



3.0 Les grands axes thématiques

Tout au long du programme, six grands thèmes transversaux se sont dégagés. Ils ont été débattus de différentes manières et se sont chevauchés par moment. Quelle que soit la problématique spécifique liée aux données, discutée, elle peut être considérée au même titre que les autres, comme un élément fondamental du débat.

Ces grands thèmes sont les suivants :

1. Les problématiques liées à la collecte et à l'utilisation des données personnelles – **Mes données à moi** ;
2. Les questions liées à la propriété et à la valeur des données – **Propriété et valeur** ;
3. Les problématiques de **Pouvoir et influence** ;
4. Les préoccupations liées à l'échelle géographique des activités liées aux données – **Penser mondial, régional ou local ?**
5. Les différentes perspectives sur la notion de confiance – **Une confiance qui se mérite,**
6. La nécessité de parler le même langage pour éviter les malentendus et confusions et de contribuer à la clarification et à la progression du débat – **Tous sur la même longueur d'onde.**



3.1 Mes données à moi



Les préoccupations grandissantes au sujet de la collecte et de l'utilisation des données personnelles couvrent plusieurs problématiques. La pression en faveur de solutions qui apportent sensibilisation et garanties aux personnes est de plus en plus forte.

Lors de nos ateliers, l'essentiel du débat sur les données a tourné autour des données personnelles. Cela n'est pas surprenant. Les données personnelles sont par essence, en rapport direct avec la vie des personnes et cela, sous différents aspects. Les données sur une personne, peuvent révéler des éléments intimes de sa vie. Ces données pourraient être utilisées pour lui procurer de nombreux avantages, c'est déjà le cas, notamment en termes d'innovation et de services personnalisés. Mais ces mêmes données pourraient également rendre la personne vulnérable surtout si elles tombent entre de mauvaises mains (par exemple en cas d'usurpation d'identité) ou si elles sont utilisées à l'encontre de la personne concernée plutôt qu'en sa faveur (discrimination envers des personnes ou groupes de personnes, basées sur ce que les données les concernant révèlent sur elles).

C'est lorsque l'on aborde le sujet des données personnelles que les débats les plus houleux sur le pouvoir et l'équité sont soulevés. Des entreprises sont en train de se faire des profits incommensurables à travers la collecte et la monétisation des données concernant des milliards de personnes. Beaucoup se sentent impuissants face à ces consortiums et à la forte concentration de pouvoir dont ils disposent grâce aux données.

Ces problématiques ont fait réfléchir de nombreux participants aux ateliers qui ont souhaité analyser avec précision le processus de collecte et d'utilisation des données personnelles et trouver des issues favorables aux problématiques observées. La démarche n'a pas été facile, en partie parce que les problématiques liées aux données personnelles peuvent être bien plus complexes qu'il n'y paraît de prime abord, à commencer par les définitions.

Beaucoup de gens font référence à des éléments de données tout à fait évidents comme le nom, l'adresse, les informations sur la carte de crédit, les informations médicales ou l'historique des achats sur un site internet, lorsqu'ils parlent de données personnelles. Mais le Règlement général sur la protection des données de l'Union européenne (RGPD) va beaucoup plus loin en définissant les « données à caractère personnel », comme : « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »); est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

En incluant des points de données tels que les cookies (identifiants en ligne) et les données de localisation, cette définition européenne des données personnelles cible un cadre bien plus large que ne le prévoient certains. Comme nous le verrons dans notre rubrique consacrée à l'« Internet des objets », et à la « transmission de données entre machines » (M2M), lorsque des données relatives à une personne identifiable sont générées par un appareil (par exemple concernant son utilisation de l'appareil), dans certaines juridictions, ces données sont considérées comme des données personnelles. La frontière entre données « personnelles » et « non personnelles » n'est pas aussi étanche que l'on pourrait croire surtout lorsque des notions telles que l'anonymat et le pseudonymat entrent en jeu.

Ces aspects prennent toute leur importance lorsque l'on discute de la valeur potentielle des données personnelles. Alors qu'une grande partie de « mes données » peut inclure des données qui pourraient être personnellement identifiables, il y a par ailleurs beaucoup de données sur les gens et leurs comportements qui sont de nature statique (c-à-d non identifiables) mais qui sont la source

d'importantes réflexions et qui offrent un grand potentiel pour améliorer la vie des citoyens.

Beaucoup de questions complexes sont alors posées sur la manière dont les données personnelles sont en train d'être collectées et utilisées. Parmi ces questions, figure la volonté de savoir si les gens savent ou comprennent pourquoi les données sont collectées et à quels usages elles sont destinées, s'ils seraient à l'aise avec cette collecte et les usages s'ils avaient les réponses, si cette collecte et cette utilisation des données enfreint le droit à la vie privée des personnes et si les personnes concernées reçoivent une rétribution équitable des avantages financiers et des autres avantages que leurs données ont contribué à générer.

Plusieurs solutions sont offertes, notamment :

- Garantir plus de transparence.
- Déterminer qui serait digne de confiance.
- Eduquer les usagers.
- Solliciter une réglementation qui protège les personnes physiques dans leurs interactions avec les organisations.
- Solliciter une réglementation pour restreindre les possibilités des organisations de collecter ou d'utiliser des données ou d'exercer un « pouvoir sur les données ».
- Proposer une nouvelle répartition du pouvoir et du contrôle notamment en mettant à la disposition des personnes des entrepôts de données personnelles leur permettant de collecter et de contrôler leurs propres données indépendamment des organisations avec lesquelles elles interagissent.

Il n'est donc pas surprenant que plusieurs ateliers se soient particulièrement penchés sur ces problématiques relatives aux données personnelles. Nous y revenons de manière plus approfondie dans des chapitres spécifiques, mais les propos suivants vous en donnent un avant-goût.

Ce que nous ont dit les participants

La plupart des participants sont d'avis que les problématiques relatives au contrôle des données personnelles occupent de plus en plus de place dans le débat public. A Dakar, on estime que « *quoi qu'il arrive, l'homme sera toujours au cœur du système et non la machine. Ce sera certes un défi car l'intelligence artificielle est en train de gagner du terrain* ».

A mesure que les concepts se sont précisés dans l'esprit des participants, beaucoup d'entre eux ont eu le sentiment que nous vivons une époque de transition d'un pouvoir porté par les multinationales vers une marge de manœuvre plus importante des personnes physiques. A Singapour, on reconnaît qu'il y a une contradiction entre ce que les consommateurs conçoivent comme une propriété et les entreprises comme un accès, mais que « *les citoyens reprennent possession des données – qu'il se pourrait bien qu'il y ait un transfert du pouvoir de contrôle vers les personnes physiques* ». Ce sentiment est partagé à Johannesburg mais avec une certaine réserve, « *cela dépendra de la manière dont la propriété des données sera définie* ». A Tokyo, l'opinion majoritaire est que « *les personnes physiques détiendraient progressivement la propriété des données au détriment des gouvernements et des entreprises* ». Par ailleurs, certains estiment que ce débat est un leurre. Lors d'un atelier regroupant des étudiants à Pretoria, il a été suggéré que « *les données ne devraient appartenir à personne* ».

Ces discussions ont mis en évidence un certain nombre de différences culturelles. Par exemple, en Europe, où la vie privée est inestimable, c'est le cas à Londres où l'on considère que « *la vie privée et la confidentialité correspondent à une réalité autant sur le plan individuel que sur le plan national, il faut rester intraitable sur ce point* ». Par contre, à Tokyo, on pense plutôt que « *la plupart des gens ne tiennent pas tellement à leur vie privée – quoi qu'en disent les experts* ».

Quant à l'analyse de la valeur des données, l'opinion exprimée à Bangalore est « *qu'il y aura une prise de conscience croissante de la valeur des données personnelles et que cela renforcera la position des personnes physiques...mais que l'attrait de la monétisation favorisera la collaboration. Il faut trouver un équilibre entre la protection des données personnelles sensibles et les avantages du partage des données* ». A Copenhague, on a le sentiment « *qu'il y a une volonté de vendre les données à bon marché, en guise de compromis, au nom des avantages que cela apporte* ».

3.2 Propriété et valeur



Beaucoup font l'amalgame entre le droit de propriété et le droit d'exploitation des données pour en tirer de la valeur. Cependant les notions liées à la propriété ne s'appliquent pas en l'occurrence, donc de nouveaux modèles doivent être explorés et testés.

Lors des discussions, une forte volonté de clarification des règles pour désigner, en toutes situations, les véritables propriétaires des données, a été manifestée. L'on présume naturellement qu'une fois la question de la propriété tranchée, tous les points connexes tels que les droits, avantages, responsabilités, etc. le seront également.

Dans certains cas, la propriété des données est une question facile à résoudre : c'est le cas des données générées par une organisation dans le cadre de ses processus internes, qui constituent donc la propriété de ladite organisation. Cependant, de manière générale, les données ne fonctionnent pas de la même manière que les formes classiques d'actifs corporels privés. Dans la plupart des cas, les données sont cocréées par au moins deux parties par le biais de transactions, interactions, communications, ce qui justifie l'existence d'au moins deux propriétaires potentiels de ces données. Les données peuvent être utilisées sans s'épuiser, les mêmes données peuvent être utilisées par plusieurs parties pour des finalités différentes. Les données peuvent également être répliquées de différentes manières à un coût

insignifiant, ce qui constitue une limite sur le plan économique. Cela peut également compliquer l'application à l'utilisation des données, des restrictions habituelles relatives à la notion juridique de propriété.

