ILLUSTRATION : ISTOCK/DANLEAP

Bâtissons ensemble

UNE MEILLEURE ÉCONOMIE DES DONNÉES

Notre empreinte numérique génère une valeur considérable, mais une trop grande partie finit dans les silos des géants de la technologie

Yan Carrière-Swallow et Vikram Haksar

Jamais n'a-t-on enregistré autant de données sur l'humanité. Les montres intelligentes captent notre pouls en temps réel pour qu'une intelligence artificielle (IA) distante cogite sur les risques de maladie cardiaque. Le Bluetooth et le GPS nous suivent et savent si certains d'entre nous font leurs courses dans des épiceries fines et s'attardent au rayon des bonbons. Nos « likes » et les heures que nous passons sur les réseaux sociaux sont collectés pour prédire notre risque de crédit. Nos recherches sur les sites de vente en ligne sont traitées par des processeurs de langage naturel pour générer des publicités précisément ciblées dont les liens invisibles remodèlent subtilement nos goûts et nos habitudes.

La production et la collecte de données sur les individus tiennent une place importante dans l'économie moderne. Et elles produisent une valeur considérable. Les mégadonnées et les analyses d'IA sont utilisées dans la recherche et le développement pour améliorer la productivité. Elles peuvent renforcer l'inclusion financière. Pendant la pandémie, les données sur les mouvements en temps réel de populations tout entières ont informé les dirigeants sur les répercussions des confinements. Des applications de traçage ont alerté les individus qui pouvaient s'être trouvés à proximité de personnes infectées par la COVID-19.

Mais au moment même où les données nous aidaient à suivre l'évolution de la COVID-19, à nous y adapter et à prendre des mesures d'endiguement, la pandémie a mis en lumière deux problèmes fondamentaux relatifs à leur circulation dans l'économie mondiale (Carrière-Swallow et Haksar, 2019). D'une part, l'économie des données est opaque et ne respecte pas toujours la vie privée des individus ; d'autre part, les données sont conservées dans des silos privés, ce qui diminue leur valeur de bien public pour la société.

Mais d'abord, à qui appartiennent les données ?

Dès lors que le GPS, les micros et les accéléromètres intégrés aux appareils intelligents qui se trouvent dans toutes les poches, sur toutes les tables de nuit et dans toutes les cuisines commencent à surveiller notre comportement et notre environnement, où vont les données ? Dans la plupart des pays, elles sont collectées, traitées et revendues par ceux qui peuvent s'en emparer. Le consentement de l'utilisateur est trop souvent donné en cochant une case au-dessous d'un long texte juridique en petits caractères — ce qui n'est pas le meilleur moyen d'obtenir un véritable consentement éclairé. L'analyse basée sur des données aussi précises est une porte d'accès à l'exercice d'une influence sur les comportements et possède une valeur commerciale considérable. Certes, ce n'est pas à sens unique : les consommateurs obtiennent de multiples fonctionnalités fondées sur les données pour un coût financier direct nul. Mais est-ce suffisant ?

La plupart des transactions impliquant des données personnelles se font à l'insu des utilisateurs, qui n'ont probablement même pas conscience qu'elles ont eu lieu et, *a fortiori*, qu'ils ont donné leur autorisation. Cela engendre ce que les économistes appellent une externalité :

Pourquoi les individus sont-ils prêts à céder leurs données de localisation en contrepartie d'un bulletin météo, mais non à les partager pour protéger leur santé ?

le coût de la perte de vie privée n'est pas parfaitement pris en compte lorsqu'un échange de données a lieu. La conséquence est que l'opacité du marché conduit sans doute à collecter *trop de données* et à partager une *trop faible fraction de leur valeur* avec les individus.

En autorisant l'installation d'une application de météorologie et la détection automatique de la ville dans laquelle ils se trouvent, les individus risquent de permettre involontairement à un concepteur d'applications de suivre en continu leur localisation exacte. Les utilisateurs qui s'abonnent à un service de prévisions météorologiques avec une interface conviviale acceptent de partager leurs données de localisation, croyant qu'elles servent uniquement à activer les fonctionnalités de l'application. Mais ce qu'elles fournissent en réalité, ce sont des traînées de données sur leurs habitudes quotidiennes, leurs itinéraires de déplacement et leurs activités sociales. Le météorologiste n'améliorera peut-être jamais ses capacités à prévoir la pluie, mais il pourrait obtenir une prévision de la solvabilité de l'utilisateur plus fiable que les scores établis par les bureaux de crédit traditionnels (Berg *et al.*, 2020).

