

Plus qu'une simple réalité virtuelle

L'application des lois canadiennes relatives à la protection
des renseignements personnels à l'ère de la « XR »



Plus qu'une simple réalité virtuelle : L'application des lois canadiennes relatives à la protection des renseignements personnels à l'ère de la « XR »

Rapport de la Clinique d'intérêt public et de politique d'Internet du
Canada Samuelson-Glushko (CIPPIC) pour le programme de
contributions du Commissariat à la protection de la vie privée du
Canada



© 2024 La Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko (CIPPIC), Christian Clavette, Emily Chu, Renae Pennington, Chloe Bechard, Shaarini Ravitharan, Harmon Imeson Jorna, Eve Gaumond et Drew May.

Page couverture. Crédit photo : [Giu Vicente](#) sur Unsplash



CC BY-NC-SA 2.5 CA DEED

Ce travail est sous licence Creative Commons BY-NC 2.5 (Attribution-Pas d'Utilisation Commerciale-Partage dans les Mêmes Conditions 2.5 Canada). Version électronique publiée pour la première fois sur cippic.ca en 2024 par CIPPIC.

CIPPIC—la Clinique d'intérêt public et de politique d'Internet Samuelson-Glushko du Canada—est une clinique juridique basée à la Faculté de droit de l'Université d'Ottawa. Son mandat est de défendre l'intérêt public sur des questions à l'intersection du droit et de la technologie.

Ce rapport et les documents correspondants ont été préparés par la **Clinique d'intérêt public et de politique d'Internet Samuelson-Glushko du Canada** (CIPPIC) à l'Université d'Ottawa et financés par le **programme de contributions du Commissariat à la protection de la vie privée** pour le projet intitulé : « Plus qu'une simple réalité virtuelle : L'application des lois canadiennes relatives à la protection des renseignements personnels à l'ère de la 'XR'. » Ce document est destiné à des fins d'information seulement et ne doit pas être interprété comme un avis juridique. Pour toute demande ou information supplémentaire, veuillez contacter admin@cippic.ca.

Le personnel de CIPPIC et les chercheurs collaborateurs Emily Chu, Renae Pennington, Chloe Bechard, Shaarini Ravitharan, Harmon Imeson Jorna, Eve Gaumond et Drew May ont contribué à ce projet sous la direction de l'administrateur du projet Christian Clavette.

Les auteurs conservent l'entière propriété des droits d'auteur de ce travail, et tous les droits relatifs à l'œuvre restent la propriété des auteurs respectifs. Les auteurs n'ont aucun lien avec les marques mentionnées dans ce rapport

Remerciements

Ce rapport sur les implications en matière de confidentialité des technologies de la réalité étendue (XR) au Canada, témoigne de l'effort collaboratif et du dévouement d'un large éventail de contributeurs, dont l'expertise et les perspectives ont été inestimables pour la profondeur et l'étendue de notre analyse. Nous adressons nos sincères remerciements à tous ceux qui ont généreusement partagé leur temps, leurs connaissances et leurs ressources pour rendre cette étude exhaustive possible.

Des remerciements spéciaux vont au professeur Vivek Krishnamurthy pour avoir mis en oeuvre ce projet et fourni des conseils inestimables. Nous apprécions également le leadership de la professeur Teresa Scassa dans la navigation des défis liés à l'IA et à la XR, ainsi que les premiers retours du professeur Brittan Heller.

Notre gratitude s'étend aux parties prenantes du monde académique et de l'industrie, y compris les professeurs Jacquie Burkell, Leslie Regan Shade, Jane Bailey, Valérie Steeves, et les professionnels de l'industrie Chantal Bernier, Caroline Dupuis, Matthew Sheardown et Alex Gimson.

Enfin, nous remercions nos étudiants stagiaires dévoués Emily Chu, Renae Pennington, Chloé Bechard, Shaarini Ravitharan, Harmon Imeson Jorna, Eve Gaumond et Drew May pour leur professionnalisme, leurs idées novatrices et leur travail acharné dans la recherche, l'analyse et la compilation de ce rapport.

