire des arbitrages entre une approche commerciale et une approche éthique. Il faut trouver un équilibre afin qu'elles fassent preuve de responsabilité et adoptent un comportement éthique sans renoncer à promouvoir et à protéger leurs intérêts commerciaux ou stratégiques dans des contextes où certaines activités lucratives ou d'autres considérations sont susceptibles de l'emporter sur l'éthique ». ¹⁴⁴ Lors de notre atelier à Bangkok, par exemple, une anecdote marquante sur Apple, qui se conforme maintenant aux exigences chinoises en matière de localisation des données, a été évoquée. ¹⁴⁵ Les échanges ont abouti à la conclusion suivante : *« c'est pour redorer leur image. Regardez l'accord d'Apple avec la Chine, Apple a flanché. L'éthique ne peut pas l'emporter sur la tentation des marchés. La réalité c'est que les profits l'emportent sur l'éthique mondiale »*.

Différences culturelles

Le fait que tout cadre éthique relatif à la valeur des données doive reconnaître les différences culturelles importantes comme c'est le cas dans l'ensemble du paysage éthique, a été souvent réitéré. Les participants de Johannesburg se sont posé la question suivante : *« comment intégrer les innombrables croyances éthiques et morales des différentes cultures ? »* Lors des discussions à Manille, certains ont avancé l'idée que *« l'éthique est foncièrement culturelle et subjective et donc par nature, difficile à établir dans des cadres universels. S'il y avait un cadre universel, il y a de fortes chances qu'il provienne de l'Occident, où les débats sur les*

données et les infrastructures sont plus matures et où les entreprises de méga données sont domiciliées. Cela serait une nouvelle façon d'imposer une culture à des pays comme les Philippines ».

A Singapour, les participants constatent *« qu'il y a une présomption selon laquelle nous n'avons pas un langage commun sur l'éthique des données. Cette notion est compliquée par l'ampleur des différences culturelles et la diversité des traditions juridiques »*. Ils ont également souligné les éventuelles *« contradictions entre les philosophies orientales et occidentales »* et se sont demandé comment les choses évolueraient si, par exemple, Tencent atteignait une influence égale à celle de Google. Est-ce qu'une conception éthique chinoise de l'utilisation et de la valeur des données serait très différente d'une vision californienne ? Probablement. A San Francisco, on a admis que l'éthique des données dans son ensemble *« pourrait évoluer et susciter des visions alternatives à l'échelle mondiale, une vision inspirée des approches occidentales et une autre inspirée par la Chine »*.

A Madrid des analogies ont été faites avec les préceptes religieux : *« chaque religion a un ensemble de valeurs mais dans une religion des données (le donnée-isme), le facteur de convergence est absent. Il faut reconnaître que les données ne constituent pas une vérité, ce sont des informations présentées sous des angles différents et nous devons apprendre à déceler les données biaisées sinon, nous perdrons notre liberté de choix »*. L'éthique se définit généralement en fonction des religions et des cultures, il en est de même des visions éthiques liées au partage de la valeur des données.

Ethique et réglementation

Les avantages et les inconvénients de l'autorégulation et de la réglementation étatique ont été souvent évoquées sans doute à cause des révélations liées à l'affaire Cambridge Analytica – Facebook. Beaucoup de participants se sont inquiétés du fait que le modèle actuel dans lequel les entreprises gèrent leurs propres comportements ait échoué et que la réglementation soit devenue nécessaire pour limiter les risques de comportements répréhensibles dans certaines entreprises.¹⁴⁶ Les participants ont tout d'abord tenté de savoir si la réglementation sectorielle serait suffisante ou si la réglementation gouvernementale serait une meilleure alternative. A Bangalore, on estime que « *la loi à elle seule ne suffit pas* » et que même au-delà de la réglementation, il y a une obligation morale pour les entreprises et leur partenaires et employés, de se comporter de manière intègre. Les discussions de Bangkok ont véhiculé une perception différente, suggérant que la réglementation nationale constitue un cadre moral plus fort que celui qui serait établi en fonction d'intérêts commerciaux. « *L'éthique et la régulation sont intimement liées* ». Afin de trouver un équilibre entre les impératifs de protection des citoyens et le maintien d'un environnement concurrentiel pour les affaires, les participants ont reconnu qu'un ensemble d'approches réglementaires pourrait être envisagé, notamment dans le cadre d'une collaboration intersectorielle semblable à celle du Partenariat pour l'intelligence artificielle.¹⁴⁷ Une autre idée qui a été examinée est celle de l'établissement d'un « Serment d'Hippocrate » pour les experts en données. Comme le font les professionnels de santé qui prêtent le serment de ne point « causer la perte » des malades, les personnes travaillant avec des données devraient signer et respecter un ensemble de principes communs.

A Mexico, il y a un consensus autour de la prédiction suivante : « *il y aura deux approches différentes à l'établissement d'une éthique des données, une approche publique et une approche privée. C'est la contradiction entre réglementation et autorégulation et entre ces deux concepts, des communautés différentes orienteront les interventions* ». A Sydney, on a l'impression que des changements sont nécessaires et que « *certaines de ces changements seront portés par les entreprises, d'autres se feront spontanément par l'autorégulation et d'autres enfin seront orientés par l'action publique* ». Une opinion exprimée à Washington DC, également sur une note prédictive est que l'autorégulation serait un moyen efficace seulement si elle suivait une « *approche multipartite pour l'établissement des principes et des normes* ».

Les participants de Bogota sont largement en faveur de l'autorégulation. Même s'ils reconnaissent les difficultés qui se posent, ils ont espoir « *qu'avec une bonne coopération, il y aura une entente sur les normes de base et que l'autorégulation permettra de mettre en place un cadre éthique qui pourra être appliqué à tous les secteurs* ».

« Avec une bonne coopération, il y aura une entente sur les normes de base et l'autorégulation permettra de mettre en place un cadre éthique qui pourra être appliqué à tous les secteurs ».

Atelier de Bogota

Respect des droits liés aux données

Lors de nos ateliers, il y a eu de nombreux débats sur l'application de l'éthique dans des marchés peu ou non régulés et dans lesquels le concept de droits numériques, qui est bien établi en Europe, n'est pas assez bien compris. Les participants de l'Afrique du Sud ont eu le sentiment que le respect et la reconnaissance des droits liés aux données « *pourraient prendre une forte dimension régionale* » comme les droits humains et les perceptions culturelles de la valeur des données. Toutefois, si nous voulons aller vers une approche des données vertueuses, favorables au développement social et à l'intérêt général, « *nous aurons besoin d'un mécanisme de suivi et d'évaluation du niveau de sincérité de l'intention chez les acteurs, d'utiliser les données pour l'intérêt général* ».

A Manille, on constate que « *les citoyens sont passés d'un stade de méconnaissance de leurs droits, sans parler de leurs droits numériques, à une période de forte prise de conscience* ». Plus la culture numérique se développe, et que la compréhension de la valeur des données se précise chez les citoyens, plus ils attendront des entreprises qu'elles respectent les normes éthiques prescrites. En outre, « *nous devrions envisager des droits d'un nouveau genre. Les algorithmes et l'IA vont susciter des besoins légaux en relation avec des situations inédites* ».

