



IDÉE 9

LES DONNÉES COLLECTÉES SUR LES ENFANTS POURRAIENT REMODELER LEUR VIE AU PRÉSENT ET À L'AVENIR



Les juridictions s'inquiètent de la protection de la vie privée des enfants à mesure que les technologies de l'IA deviennent plus omniprésentes. La collecte omniprésente de données pendant l'enfance pourrait offrir de nouvelles possibilités en matière d'accessibilité et d'éducation, mais aussi aggraver les vulnérabilités existantes, éroder la vie privée et remodeler la vie des adultes à l'avenir.

AUJOURD'HUI

Les jeunes sont un groupe particulièrement vulnérable en ce qui concerne la confidentialité des données¹.

Leur sens de l'autonomie et leur capacité à prendre des décisions sont encore en cours de développement. Un développement sain de l'enfant implique la capacité d'expérimenter et de faire des erreurs sans conséquences graves et durables. De plus en plus de juridictions étudient les moyens de protéger les droits des enfants en matière de données et de vie privée, et de relever les défis liés à l'obtention d'un consentement valable².



Les cas d'acteurs malveillants utilisant les données des enfants de manière à nuire à leur santé mentale et à leur bien-être sont de plus en plus nombreux.

Les critiques soulignent la manière dont les grandes entreprises technologiques captent l'attention et les revenus par l'intermédiaire d'expériences d'utilisation addictives³ et de motifs sombres⁴. Les « motifs sombres » sont un type de conception de sites Web ou d'applications qui peut être utilisé pour influencer votre prise de décision lorsque vous utilisez une application ou naviguez sur un site Web; par exemple, en rendant intentionnellement difficile l'annulation d'un service⁵. Les algorithmes des médias sociaux exacerbent les problèmes liés à une image corporelle négative⁶. L'IA générative a été impliquée dans la circulation⁷ et le développement⁸ de matériel pédopornographique, tant réel que généré par l'IA, par des adultes et des enfants.

Les parents disposent d'une marge de manœuvre extraordinaire pour obtenir et offrir une visibilité sur la vie privée de leurs enfants.

Par exemple, les applications d'enregistrement de frappe peuvent permettre aux parents de voir non seulement les messages envoyés par un enfant, mais aussi les messages qu'il a tapés, mais qu'il a décidé de ne pas envoyer⁹. Les parents peuvent également diffuser les informations privées de leurs enfants à d'autres personnes. Certains gèrent des comptes d'enfants influents qui génèrent des revenus et diffusent régulièrement des informations personnelles et des images de leurs enfants. Ces comptes sont parfois ouvertement suivis par des pédophiles, qui bénéficient des politiques de la plateforme qui récompensent l'engagement¹⁰.

Les ombres de « données » non désirées pourraient suivre les enfants jusqu'à l'âge adulte.

Que les données soient diffusées par les parents ou collectées par des plateformes ou des appareils¹¹, elles peuvent créer une « ombre de données » qui suit les enfants tout au long de leur vie¹². Cette ombre de données peut commencer avant la naissance; par exemple, lorsque les parents utilisent des services de tests ADN pour connaître la susceptibilité génétique de leurs enfants à certaines maladies¹³. Puisque ces vastes ensembles de données pouvant être stockés indéfiniment, les futurs systèmes d'IA pourraient s'en servir pour faire de nouvelles déductions sur les personnes au fur et à mesure qu'elles deviennent adultes.

Les écoles collectent de plus en plus d'informations sur les élèves, à l'aide de logiciels tiers et d'outils d'analyse à intelligence artificielle. Depuis la pandémie, l'utilisation des applications de gestion des élèves a augmenté de façon exponentielle dans les crèches, les écoles primaires et les écoles secondaires du Canada. Par exemple, on estime que 70 % des écoles primaires utilisent Class Dojo. Sa politique de confidentialité indique qu'elle peut communiquer des données à des fournisseurs de services tiers, notamment Facebook et Google¹⁴.



Les violations de données ont nui aux enfants et aux jeunes au Canada et ailleurs. En 2024, les photos scolaires de 160 élèves de l'Alberta ont été volées lorsque des pirates ont accédé au fournisseur de stockage en nuage d'une société d'annuaires scolaires¹⁵. Des gangs de rançongiciels ont pris pour cible des écoles publiques américaines, divulguant des données sensibles sur la santé mentale des élèves, les agressions sexuelles et les plaintes pour discrimination¹⁶. En 2023, des attaques de rançongiciels ont touché des institutions telles que le Sick Kids Hospital de Toronto¹⁷, Family and Children's Services of Lanark, Leeds and Grenville¹⁸, et le registre et réseau des bons résultats dès la naissance de l'Ontario, où 3,4 millions de dossiers médicaux ont fait l'objet d'une violation¹⁹.