Table des matières

Remerciements.....	vii
Sommaire exécutif.....	xi
Introduction	1
1. Qu'est-ce que la « XR » ?	2
2. Quels sont les impacts de la XR en matière de vie privée ?	6
3. Le droit canadien protège-t-il bien les utilisateurs de XR?	7
3.1. La LPRPDE – La loi qui régit actuellement le traitement des données dans le secteur privé	8
3.2. La LPVPC – La loi proposée pour régir le traitement des renseignements personnels dans le secteur privé	10
4. Recommandations – Que propose CIPPIC ?	13
4.1. La Loi - Adopter une lecture intentionnelle de la LPRPDE et amender la LPVPC.....	14
4.2. Les normes sociales – Besoin de plus d'éducation face à la confidentialité.....	15
4.3. Le marché - Introduire un système de notation de la confidentialité	16
4.4. La technologie – Promouvoir la confidentialité par conception.....	17
Conclusions	18
Annexe.....	19
Entretiens avec les parties prenantes – Processus de recrutement.....	19
Entretiens avec les parties prenantes – Biographies des participants	20
Entretien avec les parties prenantes – Questionnaire	22

Sommaire exécutif

L'expression XR désigne les technologies de réalité étendue (extended reality). Elle englobe trois types de technologies : la réalité augmentée (AR), la réalité virtuelle (VR) et la réalité mixte (MR) qui seront toutes décrites plus amplement dans les prochaines pages.

Si ces technologies ouvrent un monde de nouvelles possibilités, notamment en termes de divertissement immersif, les lois canadiennes peinent à suivre le rythme pour s'y adapter. Dans le cadre de ce rapport, nous nous intéressons particulièrement aux casques de XR comme le Apple Vision Pro qui offrent aux utilisateurs des expériences tridimensionnelles grâce à un mélange de capteurs, caméras, microphones et gyroscopes. Ces casques de XR mobilisent une série de capteurs et de caméras intégrées pour cartographier l'environnement de l'utilisateur et suivre ses mouvements. Certains capteurs sont également mis à profit pour assurer le suivi du mouvement des mains et des yeux afin de permettre à l'utilisateur de contrôler l'appareil.

La manière dont fonctionnent ces casques soulève des enjeux en matière de vie privée, qui sans être uniques en eux-mêmes, interagissent entre eux de manière particulièrement préoccupante. D'abord, les casques collectent une quantité considérable de données biométriques sensibles, qui peuvent être utilisées pour déduire des renseignements personnels sur l'utilisateur du casque. Et puis, ils peuvent aussi recueillir des informations sur les personnes qui se trouvent au tour de l'utilisateur, et ce sans que ceux-ci n'y aient consenti.

Ces enjeux combinés créent des situations que les lois canadiennes actuelles ne prennent pas tout à fait en compte. En matière de vie privée et de protection des renseignements personnels, le droit canadien a des allures de courtepoinette. Plusieurs lois différentes peuvent s'appliquer dépendamment du contexte. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) régit le traitement des données dans le secteur privé. Or, l'Alberta, la Colombie-Britannique et le Québec ont des lois provinciales qui s'appliquent à sa place dans certains contextes. Par ailleurs, la LPRPDE est vraisemblablement sur le point d'être remplacée par la *Loi sur la protection de la vie privée des consommateurs* (LPVPC), qui est en quelque sorte une version mise à jour de la LPRPDE.

Dans ce rapport, CIPPIC s'intéresse aux manières dont ces lois s'appliquent à la XR. Afin de produire ce rapport, nous avons conduit une série d'entretiens avec des universitaires et des acteurs de l'industrie, et nous avons analysé la législation, la technologie et les politiques de confidentialité connexes pour étayer et contextualiser leurs réponses. À l'issue de ce processus, CIPPIC propose trois recommandations juridiques clés pour relever les défis que la XR pose en matière de vie privée :

- En vertu de la LPRPDE, il devrait être obligatoire d'obtenir un consentement explicite pour procéder à la collecte et l'utilisation des renseignements personnels des utilisateurs qui interagissent avec la XR. Une explication détaillée de la manière dont la plateforme entend utiliser ces renseignements devrait aussi être fournie.

- Le CPVP devrait envisager un modèle de co-régulation qui lui permettrait de collaborer avec les parties prenantes associées à la XR pour arriver à des consensus quant aux exigences légales applicables à ceux-ci.
- La LPVPC devrait inclure une définition de la notion « d'informations sensibles », adopter une conception du consentement centré sur l'utilisateur et renforcer les protections pour les enfants.