Cette vision est partagée par les participants de Mexico qui sont convaincus « *qu'avec le temps des mesures de contrôles suffisantes seront maintenues afin de garantir la préservation des pratiques éthiques établies* ». Il y aura une « *législation et une gouvernance renforcée, chargée de perpétuer les opportunités d'innovation dans le secteur numérique sans mettre en péril les droits humains* ».

Enjeux pour la valeur des données

Y a-t-il un terrain d'entente pour toutes ces perspectives ? Malgré les différences culturelles évidentes, l'espoir partagé par de nombreux participants aux ateliers est qu'un cadre mondial puisse être établi, ou du moins, un ensemble de principes relatifs à l'éthique des données. Si ces principes s'avèrent performants, elles permettront non seulement d'améliorer la compréhension mais également de susciter de nouveaux comportements. C'est une noble ambition. Toutefois, compte tenu des défis culturels, politiques et technologiques, de nombreux acteurs estiment qu'il est peu probable qu'un modèle mondial unique puisse voir le jour de sitôt.

A Sydney, les participants ont proposé « l'établissement d'un cadre et d'un ensemble de principes. Ces derniers devraient être universels, flexibles et tournés vers l'avenir. Les citoyens et les organisations devraient être en mesure d'affirmer leurs droits et de les changer si nécessaire. Ils devraient aussi pouvoir connaître les enjeux des acteurs et des interventions (qui, quoi, comment) ». A Singapour, on plaide pour un « cadre universel ». Toutefois, des participants de Manille remettent en question « l'idée de l'établissement prochain de normes universelles ». Les experts canadiens sont du même avis et soulignent « *qu'il n'y a pas de cadre universel dans ce domaine mais plutôt des systèmes et visions différentes qui peuvent et doivent s'aligner, sinon, les organisations choisiront les juridictions qui leur conviennent le mieux soit par leur facilité, leur indulgence ou leur lenteur dans l'application de normes ou la sanction de contraventions aux principes éthiques, comme elles le font déjà pour la fiscalité. Il faudrait, par conséquent, un cadre extrêmement collaboratif, mais ce ne sera pas possible à l'échelle mondiale* ». En Inde, on estime « *que l'objectif en fin de compte est de créer un cadre éthique...mais ce dernier doit se fonder sur des principes culturels préétablis* ».

La gestion des données est une tâche délicate, tout autant que l'élaboration de solutions pratiques aux problématiques éthiques. Concilier ces deux aspects relève d'une gageure. Sommes-nous légèrement surpris que nos discussions n'aient pas fait émerger une solution miracle ? Il n'en existe pas. Cependant, il y a eu une forte convergence autour de l'idée que le seul moyen de garantir la pérennité de la valeur des données générées, compilées, traitées et monétisées est d'aller vers un accord universel autour des principes éthiques liés à l'utilisation des données.

Les modalités envisagées continuent de faire l'objet de discussions. Les modèles de réglementation descendants ainsi que les initiatives « populaires » semblent susciter plus d'interrogations qu'ils n'apportent de réponses sur la définition de l'équité, la lutte contre les biais dans les données et l'élaboration de recommandations éthiques pour la science des données et l'IA. Garantir une approche proactive et pertinente de l'éthique des données, à l'avenir, pourrait impliquer plus de transparence et plus d'engagement de la part des experts. Pour les entreprises, cela pourrait impliquer des compromis à court terme sur l'efficacité et l'efficience, mais rares sont les entreprises qui contestent le fait qu'à long terme, le jeu en vaille la chandelle.

« Il n'y a pas de cadre universel dans ce domaine mais plutôt des systèmes et visions différentes qui peuvent et doivent s'aligner, sinon, les organisations choisiront les juridictions qui leur conviennent le mieux soit par leur facilité, leur indulgence ou leur lenteur dans l'application de normes ou la sanction de contraventions aux principes éthiques, comme elles le font déjà pour la fiscalité. Il faudrait, par conséquent, un cadre extrêmement collaboratif, mais ce ne sera pas possible à l'échelle mondiale ».

Atelier de Toronto



4.11 Réponse organisationnelle



La gestion des données nécessite une approche du 21 siècle et non une approche des affaires erronée, du 19ème siècle. A l'ère du numérique, les principes axés sur des produits physiques sont devenus obsolètes.

Contexte

Il est clair que la plupart des organisations axées sur le numérique n'a plus grand-chose à voir avec les entreprises traditionnelles. De nombreux dirigeants d'entreprises et une multitude de licornes en forte croissance cherchent constamment à se démarquer par le changement, et essentiellement grâce à la création de valeur à partir des données. Toutefois, des questions se posent sur le fonctionnement de ces entreprises, sur leurs valeurs et sur la manière dont leur influence est mesurée et justifiée. Bien que les géants du numérique, que l'on appelle les Big Tech aient remplacé leurs pendants des secteurs du pétrole, de l'acier, de la finance et les 4 plus grands noms

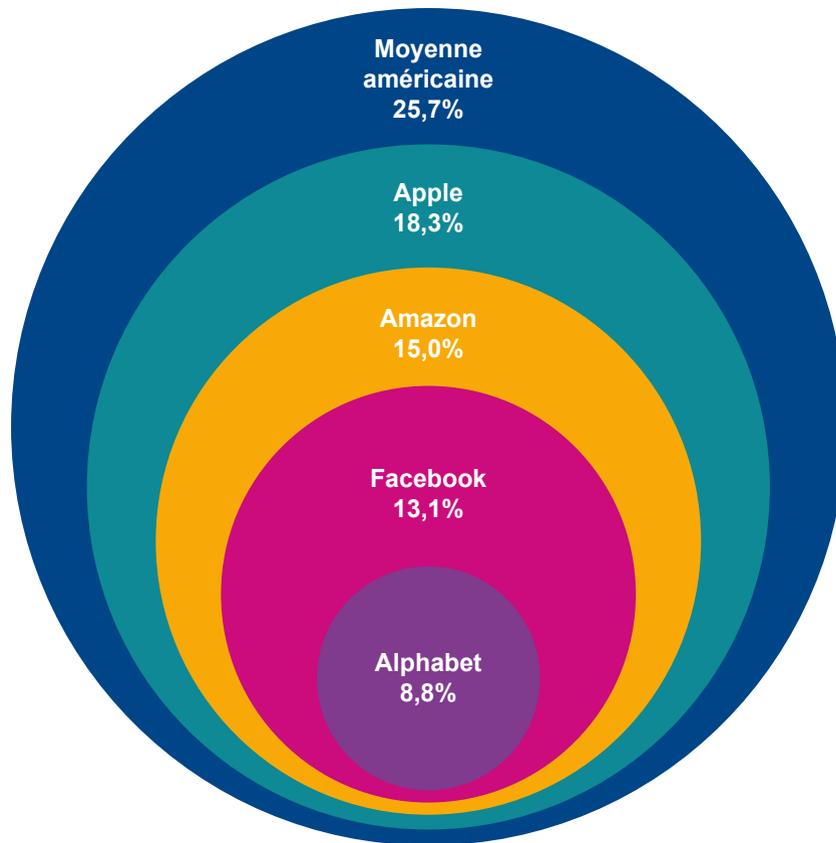
du secteur automobile en devenant les entreprises les plus riches et les plus puissantes au monde, les gens voient bien qu'ils ne leur ressemblent pas. Alors que Google et Amazon ont la même forme juridique que les entreprises telles que General Motors, Coca-Cola et JP Morgan, la façon dont ils se comportent en interne et en externe est très différente. Il semble que les outils réglementaires actuels, ainsi que les normes commerciales courantes sont dépassés, inappropriés ou insuffisants, au regard de leurs modèles économiques en constante évolution.¹⁴⁸ Au cours des dix prochaines années, la plupart des organisations deviendront progressivement des entreprises axées sur les données à un degré plus ou moins important. Par conséquent, beaucoup de gens pensent que de nouveaux indicateurs sont nécessaires pour les gérer et évaluer leurs performances.¹⁴⁹