« Les données ne sont pas créées par une personne en soi, elles sont le résultat d'efforts conjoints, dans ce sens, il n'est pas réaliste de considérer que le vrai débat se situe au niveau de la propriété. La propriété des données est partagée par de multiples acteurs, prenez l'exemple des transactions bancaires... La propriété est alors un terme inapproprié, les fondements de cette notion de propriété ne sont pas assez solides pour qu'une alternative soit formulée sur leur base. »

Atelier de Bangalore

Droits et responsabilités

Ces problématiques complexes poussent à explorer des moyens alternatifs pour cadrer le débat notamment en tournant l'attention vers les questions relatives aux droits d'accès et d'exploitation et vers la fonction de gardien des données, plutôt que vers celle de propriétaire des données. Les ateliers ont permis d'identifier et de distinguer les rôles de multiples acteurs de la filière des données : générateurs, gardiens, exploitants et utilisateurs. Une bonne partie de la discussion a porté sur la définition des droits, responsabilités, obligations et opportunités pour chacune de ces fonctions. Les problèmes et dilemmes sont particulièrement houleux lorsque l'on aborde la question des données personnelles, car au-delà des complexités liées à la cocreation des données, il y a des chevauchements ou des contradictions entre des questions de droits humains et des notions juridiques bancales de propriété privée. Par ailleurs, le débat prend de l'ampleur avec l'Internet des objets, domaine où plusieurs parties prenantes dont les fabricants et les utilisateurs d'appareils électroniques ainsi que les appareils eux-mêmes, jouent chacun un rôle dans la génération des données.

Partager la valeur

Les débats les plus animés de plusieurs de nos ateliers ont porté sur la répartition de la valeur des données entre les différents intervenants de la filière des données. L'opportunité de séparer les notions de « propriété » et « d'utilisation » par les tiers est une question qui est revenue régulièrement. C'est ainsi que la nouvelle notion de gardiens des données a été discutée, dans une certaine mesure. Il a été suggéré que les « gardiens des données » puissent jouer un double rôle pour lequel ils seraient rétribués : protéger les entrepôts de données et les sources de données (comme dans le cas des coffres dans les banques), contrôler l'accès et les prix (comme le ferait un agent littéraire). Certains ont avancé l'idée que le générateur devrait aussi être le gardien, en sorte que

toutes les données soient contrôlées et possédées par leurs générateurs ; d'autres toutefois, pensent que ce rôle conviendrait mieux à un intermédiaire ou à une plateforme indépendante.

Gérer la valeur

Bien que des modèles de gestion de données continuent à émerger, l'idée que certains d'entre nous puissent progressivement accepter de payer pour que leurs données personnelles soient surveillées, partagées en échanges de paramètres convenus, et le cas échéant monétisées, a été débattue. Le choix entre une approche normalisée ou différentes plateformes fonctionnant sur la base de différents modèles adaptés aux secteurs, aux cultures et aux types de données concernés, reste une question entière. Beaucoup pensent que si nos données personnelles ont de la valeur, alors nous devrions être en mesure de le constater, d'en jouir, de contrôler ces données de manière plus efficace, et par conséquent de pouvoir choisir qui, en dehors de nous, pourrait y avoir accès et en jouir.

« La valeur des données est très régionale et porte autant sur ceux qui en profitent que sur ceux qui les possèdent. »

Atelier de San Francisco

Des meilleures pratiques relatives aux processus et modes d'exploitation, destinées aux propriétaires et aux gardiens des données ont été présentées et discutées. Elles portaient essentiellement sur le paiement de l'accès aux données et des modalités de transfert des droits de propriété entre les différentes parties prenantes. Chacun des modèles est différent de ceux qui sont appliqués de nos jours et dans lesquels le système est axé sur l'exploitant des données.

Problèmes et dilemmes :

- La « propriété » est-elle une notion utile ou pratique lorsque l'on envisage certains types de données, comme les données personnelles ?
- Sinon, quels autres concepts de substitution pourrait-on envisager ?
- Quelles autres modalités pourrions-nous appliquer pour attribuer des droits, des avantages et des responsabilités en relations aux données, aux différentes parties prenantes telles que les gouvernements, les entreprises de technologies, les multinationales et les particuliers ?
- Dans quelles circonstances la notion de « propriété » est-elle pertinente ?

Ce que nous ont dit les participants

A Francfort, on est d'avis que pour comprendre la valeur de nos données personnelles, il faut passer « *d'un monde où la notion de données est synonyme de nébuleuse, de panique, d'incertitude et d'impasse quant à ce que l'on pourrait faire de nos données en dehors de ce que nous offre une poignée de grandes multinationales de la technologie, à un monde offrant une vision claire de la valeur, de la propriété et des droits liés aux données.* »

Partager le gâteau

Saisissez dans Google Search « à qui appartient vos données ? » et vous trouverez des dizaines d'articles intéressants, toutes présentant des opinions divergentes. Mais, est-ce réellement important ? La plupart des participants ont pensé que non et partageaient plutôt cette perspective exprimée à Bangalore : « *les données ne sont pas créées par une personne en soi, elles sont le résultat d'efforts conjoints, dans ce sens, il n'est pas réaliste de considérer que le vrai débat se situe au niveau de la propriété. La propriété des données est partagée par de multiples acteurs, prenez l'exemple des transactions bancaires. Les clients interagissent avec les banques, initiant ainsi un processus à double sens. La propriété est alors un terme inapproprié, les fondements de cette notion de propriété ne sont pas assez solides pour qu'une alternative soit formulée sur leur base.* » Un moyen de résoudre la problématique serait que les personnes physiques détiennent la propriété exclusive de leurs données personnelles sur un format numérique lisible et sous-traitent leur gestion et leur répartition à des gardiens professionnels, des agents de promotion ou des courtiers de données.

Gérer la valeur des données

Un moyen de gérer la valeur des données serait de recourir à des entrepôts de données. Ces derniers permettraient aux individus d'obtenir plus de transparence quant à l'utilisation qui est faite de leurs données. Il s'agirait essentiellement « d'un entrepôt centralisé destiné aux données personnelles, où les personnes physiques pourraient accéder à leurs données et en contrôler l'accès par le tiers. »⁵ On a envisagé également la création d'une nouvelle profession, celle d'agent de confidentialité ou de courtier des données. A Londres, le rôle de ces acteurs a été comparé à celui d'un gestionnaire de patrimoine « dans la mesure où nous faisons confiance à un tiers dans un domaine essentiel, pour prendre des décisions à notre place et que nous pouvons orienter ses décisions (ex : actives, passives, éthiques). Il pourrait en être de même dans le domaine des données avec des tiers de confiance, qui pourraient soulager le consommateur de ce type de tâches.

Lors de notre atelier au Kenya, les participants sont parvenus à l'idée suivante. A Nairobi, on a suggéré, dans l'éventualité de la création d'un entrepôt de données centralisé, « ...de permettre aux entreprises et aux gouvernements d'accéder aux données personnelles mais de faire en sorte que les personnes physiques gardent le contrôle de leurs données et puissent jouir des avantages, et ainsi « ...il y aura un accès plus large aux informations sans que les données personnelles ne soient mises en péril. »

De la propriété au gardiennage des données

Il y avait un consensus autour de la nécessité d'une transition de la notion de « propriété » à la notion de « gardiennage » dans les dix prochaines années. A Bogota, il a été suggéré que « même si ceux qui possèdent les données vont continuer à exploiter leur valeur...de plus en plus de données seront utilisées dans l'intérêt général. » A Whashington DC, les participants ont estimé que cela mènerait à « une meilleure utilisation des données issues d'ensembles de données plus conséquent et mieux agrégés » qui auraient plus d'impacts. Enfin, à Sydney, on anticipe une utilisation collaborative en « se servant des données pour optimiser le bien être social, ce serait alors une « mutualisation des données pour le bien de tous » notamment pour diminuer les accidents de la route ou le suicide des adolescents, pour lever des fonds en vue de résoudre des problèmes de santé, pour renforcer l'appartenance sociale, combattre l'isolement et la marginalisation, ainsi les données pourraient rendre la vie meilleure. »

On comprend qu'il y a un besoin de transparence, d'information plus poussées, d'action mieux ciblée et de points de vue plus consensuels et mieux éclairés sur la propriété des données et sur ses implications. Imprégnés d'une culture où la confiance est un acquis par défaut, les danois pensent que « nous pouvons aller vers une propriété commune des données par le biais de coopératives au sein de la société. Cela fournirait un cadre propice à la création des plateformes fiables qui constitueraient plus tard des écosystèmes plus larges. » A San Francisco, une réflexion indiquait que « la valeur des données est très régionale et porte autant sur ceux qui en profitent que sur ceux qui les possèdent. »

3.3 Pouvoir et influence



Apporter de la valeur par les données

Les données constituent autant un moyen d'exercer le pouvoir que la source de nombreuses luttes de pouvoir. La réglementation vise à rééquilibrer les influences des entreprises, des gouvernements et de la société.

Les participants aux ateliers à travers le monde étaient extrêmement conscients du fait que les données confèrent du pouvoir ; Ils savent, en effet, que plus une organisation collecte, utilise et contrôle des données, plus elle renforce son pouvoir. Ce pouvoir peut prendre différentes formes. Il peut s'agir du pouvoir de prendre des décisions qui ont un impact sur la vie des gens, notamment en leur donnant ou en leur refusant l'accès à des services. Certaines organisations utilisent le pouvoir qui leur est conféré par les données pour agir en « architectes des choix », décidant ainsi des informations qui doivent être présentées au public et de la manière dont celles-ci doivent être présentées. La concentration des données peut entraîner une concentration du pouvoir économique, ce qui peut par ricochet influencer la répartition des avantages disponibles.

Selon les différentes manières dont les données sont collectées et utilisées par les différentes parties, nous avons constaté qu'il peut y avoir différentes sortes de rapports de force, notamment entre :

- Les décideurs politiques/régulateurs et les grandes entreprises dépendant des données ;
- Les gouvernements et leurs citoyens ;
- Les entreprises et leurs clients ;
- Les responsables politiques dont les compétences sont distinctes ou se chevauchent.