Les entreprises et les ONG détiennent un grand nombre de données sensibles sur les jeunes, qui peuvent faire l'objet d'une violation. Des applications privées de contrôle parental ont été piratées, exposant les données des enfants surveillés²⁰. En 2023, TikTok²¹, Microsoft²², et Amazon²³ ont été condamnés à des amendes pour violation de la vie privée des enfants dans diverses juridictions. En tant qu'organisation non gouvernementale, Jeunesse, J'écoute, qui détient la plus grande base de données sur la santé mentale des jeunes au Canada²⁴, déclare avoir mené une évaluation des incidences sur la vie privée²⁵ et avoir regroupé et anonymisé ses données²⁶.





AVENIRS

La vente, la circulation et l'analyse opaques des données relatives aux enfants deviendront plus courantes, commenceront beaucoup plus tôt dans la vie et seront utilisées à l'avenir à des fins imprévues. Le nombre de dispositifs de collecte de données avec lesquels les enfants interagissent, à la maison, à l'école et ailleurs, augmentera (voir les idées 7 et 8). Certains de ces appareils pourraient être plus vulnérables aux violations d'informations sensibles²⁷.

Les technologies de surveillance alimentées par l'IA pourraient devenir plus importantes, mais elles pourraient aussi être détournées. Les parents pourraient se tourner vers des technologies de surveillance alimentées par l'IA pour les aider à contrôler les activités en ligne de leurs enfants et à garder le contrôle sur des environnements informationnels et médiatiques de plus en plus complexes²⁸. Cependant, les jeunes pourraient aussi développer des moyens de plus en plus sophistiqués pour échapper au contrôle parental.

Les enfants et les jeunes pourraient vivre dans des environnements médiatiques plus personnalisés. Les contenus de divertissement et la publicité pourraient de plus en plus être générés ou conçus par des compagnons d'IA personnalisés. Les sous-cultures et les cultures partisans pourraient devenir de plus en plus personnalisées et politisées. Les sentiments d'isolement social pourraient devenir plus fréquents, ainsi qu'une cohésion sociale réduite. Certains jeunes pourraient être désillusionnés par les technologies invasives alimentées par l'IA et choisir de passer plus de temps hors ligne. Toutefois, compte tenu de l'omniprésence de l'IA, cette option pourrait ne pas être envisageable à l'avenir.

Le marché des données sur les jeunes pourrait devenir plus compétitif à mesure que les préoccupations concernant la confidentialité des données sur les jeunes augmentent. Cela pourrait conduire les entreprises technologiques à développer des moyens plus insidieux d'extraire et de commercialiser les données des jeunes. L'âge limite pour être considéré comme un « enfant » peut varier selon les contextes. Les données pourraient devoir être divulguées lorsque l'enfant atteint l'âge de la majorité²⁹. Les technologies de vérification de l'âge³⁰, comme celles qui sont actuellement utilisées dans certains États américains pour les sites Web pornographiques³¹, pourraient être utilisées plus largement pour protéger les jeunes des adultes prédateurs et des espaces réservés aux adultes.

Malgré les nombreuses préoccupations qu'elles soulèvent, les nouvelles technologies basées sur l'IA pourraient également collecter des données de manière à favoriser l'accessibilité.³² Ils pourraient être utilisés pour développer des outils d'apprentissage individualisés qui aideraient les élèves à progresser à leur propre rythme. Ils pourraient également améliorer la qualité des soins de santé pédiatriques en facilitant le diagnostic, le suivi des patients et la médecine de précision³³.