Paradoxes de la vie privée

Tenons-nous à notre vie privée ou non ? Des chercheurs ont documenté ce que l'on appelle le « paradoxe de la vie privée ». Lors des enquêtes, les personnes invitées à évaluer leur vie privée lui accordent souvent une très forte priorité. Cependant, dans leur quotidien, ces mêmes personnes sont souvent prêtes à donner des données personnelles très sensibles moyennant une faible contrepartie.

Ce paradoxe aurait dû être une bonne nouvelle pour les applications de traçage des contacts, dont l'efficacité dépend du nombre d'utilisateurs (Cantú *et al.*, 2020). Malheureusement, dans de nombreux pays où l'usage de ces outils est facultatif, leur adoption a été très lente. Pourquoi les individus sont-ils prêts à céder leurs données de localisation en contrepartie d'un bulletin météo, mais non à les partager pour protéger leur santé tout en aidant à combattre une pandémie mondiale qui a fait plus de 2 millions de victimes ? Une première explication pourrait être que les autorités de santé publique — contrairement aux concepteurs d'applications de météorologie — ont conçu leurs applications de traçage de telle manière qu'elles annoncent en toute transparence comment les données seront collectées et utilisées, et cela suscite des préoccupations en matière de protection de la vie privée. Une autre explication est qu'autoriser les pouvoirs publics à combiner des données de localisation et des données sur un diagnostic médical peut être jugé particulièrement sensible. Après tout, la connaissance préalable de l'état de santé d'une personne pourrait amener à l'exclure ultérieurement des marchés de l'assurance ou ouvrir la porte à d'autres formes de stigmatisation ou de discrimination.

Comment faire un usage responsable des données ?

Les données produites par nos dispositifs intelligents sont essentiellement un bien privé détenu par les grands groupes numériques qui dominent les réseaux sociaux, la vente en ligne et les outils de recherche. Compte tenu de la valeur de ces données, il n'est pas surprenant que ces entreprises tendent à les garder pour elles (Jones et Tonetti, 2020). Sachant que des données plus nombreuses permettent de meilleures analyses, qui entraînent à leur tour plus d'usage, plus de données et plus de profits, ces impressionnants trésors de guerre fortifient leurs réseaux de plateformes et peuvent asphyxier la concurrence.

Ce modèle de la propriété des données acquise à celui qui les trouve tend à engendrer une collecte excessive de données, mais les données sont en outre *insuffisamment exploitées* là où elles pourraient être le plus utiles, car elles sont conservées dans des silos privés alors que les besoins publics ne sont pas couverts. Le partage de données peut soutenir le développement de nouvelles technologies, y compris dans le domaine des sciences de la vie. Pensons aux bénéfices qu'une montée en puissance de l'analyse des mégadonnées pourrait apporter aux recherches épidémiologiques. Un chercheur qui analyse l'expérience des patients dans leur pays peut être un bon début, mais sans commune mesure avec les travaux de nombreux chercheurs qui travaillent ensemble et puisent dans l'expérience de patients bien plus nombreux tout autour du monde — la clé du succès de plusieurs collaborations internationales.

Comment fortifier le caractère de bien public des données ? Il faut concilier les intérêts commerciaux et les incitations à l'innovation avec la nécessité de renforcer la confiance du public en protégeant la vie privée et l'intégrité. Une clarification des règles de l'économie des données est un bon point de départ. Des progrès considérables ont résulté, par exemple, de la mise en œuvre en 2018 en Europe du règlement général sur la protection des données (RGPD), qui a précisé un certain nombre de droits

et d'obligations gouvernant l'économie des données. Les résidents de l'Union européenne ont désormais le droit d'accéder à leurs données et d'en limiter le traitement, et les atteintes à ces droits sont sanctionnées par des amendes de plus en plus lourdes. Mais bien que les chercheurs commencent à constater l'effet du RGPD sur l'économie numérique, des préoccupations persistent quant à la concrétisation de ces droits et aux moyens d'empêcher qu'ils se limitent à une case à cocher.

Les individus devraient avoir davantage de pouvoir sur leurs données. Il pourrait être intéressant d'envisager la création de services publics des données — peut-être comme un prolongement des registres du crédit — qui pourraient concilier les besoins publics et les droits individuels. Imaginons une autorité indépendante chargée de collecter et d'anonymiser certaines catégories de données individuelles, qui pourraient ensuite être mises à disposition pour l'analyse sous réserve du consentement des parties intéressées. Ces données pourraient être utilisées, par exemple, pour le traçage des contacts en temps de pandémie, pour de meilleures prévisions macroéconomiques ou encore pour la lutte contre le blanchiment de capitaux et le financement du terrorisme.