Toutefois, le droit à lui seul ne suffira pas à régler les enjeux soulevés par la XR en matière de vie privée. En complément des mesures juridiques, le CPVP devrait adopter une approche mobilisant également d'autres types de normativités. Il pourrait notamment s'engager encore plus dans l'éducation à la vie privée en développant des ressources pour les utilisateurs et les concepteurs—un système de notation de la vie privée, par exemple. Il pourrait aussi se doter de mécanismes de type « se conformer ou expliquer » pour aborder les préoccupations plus larges en matière de vie privée autour de la XR. Ces mesures aideraient à répondre à bon nombre des préoccupations soulevées dans ce rapport.

En somme, la XR est une technologie prometteuse qui pourrait contribuer à des avancements importants, entre autres dans le domaine du divertissement, de l'éducation et des affaires. Il s'agit simplement de s'assurer que ces progrès ne se fassent pas au détriment de la vie privée des Canadiens

Introduction

Ce rapport est le résultat d'un travail collaboratif impliquant des universitaires, des professionnels de l'industrie et des étudiants. Il a été financé par le programme de contributions du Commissariat à la protection de la vie privée du Canada. La question à laquelle il cherche à répondre est la suivante : les lois canadiennes sont-elles bien équipées pour faire face aux enjeux en matière de vie privée que soulèvent les technologies de réalité étendue (XR). Une attention particulière est portée aux questions de la vie privée des enfants¹.

Pour explorer ces enjeux, CIPPIC a mené huit entretiens semi-dirigés avec des acteurs du monde universitaire et de l'industrie². En ce qui concerne les universitaires, nous avons interviewé des professeurs dans les domaines du droit, de la criminologie et des sciences de l'information et des médias. Pour ce qui est de l'industrie, nous avons interviewé trois employés travaillant dans deux entreprises de XR différentes ainsi qu'une avocate en pratique privée dont les clients incluent des entreprises technologiques, des institutions financières, des entreprises de biotechnologie, des entreprises d'analyse de données et des institutions gouvernementales. Leurs réponses sont au cœur de ce rapport.

Il aborde quatre questions principales :

- Qu'est-ce que la XR ?
- Comment la XR impacte-t-elle la vie privée ?
- Le droit canadien est-il bien équipé pour protéger les utilisateurs de XR ?
- Quelles sont les suggestions de CIPPIC pour mieux protéger les Canadiens interagissant avec la XR ?

¹ The most comprehensive studies on XR consider XR technology from the perspective of European and American law, respectively. See Emil Albihn Henriksson, "[Data Protection Challenges for Virtual Reality Applications](#)" (2018) 1:1 Interactive Entertainment L Rev; see also Yeji Kim, "[Virtual Reality Data and Its Privacy Regulatory Challenges: A Call to Move Beyond Text-Based Informed Consent](#)" (2022) 110:1 Cal L Rev; Brittan Heller, "[Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law](#)" (2020) 23: 1 Vanderbilt J Entertainment & Tech L; Suchismita Pahi & Calli Schroeder, "[Extended Privacy for Extended Reality: XR Technology Has 99 Problems and Privacy is Several of Them](#)" (Forthcoming 2023) 4 Notre Dame J Emerging Tech; Mark A Lemley & Eugene Volokh, "[Law, Virtual Reality, and Augmented Reality](#)" (2018) 166: 5 U Pa L Rev.

² Le questionnaire ainsi que les biographies des participants se trouvent dans l'appendice.

1. Qu'est-ce que la « XR » ?

La « XR » est un terme générique qui englobe trois principales technologies : la réalité augmentée, la réalité virtuelle et la réalité mixte :

La Réalité Augmentée (AR) superpose des informations numériques sur le monde réel. Par exemple, l'AR peut être utilisée dans des applications comme Pokémon Go, où des personnages virtuels apparaissent dans le monde réel via l'écran d'un téléphone intelligent. En plus de ces téléphones et des tablettes, il existe également des lunettes AR qui utilisent des caméras et des capteurs pour détecter l'environnement et placer des objets, animations ou données virtuels sur les environs physiques. Les lunettes intelligentes Ray-Ban Meta, par exemple, intègrent un assistant AI et permettent aux utilisateurs de publier directement du contenu multimédia sur les propriétés, Instagram et Facebook de l'entreprise.

La Réalité Virtuelle (VR) immerge les utilisateurs dans un environnement entièrement virtuel. Les casques VR comme l'Oculus Quest utilisent des écrans, des capteurs de mouvement et des gyroscopes pour suivre les mouvements de la tête et des mains, permettant aux utilisateurs de naviguer et d'interagir dans un espace numérique 3D. Ce type de technologie est utilisé dans des applications allant des jeux vidéo aux visites virtuelles et aux simulations de formation médicale.