Un arsenal réglementaire différent

Au cours des dix dernières années, les organisations riches en données qui ont connu une certaine expansion ont réussi à le faire d'une manière qui était inaccessible aux générations précédentes d'entreprises. Des recherches récentes ont identifié plusieurs raisons à ce constat :¹⁵⁰

- Les logiciels ont remplacé les machines, le coût de l'innovation a considérablement chuté permettant de réaliser des profits très substantiels avec de petits investissements.
- Les plateformes en ligne contrôlent de grandes quantités de données précieuses qui sont obtenues gratuitement auprès des clients. Les propriétaires de ces plateformes profitent d'avantages conséquents grâce à l'accès aux données de leurs consommateurs, c'est un processus très difficile à reproduire pour d'autres secteurs.
- La vitesse du changement est si fulgurante que beaucoup de régulateurs sont à la traîne et se trouvent dans l'impossibilité de rattraper le décalage et d'être sur le même front que les innovateurs.



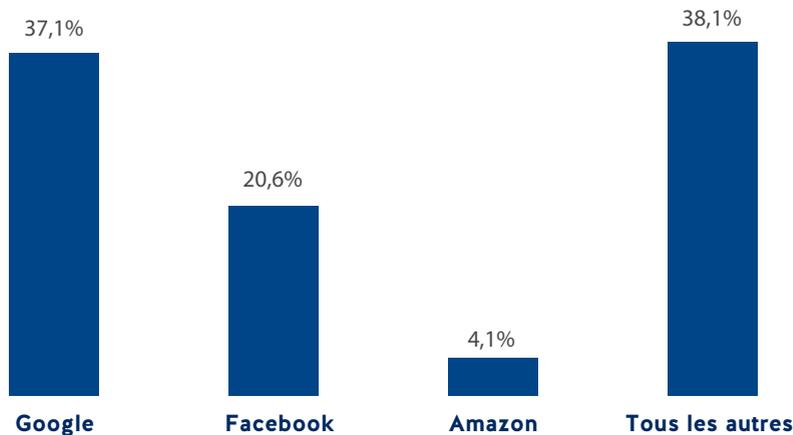
Taux effectifs de l'impôt sur les sociétés aux États-Unis (2018)

L'une des conséquences de cette situation est que les paramètres fondamentaux, la personnalité juridique, la responsabilité limitée, la cessibilité des parts et même la notion de propriété intellectuelle, qui ont orienté le fonctionnement de la plupart des entreprises au cours du siècle dernier, ne sont plus aussi adaptés aux nouvelles réalités. Dans ce sens, de nombreux participants à nos ateliers estiment qu'il y a une différence fondamentale entre l'économie de la production de biens physiques et l'économie numérique et donc les produits numériques. La création de valeur à partir des ressources et matériaux épuisables, avec des coûts implicites, est très différente de la création de valeur à partir des données, qui sont une matière première pratiquement inépuisable. Le coût de la création et de la reproduction des données baisse très rapidement et devient nul à un moment donné. Les travaux de chercheurs tels que Mariana Mazzucato et Shoshana Zuboff, ainsi que ceux de la *Future of the Corporation Project* explorent le potentiel de nouveaux paradigmes dans ce domaine, mais pour le moment, il n'y a pas de consensus sur la manière d'aborder une telle problématique.^{151 152}

Changer les règles du jeu

En même temps, il faut dire que la taille et l'échelle de l'entreprise moderne a changé. En 1975, 17% de la valeur du S&P 500 étaient basée sur des actifs incorporels. En 2015, cette valeur a atteint 84%.

De nombreuses entreprises leaders dans leurs marchés se concentrent sur l'innovation pour créer de la propriété intellectuelle, du capital de marque et d'autres actifs essentiels, de plus, près de 90% de la valeur de certaines entreprises est associée à des actifs incorporels. Les données sont au cœur de cette transformation. En 2008, les dix entreprises les plus riches du monde avaient une valeur cumulée de 3,5 trillions de dollars et comptaient au total plus de 3,5 millions d'employés. En 2018, les dix premières compagnies les plus riches valent deux fois autant, mais ne comptent plus que 50% du nombre d'employés à temps plein de la décennie précédente. Les nouvelles technologies permettent d'augmenter la rentabilité et donc le revenu par employé, à ce rythme, d'ici dix ans, il est possible que, les dix entreprises les plus riches, cumulent une valeur totale de 10 trillions de dollars pour un personnel total de seulement 1 million d'employés.



Part des revenus numériques de source publicitaire aux Etats-Unis (2018)

Cela dénote plusieurs enjeux :

- **Pouvoir économique** : il y a une concentration de plus en plus rapide du pouvoir chez les organisations dont le cœur de métier est axé sur les données. L'analyse du FEM montre que près de 2,3 trillions de dollars ou 40% de la valeur totale de la capitalisation boursière des 20 entreprises internationales les plus riches du monde pourraient être associées aux données qu'elles possèdent, consultent ou monétisent. Pour donner un ordre de grandeur, cela est supérieur au PIB de l'Italie, la septième économie du monde. En outre, plusieurs participants à nos ateliers et d'autres acteurs encore, estiment que certaines sociétés numériques « n'ont aucune limite d'échelle, elles peuvent croître à l'infini ». ¹⁵³ Cela pose de nombreuses questions autour de l'échelle et de l'influence d'une entreprise.
- **Inégale répartition des richesses** : il se pose par ailleurs la question de la concentration des revenus chez les employés et leur éventuel décalage par rapport au reste de la société. Bien que les actionnaires externes perçoivent naturellement des revenus d'une entreprise rentable, la plupart des grandes sociétés numériques proposent des bonus et de la participation à leurs employés, ces

revenus ont considérablement augmenté. En effet, le revenu moyen par employé des 5 entreprises les plus riches du monde pour la période 2017/2018 (Apple, Amazon, Alphabet, Microsoft et Facebook) était de 1,4 million de dollars. Alors que de nombreux employés sont devenus des multimillionnaires, certains se demandent si la majorité d'entre eux comprennent ce qu'est la vraie vie, ce que vivent la plupart des citoyens. Du coup, les citoyens ont moins d'empathie à leur égard. Cela ne concerne d'ailleurs pas que la Côte Est des Etats-Unis. Au Royaume-Uni, Cambridge, le domicile des laboratoires de recherche des entreprises et de nombreuses start-ups, est également devenu la ville qui présente le plus haut niveau d'inégalités. Ces inégalités sont en grande partie due au franc succès de la politique d'attraction de capital, menée ces 20 dernières années, par la ville, pour n'en faire profiter qu'à quelques-uns. ¹⁵⁴ Il y a un risque de plus en plus élevé que ceux qui administrent ces puissantes organisations et œuvrent pour elles, se déconnectent assez rapidement de la société qui les nourrit.