« Lorsque les entreprises s'engagent dans des procédures trop compliquées à gérer ou à comprendre, alors les déclarations de consentement deviennent des actes vides de sens »

Atelier de Londres

Perspective de nombreux experts lors d'échanges à travers le monde

Par ailleurs de nombreuses manières d'aborder les problèmes de déséquilibres de pouvoir ont été abordées. Les solutions suivantes ont suscité un intérêt particulier :

Transparence : plusieurs participants aux ateliers sont préoccupés par ce qu'ils ont perçu comme le pouvoir incontrôlé des algorithmes propriétaires qui, de fait, sont exempts de tout examen et permettent aux organisations qui les élaborent d'exercer une très forte influence. Le manque de transparence fait qu'il est presque impossible à tout acteur externe de comprendre les motivations économiques, politiques et culturelles qui suscitent leur création.

Redevabilité : Il y avait également une grande préoccupation au sujet de la capacité des moteurs de recherche et des réseaux sociaux à influencer la nature des informations présentées aux internautes. Le pouvoir d'inclure, de retirer, d'agencer la présentation des informations permet à ces sociétés de s'assurer que certaines impressions laissent une empreinte permanente chez le public tandis que d'autres se dissipent rapidement. Lorsque l'on ne sait pas exactement comment un moteur de recherche est paramétré pour classer des sites internet, on ne peut pas vérifier si l'outil agit en toute bonne foi pour aider les utilisateurs ou s'il intervient de manière biaisée pour mettre en avant ses propres intérêts commerciaux, culturels ou politiques.

Rééquilibrage des pouvoirs : les débats ont essentiellement porté sur la question de savoir si les multinationales de la technologie détiennent un pouvoir excessif. Des interrogations portant sur l'exercice responsable de ce pouvoir, sur les sauvegardes, réglementations et réformes nécessaires pour favoriser un environnement plus sain, plus équitable, plus sûr et un écosystème de données plus innovant ou résilient, ont été exprimées. Certains participants ont estimé que les activités des acteurs qui détiennent un pouvoir disproportionné sur les données devraient faire l'objet d'une réglementation plus stricte. D'autres souhaitent des

réactions plus radicales notamment une répartition plus égalitaire du pouvoir (par des règles de compétitions et une législation anti-trust, notamment).

Problèmes et dilemmes :

- Les organisations qui collectent et utilisent de grandes quantités de données peuvent générer une valeur substantielle au profit des personnes physiques, de la société, de l'économie et pour elles-mêmes. Mais en même temps, elles peuvent mobiliser un pouvoir excessif ou utiliser le pouvoir dont elles disposent de façon injuste ou inappropriée. Comment éviter au mieux ces écueils ? Qui serait en mesure de le faire ?
- Par ailleurs, par quels critères devrions-nous déterminer si une organisation détient un pouvoir excessif ou utilise son pouvoir de façon injuste ou inappropriée ? qui devrait être chargé de porter de tels jugements ?
- Si l'on considère qu'une entité détient trop de pouvoir ou exerce son pouvoir de façon irresponsable, quelles sont les mécanismes appropriés pour une action efficace ?
- Comment les décisions pourraient-elles être mises en œuvre ?
- Comment pourrait-on et comment devrait-on gérer les litiges liés à la collecte et à l'utilisation des données entre différentes entités et juridictions (locales, régionales, mondiales) ?

« Quoi qu'il arrive, l'homme sera toujours au cœur du système et non la machine. Ce sera certes un défi car l'intelligence artificielle est en train de gagner du terrain ».

Atelier de Dakar

Ce que nous ont dit les participants

Les problématiques liées à l'exercice du pouvoir conféré par les données ont été soulevées dans la plupart des discussions. Pour donner un aperçu des discussions, nous vous livrons ici quelques réflexions des participants.

On a de plus en plus l'impression que les entreprises profitent excessivement de la collecte, de l'utilisation et souvent de la vente des données personnelles. A l'atelier de Bangalore, on soulignait ce fait en estimant que « *les droits des consommateurs sont toujours négligés, ils n'ont pas le pouvoir comme Google ou Facebook* ». Cela suscite chez eux, le désir de donner plus de pouvoir aux personnes physiques, sur leurs propres données. Il a été admis tout de même, qu'accorder plus de pouvoir aux personnes ferait émerger un nouveau dilemme. Comment garder le contrôle sur nos données sans perdre les avantages et les commodités indéniables du troc, données personnelles contre services numériques ?

Transparence : nous avons entendu plusieurs appels en faveur de cadres législatifs plus efficaces qui contribueraient à orienter l'économie des données émergente, de façon plus équitable, afin d'encourager la transparence et de rendre les entreprises de technologie plus comptables et responsables. Beaucoup de participants en Afrique et en Asie, inspirés par la position de l'Union européenne, matérialisée par le RGPD, sont prêts à relever le défi. A Mexico City, on pense que « *le plus grand changement sera guidé par la manière dont les gouvernements vont contrôler les données* ».

« Personne n'a encore pu déterminer l'ampleur de l'impact de la diffusion des données médicales sur la sécurité publique. »

Atelier de Singapour

A Dakar, on a noté que « *plus on a de pouvoir sur les données, plus on peut les utiliser pour tordre les réalités. Les fausses nouvelles sont tout juste un aperçu de ce qui pourrait advenir dans ce domaine...* ». Au fil des ateliers, nous avons entendu de nombreux appels à la promotion de la culture numérique afin que les personnes puissent choisir les produits et services qu'ils utilisent en connaissance de cause et puissent exercer un meilleur contrôle sur leurs données personnelles. Beaucoup ont plaidé en faveur de plus de transparence et d'intelligibilité autour de l'utilisation des données. Ils ont souligné que s'il est trop difficile de comprendre l'utilisation qui est faite des données, il est alors impossible pour les personnes (et les organisations) d'avoir un rapport d'égal à égal avec les sociétés qui les exploitent. Certains estiment qu'une transparence accrue permettrait sans doute de progresser considérablement mais ne constitue pas une solution à elle seule. A Londres, on observe que « *lorsque les entreprises s'engagent dans des procédures trop compliquées à gérer ou à comprendre, alors les déclarations de consentement deviennent des actes vides de sens* ». Pour que le pouvoir des données soit mieux réparti, il faut une meilleure compréhension par le public, des processus en œuvre pour l'utilisation de leurs données. Certains participants de Londres ont même suggéré que les transactions qui sont « *trop complexes à exposer aux acteurs externes, soient considérés comme trop complexes pour mériter d'exister* ».

Redevabilité : en Afrique et en Inde, il y a un grand sentiment de frustration au sujet de la domination des entreprises américaines de la Silicon Valley. Beaucoup pensent qu'ils exercent une forme de néocolonialisme, les données personnelles devenant la dernière sorte de matière première exploitée par l'Occident. Les participants de Singapour et de l'Australie estiment que la gestion des flux nationaux de données est une affaire de sécurité nationale. Lors d'un atelier à Singapour, qui était dédié aux données des patients, nous nous sommes vu confier que la législation du pays restreint le partage des données médicales au-delà des frontières nationales parce que « *personne n'a encore pu déterminer l'ampleur de l'impact de la diffusion des données médicales sur la sécurité publique.* »

A Bangalore, les participants ont le sentiment que le manque de transparence concernant l'utilisation et la manipulation des données mène à « *un fossé numérique grandissant au sein du pays, mais aussi entre les citoyens* ». Cela a été également évoqué à Madrid où l'on estime que cette fracture numérique pourrait devenir un abîme et que cette problématique « *restera dominée par les notions de transparence, omniprésence et contrôle* ». D'autres ont réitéré le besoin de transparence autour des données, de leur gestion et de leur partage afin de permettre aux usagers d'avoir un meilleur contrôle sur leurs données.

Règlementation : un certain nombre de mécanismes permettant d'assurer une répartition plus juste du pouvoir ont été discutés. Par exemple, l'interopérabilité et la portabilité (démocratiser l'accès) ainsi que la possibilité de démanteler les organisations qui sont devenues des monopoles. A Bogota, les participants ont suggéré que les partenariats public/privé seraient le meilleur moyen de promouvoir et d'asseoir la bonne gouvernance. Plusieurs participants se sont prononcé en faveur de la mise en place d'une Vision mondiale sur les données⁶ et d'une structure internationale pour l'élaboration et la supervision de la mise en œuvre d'une réglementation internationale. Cela a paru très intéressant, toutefois, en poussant la discussion, personne n'a pu décrire en pratique son futur fonctionnement et quelles en seraient en définitive les personnes ou entités comptables.

Enfin, en Asie et surtout aux Etats-Unis, nous nous sommes entretenus sur la géopolitique et sur la manière dont les différentes idéologies pourraient influencer l'utilisation des données. A Hong Kong, la question se pose en ces termes : « *quelles seraient les implications de la victoire de la Chine sur le débat lié aux données, et que se passerait-il si cette dernière exporte ses valeurs à travers le monde ?* ». A Washington DC, l'opinion était que « *si vous considérez ces différents modèles comme des dynamiques en compétition, alors cela a de l'importance, parce que la Chine grandit et d'autres populations ou nations vont l'imiter* ». De manière plus prosaïque, à Dakar, on affirme plutôt : « *qu'on nous serve des nouilles au petit-déjeuner ou des hamburgers au déjeuner, cela nous est égal, nous devons créer nos propres solutions* ».

3.4 Penser mondial, régional ou local ?



Apporter de la valeur par les données

Perspective de nombreux experts lors d'échanges à travers le monde

Tandis que certains soutiennent une plus forte dynamique de mondialisation des données, d'autres souhaitent un contrôle régional et national plus ferme pour protéger leurs citoyens et renforcer leur économie.

