



IDÉE 8

L'IA COMPROMET ENCORE PLUS LA VIE PRIVÉE

À mesure que les appareils dotés d'IA collectent davantage de données en ligne et dans la vie réelle, les efforts visant à transformer les données en nouvelles sources de revenus pourraient se heurter à des attitudes et des appareils plus soucieux de la protection de la vie privée. Un nouveau statu quo pourrait voir le jour, très différent de la manière opaque dont les utilisateurs échangent aujourd'hui leurs données contre des services gratuits.

AUJOURD'HUI

Les progrès de l'IA exacerbent les problèmes de protection de la vie privée liés à la technologie.

La plupart des Canadiennes et Canadiens ont pris l'habitude d'accéder à des services en ligne gratuits, tels que les sites de médias sociaux, les plateformes d'IA générative ou les applications mobiles. Dans de nombreux cas, ils consentent sans le savoir à ce que des entreprises collectent leurs données, les vendent à des tiers et utilisent l'IA pour les exploiter et en tirer des conclusions à leur sujet. Par exemple, Facebook utilise l'IA pour déduire le risque de suicide des utilisateurs sur la base de leurs publications sur les médias sociaux¹. Les progrès de l'IA permettent aux entreprises d'analyser une plus grande variété et une plus grande quantité de données, et de les transformer en flux de revenus d'une nouvelle manière.



Non seulement les environnements en ligne, mais aussi les espaces physiques deviennent moins privés.

Comme il est indiqué dans l'idée 7, les objets ménagers de tous les jours sont équipés de capteurs pour collecter des données; des toilettes aux brosses à dents en passant par les jouets. La réalité virtuelle (RV) et les jeux vidéo peuvent collecter des données sur le comportement des utilisateurs à la maison et utiliser l'IA pour déduire les émotions et les traits de personnalité². En dehors de la maison, des dispositifs tels que les lunettes intelligentes³ et les épingles d'intelligence artificielle⁴ soulèvent de nouvelles questions sur la protection de la vie privée en public. Les fragments d'ADN humain, connus sous le nom d'ADN environnemental, collectés dans les espaces publics à des fins telles que la surveillance des maladies, peuvent potentiellement être utilisés pour suivre les personnes, prélever illégalement des génomes et s'engager dans des formes cachées de surveillance et d'analyse génétiques^{5, 6}.

Les voitures intelligentes posent des problèmes particuliers en matière de respect de la vie privée.

En 2023, la Fondation Mozilla a enquêté sur 25 marques de voitures et a constaté que chacune d'entre elles collectait des données personnelles qui n'étaient pas nécessaires au fonctionnement du véhicule⁷. Généralement obtenues à partir d'appareils mobiles connectés aux voitures par l'intermédiaire d'applications, ces données peuvent inclure le revenu annuel d'une personne, son statut d'immigré, sa race, ses informations génétiques, son activité sexuelle, ses photos, son calendrier et sa liste de choses à faire. Sur les 25 marques, 22 utilisent ces données pour faire des déductions; par exemple, à partir de la localisation et des contacts téléphoniques, et 21 communiquent ou vendent des données. Treize recueillent des informations sur les conditions météorologiques, l'état de la chaussée, les panneaux de signalisation et les « autres environnements », qui peuvent inclure les passants⁸. Quatre-vingt-quinze pour cent des nouveaux véhicules seront des véhicules connectés d'ici à 2030⁹.





AVENIRS

L'Internet des objets devenant l'« IA des objets », les données pourraient prendre encore plus de valeur, ce qui inciterait à en extraire toujours plus. Il pourrait devenir possible de tirer des conclusions plus sophistiquées pour prédire le comportement humain, les mouvements ou identifier les personnes, comme il est indiqué dans l'idée 5.

Toutefois, le refus de la réglementation internationale pourrait remodeler le paysage de la protection de la vie privée. De plus en plus de juridictions adoptent et appliquent de nouvelles lois sur la confidentialité des données¹⁰, telles que l'American Privacy Rights Act¹¹ aux États-Unis. Cela pourrait modifier certains, voire de nombreux aspects du « capitalisme de surveillance »¹² en donnant aux utilisatrices et utilisateurs un plus grand contrôle sur leurs données. De futures réformes juridiques pourraient redéfinir les déductions en tant qu'informations personnelles¹³, ce qui rendrait plus difficile leur vente à des tiers.