IMPLICATIONS

- ▶ Les enfants d'aujourd'hui pourraient être confrontés à des violations de données **plus fréquentes et plus dévastatrices** tout au long de leur vie
- ▶ Ces violations peuvent donner lieu à des formes d'**usurpation d'identité** qui entraînent des pertes financières ou la divulgation d'informations personnelles sensibles
- ▶ **La réidentification des données personnelles anonymes** pourrait devenir plus facile à mesure que les violations de données deviennent plus courantes et que les technologies progressent; les données qui semblent **privées aujourd'hui pourraient ne plus l'être demain**
- ▶ Des restrictions laxistes pourraient conduire à l'utilisation de données pour faire **des déductions formulées par l'IA** sur les jeunes qui **nuisent à leurs relations et à leur accès à l'emploi, au crédit ou à l'assurance** dans l'enfance et à l'âge adulte
- ▶ **L'utilisation accrue des technologies de contrôle parental** pourrait entraîner une surveillance induite et **une perte de vie privée et d'autonomie pour les enfants**
- ▶ L'IA pourrait **compliquer l'identification par les parents des contenus problématiques ou préjudiciables**, ou faciliter la dissimulation par les jeunes de leur participation à ces contenus
- ▶ Si la prise de conscience des problèmes liés à la confidentialité des données des enfants s'accroît, davantage de développeurs pourraient être amenés à lancer **des applications et des plateformes propres aux enfants, soumises à des normes de confidentialité plus strictes³⁴** ou prenant en compte des questions telles que la santé mentale et la dépendance

Notes de fin de texte

- 1 Irwin, Jasmine; Dharamshi, Alannah et Zon, Noah. « [La sécurité et la confidentialité des enfants à l'ère numérique](#) ». Groupe CSA, mars 2021.
- 2 Irwin, Jasmine; Dharamshi, Alannah et Zon, Noah. « [La sécurité et la confidentialité des enfants à l'ère numérique](#) ». Groupe CSA, mars 2021.
- 3 Murphy, Chris. « [Opinion | Algorithms Are Making Kids Desperately Unhappy](#) ». *The New York Times*, 18 juillet 2023, sec. Opinion.
- 4 Leiser, M. R. « [Protecting Children from Dark Patterns and Deceptive Design](#) ». SSRN, 11 décembre 2023.
- 5 Bureau de la consommation. « [Les interfaces truquées](#) ». Gouvernement du Canada, 19 July 2023.
- 6 Hill, Amelia. « [Social Media Triggers Children to Dislike Their Own Bodies, Says Study](#) ». *The Guardian*, 1^{er} janvier 2023, sec. Society.
- 7 David, Emilia. « [AI Image Training Dataset Found to Include Child Sexual Abuse Imagery - The Verge](#) ». *The Verge*, 20 décembre 2023.
- 8 Duboust, Oceane. « [Society Needs to Be Alert](#) »: Most People Are Unaware AI Is Being Used to Create Child Abuse Content | Euronews ». *Euronews Next*, 19 février 2024.
- 9 SecureKin. « [Keylogger App To Record Your Child's Keystrokes](#) ». Consulté le 23 mai 2024.
- 10 Valentino-DeVries, Jennifer et Keller, Michael H. « [A Marketplace of Girl Influencers Managed by Moms and Stalked by Men](#) ». *The New York Times*, 23 février 2024, sec. U.S.
- 11 Owen. « [New AI Toys Spark Privacy Concerns for Kids](#) ». *GZERO Media*, 12 décembre 2023.
- 12 Irwin, Jasmine; Dharamshi, Alannah et Zon, Noah. « [La sécurité et la confidentialité des enfants à l'ère numérique](#) ». Groupe CSA, mars 2021.
- 13 Bala, Nila. « [Opinion | Why Are You Publicly Sharing Your Child's DNA Information?](#) » *The New York Times*, 2 janvier 2020.
- 14 ClassDojo. « [Third Party Service Providers](#) ». Consulté le 23 mai 2024.
- 15 DaSilva, Tomasias. « [Hackers Steal Children's School Photos Following a Privacy Breach](#) ». *Global News*, 14 février 2024.
- 16 Bajak, Frank; Hollingsworth, Heather et Fenn, Larry. « [Ransomware Criminals Are Dumping Kids' Private Files Online after School Hacks](#) ». *Canadian Security Magazine*, 5 juillet 2023.
- 17 Omstead, Jordan. « [SickKids Cyberattack: Ransomware Group LockBit Apologizes Saying "partner" Was behind Attack](#) ». *CTV News*, 3 janvier 2023.
- 18 Lee, Austin. « [I Am Deeply Troubled": Data Breach Impacts Clients at Lanark County Family Services Organization](#) ». *CTV News*, 14 février 2024, sec. Ottawa.
- 19 Tsekouras, Phil. « [Did You Give Birth between 2010 and 2023 in Ontario? Your Personal Health Information Was "likely" Impacted by a Data Breach](#) ». *CP24*, 25 septembre 2023.
- 20 Ali, Suzan; Elgharabawy, Mounir; Duchaussoy, Quentin; Mannan, Mohammad et Youssef, Amr. « [Betrayed by the Guardian: Security and Privacy Risks of Parental Control Solutions](#) ». In *Proceedings of the 36th Annual Computer Security Applications Conference*, p. 69-83. ACSAC 2020. New York (N.Y., États-Unis) : Association for Computing Machinery, 2020.
- 21 Woollacott, Emma. « [TikTok condamné à une amende de 345 millions d'euros pour violation de la vie privée des enfants](#) ». *Forbes*, 18 septembre 2023.
- 22 Matza, Max. « [Microsoft va payer 20 millions de dollars pour violations de la vie privée des enfants](#) ». *BBC*, 6 juin 2023.