	2008	2018	2028
Total Value (\$tn)	 2.60	 5.98	 10
Total Employees (m)	 3.51	 1.73	 1

Grandes entreprises, petites équipes - Valeur et effectifs du Top 10 mondial des entreprises

- Faiblesse des contributions fiscales : la gestion des sociétés basées sur les données implique souvent de l'optimisation fiscale (exercée de manière tout à fait légale). Les entreprises de la génération précédente appartenaient généralement au secteur de la manufacture, de la production de biens et de la vente et payaient généralement leurs impôts dans le pays d'activité. Même dans le secteur des services, la co-location de ressources humaines et la plupart des activités des entreprises permettaient de soutenir la fiscalité régionale. En 2017, l'Autorité des services financiers du Royaume-Uni contribuait pour 72 milliards de livres sterling aux recettes du Gouvernement, soit 11% desdites recettes, dont 12 milliards de livres sterling de contributions fiscales des entreprises.¹⁵⁵ Toutefois, en 2018, Apple a acquitté l'impôt sur les sociétés à un taux de 18,3%, Amazon 15,0%, Facebook 13,1% et Alphabet seulement 8,8%, alors que le taux normal d'imposition était de 21%.¹⁵⁶ De nombreux participants à nos ateliers ont estimé que cela constitue un piètre témoignage de leur contribution globale à la société.

Alors que la confiance dans les Big Tech est en berne, les structures et pratiques de plusieurs sociétés sont l'objet d'une attention particulière. Leur influence est exposée au grand jour et certaines d'entre elles font face à des mesures réglementaires visant à infléchir leur domination.¹⁵⁷ L'Union européenne est la pionnière de l'initiative d'inflexion de cette tendance économique, mais l'Inde ainsi que certains acteurs américains veulent également enclencher des changements.¹⁵⁸ Plusieurs approches s'offrent aux différents acteurs. La démocrate Elizabeth Warren, candidate aux élections présidentielles américaines appelle au démantèlement des Big Tech, d'autres cherchent à réduire leur pouvoir en partageant leurs données avec d'autres entreprises et en facilitant aux consommateurs la transition vers d'autres concurrents.¹⁵⁹

Les entreprises de demain, une prospective

Beaucoup de participants à nos ateliers estiment qu'il est important d'envisager l'allure des entreprises de demain, qu'elles soient du secteur de la technologie ou non ; pas uniquement sur le plan économique, mais sur le plan de leurs contributions à la société et sur la portée de leurs rôles au-delà de la logique de rentabilité qu'elles incarnent pour leurs employés et leurs actionnaires. Cinquante ans après que plusieurs sociétés anglo-saxonnes aient adhéré à la vision de Milton Friedman selon laquelle l'attention d'une entreprise devrait être exclusivement portée vers la maximisation des dividendes et que la poursuite de tout autre objectif que le profit (légal) relèverait du « socialisme le plus pur », il y a du changement dans l'air.¹⁶⁰ L'article de Friedman publié en 1970 dans le *New York Times* qui expliquait que la responsabilité sociale d'une entreprise est d'augmenter les bénéfices, apparaîtrait à de nombreuses personnes, mais certainement pas à tout le monde, comme une déviation vers une mauvaise direction qui a abouti à la création de richesse pour les investisseurs et les dirigeants, au prix fort pour les employés, les consommateurs, l'environnement et la société en général.¹⁶¹ En août 2019, le plus grand groupe de lobbying commercial américain, Business Roundtable a remplacé sa vision phare de maximisation de la valeur des bénéfices dévolues aux actionnaires comme base de définition des objectifs commerciaux, adoptée depuis des lustres, pour une vision plus inclusive qui prend en compte les autres acteurs de l'entreprise.¹⁶² Portée par des pionniers de haut niveau dont des entreprises comme Patagonia, Unilever et Virgin, cette vision est en train de convaincre un nombre croissant d'entreprises qui adoptent déjà des objectifs sociaux qui complètent leurs objectifs commerciaux. Il serait intéressant de voir comment les sociétés axées sur les données vont intégrer cette nouvelle donne.

Organisation 4.0

Plusieurs participants à nos ateliers pensent qu'il pourrait y avoir des alternatives plus viables à la structure actuelle des entreprises, dans les dix prochaines années. On pourrait même voir l'émergence d'entités d'un autre genre chez les organisations axées sur les données. Il y a déjà des innovations en la matière, avec des formes juridiques hybrides telles que les sociétés d'intérêt public (*Public benefit corporations*). Ce type de société est très orienté vers les objectifs sociaux ambitieux. Certains acteurs s'orientent vers l'actionnariat à double catégorie, très controversé au départ, mais adopté par Google et IPO et qui, par la suite, est devenu le choix de nombreuses sociétés de technologies. Ce modèle permet aux entrepreneurs de contrôler l'entreprise sans en détenir la majorité des parts (*clash flow rights*). Ce type de structure est devenu si populaire que les bourses ont modifié leurs règles de cotation pour permettre aux sociétés de technologies ayant une structure de vote différentielle, de faire coter leurs actions.

On pourrait voir émerger à l'avenir, deux systèmes distincts pour les entreprises ayant des structures, une gouvernance et une réglementation différentes. Un système pour les entreprises proposant des produits et services traditionnels et un autre pour les entreprises fondamentalement basées sur les données. S'il y a un fossé de plus en plus profond entre deux types d'économies très divergentes et très déconnectées l'une de l'autre, les gouvernements et les bourses pourraient finir par les dissocier. Cela pourrait entraîner une transition des places boursières du NASDAQ et du Dow Jones aux Etats-Unis. Il pourrait y avoir différentes approches de gouvernance, d'imposition, de financement de la recherche, de financement public et de valorisation des sociétés.

Ce que nous ont dit les participants

Lors de nos échanges en Afrique du Sud, les participants ont suggéré que « *les données vont susciter une toute nouvelle gamme d'indicateurs* » tandis qu'à Sydney, plusieurs participants trouvent « *qu'à l'avenir, les Big Tech détiendront tout le pouvoir* ». Les données apporteront toujours plus de pouvoir et d'influence à ceux qui les contrôlent, la manière de structurer, orienter, gouverner et justifier les actions des entreprises pourrait fondamentalement changer. A San Francisco, les participants pensent « *qu'on n'est pas loin d'un oligopole des données, le contrôle étant concentré entre les mains d'un petit nombre d'acteurs* ».

Dans le fond, certains perçoivent qu'il y a eu un passage du pouvoir des mains des gouvernements, de la société et des grandes multinationales vers les sociétés numériques internationales et transnationales. De Jakarta à Bangkok en passant par Washington DC, Bogota et Mexico, nous avons souvent entendu dire que « *les données c'est le pouvoir* », tandis qu'à Francfort, on a soutenu que « *ceux qui détiennent des données détiennent le pouvoir* ». Lors de nos échanges à Londres, les questions liées au pouvoir et à l'autorité comme par exemple : « qui détient le pouvoir ? Comment rendre compte ou justifier de ce pouvoir ? » ont été évoquées. En outre, on a suggéré que « *les données procurent du pouvoir, sous-tendent son contrôle, son équilibre et sa justification* ».