Dans de nombreuses sphères, il y a souvent cette certitude que les multinationales de technologies (Big Tech) peuvent et vont continuer à « faire ce qu'elles veulent ». Pourtant, il y a un fort sentiment, surtout dans les régions en forte croissance de l'Afrique et de l'Inde, que les gouvernements devraient avoir davantage de contrôle sur les données, pour protéger les droits des citoyens, développer l'économie et conserver un sens de l'identité culturelle. Cela pourrait être source de conflit avec ceux qui considèrent que la libre circulation des données est essentielle à la croissance économique.

Si le monde était dirigé par une seule autorité capable de prendre des décisions sages et légitimes et de les mettre en œuvre de manière efficace et efficiente, la vie serait simple. Mais ce n'est pas le cas. Nous vivons plutôt des réalités extrêmement complexes. Nous sommes guidés par des multitudes d'autorités différentes ayant des compétences qui se croisent et nous portons des héritages historiques et des valeurs culturelles très diverses ainsi que des conceptions de nos êtres, de nos intérêts, de nos

motivations, de nos priorités et de nos pouvoirs tous aussi variés. Ces prérogatives qui peuvent parfois se déclinier en doublons et en contradictions mènent à la confusion et aux conflits sur la légitimité des acteurs, des décisionnaires, des bénéficiaires dans différents domaines spécifiques, ce qui mène à une situation où toutes les parties prenantes concernées s'estiment habilitées à agir. A l'inverse, pour d'autres problématiques, nul n'est prompt à agir, ni à assumer des responsabilités.

La révolution des données se met en marche dans ce contexte de conceptualisation et de réglementation effréné et émaillé de confusion quand il faut désigner la figure de proue. On en arrive à des guerres d'influences et à la course au pouvoir. Arènes de combats et zones rouges s'installent dans le paysage des données, théâtre d'avidité et d'ambition dévorante.

« Il faudrait un cadre de principes communs permettant l'utilisation publique et privée des données dans plusieurs juridictions. Pour ce faire, il faudrait d'abord une collaboration internationale pour établir un ensemble de normes universellement reconnues »

Atelier de Hong Kong

Problèmes et dilemmes :

- Quand faut-il ou quand est-il souhaitable de laisser circuler les données au-delà des frontières nationales ?
- Quelles sont les différentes règles à appliquer aux différents types de données ? (données personnelles, données non personnelles) aux différentes situations et aux différents types d'utilisation ?
- Quelles entités et à quelle échelle (locale, régionale, mondiale) sont-elles mieux placées pour orienter la dynamique autour des données ?
- Comment garantir : a) leur légitimité aux yeux des autres acteurs clés et b) leur efficacité ?
- Comment dissiper les principales préoccupations (ex : dangers du nouvel impérialisme des données, risques que le confinement des données puisse ralentir l'innovation et la prospérité économique) ?
- Comment s'assurer que les pays tirent profit des données qu'ils produisent ?
- Les innovations autour de l'apprentissage machine nécessitent-elles une forme de gouvernance et une approche réglementaire différentes ?

Ce que nous ont dit les participants

Lors de nos ateliers, nous avons souvent entendu le même refrain. Les données ont suscité de nombreuses problématiques et les décideurs politiques et les régulateurs doivent se mettre à jour. Partout où nous sommes allés, les participants ont évoqué la nécessité de renforcer les mesures réglementaires ainsi que la collaboration et la coordination entre les gouvernements et le secteur privé. Toutefois, il n'y avait pas une convergence marquée quant à désigner qui devrait, ou qui serait le mieux placé pour relever les défis et à quelle échelle porter le combat : local (ou national), régional (ex : UE) ou mondial ? avec une entité internationale ?

Plusieurs solutions ont été examinées. On peut les classer globalement dans trois catégories :

- Entité internationale de régulation
- Entités régionales de régulation : Amérique, Union européenne, China – Asie centrale
- Règlementation internationale

Dans un monde où de multiples juridictions se croisent, on a le sentiment que : tout d'abord, la gestion des données suscite des questions très universelles par essence, comme c'est le cas de la vie privée et de la confidentialité, de la propriété, de l'éthique, de l'équité dans la répartition des avantages, qu'il paraît indispensable de trouver des solutions communes ; ensuite, qu'il n'y a pas pour l'heure une organisation capable de jouer ce rôle. Par conséquent, beaucoup de participants ont suggéré la mise en place d'une haute autorité qui pourrait redresser la barre, notamment pour créer un cadre éthique établissant des principes et des pratiques communes pour tous.

L'idée a été évoquée pour la première fois à Bangalore, où les participants ont suggéré la « *création d'un Conseil mondial des données qui pourrait faciliter les échanges internationaux* ». Ce Conseil pourrait, par exemple, contribuer à établir un consensus autour des problématiques telles que la souveraineté des données et à concilier les différences culturelles autour de la confidentialité. Certains ont fait des analogies avec les différentes initiatives engagées en vue d'adopter une approche collective du changement climatique. A Hong Kong, il a été proposé un « *cadre de principes communs permettant l'utilisation publique et privée des données dans plusieurs juridictions. Pour ce faire, il faudrait d'abord une collaboration internationale pour établir un ensemble de normes universellement reconnues* ». Les participants des ateliers de Jakarta, Bangkok, Singapour, Mexico et Londres appellent de leurs vœux la mise en place d'un « *cadre de réglementation international indépendant des données (éventuellement comme le G20)* ».7 A Dakar, on suggère que « *les gouvernements et les nations (voire les organisations) entament une*

réflexion collective sérieuse sur une Vision pour les données...un modèle stratégique orientant l'utilisation des données et des technologies axées sur les données ». Quelle que soit l'approche retenue, il est clair qu'il y a un penchant collectif pour une haute autorité indépendante chargée d'établir les normes, de déterminer un terrain d'entente et de garantir l'équilibre et l'indépendance.

Mais quelles seraient les organisations dignes de confiance et capables d'orienter cette dynamique ? Lors des discussions, on a pu noter une volonté commune de voir « quelqu'un d'autre » intervenir et déterminer les modalités de régulation des données, toutefois de nombreux participants sont conscients qu'une harmonie à l'échelle mondiale serait difficile à obtenir, pas uniquement à cause de l'ampleur du défi et des accords nécessaires, mais aussi à cause de la méfiance qu'il y a entre certains gouvernements et certaines multinationales. Cela était très évident en Afrique, en Inde et dans certaines parties de l'Asie. Cela a été également reconnu en Europe continentale.

Le Forum économique mondial fait partie d'un certain nombre de grandes organisations qui tentent d'élaborer une approche internationale collaborative, toutefois, un nombre très limité de participants estime que cela serait efficace.⁸ A Madrid, par exemple, on estime que « les services occidentaux dominants, conçus par des ingénieurs occidentaux, qui reflètent des valeurs occidentales, et qui sont axés sur des données occidentales seront de plus en plus perçus comme impérialistes, inconséquents ou inadaptés dans différentes régions culturelles ». Il sera donc extrêmement difficile de dépasser des impératifs politiques conflictuels et des intérêts commerciaux divergents.

Règlementation à l'échelle régionale

Une alternative peut-être plus pratique serait une approche régionale de la régulation des données. Les entités régionales peuvent traiter ces problématiques complexes plus facilement dans un contexte culturel et politique local. En Europe, l'Union européenne a déjà adopté de nouvelles doctrines

qui sont en train de donner naissance à des règles régionales sur la vie privée et la confidentialité, les données et l'espionnage. A Pretoria, il a été avancé qu'une solution panafricaine sur les données pourrait marcher, « *cela devrait se faire idéalement sous la forme d'un ensemble de normes régionales plutôt qu'une seule norme locale, ainsi cela contribuerait à améliorer les effets et à empêcher les gouvernements de se servir de la réglementation des données pour établir un contrôle étatique directif de puissants ensembles de données personnelles* ».⁹

Beaucoup de nos interlocuteurs se sont montrés très intéressés par ce qui se fait ailleurs. Par exemple, les participants en Asie et en Afrique observent avec intérêt l'évolution du RGPD de l'UE et pourraient tout à fait encourager ce type de mesures. « *le RGPD va changer le paysage des données au Nigéria et va susciter l'avènement de nouvelles normes* ». Il n'y a pas que l'Europe comme précurseur dans ce domaine. Le poids économique de la Chine ainsi que son influence croissante en Asie et en Afrique pourrait signifier un basculement vers sa stratégie de préservation du pré carré numérique. Il sera intéressant de voir quelle stratégie va dominer, au final.

En Afrique, nous avons entendu à maintes reprises que « *l'économie libérale ou la société capitaliste/occidentale a la mainmise sur les pays les plus pauvres* »¹⁰ et que les « *données africaines devraient rester dans des serveurs africains* »¹¹. La logique derrière ce raisonnement est de rendre les données locales plus accessibles et favorable à l'économie locale, mais également d'empêcher les multinationales (essentiellement américaines) d'exploiter la valeur des données africaines à leur propre avantage. La préservation des données culturelles est une préoccupation toute particulière au Kenya et au Nigéria : « *les données culturelles constituent une réserve d'actifs et elles devraient être sous licence, elles devraient être considérées comme de la propriété intellectuelle* »¹². A Dakar, certains ont estimé que les « *données devraient être utilisées dans l'intérêt national, pas uniquement à l'avantage des compagnies multinationales* ». Sur un continent en rapide croissance, qui a déjà eu une amère

expérience de l'exploitation par l'Occident, on est peu enclin à laisser les données devenir encore une autre ressource à exploiter au profit d'un autre pays.

Règlementation à l'échelle nationale

Les avantages et les inconvénients de la réglementation nationale ont été discutés de manière approfondie et vus à travers le prisme de la souveraineté et de la localisation, les deux ayant pour effet de réfréner les flux de données au-delà des frontières. La souveraineté des données implique un assujétissement des données aux lois et structures de gouvernance du pays dans lequel elles sont connectées et la localisation des données implique la restriction des flux de données entre frontière soit en exigeant que les entreprises maintiennent les données au sein d'une juridiction particulière ou en imposant des conditions préalables à leur transfert hors des frontières. Les objectifs derrière ces restrictions peuvent être multiples et incluent notamment la vie privée et la confidentialité, la cybersécurité, la sécurité nationale, l'ordre public, la répression, la fiscalité et le développement économique entre autres. Les deux approches renvoient à un sentiment de plus en plus fort d'identité nationale et elles sont de plus en plus encouragées dans un certain nombre de marchés que nous avons visités, surtout en Afrique et en Asie.