Les nouvelles technologies pourraient également modifier l'équilibre en matière de protection de la vie privée.

L'informatique périphérique, qui fait référence aux réseaux ou aux appareils physiquement proches de l'utilisateur, pourrait améliorer la confidentialité et la sécurité des données¹⁴. Lorsque les données des utilisateurs sont stockées et traitées sur un appareil appartenant à l'utilisateur, il peut être plus difficile pour les entreprises de les collecter et de les vendre¹⁵. Cependant, l'informatique en périphérie peut également introduire de nouveaux risques, comme la reconnaissance faciale sur les appareils locaux et un accès potentiellement plus facile pour les acteurs malveillants¹⁶.



IMPLICATIONS

- Les **distinctions** telles que public par rapport au privé et en ligne par rapport à hors ligne pourraient devenir **de plus en plus floues**. Les maisons et autres espaces peuvent être perçus comme plus ou moins privés en fonction de l'utilisation des appareils. Les visiteurs des maisons et les passagers des voitures peuvent exiger **de nouveaux protocoles de consentement pour protéger leur vie privée**
 - Les données transmises à des tiers pourraient conduire à ce que **les informations sensibles soient communiquées** aux compagnies d'assurance¹⁷
 - Les écoles et les services de garde d'enfants pourraient utiliser les **protections de la vie privée comme un avantage concurrentiel** pour attirer les familles
 - La surveillance pourrait modifier les **pratiques de la police et des criminels**
 - › Certaines formes de **criminalité** pourraient s'enfoncer davantage dans la clandestinité et **devenir plus organisées** afin d'échapper à la détection
 - › Les nouvelles capacités technologiques pourraient créer de nouvelles possibilités de piratage, de fraude et de harcèlement
 - › La police de la circulation pourrait être moins nécessaire, car la surveillance des conducteurs par les gouvernements
- et les compagnies d'assurance permet de **remettre automatiquement des contraventions**
- Les militants¹⁸ et les journalistes¹⁹ pourraient de plus en plus utiliser l'informatique omniprésente pour « retourner le regard » en **recueillant des informations sur des organisations ou des personnes puissantes**. Cette pratique est connue sous le nom de « sousveillance » ou « équivalence ». Il peut s'agir du piratage d'informations sensibles sur la vie privée de représentants politiques ou d'autres personnalités publiques²⁰
 - Les régimes de protection des données pourraient devenir **plus complexes** et moins harmonisés au niveau mondial
 - Les juridictions pourraient avoir du **mal à trouver un équilibre** entre la protection de la vie privée et le besoin des chercheurs de disposer d'ensembles de données représentatifs dans des domaines tels que la médecine²¹
 - Les juridictions dont les lois sur la protection de la vie privée sont moins strictes pourraient devenir des **destinations de travail ou de voyage de plus en plus « risquées »**
 - **Les dispositifs de protection de la vie privée** pourraient faire pencher la balance du pouvoir en faveur des utilisateurs