« Nous voyons que des acteurs dont les bénéfices excèdent les revenus de la plupart des pays vont détenir encore plus de pouvoir ...ce pouvoir pourrait s'exercer en dehors de tout contrôle externe et devenir dangereux »

Atelier de Hong Kong

Beaucoup d'acteurs estiment que la redevabilité, cette justification du pouvoir, a fait cruellement défaut au cours des dernières années et a suscité le besoin de renforcer la réglementation.

Une remarque prédictive a été faite lors de nos discussions : « *à mesure que la conscience que les entreprises ont de leur pouvoir va évoluer, on observera une concentration du pouvoir sur les flux de données* ». Alors que « *nous irons d'un système d'autorégulation vers l'intervention de régulateurs de confiance, avec une précision claire des droits* », des questions concernant les modalités de dévolution de pouvoir se poseront probablement. Au Mexique, on prévoit que dans quelques années, « *les algorithmes seront partout, et les entreprises qui les mettent en œuvre se soucieront peu de leur impact social* ». Les participants de Francfort ont proposé une orientation en précisant que « *nous avons besoin d'algorithmes plus transparents* » puisque « *nous ne remettons pas en question les décisions que les machines ont prises à notre place* ».

Certains participants de San Francisco prévoient « qu'il y'aura une réglementation algorithmique pour couvrir les aspects qui ne peuvent pas être réglementés par les humains. Toutefois « *la gouvernance algorithmique pourrait permettre aux entreprises qui ont recours aux algorithmes de générer davantage de revenus en mobilisant moins de capital humain* ». À Copenhague, on est généralement d'avis que pour la plupart des entreprises, « *la compréhension de la valeur des données par les directeurs de l'expérience utilisateur va changer* », alors qu'à Hong Kong on a rajouté dans cette veine, que de nombreuses « *institutions sont en décalage total* » et que cela doit changer « *parce que nous voyons que des acteurs dont les bénéfices excèdent les revenus de la plupart des pays vont détenir encore plus de pouvoir* ». En effet, « *ce pouvoir pourrait s'exercer en dehors de tout contrôle externe et devenir dangereux* ».

Alors que ces transitions évoquées ci-dessus sont restés des enjeux de second plan lors de nos échanges, les défis supplémentaires qu'ils peuvent poser aux sociétés numériques ont été mentionnés à plusieurs reprises. Par exemple, à Jakarta, on a recommandé « *de voir au-delà de la finalité de l'entreprises* » parce que les données peuvent être partagées et utilisées pour un impact de portée supérieure à celle des autres actifs.

Lors de l'atelier de San Francisco, il a été suggéré que « *l'accès aux données vraiment précieuses est l'apanage de quelques-uns* » et que « *les entreprises de technologies deviennent les sources privilégiées des données et des services y compris des services sociaux et de santé* ». Par ailleurs, on pourrait bientôt « *voir les gouvernements céder l'administration de nombreux services publics à des sociétés privées mieux équipées et mieux averties* ».

« Il faudrait regarder au-delà de la finalité de l'entreprises »

Atelier de Francfort

Enjeux pour la valeur des données

Les fondements du comportement des entités commerciales et du développement de leur culture d'entreprise sont jaugés par la société, récompensés par les marchés et peuvent évoluer dans certains secteurs d'activité. Comment et pourquoi la rétribution financière est activée constitue une problématique étudiée par les chercheurs, les gouvernements et dans certains domaines, par les médias. Comment une entreprise peut-elle valoir 1 trillion de dollars et employer seulement 100 000 personnes ? C'est un fait qui sera de plus en plus juxtaposé avec la situation dans des entreprises qui ont une valeur financière inférieure et emploient plus de monde. Les sociétés axées sur les données et l'économie numérique sont clairement différentes des économies où les produits et services sont de nature plus tangible, pourtant à l'heure actuelles, elles sont encore jugées selon les mêmes paramètres et souffrent le voisinage inconmode qui leur est imposé.

Le pouvoir se meut, la valeur aussi, il n'y a rien de nouveau en cela, mais les normes par lesquelles une entreprise et ses performances sont comparées à une autre, sont sous pression. Au-delà des comportements monopolistiques, les moyens traditionnels d'évaluer la valeur pour les actionnaires, comparés à ceux qui permettent d'évaluer la valeur pour les acteurs, plus nombreux, de la société, sont en train d'évoluer : la recherche actuellement menée par *Future of the Corporation* est juste l'un des divers programmes qui tentent de suggérer de nouvelles voies pour la gestion, la supervision et la valorisation des entreprises.¹⁶³ Les enjeux sont considérables pour les entreprises basées sur les données. Leur valeur commerciale sera observée avec attention, de même que leurs comportements, le niveau de transparence de leurs déclarations, les changements dans leur régime d'imposition. Certaines organisations seront

proactives, reconnaîtront le besoin de changement et tenteront de réaliser une répartition plus équitable des bénéfices et des impacts. A l'inverse, d'autres prendront des postures plus défensives. Attention toutefois à ceux qui en parlent le plus et qui en font le moins.

« On pourrait bientôt voir les gouvernements céder l'administration de nombreux services publics à des sociétés privées mieux équipées et mieux averties »

Atelier de San Francisco



4.12 Redevabilité et réglementation



L'inquiétude croissante au sujet de l'utilisation des données influence l'opinion publique. Les décideurs cherchent une approche plus globale de la réglementation, de la gouvernance et de la redevabilité.

Contexte

Il y a dix ans, la confiance et la foi dans les nouvelles entreprises de technologie étaient telles, que beaucoup de citoyens croyaient que la meilleure approche était de permettre au secteur de s'autoréguler. C'était certainement l'approche la moins coûteuse et la moins fastidieuse. On pensait qu'en créant un cadre d'autorégulation efficace et crédible, les entreprises seraient en mesure de réagir plus rapidement au rythme rapide de l'innovation. Cette logique s'est appuyée sur une relation de confiance tacitement établie avec la conviction que les entreprises de technologie agissent pour le bien de la société.

Le message lancé lors de nos ateliers était évident : aujourd'hui, cette confiance s'est évaporée. Très peu de gens croient encore que les « données libres pour tous » engendrera naturellement le meilleur des mondes possible. Compte tenu de la portée des problématiques technologiques qui façonnent maintenant nos économies, nos démocraties et notre vie personnelle, les gouvernements doivent adopter une approche plus active et plus affirmée de la réglementation. La question n'est plus de savoir si les entreprises de technologie devraient être réglementées, mais plutôt comment ?



Ce débat est à la fois intense et complexe. Les questions et les dilemmes abordés dans les ateliers incluent :

- Comment combiner une réglementation efficace avec la rapidité du changement technologique ? En général, le cycle politique/réglementation peut durer 5 à 20 ans, alors qu'un nouveau service numérique peut couvrir le monde en quelques années. Comment les décideurs et les organismes de régulations pourront-ils tenir le cap ?
- Compte tenu du rythme du changement, du manque de transparence de certaines organisations et des difficultés qui en découlent, les décideurs et les régulateurs doivent se tenir au courant des nouvelles technologies et de leurs implications. Quel est le meilleur processus pour élaborer de nouvelles règles ? Si l'élaboration de la réglementation doit être un effort collaboratif secteur privé/ gouvernement, comment cette collaboration devrait-elle être organisée ?
- Quel est la meilleure échelle de réglementation ? La révolution numérique est un phénomène mondial. Certains participants à nos ateliers ont plaidé pour qu'une entité internationale établissent des règles et un cadre communs adaptables sur le plan mondial. Mais est-ce bien pratique ? Si ce n'est pas le cas, une approche régionale est-elle meilleure - ou cela favoriserait-il l'éclatement du système ? Et les régulateurs nationaux feraient-ils vraiment le poids pour négocier avec les multinationales dont les ressources éclipsent parfois celles des états ?
- Quelles serait la finalité et la portée de toute nouvelle règle ou réglementation ? Au cours des dernières décennies, la priorité réglementaire a été de s'attaquer aux préjudices réels/potentiels pour les consommateurs. Mais devrait-on élargir cette situation pour inclure la santé des écosystèmes de données et des économies dans leur ensemble ? Si oui, comment ?