Dans les pays à forte démographie comme la Chine et l'Inde, on pense que le confinement des données nationales facilitera la croissance économique, permettra de construire ou de protéger le pouvoir politique et stimulera l'innovation locale. En Afrique, cette perception est associée avec l'idée qu'il faut empêcher « les organisations extérieures de profiter de l'occasion » et donc, protéger les citoyens de la « colonisation des données »¹³. Parallèlement, en Europe, même s'il y a une volonté générale de laisser libre cours aux données, il y a également le sentiment qu'il faut un équilibre savamment dosé entre la circulation des données et le respect du principe de vie privée en tant que droit humain.

Les détracteurs de la libre circulation des données estiment que les législations nationales sapent le libre échange en imposant des obligations onéreuses

en termes de commerce. Cela inclut notamment la construction, l'exploitation et la maintenance de centres de données dans plusieurs pays ainsi que la création et la mise à jour de plusieurs ensembles de données séparés, même s'il s'agit de bases de données miroirs. 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, c'est sûr selon eux, cela va réduire les opportunités.¹⁴ Un rapport de 2016 suggérait que les effets de la libéralisation des mesures en place actuellement pourrait permettre d'injecter 8 millions d'euros de plus par an, rien que dans l'économie européenne.¹⁵ Dans les pays émergents, certains estiment que le maintien continu des mesures de localisation va non seulement impacter la croissance économique mais va avoir un impact négatif sur le développement social. A Dakar, on a observé que le « *protectionnisme et les approches cloisonnées vis-à-vis des données pourraient étouffer l'innovation, entraîner des soulèvements sociaux, susciter une désillusion quant à la capacité des données à engendrer le bien, isoler des segments entiers de la population mondiale et favoriser une corruption nationale de grande ampleur* ». D'autres ont souligné que localisation des données pourrait éventuellement affaiblir la sécurité nationale, dans la mesure où, plus il y aura de centres de données, plus les données seront vulnérables aux hacking.

Conserver et optimiser les acquis de la croissance et de l'utilisation des données ne sera pas possible sans les inconvénients de l'ajustement de la réglementation pour accompagner cette expansion. A l'avenir, il est clair qu'il faudra de nouvelles techniques et des scénarii juridiques réfléchis pour garantir la possibilité d'exploiter la valeur des données tout en protégeant les droits des personnes et en reconnaissant les différences culturelles. Ce n'est toutefois pas évident de concevoir la manière d'y arriver, de manière efficace et bénéfique.

3.5 Une confiance qui se mérite



Les organisations veulent renforcer chez les usagers, le sentiment de confiance lorsqu'ils utilisent les données. Il importe de plus en plus d'être « digne de confiance », ce qui va de pair avec une attitude sincère et transparente.

Lors des ateliers que nous avons organisés à travers le monde, il était largement admis que très peu d'organisations, s'il en est, sont dignes de confiance en ce qui concerne les données. En effet, alors que le renforcement de la confiance s'avère indispensable, à part dans quelques pays où le niveau de confiance au gouvernement reste encore élevé, l'impression qui a dominé lors des ateliers est que le niveau de confiance est en baisse. Le nouveau défi pour les organisations, les décideurs politiques et les régulateurs est de savoir comment prouver qu'ils sont dignes de confiance. Sur quelles bases devrions-nous faire confiance aux organisations en ce qui concerne les données ?

Contexte

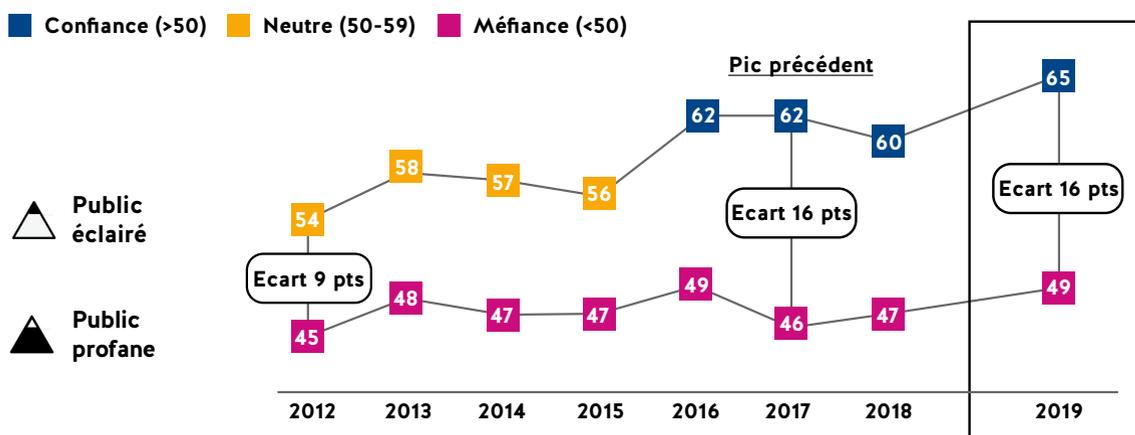
La confiance est un atout économique puissant. Quand la confiance règne parmi les citoyens, le coût des affaires baisse (car l'on passe moins de temps à négocier, calculer, élaborer des stratégies, contrôler, réglementer et réprimer) et les opportunités se multiplient car les citoyens sont plus enclins à collaborer y compris en partageant des données. De la même manière, dans les sphères où la méfiance est de mise, les coûts d'exploitation ont tendance à être élevés (à cause de tout le temps passé à négocier, calculer, élaborer des stratégies, contrôler, réglementer et réprimer) et les opportunités s'amenuisent parce que, les citoyens sont moins nombreux à prendre le risque de collaborer avec d'autres, notamment en partageant des données.

« A mesure que les préoccupations autour de la sécurité augmentent et que la confiance des développeurs africains se raffermi, les Ivoiriens souhaitent contrôler les données qu'ils produisent et devenir moins dépendants vis-à-vis des pays occidentaux ».

Atelier d'Abidjan

Nos ateliers se sont tenus à un moment très particulier : le scandale de Cambridge Analytica battait son plein, avec des impacts certains sur le degré de confiance accordé par les usagers, non seulement à Facebook, avec les données personnelles, mais également aux organisations de manière générale. Des interrogations sur le secteur des technologies

dans son ensemble, ont été suscitées. Comme l'a exprimé un étudiant : Facebook, Amazon et Uber sont toutes des « marques auxquelles nous avons moins confiance qu'avant ». ¹⁶



Edelman Trust Barometer (2019)

Le fossé en termes de confiance : il y a un écart de 16 points entre un public éclairé plus prompt à faire confiance et la masse de population plus sceptique, ce qui illustre un retour à une hausse sans précédent de l'inégalité en matière de confiance

Ce contexte particulier a rajouté une dimension supplémentaire de controverse à une problématique déjà très complexe. Lorsqu'il s'agit de confiance, il y a plusieurs dimensions à envisager, notamment :

- **A qui faire confiance ?** Parlons-nous des grandes entreprises, des petites entreprises, des gouvernements, des organisations supranationales ou des citoyens ? Ces acteurs ont des rapports spécifiques les uns avec les autres. Que les clients fassent confiance aux entreprises ou non, que les citoyens fassent confiance aux gouvernements ou pas, impliquent des enjeux et des dynamiques tout à fait différents de ceux qui sont en œuvre lorsque l'on évoque la confiance entre les régulateurs et les multinationales ou encore entre les multinationales et les hommes politiques.
- **Faire confiance pourquoi ?** Nous pourrions avoir une confiance totale aux capacités et aux compétences d'une personne donnée mais n'avoir aucune confiance en ses motivations, ou l'inverse. Les raisons de ces réticences sont nombreuses et imposent des limites au-delà desquelles on n'a plus confiance en l'autre.

Dans ce sens, les raisons pour lesquelles on gagne et préserve la confiance de l'autre peuvent varier considérablement d'une situation à l'autre. D'autres questionnements peuvent surgir lorsque l'on examine la dynamique de la confiance.

L'une de ces problématiques complexes concerne la relation entre confiance et transparence. Si l'une des parties ne sait pas ce que fait l'autre, le niveau de confiance mutuelle peut être élevé mais cette confiance peut être injustifiée. Dans ces cas où, comme le dit l'adage « le bonheur est dans l'ignorance », le niveau de confiance peut chuter de manière vertigineuse quand les gens sont choqués de découvrir la vérité. Un climat de méfiance et de suspicion pourrait alors s'installer, un retour de balancier qui ferait que, même les plus dignes de confiance n'auront plus le bénéfice du doute.

Il y a une présomption assez courante mais trompeuse qui consiste à penser que le changement du niveau de confiance entraîne directement un changement dans le degré de comportement, comme cela pourrait être le cas pour le partage d'informations. Toutefois, de nombreux facteurs peuvent intervenir et remettre en question une telle logique. Par exemple, une partie peut ne pas faire confiance à l'autre mais estimer qu'elles doivent toutes deux échanger des informations car autrement elles devront renoncer à proposer un service. Dans ces circonstances, les acteurs envers lesquels il y a de la méfiance (à raison) ne sont pas directement sanctionnés pour leur manque de fiabilité. L'expansion des nouvelles technologies tels que l'Internet des objets (IdO) et l'intelligence artificielle (IA) pourrait signifier que pour de simples raisons opérationnelles, les citoyens soient, bon gré, malgré, obligés de « faire confiance ».