Notes de fin de texte

- 1 Singer, Natasha. « [In Screening for Suicide Risk, Facebook Takes On Tricky Public Health Role](#) ». *The New York Times*, 31 décembre 2018, sec. Technology.
- 2 Kröger, Jacob Leon; Raschke, Philip; Percy Campbell, Jessica et Ullrich, Stefan. « [Surveilling the Gamers: Privacy Impacts of the Video Game Industry](#) ». *Entertainment Computing*, vol. 44 (1^{er} janvier 2023) : 100537.
- 3 Chen, Brian X. « [Comment la nouvelle caméra faciale de Meta annonce une nouvelle ère de surveillance](#) ». *The New York Times*, 13 décembre 2023, sec. Technology.
- 4 Brianna R. « [Humane AI: Privacy Implications of This New AI-Powered Lapel](#) ». *Medium* (blogue), 22 décembre 2023.
- 5 While, Jenny; Farrell, Jessica Alice et La Conversation. « [The DNA You Shed Could Identify You](#) ». *Scientific American*, 15 mai 2023.
- 6 Whitmore, Liam; McCauley, Mark; Farrell, Jessica A.; Stammnitz, Maximilian R.; Koda, Samantha A.; Mashkour, Narges; Summers, Victoria; Osborne, Todd; Whilde, Jenny et Duffy, David J. « [Inadvertent Human Genomic Bycatch and Intentional Capture Raise Beneficial Applications and Ethical Concerns with Environmental DNA.](#) » *Nature Ecology & Evolution*, vol. 7, no 6 (juin 2023) : p. 873-888.
- 7 Caltrider, Jen; Rykov, Misha et MacDonald, Zoe. « [Les voitures sont la pire catégorie officielle de produits en matière de confidentialité que nous ayons jamais examinée](#) » *Confidentialité non incluse de Mozilla* (blogue), 6 septembre 2023.
- 8 Caltrider, Jen; Rykov, Misha et MacDonald, Zoe. « [Les voitures sont la pire catégorie officielle de produits en matière de confidentialité que nous ayons jamais examinée](#) » *Confidentialité non incluse de Mozilla* (blogue), 6 septembre 2023.
- 9 McKinsey. « [Unlocking Connected Cars with Corporate Business Building](#) », 31 août 2023.
- 10 Rimol, Meghan. « [Gartner Identifies Top Five Trends in Privacy Through 2024](#) ». *Gartner Press Release* (blogue), 22 mai 2022.
- 11 Hunton Andrews Kurth. « [New Bipartisan Federal Privacy Proposal Unveiled: American Privacy Rights Act](#) », 23 avril 2024.
- 12 Zuboff, Shoshana. « *L'ère du capitalisme de surveillance : la lutte pour l'avenir à la nouvelle frontière du pouvoir* ». Affaires publiques, 2019.
- 13 Commissariat à la protection de la vie privée du Canada. « [Principes pour des technologies de l'intelligence artificielle \(IA\) générative responsables, dignes de confiance et respectueuses de la vie privée](#) », 7 décembre 2023.
- 14 Schulze, Kris. « [Cloud Computing vs. Edge Computing | Blog](#) ». *Scale Computing*, 2 mai 2024.
- 15 Earney, Shandra. « [Is the Edge or Cloud Better for Security and Privacy?](#) » *Xalient*, 17 octobre 2022.
- 16 Swabey, Pete. « [Why Edge Computing Is a Double-Edged Sword for Privacy](#) ». *Tech Monitor* (blogue), 31 mars 2023.
- 17 Beasy, John; Hagerman, Chris; Joy, Amanda; Rigillo, Nicole; Robertson, Simon; Thomas, Tieja; Van der Elst, Kristel et Wester, Meaghan. « [Vies futures : Incertitudes](#) ». Ottawa : Horizons de politiques Canada, 2024.

- 18 Miller, Lloyd. « [RECON VILLAGE - Applied OSINT For Politics: Turning Open Data Into News - TIB AV-Portal](#) ». Présenté lors de la DEF CON (Las Vegas), 2018.
- 19 Vincent, Subramaniam. « [How Open Source Intelligence Can Help Journalists Cover Conflicts.](#) » Markkula Center for Applied Ethics » (blogue), 3 octobre 2023.
- 20 Pierson, Chris. « [Celebrities Are a Big Target for Hackers - Cyber Threats](#) ». *BlackCloak | Protect Your Digital LifeTM* (blogue), 15 octobre 2020.
- 21 Lobel, Orly. « [The Problem With Too Much Data Privacy](#) ». *Time Magazine*, 7 octobre 2022.

© Sa Majesté le Roi du chef du Canada, 2025

Pour obtenir des informations sur les droits de reproduction : <https://horizons.gc.ca/fr/contactez-nous/>

PDF : PH4-218/2025F-PDF

ISBN : 978-0-660-76896-0

Also available in English under the title: AI further erodes privacy.

AVERTISSEMENT

Horizons de politiques Canada (Horizons de politiques) est le centre d'excellence en prospective du gouvernement du Canada. Notre mandat est de doter le gouvernement du Canada d'une perspective et d'un état d'esprit tournés vers l'avenir afin de renforcer la prise de décisions. Le contenu de ce document ne représente pas nécessairement le point de vue du gouvernement du Canada ou des agences et ministères participants.