- Quels seraient les meilleurs leviers et cadres par lesquels élaborer les règles et réglementations ? Devraient-ils s'articuler autour de questions telles que la concurrence, ou devraient-ils peut-être se concentrer sur des questions plus techniques de l'information financière, de la comptabilité et de la fiscalité ?
- À qui devrions-nous faire confiance pour élaborer des politiques ? Devons-nous faire confiance aux décideurs et aux organismes de régulation nationaux, vu qu'ils peuvent avoir un intérêt direct à installer des opérations de capture et de surveillance des données, qu'il s'agisse de données nuisibles ou de données favorables aux citoyens ? Alternativement, pouvons-nous faire confiance aux entreprises de technologie qui sont fondées pour générer des profits et pas nécessairement pour protéger l'intérêt des citoyens ?
- Comment pourrait-on éviter les pièges d'une réglementation mal formulée qui a des effets contre-productifs ou étouffe l'innovation ?

« Il faudrait concevoir ensemble un cadre réglementaire pour l'ère numérique »

Atelier de Francfort

Suivre le rythme du changement

Tout au long de nos ateliers, nous avons eu l'impression qu'au cours des 20 dernières années, la capacité des gouvernements à fournir des services à leurs administrés ne cesse de diminuer, pendant que les entreprises de technologies deviennent une force politique à part entière. Certaines entreprises, notamment celles qui sont basées aux États-Unis, ont été encouragées par une longue période de laxisme affichée par le gouvernement, à innover et à bousculer le système à volonté. Ce faisant, ils ont créé des avantages sociaux importants. Mais le mépris des normes éthiques reconnues autour des questions telles que la vie privée, la sécurité et même la fiscalité, par quelques entreprises technologiques très rentables, a provoqué une alarme généralisée. Il n'est donc pas surprenant qu'il y ait une réaction réglementaire et politique.

Il est clair que les entreprises de technologies et les régulateurs doivent conjuguer et harmoniser leurs efforts pour trouver de nouvelles solutions de protection des données des citoyens. Il y a de nombreux acteurs bienveillants des deux côtés, qui, en associant leur expertise, sont capables de formuler les mesures réglementaires appropriées pour protéger les usagers sans pour autant étouffer l'innovation, peut être en envisageant une réglementation progressive au lieu d'attendre que les problèmes s'installent. Quelle que soit l'approche retenue, en définitive, la quasi totalité des participants aux ateliers sont d'avis qu'il faut un changement d'état d'esprit des deux côtés et que la première étape de ce parcours devrait être la création d'un langage commun sur les données, l'établissement de principes communs autour de l'utilisation des données et une approche collective de leur mise en œuvre.

Avoir un objectif commun

Bien que nous vivions à une époque où le paysage géopolitique semble se fracturer, les gouvernements doivent coopérer plus efficacement les uns avec les autres, étant donné que la technologie est peu sensible aux frontières nationales. Comme pour la réglementation sur le contrôle de l'armement, la création de règles internationales aiderait les nations à réagir et à riposter collectivement, si celles-ci venaient à être violées. Des travaux sont déjà en cours dans ce sens. Par exemple, le bouclier de protection de la vie privée de l'UE et des États-Unis (EU-U.S. Privacy Shield), sert de cadre pour réglementer les échanges transatlantiques de données personnelles à des fins commerciales. Par ailleurs, en 2018, le président Emmanuel Macron a lancé l'Appel de Paris pour la confiance et la sécurité dans le cyberspace. Cette déclaration de haut niveau en faveur de l'élaboration de principes communs pour la sécurisation du cyberspace a déjà reçu un franc soutien de la part de nombreuses structures nationales, internationales, de la société civile et du secteur privé. Bien qu'il n'oblige pas les gouvernements ou les entreprises à adhérer légalement à des principes spécifiques, il agit comme un symbole illustrant la nécessité d'une diplomatie et d'une coopération dans le cyberspace, où il est difficile d'appliquer les lois d'un seul pays.¹⁶⁴ Dans le même temps, certains pays ont choisi d'agir unilatéralement sur des questions telles que les méfaits du numérique, la modération des contenus et les attaques malveillantes.

« A mesure que nous avançons, il est probable que nous observions davantage de poches de réglementation qui tentent d'imiter ou de s'inspirer de ce qui se fait ailleurs, à l'image du RGPD »

Atelier de Johannesburg

Beaucoup de participants à nos ateliers ont exprimé l'idée que, pour développer des cadres internationaux solides et adaptés, il est essentiel de rassembler les pays qui sont prêts à relever ces nouveaux défis en évolution rapide, et de créer une dynamique, en laissant la porte ouverte à d'autres qui souhaiteraient se joindre à l'initiative. Les Etats-Unis, par exemple, n'ont pas encore soutenu l'Appel de Paris, mais la création d'une coalition des soutiens de l'initiative est un bon moyen de susciter son implication et son appui.¹⁶⁵ En outre, la création de règles à l'échelle internationale rendrait certainement plus facile pour les pays, la mise en œuvre de réponses efficaces, en cas de violations.

Nous devons reconnaître que certaines questions peuvent ne pas conduire à un consensus mondial. Les opinions liées à la vie privée, à la liberté d'expression et aux droits de l'homme sont très différentes selon les pays. Par exemple, la Chine, qui a la plus grande base d'utilisateurs d'Internet au monde a l'ambition d'être la principale superpuissance numérique, et bien qu'elle ait pris des mesures pour protéger les jeunes contre les méfaits du numérique, elle a peu d'intérêt à autonomiser ses citoyens - elle a plutôt suivi sa propre politique notamment avec des mesures comme l'arrêt de sites Web et la censure de contenus.

Malgré cela, les questions entourant le développement de nouvelles technologies exigent des initiatives qui ont à la fois une portée multilatérale et multipartite. Dans les démocraties, les décideurs publics, qui sont habilités à mettre en application les lois qui nous gouvernent sont particulièrement bien placés pour diriger ces initiatives.

Encourager ou réduire les monopoles ?