Parfois la confiance s'établit dans un cadre bilatéral, ici, la Partie A fait confiance à la partie B pour une action spécifique convenue. Mais quelquefois, la confiance s'avère diffuse et impersonnelle : c'est le cas lorsque l'on a l'impression que « l'on ne peut faire confiance en personne » dans un environnement donné. Ces différentes dynamiques entraînent des comportements différents. A l'échelle bilatérale, le niveau de confiance peut avoir une influence sur la volonté des parties de coopérer et la nature de leur coopération. Au niveau impersonnel, les effets seraient plutôt susceptibles de se matérialiser sous forme de pressions en faveur d'interventions politiques ou réglementaires touchant tout un système.

« Il faut que les gens comprennent que les données ne correspondent pas à une vérité, il s'agit d'informations qui sont présentées d'une façon ou d'une autre et nous devons apprendre à déceler les données biaisées sinon nous perdrons notre liberté de choix ».

Atelier de Madrid

Ces questions et problématiques ont été abordées de manière récurrente lors des ateliers. Par exemple, on a noté une suspicion généralisée à l'égard des motivations de certaines sociétés de technologies et de leur volonté de monétiser les données (le baromètre de confiance d'Edelman (Trust Barometer) pour 2019 montre que 60 pour cent des répondants pensent globalement que « les sociétés de technologie ont trop de pouvoir et ne mettront pas notre bien-être au-dessus de leur profit »).

Il y avait également des divergences d'opinion en ce qui concerne les acteurs dignes de confiance : dans certaines cultures, on a foi aux gouvernements mais pas aux grandes entreprises ; dans d'autres, plus particulièrement aux Etats-Unis, c'est le contraire. Cela est en contraste frappant avec les attitudes en vigueur dans certaines parties de l'Asie, surtout au Japon et à Singapour, où l'on pense que la majorité des gouvernements agissent dans l'intérêt de leurs citoyens, dans ces contrées, on fait moins confiance aux entreprises pour se comporter de la même manière que les gouvernements. Il en va de même au Canada et en Scandinavie. En Afrique, on reconnaît largement que la corruption est un phénomène courant, autant au sein des gouvernements que dans le secteur privé. En effet, dans ces zones, la confiance est inexistante. (Une des questions que cette situation soulève, et que nous aborderons plus loin, est qu'en Afrique, il est courant de mentir sur les données, ce qui implique des répercussions substantielles sur la nature des données collectées).

« Le faible niveau de confiance aux gouvernements, institutions et grandes entreprises de technologies dévalue les données dans la mesure où il remet en question la fiabilité des données. Les citoyens choisissent de ne pas partager des informations exactes ».

Atelier de Washington

Ce que nous ont dit les participants

Bien qu'il y ait un grand enthousiasme en ce qui concerne la manière dont les données sont en train de transformer la société et une large reconnaissance des avantages qu'elles apportent, certains participants à nos ateliers ont exprimé leur prudence. En effet, certains craignent que le simple fait que les données soient devenues si omniprésentes nous poussent à montrer une confiance excessive et à ne plus nous interroger sur leur pertinence ou leurs sources. « *Nous devons reconnaître que données ne riment pas avec vérité ; il s'agit juste d'une façon différente de présenter de l'information. Nous devons apprendre à distinguer les biais sinon nous allons perdre notre liberté de choix* ». C'est la perception exprimée à Madrid où les participants ont avancé que la question est d'une certaine façon une affaire « d'excès de confiance », car il y a un clivage de plus en plus important entre notre dépendance à l'égard des données pour organiser nos vies et notre compréhension de la manière dont il faut les interpréter. Ils ont en outre suggéré que le public risque de devenir de plus en plus vulnérable à l'exploitation par les acteurs politiques et commerciaux. « *Les données seront de plus en plus utilisées pour contrôler les émotions surtout chez les jeunes et les personnes sensibles. Les marques et les gouvernements n'hésiteront pas à en profiter et à trouver de nouveaux moyens d'influencer les usagers et les consommateurs.*¹⁷ » Cela ne pose pas du tout de problème si les entreprises se comportent de manière responsable, mais si c'est plutôt l'ambiance « *Trust Chernoby*¹⁸ » qui règne, alors la confiance sera brisée entre les citoyens et les entreprises ou les gouvernements. En conséquence, les citoyens pourraient ne plus être disposés à partager leurs données personnelles et seraient moins enclin à croire aux informations fournies par les gouvernements ou d'autres organisations. « *Il serait intéressant de voir jusqu'à quel point nous pouvons supporter les intrusions dans notre vie privée (santé, finances, informations personnelles)* »¹⁹

De manière générale, nos échanges sur la problématique de la confiance ont porté sur deux optiques : la confiance en ce qui concerne la gestion et le contrôle des données, et la confiance en ce qui concerne la pertinence des données.

A qui faire confiance ?

A Madrid, les participants ont constaté que la familiarité croissante des usagers avec les technologies et l'assurance gagnée dans leur capacité à accéder aux données sont en train de redéfinir les paramètres de la confiance. Par exemple, au lieu de faire appel à un expert, nous utilisons des données issues de plateformes collaboratives pour prendre des décisions de nature variée, allant de l'endroit où nous mangeons à des conseils d'ordre médical. De même, la popularité des réseaux sociaux a fait évoluer la manière dont nous accordons notre confiance.

« *Nous avons observé une transition du pouvoir des gouvernements vers les entreprises et maintenant nous observons un passage du pouvoir des mains des entreprises vers celles du peuple* ». Lors de nos échanges, il s'est certainement dégagé le sentiment que la confiance s'est fortement dirigée vers les groupes ou communautés de pairs, au détriment des institutions traditionnelles ou de statut supposé supérieur. Beaucoup de citoyens qui cherchent des alternatives fiables aux sources traditionnelles d'actualités et d'informations reconnues, ont recours aux médias sociaux et à un réseau « d'amis » sur Internet ou à des communautés de partage d'opinions pour trouver ce qu'ils estiment être la vérité.

Les différences culturelles sont également importantes lorsque l'on veut déterminer à qui accorder sa confiance. A Abidjan, le manque de confiance dans les intentions des organisations occidentales pousse à plébisciter la Communauté Economique des États de l'Afrique de l'Ouest (CEDEAO). Cela va dans le sens d'une confiance accrue en la capacité technologique des talents africains. « *A mesure que les préoccupations autour de la sécurité augmentent et que la confiance des développeurs africains se raffermi, les Ivoiriens souhaitent contrôler les données qu'ils produisent et devenir moins dépendants vis-à-vis des pays occidentaux* ».

« Les méga données et l'IA ouvrent grand la voie aux discriminations intentionnelles et non intentionnelles »

Atelier de Bangalore

(Im)pertinence des données

Beaucoup de participants aux ateliers ont avoué avoir le sentiment que les données libres accessibles au public inspirent moins confiance de nos jours car il est de plus en plus difficile de vérifier l'exactitude des informations qui nous sont présentées. Cela est aussi valable pour les données des gouvernements que pour les informations diffusées dans les média sociaux. Les participants ont reconnu qu'il est particulièrement difficile de déceler la vérité dans les média sociaux dans la mesure où il est souvent difficile d'identifier la source originale d'un billet ou d'un article d'actualité. Compte tenu de ce constat, des participants de Hong Kong ont recommandé aux citoyens de s'attacher davantage à comprendre et distinguer ce qui est factuel de ce qui ne l'est pas : « *Il faut que les gens comprennent que les données ne correspondent pas à une vérité, il s'agit d'informations qui sont présentées d'une façon ou d'une autre et nous devons apprendre à déceler les données biaisées sinon nous perdrons notre liberté de choix* ». Si des précautions ne sont pas prises afin que les citoyens soient suffisamment outillés pour distinguer la réalité de la fiction, il pourrait y avoir une crise de la confiance susceptible d'aboutir à des troubles voire à l'agitation sociale. « *Il y a une boucle de rétroaction, c'est-à-dire que les fausses nouvelles sapent la confiance et le manque de confiance engendre des fausses nouvelles. Les retombées sont négatives. Il faut préserver la confiance pour garantir une société sûre et exemplaire* ».

Le cercle vicieux qui s'établit entre le manque de confiance dans les gouvernements et la capacité des gouvernements à fournir des données fiables a été évoqué à Washington DC lors d'une discussion sur le fait que les gens publient sciemment des fausses nouvelles. L'exemple donné concerne des requêtes dans les données de recensement des Etats-Unis qui montrent que 20% des informations fournies étaient fausses parce que les citoyens ne font pas confiance au gouvernement et craignent que les informations exactes soient utilisées à leur encontre.

Un participant a fait remarquer que « *le faible niveau de confiance aux gouvernements, institutions et grandes entreprises de technologies dévalue les données dans la mesure où il remet en question la fiabilité des données. Les citoyens choisissent de ne pas partager des informations exactes* ».

Nous avons entendu le même son de cloche à Lagos où les participants nous ont déclaré que le degré de méfiance à l'égard du gouvernement central et du secteur privé est tel que les citoyens ne veulent point partager leurs données personnelles, ce qui rend les statistiques nationales si peu fiables qu'elles en deviennent inutiles à une analyse pertinente. Une des solutions proposées est de mettre en place une réglementation rigoureuse autour de la collecte et de l'utilisation des données publiques. « *Des politiques améliorées sur les données permettront de rétablir la confiance au gouvernement – à l'heure actuelle, la confiance est limitée parce que la redevabilité l'est aussi* »,²⁰

Des préoccupations ont été également exprimées au sujet du recours croissant à l'IA, surtout en matière de services publics. Les participants se soucient surtout de la capacité des programmeurs à exclure les données biaisées lors de la sélection des données utilisées, afin d'entraîner les dispositifs d'IA à les identifier rapidement lorsqu'il y en a. A Bangalore, par exemple, on estime que « *les méga données et l'IA ouvrent grand la voie aux discriminations intentionnelles et non intentionnelles* ». A Johannesburg, on estime que si les préoccupations liées aux biais dans les données augmentent, les produits et les services réalisés à partir de ces données n'inspireront plus confiance et le public ne sera certainement pas enclin à s'impliquer dans le processus en partageant ses données personnelles. Pour remédier à ce problème, il a été suggéré de « *créer un label de « dignité des données » avec des indicateurs mesurables, qui permettrait de superviser l'utilisation des données pour l'intérêt général tout en préservant la dignité des personnes (notamment en garantissant un niveau décent de vie privée et de confidentialité)* ».