Les politiques publiques peuvent également aider les consommateurs à ne pas être pris en otage par des écosystèmes individuels, ce qui contribuerait à la contestabilité des marchés et à la concurrence. Les propositions de règlement sur les marchés numériques et sur les services numériques de l'Union européenne publiées fin 2020 présentent de nombreuses caractéristiques inédites, parmi lesquelles des obligations d'interopérabilité avec les tiers faites aux contrôleurs d'accès que sont les géants numériques (y compris les réseaux sociaux et les places de marché en ligne) dans certaines situations et des efforts pour qu'il soit plus facile aux consommateurs de transférer leurs données sur d'autres plateformes.

Les politiques publiques ont aussi un rôle à jouer dans la protection des données contre les cyberattaques. Une entreprise n'internalise pas toutes les atteintes causées par une violation des données de ses clients à la confiance du public dans le système tout entier ; de ce fait, elle peut moins investir dans la cybersécurité que ce que commanderait l'intérêt général. Cette préoccupation a une résonance particulière dans le système financier, où la confiance du public est cruciale. C'est pourquoi une infrastructure sûre, des normes de cybersécurité et une réglementation sont les piliers fondamentaux des politiques bancaires ouvertes que de nombreux pays ont adoptées pour faciliter l'interopérabilité concernant des données financières sensibles.

Une approche mondiale

De nombreux pays ont commencé à élaborer des politiques visant à instaurer une économie des données plus claire, plus juste et plus dynamique. Mais leurs approches sont différentes, ce qui engendre un risque de fragmentation accrue de l'économie numérique mondiale. Ces risques se posent dans de nombreux secteurs faisant un usage intensif des données, du commerce de marchandises aux flux financiers internationaux. Dans le contexte de la pandémie, les différences de normes en matière de protection de la vie privée compliquent la collaboration internationale dans le cadre d'activités de recherche médicale cruciales — ce qui était vrai même avant la pandémie — en raison de la difficulté à partager les résultats d'essais biomédicaux (Peloquin *et al.*, 2020).

La coordination mondiale est toujours difficile, surtout dans un domaine aussi complexe que la politique des données, où se côtoient une multitude d'intérêts et d'autorités de réglementation, même à l'échelle d'un pays, et à plus forte raison à l'international. La gestion des répercussions de la pandémie a offert une nouvelle occasion de poser des questions difficiles sur la nécessité de principes communs minimaux à l'échelle mondiale pour le partage international des données tout en protégeant les droits individuels et les prérogatives en matière de sécurité nationale.

La conjoncture actuelle offre aussi l'opportunité d'étudier des solutions techniques innovantes. La relance des voyages internationaux pourrait éventuellement être facilitée par un registre mondial des vaccins. Celui-ci pourrait exploiter les carnets de vaccination internationaux que l'on connaît, mais demanderait d'élaborer des normes et de concevoir un système interexploitable de gestion des données qui permet de communiquer et de vérifier le statut vaccinal des individus — peut-être lié à une identité numérique — et de conclure des accords relatifs à la protection de la vie privée et aux barrières à l'accès pour d'autres fins.

Une coopération internationale est hautement souhaitable pour que les bénéfices de l'économie mondiale des données puissent construire une société mondiale plus résiliente, en meilleure santé et plus juste. Pour trouver la bonne voie, nous pouvons commencer par poser les bonnes questions. FD

YAN CARRIÈRE-SWALLOW est économiste au département de la stratégie, des politiques et de l'évaluation du FMI. **VIKRAM HAKSAR** est directeur adjoint au département des marchés monétaires et de capitaux du FMI.

Bibliographie :

Berg, Tobias, Valentin Burg, Ana Gombovic, and Manju Puri. 2020. "On the Rise of FinTechs: Credit Scoring Using Digital Footprints." *Review of Financial Studies* 33:2845–97.

Cantú, Carlos, Gong Cheng, Sebastian Doerr, Jon Frost, and Leonardo Gambacorta. 2020. "On Health and Privacy: Technology to Combat the Pandemic." *BIS Bulletin* 17 (May).

Carrière-Swallow, Yan, and Vikram Haksar. 2019. "The Economics and Implications of Data: An Integrated Perspective." Departmental Paper 19/16, International Monetary Fund, Washington, DC.

Jones, Charles I., and Christopher Tonetti. 2020. "Nonrivalry and the Economics of Data." *American Economic Review* 110 (9): 2819–58.

Peloquin, David, Michael DiMaio, Barbara Bierer, and Mark Barnes. 2020. "Disruptive and Avoidable: GDPR Challenges to Secondary Research Uses of Data." *European Journal of Human Genetics* 28:697–705.