Comme l'a résumé John Naughton, pour sa part, « l'une des choses paradoxales de la technologie numérique est que, bien qu'en théorie elle favorise la concurrence, elle mène en pratique à des situations où le gagnant rafle la mise. Les raisons en sont complexes : il n'y a pas de coûts marginaux, d'effets de réseau puissants, de rapport législation- pouvoir ni de blocage technologique. Les cinq plus grandes entreprises du monde sont aujourd'hui toutes des géants du numérique, chacune exerçant un pouvoir énorme sur son marché. Tout comme lors des interventions précédentes dans les secteurs du pétrole, de l'acier et des télécommunications, les organismes de réglementation cherchent à réduire leur influence.¹⁶⁶ L'UE à Bruxelles est souvent considérée comme la pionnière de cette campagne, mais elle n'est pas la seule. En effet, en 2018, beaucoup ont souligné le rôle potentiel de l'OCDE, qui pourrait avoir un impact universel. La proposition de l'OCDE d'octobre 2019 visant à faire bouger la fiscalité mondiale concernant les leaders du numérique est l'un des premiers exemples visibles de cette dynamique de réglementation.¹⁶⁷ Dans l'UE, les efforts visant à maîtriser les entreprises qui abusent de leur pouvoir monopolistique ont entraîné, par exemple, une amende record de 5 milliards de dollars contre Google - ce qui est supérieur à l'impôt qu'elle paie actuellement. En outre, le RGPD a un impact profond sur l'écosystème de la publicité et de la collecte de données.¹⁶⁸

« Il faudrait une stratégie gouvernementale des données plus clairement articulée pour permettre des initiatives communautaires qui soient d'un grand intérêt public ».

Atelier de Singapour

Sous d'autres horizons, la Californie a déjà adopté une vaste loi sur la protection des données, qui doit entrer en vigueur en 2020. Le Gouvernement indien, en réaction à ce que certains considèrent comme une tentative de colonialisme, a interdit à Facebook de permettre aux utilisateurs de naviguer sur ses sites, sans payer la connexion à l'Internet mobile¹⁶⁹. Même en Chine, le Gouvernement est de plus en plus impliqué dans le contrôle de la domination d'Alibaba, Tencent, Baidu, et JD.com, rejetant, par exemple, un système de notation de crédit proposé par la société de paiement affiliée à Alibaba, Ant Financial, en faveur de l'un des siens. Certains disent qu'il s'agit d'un coup de force économique au profit de ses propres acteurs nationaux. Pensez à l'énorme industrie technologique de la Chine, ou à Flipkart, le géant indien du commerce électronique qui est en plein essor. D'autres y voient la preuve que le vent a tourné en défaveur d'un climat flexible et peu réglementé.

Le problème de la fiscalité

Comprendre la meilleure façon de taxer les différentes parties prenantes de la filière des données peut devenir essentiel pour permettre une répartition plus équitable des bénéfices que les entreprises axées sur les données peuvent générer, tout en maximisant la croissance de l'économie des données et en assurant de bonnes pratiques. La taxe sur les services numériques proposée par l'UE, qui vise à taxer les recettes générées au sein des juridictions nationales ou de l'Union et à contourner la question épineuse de l'imposition des bénéfices enregistrés à l'étranger, est une réponse potentielle, mais elle soulève également des questions sur l'équité et la mise en œuvre. Dans certains de nos ateliers, des participants ont prédit une époque chaotique avec les différentes tentatives des gouvernements de taxer les entreprises numériques axées sur les données, avant que des stratégies plus cohérentes autour de la redistribution de la richesse numérique et des données ne voient le jour.

Surveillance et ingérence de l'Etat

L'autre préoccupation majeure est le contrôle de plus en plus soutenu des données par les gouvernements, et en particulier l'accent mis sur le renseignement comme objectif principal. Bien que les cas russe, chinois et américain soient les plus fréquemment évoqués à l'échelle mondiale, il y a eu plusieurs autres exemples. Le contrôle des données a été évoqué à Hong Kong et à Londres, où l'impact négatif de la surveillance nationale sur la démocratie, surtout à cause de l'influence croissante de la technologie de reconnaissance faciale, devient une question d'intérêt public.

« Il est plus probable que l'autorégulation entraîne des normes communautaires qui, à leur tour, entraîneront une réglementation locale »

Atelier de Manille

Ce que nous ont dit les participants

La plupart des participants ont admis qu'au rythme fulgurant des changements technologiques, et compte tenu de la nature transnationale des données, il n'est pas réaliste de s'attendre à ce que les gouvernements élaborent, mettent à jour et appliquent une réglementation efficace des données sans la coopération des entreprises de technologie. Une forme de collaboration entre les décideurs et les entreprises de technologie est nécessaire. Bien qu'un certain nombre de consortiums plutôt privés aient émergé et proposé de servir d'organismes indépendants de normalisation, tous n'ont pas été efficaces, et le fossé entre la réglementation et l'industrie demeure.

La solution qui a été identifiée au cours de nos ateliers est une entité mondiale qui servirait de point focal pour les activités de gouvernance. À Jakarta, on a proposé « *un cadre mondial indépendant de réglementation des données (peut-être comme le G20)* ». A Bangkok, on parle d'une « *autorité mondiale des données (comme l'OMC)* ». A Singapour, on estime qu'il faut « une organisation mondiale (comme le FEM, le FMI ou l'OMS). Au Mexique, avec un objectif à l'échéance 2030, on penche pour « *un organisme international capable d'agir au niveau mondial (comme l'ONU)* », tandis que dans une discussion à Londres, les entreprises de technologie croient que l'OCDE pourrait apporter une réponse. Tous sont à la recherche d'une autorité supérieure pour établir les normes, définir un terrain d'entente et assurer l'équilibre et l'indépendance. Tous ont reconnu que cela ne se concrétiserait pas de sitôt.

Les participants de Jakarta estiment que les changements réglementaires devraient être dirigés par les gouvernements, principalement parce que les gouvernements plutôt que les entreprises ont un mandat démocratique pour représenter le peuple. D'autres, comme ceux de Francfort et de Bangalore, ont estimé que la réglementation collaborative serait plus efficace, c'est-à-dire qu'idéalement, les secteurs public et privé

« *conçoivent ensemble un cadre réglementaire pour l'ère numérique* ». ¹⁷⁰ À Hong Kong, il a été suggéré de créer un « *cadre de principes communs permettant l'utilisation publique et privée des données dans plusieurs juridictions. Pour ce faire, il faut d'abord qu'il y ait une collaboration autour d'un ensemble de principes relatifs aux normes* ».

Plutôt qu'un cadre mondial pour la gouvernance des données et une organisation dédiée pour la superviser, beaucoup ont estimé qu'il est plus probable qu'il y ait un découpage juridictionnel régional avec un certain nombre de régions au sein desquelles des politiques communes sont adoptées. L'Europe, la Chine et les États-Unis constituent trois cas déjà bien visibles et une approche axée sur l'ANASE et le cadre de confidentialité des données de l'APEC est déjà en vue. En Afrique et en Amérique latine, certains envisagent leurs propres méthodes de réglementation régionale. Le RGPD de l'Union européenne, qui a harmonisé les règles de protection des données et renforcé les droits des personnes à contrôler l'utilisation de leurs données, a souvent été mentionné comme un modèle que d'autres pays devraient suivre. « *Le RGPD va changer le paysage des données au Nigéria et inspirer de nouvelles normes* ». ¹⁷¹ À Johannesburg, on estime « *qu'à mesure que nous avançons, il est probable que nous observions davantage de poches de réglementation qui tentent d'imiter ou de s'inspirer de ce qui se fait ailleurs, à l'image du RGPD* ». Cela dit, tout le monde n'a pas jugé nécessaire de réglementer. À Manille, on pense qu'il est « *plus probable que l'autorégulation entraîne des normes communautaires qui, à leur tour, entraîneront une réglementation locale* ». Quoi qu'il en soit, les appels en faveur d'une approche plus commune de la réglementation ont

été fréquents. Jusqu'à présent, a-t-on souligné, la réponse aux changements technologiques rapides a été trop parcellaire pour être vraiment efficace. De notre premier atelier à Bangalore, où l'on a affirmé que « *la politique gouvernementale est actuellement très dispersée, avec peu de cohérence dans les finalités* », à notre dernière réunion à Santiago où l'on a pensé que « *le défi sera de savoir comment les différentes juridictions vont prendre le contrôle des problématiques liées aux données* ». Il a été reconnu que la pléthore de réglementations actuelles ne résout pas les grandes problématiques.