Utilisation irresponsable des données

Les principaux acteurs de l'économie des données, les entreprises de technologie comme les gouvernements, ont été fortement critiqués lors de nos ateliers. A plusieurs reprises, nous avons entendu des réflexions sur la manière dont beaucoup d'entreprises de technologies, surtout celles qui proposent des plateformes de média sociaux, exploitent les données que nous partageons, en négligeant la vie privée et la sécurité des personnes. Peu de participants estiment que des leçons ont été réellement tirées du scandale de Cambridge Analytica et qu'à l'avenir nous pourrions faire confiance aux organisations qui contrôlent nos données personnelles. A Hong Kong, on constate que « mieux on comprendra le fonctionnement des grandes entreprises de technologies, plus il y aura de réprobation vis-à-vis de leurs modèles économiques ». A Bogota, on dit que « les gens continueront à être manipulés ».²¹

Par ailleurs, il y a clairement une frustration par rapport à ce qui est décrit comme une absence de leadership dans le secteur des technologies. A Londres, on a l'impression que c'est cela qui est réellement à l'origine de cette crise de confiance : « ce n'est pas tant une crise de confiance qu'une crise de leadership. Nous ne pouvons pas imposer la confiance en usant d'une autorité descendante. »²² La conversation s'est poursuivie sur l'importance d'adopter des comportements qui inspirent confiance et de mettre en place des dispositifs pour les garantir, « c'est une question de vérification et non de confiance ». Des opinions similaires ont été exprimées à Singapour et à Toronto.

Parfois, nous avons entendu des échanges autour de la sécurité nationale et de la nécessité de protéger les citoyens contre les acteurs malveillants. Ce sentiment de méfiance peut se répandre, peut-être avec des effets insoupçonnés. Par exemple, des participants de Singapour et d'Afrique du Sud ont déclaré qu'une des raisons pour lesquels les données relatives à

l'ADN ne sont pas partagées avec les Etats-Unis, est la sécurité nationale.

Quelques alternatives ont été identifiées, ces dernières pourraient aider à restaurer la confiance dans l'utilisation des données et dans les organisations qui gèrent des données. Ci-dessous, sont présentées quelques pistes :

- **Une réelle transparence :** à Dakar, on est d'avis que les révélations publiques sur les défaillances liées aux données et à l'exploitation des données personnelles par certaines entreprises de technologie ont prouvé que ces dernières sont incapables de s'auto-réguler. En conséquence, « *les entreprises de technologie seront obligées de faire preuve de transparence au sujet des données qu'elles collectent et de l'usage qu'elles en font. Cette nécessité sera suscitée par la pression croissante des consommateurs et par un environnement concurrentiel dans lequel la transparence et l'utilisation responsable des données sera un élément de différenciation* ». Les autres participants étaient du même avis. De Madrid à Hong Kong, de Singapour à Bogota, on pense que les entreprises de média sociaux devraient être plus proactives dans les efforts de discernement entre les informations avérées et les informations inexactes publiées sur leurs plateformes. De nombreux exemples ont été évoqués sur la manière dont la désinformation, y compris les biais sciemment introduits dans la donne électorale ainsi que les arnaques en ligne, influence les comportements, autant dans les pays riches que dans les pays pauvres.

La transparence totale n'est toutefois pas la panacée. A Londres, on a constaté que « *la transparence totale n'est absolument nécessaire que s'il n'y a aucune confiance. Il n'y a certainement pas besoin de partager des montagnes d'informations pour garantir un comportement éthique* ». A Francfort, les participants étaient d'avis que lorsque les particuliers prendraient conscience de la quantité de données personnelles les concernant, qui est accumulée et vendue, l'exigence d'une réelle transparence s'affirmera et il y aura alors une réglementation : « *s'il n'y a pas de transparence, les services en ligne ne seront plus admis.* »

- **Une réelle redevabilité** : il y a eu un consensus général sur le fait qu'une réelle redevabilité permettrait de renforcer la confiance, mais il y a eu des divergences d'opinion sur la manière de matérialiser cette redevabilité. S'assurer que les données publiques sont pertinentes a été un aspect important pour les participants aux ateliers de Washington DC, Tokyo, Singapour, Lagos et Copenhague. A Lagos, on estime que le seul moyen d'y arriver est d'envisager une collaboration multilatérale ouverte. « *Améliorer les politiques relatives aux données convenues par plusieurs parties permettra d'améliorer la confiance aux gouvernements, actuellement, le niveau de confiance en l'utilisation des données par les gouvernements est faible parce que le niveau de redevabilité l'est également* ». Une opinion évoquée au Danemark est que la confiance accordée aux institutions publiques serait plus grande « *s'il y'avait un pendant de l'OTAN pour les données ou une organisation au sein des Nations Unies, qui pourrait élaborer et superviser des lignes directrices, des codes d'éthique et de déontologie et des normes communes* ».

- **Des solutions techniques** : Certains des participants à nos ateliers ont suggéré que les nouvelles technologies telles que la blockchain puissent faire partie de la solution, en offrant des garde-fous efficaces contre les abus, par conséquent elles pourraient aider à renforcer la confiance. À Tokyo, on estime que : « *Les nouvelles technologies permettent de ventiler les responsabilités et de renforcer la confiance dans le système.* » Le fait de créer et de répartir un stock d'informations immuables, qui ne pourra jamais être supprimé ni modifié, assurerait un certain degré de transparence. Les données pourraient être enregistrées et réparties de manière plus transparente et ne pourraient être modifiées sans que ces changements apparaissent dans la plupart des autres stocks préservés auprès d'autres usagers. Les créateurs de contenus pourraient utiliser des canaux de répartition qui garantissent des contenus protégés contre des modifications extérieures, le filtrage ou le blocage par des tiers.

En outre, des canaux de répartition dotés de la blockchain rendraient la censure et la restriction des accès aux informations plus difficiles.

Améliorer les politiques relatives aux données convenues par plusieurs parties permettra d'améliorer la confiance aux gouvernements, actuellement, le niveau de confiance en l'utilisation des données par les gouvernements est faible parce que le niveau de redevabilité l'est également »

Atelier de Lagos

- **L'influence des consommateurs** : A Bangalore, on pense que le processus de réglementation a mis trop de temps avant de commencer à contrôler le comportement de certaines entreprises de technologies en matière d'exploitation des données. Ainsi, les participants ont estimé que l'opinion publique est plus à même de provoquer le changement avant toute réaction statutaire à la crise de confiance. « La réaction du public au comportement répréhensible se manifeste avant même que la justice ne légifère ou que la réglementation appropriée ne soit élaborée, et en ce qui concerne les données personnelles « *une compréhension de plus en plus précise par le public des dangers potentiels pour les personnes va entraîner une volonté plus ferme d'élargir ses droits et d'exiger plus de redevabilité* ». Les participants de Copenhague se sont appuyés sur cette hypothèse pour soutenir l'idée d'impliquer le citoyen dans la supervision de l'utilisation et de l'exactitude des données en vue de contribuer à renforcer la confiance. « *Y aurait il un rôle pour un dispositif tel que Wikipédia dans cette approche ?* »²³
- **La culture numérique** : De nombreux participants ont estimé qu'une meilleure éducation du public à l'utilisation des données personnelles contribuerait à renforcer la confiance du public aux données libres pour le service public et permettrait de doter les citoyens de suffisamment de compétences pour identifier les contextes où la confiance serait mal placée. A Santiago, on espère que cette sensibilisation combinée à des amendes lourdes pousseraient les entreprises à modérer leur comportement. « *Lorsque le public s'implique davantage, la redevabilité devient « horizontale » plutôt que verticale.* » A mesure que les consciences se réveillent, la possibilité de « surveiller le surveillant » et « d'opérer une analyse critique » contraindra les grandes organisations de tous les secteurs à modérer leurs actions et d'agir plutôt en fonction de ce qui est considéré comme acceptable, en ligne et ailleurs.
- **Les décalages générationnels** : il a été reconnu que la confiance en la technologie et aux données qu'elle produit dépend des attentes de chaque génération. Certains estiment notamment que les Millennials s'y connaissent beaucoup mieux en sécurité et confidentialité des données que les générations antérieures et sont moins susceptibles de s'en inquiéter. « *La génération X est la dernière génération pré-numérique, la génération suivante aura une meilleure compréhension de l'importance de la gestion et du contrôle* ». ²⁴ Toutefois certains craignent que la prochaine génération soit tellement dépendante des technologies « *qu'elle prendra pour argent comptant toutes les données qui lui seront présentées sans remettre en question leur véracité* ». ²⁵ Mais nous avons également entendu dire l'inverse : « *d'ici dix ans, les choses seront plus équilibrées. Nous sommes actuellement dans une phase de transition, une situation en constante évolution, les gens étaient terrifiés par la voiture, au tout début, à son invention* ».

Perspectives

A travers les discussions des ateliers, on constate clairement que nous sommes à la croisée des chemins. Les innovations technologiques, portées essentiellement par une poignée d'organisations mastodontes de la technologie, certaines d'entre elles pourtant peu connues du public, sont en train de transformer de manière fondamentale tous les secteurs de la société et d'influencer la vie de millions de personnes. Souvent ces changements sont positifs mais pas toujours. La dynamique en est à un point où beaucoup de citoyens ont le sentiment qu'ils subissent ces changements, de gré ou de force. Dans ce contexte, la question de la confiance prend tout son sens.