- 23 Singer, Natasha. « [Amazon to Pay \\$25 Million to Settle Children’s Privacy Charges](#) ». *The New York Times*, 31 mai 2023, sec. Technology.
- 24 Jeunesse, j’écoute. « [Jeunesse, J’écoute et l’Institut Vector annoncent un partenariat important pour des innovations améliorées axées sur l’humain pour les services de santé mentale en ligne pour les jeunes d’un océan à l’autre](#) ». Consulté le 23 mai 2024.
- 25 Jeunesse, j’écoute. « [Réponses aux questions à propos de Données de Jeunesse, J’écoute!](#) » Accessed 23 May 2024.
- 26 Jeunesse, j’écoute. « [Jeunesse, J’écoute et l’Institut Vector annoncent un partenariat important pour des innovations améliorées axées sur l’humain pour les services de santé mentale en ligne pour les jeunes d’un océan à l’autre](#) ». Consulté le 23 mai 2024. https://jeunessejecoute.ca/publications/jeunesse-jecoute-et-linstitut-vector-annoncent-un-partenariat-important-pour-des-innovations-ameliorees-axees-sur-lhumain-pour-les-services-de-sante-mentale-en-ligne-pour-les-jeunes-dun-océan-a-lautre/?_ga=2.3904055.629371948.1726846218-976181761.1726846218&_gl=1*184n6jl*_ga*OTc2MTgxNzYxLjE3MjY4NDYyMTg.*_ga_TQY135CFXS*MTcyNjg0NjlxOC4xLjAuMTcyNjg0NjlxOC42MC4wLjExMDU1OTQ2MTA.
- 27 Bennett, Drake. « [How a Massive Hack of Psychotherapy Records Revealed a Nation’s Secrets](#) ». *Bloomberg*, 22 avril 2024.
- 28 Wood, Stuart. « [Explorer la sensibilisation et l’utilisation des contrôles parentaux pour soutenir la sécurité numérique](#) ». *Internet Matters* (blogue), 21 juillet 2023.
- 29 Beauvais, Michael, and Leslie Regan Shade. « [How Will Bill C-27 Impact Youth Privacy?](#) » *Schwartz Reisman Institute* (blogue), 8 octobre 2022.
- 30 McConvey, Joel R. « [Wizz Dials up Biometrics from Yoti to Prevent Sextortion, Achieve EU Compliance](#) ». *Biometric Update* (blogue), 15 février 2024.
- 31 Mithani, Jasmine. « [The 19th Explains: Why Some States Are Requiring ID to Watch Porn Online](#) ». *The 19th*, 29 janvier 2024.
- 32 Costabel, Milagros. « [I’m Totally Blind. Artificial Intelligence Is Helping Me Rediscover the World](#) ». *Slate*, 11 octobre 2023.
- 33 Shu, Li-Qi; Sun, Yi-Kan; Tan, Lin-Hua; Shu, Qiang et Chang, Anthony C. “[Application of Artificial Intelligence in Pediatrics: Past, Present and Future](#).” *World Journal of Pediatrics*, vol. 15, no 2 (1^{er} avril 2019) : p. 105-108.
- 34 UNICEF. « [Children and AI: Opportunities and Risks](#) ». Genève : UNICEF, 2018.

© 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 : PH4-219/2025F-PDF
ISBN : 978-0-660-76900-4

Also available in English under the title: Data collected about children could reshape their lives in the present and future.

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.