En ce qui concerne les leviers réglementaires, une des suggestions est que les organismes de réglementation contribuent à évaluer la valeur des données, ou du moins, à définir les paramètres selon lesquels les données pourront être évaluées. Il pourrait alors y avoir un changement important dans la perception des modalités de gestion de la valeur des données. L'évaluation de la valeur des données, a-t-on fait valoir, susciterait un débat plus éclairé sur les modalités de partage de cette valeur, l'objectif étant de savoir comment optimiser le partage. En plus d'améliorer l'information financière, l'évaluation de la valeur des données pourrait contribuer à la formulation des politiques fiscales, tout en influençant les stratégies des organisations en matière de données.

Une autre suggestion, qui a également été récemment évoquée dans le Financial Times, est de revenir à une interprétation antérieure de la réglementation antitrust qui se concentre non seulement sur les consommateurs, mais également sur la question de savoir si l'écosystème économique de manière plus globale, est lésé.¹⁷² L'idée qu'une meilleure gouvernance des données pourrait ouvrir de nombreuses opportunités positives pour la société est inspirée de cette logique. En Inde, par exemple, on espère que « *le gouvernement guide davantage le secteur privé sur l'élaboration de politiques en faveur de la « valeur sociale des données* ». À Singapour,

on souhaite « *une stratégie gouvernementale des données plus clairement articulée pour permettre des initiatives communautaires qui sont d'un grand intérêt public* ». Les participants de Nairobi veulent que les « *données stimulent le développement, deviennent plus accessibles et réduisent la pauvreté* ».

« A mesure que nous avançons, il est probable que nous observions davantage de poches de réglementation qui tentent d'imiter ou de s'inspirer de ce qui se fait ailleurs, à l'image du RGPD »

Atelier de Johannesburg

Parallèlement, une suspicion généralisée au sujet des gouvernements et des acteurs étatiques, et une crainte qu'ils puissent utiliser leurs nouveaux pouvoirs de régulateurs pour affirmer leur propre contrôle, en particulier sur les données personnelles, au profit de leurs objectifs de surveillance, ont été exprimées. À Johannesburg, on affirme « *qu'il y a un risque que certains gouvernements utilisent de plus en plus la réglementation des données pour imposer un contrôle descendant d'ensembles de données très puissants* », tandis qu'à Pretoria, les étudiants débattent de la façon dont « *la centralisation des données augmente le niveau de contrôle de l'Etat* ». Leur inquiétude est qu'en Afrique, « *certaines gouvernements puissent limiter l'accès aux données sous couvert de sécurité nationale* ». En janvier 2019, le gouvernement zimbabwéen a coupé l'accès à Internet pendant trois jours, afin de freiner les protestations de l'opposition. Plus au nord à Abuja, on prévoit un scénario dans lequel « *l'Etat va vouloir garder le contrôle sur les données, tandis que les citoyens de leur côté, ne peuvent pas profiter de la valeur des données* ». En Amérique du Sud, l'inquiétude au sujet de la surveillance croissante de l'État qui rassemble toujours plus d'informations sur les citoyens, a également été exprimée à Bogota et à Santiago. À Hong Kong, on est d'avis que les scénarii où les « *données créent le pouvoir, façonnent l'exercice du pouvoir, l'équilibre des pouvoirs et la responsabilité face au pouvoir se multiplient* ». ¹⁷³ Beaucoup se sont inquiété de l'impact que cela a sur la société.

De plus, il y a le risque permanent que la réglementation crée autant de problèmes qu'elle apporte de solutions. À Hong Kong, des préoccupations ont été exprimées: « *Nous craignons que la réglementation excessive puisse diminuer la valeur des données et entraver l'innovation dans l'intérêt général* ». ¹⁷⁴ Les effets culturels de la réglementation ont également été constatés. « *Il est également important d'envisager les objectifs et les enjeux de différentes idéologies au sein d'un territoire*

national », et de savoir « *quels serait les enjeux si la Chine remportait le débat du modèle idéologique des données, et ce qui se passerait si elle exportait ses valeurs à travers le monde* ». Le Grand pare-feu de Chine a bel et bien mené au développement de deux internets. À l'avenir, si une guerre commerciale entre les États-Unis et la Chine s'intensifie et que les dirigeants chinois estiment qu'ils doivent avoir leurs entreprises technologiques de leur côté, il est parfaitement possible de voir les pays participant à l'Initiative chinoise Belt and Road (*Belt and Road Initiative*) être tentés d'adopter les infrastructures technologiques chinoises. ¹⁷⁵

« L'Etat va vouloir garder le contrôle sur les données, tandis que les citoyens de leur côté, ne peuvent pas profiter de la valeur des données ».

Atelier de Abuja

Enjeux pour la valeur des données

Comment les régulateurs pourront-ils alors réglementer efficacement, compte tenu des défis de l'évolution technologique et de l'ampleur de la révolution des données ? De nombreux participants à nos ateliers étaient d'avis que jusqu'ici, pas grand-chose n'a été fait pour protéger l'intérêt public, et que les gouvernements doivent intervenir pour y remédier. Ils ont également reconnu que, malgré la nature pressante des défis, il serait trop difficile de parvenir à une résolution harmonieuse, à court terme, non seulement parce que la barre est très haute et que les points à concilier sont fort nombreux, mais aussi en raison de la méfiance entre certains gouvernements, institutions internationales et grandes entreprises. En effet, dans certains pays, la désillusion face à la mondialisation et le manque d'enthousiasme pour la culture occidentale, à laquelle s'ajoute une reconnaissance croissante de l'influence de la Chine, sont le signal que différents modèles de politiques régionales pourraient bien émerger, ce qui pourrait se faire au détriment d'une économie mondiale des données.

De nombreuses situations exigeront des compromis, ce sera difficile pour les chefs d'entreprises de technologie en particulier, étant donné qu'ils ne sont pas habitués à la contrainte réglementaire, mais c'est un élément qu'ils commencent à reconnaître et à accepter. À court terme, cela peut également affecter la façon dont les données peuvent être évaluées et cela peut même limiter les trajectoires de croissance de certaines organisations. Cependant, à long terme, beaucoup de participants aux ateliers se sont accordés sur le fait que la collaboration multilatérale pourrait, dans une optique plus pragmatique, être une étape intermédiaire dans le passage d'un processus politique réactif vers un processus proactif qui, en fin de compte, permettra de mieux protéger les droits humains et les libertés individuelles tout en garantissant un cadre d'évolution pérenne, favorable aux innovations technologiques axées sur les données, qui profiteront à tous.



« Nous craignons que la réglementation excessive puisse diminuer la valeur des données et entraver l'innovation dans l'intérêt général »