Etablir la confiance n'est pas un défi unique. C'est un enjeu multidimensionnel. Les systèmes basés sur les données dépendent de la pertinence des données qui les alimentent. Ils ne fonctionnent que si un nombre suffisant de personnes leur fait confiance au point de partager des données exactes avec eux et si ces personnes sont certaines qu'en retour, elles obtiendront des informations exactes. Lorsqu'il y a des incidents qui révèlent des irrégularités, de la corruption, de l'incompétence, la confiance est ébranlée et les personnes doutent de l'intérêt de leur contribution. Le risque est que de plus en plus de gens se mettent en retrait ou fournissent des données inexactes. Si une masse critique d'individus adopte cette attitude, alors ces systèmes échoueront.

Cet aspect de la confiance est essentiellement technique, cela ramène à l'opportunité de créer des systèmes adaptés aux objectifs recherchés. Une autre dimension plus complexe et plus controversée de la confiance porte sur les motivations et les intentions des différentes parties prenantes. Le défi pour ces organisations et institutions en charge de la transition vers une économie et une société des données est de prouver qu'elles sont dignes de confiance.

Être digne de confiance, ce n'est pas la même chose qu'avoir la confiance des autres. Cela signifie que les organisations acceptent de rendre des comptes, de prouver que leurs intentions sont bienveillantes, que l'éthique n'est pas un simple sujet de relations publiques mais plutôt un facteur d'influence qui pèse sur les décisions à prendre et leur mise en œuvre. Augmenter la transparence aide à renforcer cette confiance, mais ce n'est pas la seule réponse, surtout lorsque la confiance dans les entreprises est au plus bas. Un cadre réglementaire robuste, élaboré à l'échelle régionale ou internationale serait très utile pour établir des normes, des procédures de vérification et des contrepoids pour réduire le pouvoir des grandes entreprises. La plupart des personnes avec lesquelles nous avons échangé estiment que ces entreprises n'ont pas une stature responsable. Les citoyens ont aussi un rôle à jouer, en prenant conscience de leurs droits et responsabilités dans leurs activités en ligne. Si nous réussissons à créer un système durable, robuste et fiable alors la prochaine génération pourra tirer le meilleur profit de sa puissance.

3.6 Tous sur la même longueur d'onde



Les citoyens ne comprennent pas tout à fait la source de la valeur des données ni les formes qu'elle peut prendre. Une étape clé pour la compréhension de la valeur des données serait la référence à un langage commun, avec une définition claire des termes.

Le débat qui prend de l'ampleur dans les médias et dans la politique sur les données, leur propriété, leur utilisation et leur valeur dénote un manque de consensus autour de la définition de concepts fondamentaux. Cette situation sape les efforts entrepris par les gouvernements, les entreprises et la société civile pour créer un cadre harmonieux et développer des systèmes robustes. Il y a une volonté croissante d'établir une terminologie commune et accessible afin de promouvoir une compréhension commune des enjeux clés et des alternatives disponibles pour faire face à ces enjeux. Cette absence de terrain d'entente est un frein majeur aux initiatives naissantes en matière de coopération et de réglementation. Sans ce référentiel commun, les chances d'obtenir un consensus ou de prendre une décision quant à la marche à suivre sont bien minces voire inexistantes. Conscients de cette situation, les participants à nos ateliers étaient largement favorables à l'idée de consacrer du temps et de l'énergie à la définition consensuelle des termes relatifs à l'utilisation et à la valeur des données.

Problèmes et dilemmes :

- Est-il possible de créer un langage commun à l'échelle internationale, adopté par les acteurs clés qui utiliseraient tous les mêmes termes pour décrire ce qui est en train de se passer au sujet des données ?
- Est-il possible de convenir d'une compréhension commune des problématiques et des solutions possibles, même s'il y a des points de désaccord en ce qui concerne le degré d'importance de ces problématiques ou sur la conduite idéale à tenir ?
- S'il n'est pas possible de créer un terrain d'entente, comment faire évoluer le débat et la compréhension des nombreuses problématiques soulevées par l'émergence d'une économie axée sur les données ?
- S'il est possible de créer ce terrain d'entente, quel serait le meilleur moyen de le faire et qui devrait orienter ou assumer la responsabilité de cette démarche ?

Ce que nous ont dit les participants

Au-delà des diverses métaphores inspirées par la notion de données (assimilée à la lumière du soleil à Tokyo, au tableau périodique des éléments à Singapour, à la religion en Espagne) une infinité de points de vue relatifs à la définition des problématiques clés, telles que le consentement éclairé ou la culture numérique, ont été exprimées, partout dans le monde. Lors de la plupart des ateliers, l'absence d'accord sur des termes communs précis pour désigner des éléments clés du monde numérique a été souligné et fortement déploré. Il ne s'agit pas seulement d'une préoccupation globale trans-sociétale et trans-économique mais aussi un phénomène qui peut s'observer au sein d'un même secteur d'activité ou d'une même communauté. Lors de nos 12 sessions d'échange sur une prospective précédente qui est le *Futur des données patients*, réalisée en 2017/18, le faible niveau de compréhension des différences entre données agrégées et données anonymisées, propriété et contrôle, apprentissage machine et intelligence artificielle (IA) ou encore entre intelligence artificielle et intelligence générale artificielle (IGA), a été constaté. Il en est de même de la différence entre données biaisées et qualité des données. D'autres discussions sur les données relatives au secteur de l'automobile au Royaume-Uni, aux Etats-Unis et en Allemagne présentaient les mêmes symptômes de divergences interprétatives.

Lors de nos ateliers, de telles situations se sont présentées de manière récurrente à différents endroits. Les définitions employées pour la souveraineté des données et la localisation des données étaient différentes, de même que celles employées pour faire référence aux taxes sur les données et à la fiscalité numérique ou encore pour désigner la connaissance des données et la culture du numérique, et cela même chez les régulateurs. De nombreux participants sont conscients de cet écueil et l'idée d'élaborer une terminologie consensuelle, mondiale et trans-sectorielle sur les données a remporté une forte adhésion dans plusieurs localités,

notamment Jakarta, Bangkok, Dakar, Mexico City, Toronto, et même Washington DC. Les participants de Singapour ont formulé une opinion relativement populaire lorsqu'ils ont suggéré que la logique d'une telle démarche de convergence serait d'établir « *une stratégie gouvernementale mieux articulée pour encourager les initiatives de nature communautaires qui comportent des bénéfices collectifs pour l'ensemble des citoyens* ».

Le choix du langage n'est pas qu'une affaire politique. C'est aussi une question de perception. Sans langage commun sur l'utilisation des données, il est difficile d'imaginer la possibilité d'inculquer une culture numérique aux populations. Ces préoccupations ont suscité pas moins de dix-neuf (19) discussions distinctes sur la notion de culture numérique durant le programme. Indépendamment de la situation géographique, de l'âge, de l'emploi ou de la méthode, le message est clair : « *la fracture entre les personnes ayant une culture de la technologie et celles qui n'en ont pas représentera un grand défi et aura de graves conséquences si elle n'est pas comblée.* »²⁶ Il n'est pas difficile d'en deviner les raisons. Alors que le rythme de la connectivité s'accélère et que les gouvernements s'appuient de plus en plus sur les données pour interagir avec les citoyens, gérer les cyberrisques, s'assurer que les individus disposent des compétences requises pour collaborer avec l'Etat, former des ressources humaines capables d'intégrer l'économie numérique, constituent tous des actions prioritaires. L'incapacité de résoudre la problématique de la culture numérique aura des conséquences qui au-delà de la fracture numérique, touchera l'emploi car il y aura pénurie de main d'œuvre, et affectera la création de valeur à partir des données. Et puis, comment les gouvernements pourront-ils mettre en œuvre un programme d'éducation au numérique si cette nébuleuse autour de la terminologie des données persiste ?

Contexte

Notre objectif ? Mieux comprendre la façon dont les perspectives et les priorités diffèrent à travers le monde, et utiliser les diverses voix et points de vue pour aider les gouvernements, les organisations, et les individus à mieux comprendre ce qu'ils doivent faire pour réaliser le plein potentiel des données.

Notre objectif ? Mieux comprendre la façon dont les perspectives et les priorités diffèrent à travers le monde, et utiliser les diverses voix et points de vue pour aider les gouvernements, les organisations, et les individus à mieux comprendre ce qu'ils doivent faire pour réaliser le plein potentiel des données.

À partir des multiples discussions, 6 thèmes généraux ont été identifiés ainsi que 12 changements futurs connexes, tels que résumés dans le diagramme ci-dessous.



Sur Future Agenda

A propos de Future Agenda Future Agenda est un Think Tank libre et un cabinet de conseil. Nous aidons les organisations de toutes tailles à explorer les opportunités émergentes, à identifier les nouvelles plateformes de croissance et à amorcer des innovations qui font la différence. Fondée en 2010, Future Agenda a initié une approche de prospective libre en créant un forum où se rejoignent les dirigeants experts des entreprises de tous les domaines, de la sphère académique, du secteur public non financier et de l'Etat. Le but de cette émulation est de rapprocher les éclairés des influents, de mettre les hypothèses à l'épreuve et d'ouvrir une fenêtre sur l'avenir afin de susciter un impact positif et durable.

Pour plus d'information et pour consulter toutes nos études prospectives, visitez notre site et contactez-nous www.futureagenda.org

Contact:

Dr Tim Jones – Programme Director,
tim.jones@futureagenda.org

Caroline Dewing – Co-Founder,
caroline.dewing@futureagenda.org

Texte © Future Agenda
Images © istockimages.com
Version anglaise publiée pour la première fois en novembre 2019 par:
Future Agenda Limited
84 Brook Street
London
W1K 5EH

Pour plus d'informations: www.deliveringvaluethroughdata.org