La Réalité Mixte (MR), avec des dispositifs tels que l'Apple Vision Pro et le Meta Quest 3, représente les dernières avancées en matière de technologie XR. Ces dispositifs combinent les capacités de la VR et de l'AR, permettant aux utilisateurs de passer de manière transparente entre les environnements augmentés et virtuels. L'Apple Vision Pro, par exemple, utilise des scanners LiDAR, plusieurs caméras et une technologie avancée de suivi oculaire pour créer une expérience MR immersive. Ces capteurs permettent au dispositif de comprendre l'environnement de l'utilisateur et d'interagir dynamiquement avec lui, offrant une expérience utilisateur plus naturelle et intuitive.

Bien que la XR soit apparue pour la première fois dans les années 1960, les systèmes de l'époque étaient encombrants, coûteux et limités par la technologie disponible, avec des écrans à basse résolution et des capacités de suivi des mouvements limitées. Ce n'est qu'au début des années 2010 que la technologie telle que nous la connaissons aujourd'hui a vraiment commencé à éclore. L'Oculus Rift a ouvert la voie en révolutionnant la VR en offrant des expériences immersives de haute qualité à un prix relativement abordable.

Depuis lors, la XR n'a cessé de s'améliorer. Les systèmes modernes tels que l'Oculus Quest 2 et l'Apple Vision Pro sont devenus des dispositifs autonomes qui n'ont plus besoin d'être connectés à des ordinateurs externes. Ces dispositifs intègrent une puissance de traitement interne et l'informatique en nuage pour améliorer les performances et l'expérience utilisateur. Ils utilisent une gamme de capteurs, y compris des caméras intégrées, pour cartographier l'environnement de l'utilisateur et suivre ses mouvements sans avoir besoin de capteurs externes.

Un casque XR de base comme l'Oculus Quest 2 fonctionne en combinant plusieurs composants clés. Il possède des écrans haute résolution placés près des yeux de l'utilisateur, offrant un large champ de vision. Ces écrans sont divisés pour montrer des perspectives légèrement différentes à chaque œil, créant un effet 3D stéréoscopique. Le casque utilise des capteurs internes, y compris des gyroscopes, des accéléromètres et des magnétomètres, pour suivre les mouvements de la tête et ajuster l'affichage en temps réel pour correspondre à la perspective de l'utilisateur. Les paragraphes suivants explorent comment ces composants interagissent pour créer une expérience immersive pour les utilisateurs.

Le suivi oculaire améliore l'expérience immersive en surveillant où l'utilisateur regarde. Cette technologie utilise des capteurs infrarouges et des caméras à l'intérieur du casque, pointées vers le visage, pour suivre les mouvements des yeux de l'utilisateur. En déterminant la direction et le point focal précis du regard, le système peut rendre des portions de l'environnement virtuel en haute résolution là où l'utilisateur regarde — cette technique est connue sous le nom de rendu fovéal. Cela améliore non seulement la qualité visuelle, mais réduit également la charge de traitement de l'appareil, permettant une puissance de traitement plus efficace. Le suivi oculaire peut également être utilisé pour des interfaces de contrôle intuitives, permettant aux utilisateurs d'interagir avec les menus et les objets simplement en les regardant.

La pupillométrie est la mesure de la taille et de la réactivité de la pupille. C'est un aspect intégral de la technologie de suivi oculaire dans les systèmes XR. Elle fournit des informations sur l'état cognitif et émotionnel de l'utilisateur en analysant les changements de diamètre de la pupille en réponse à des stimuli, aidant à créer des expériences XR plus personnalisées et réactives. Lorsqu'elle est intégrée au suivi oculaire, la pupillométrie utilise les mêmes capteurs infrarouges et caméras pour détecter et mesurer la réponse de la pupille à divers facteurs visuels et environnementaux. Cette intégration permet au dispositif d'ajuster l'éclairage, la mise au point et d'autres éléments en temps réel en fonction des réponses physiologiques de l'utilisateur, améliorant l'expérience immersive globale.

Le suivi inside-out dans les casques VR consiste à utiliser des caméras montées sur le casque lui-même pour observer et cartographier l'environnement environnant. Ces caméras capturent l'espace physique et détectent des caractéristiques telles que les murs, les meubles et d'autres objets. Le logiciel crée ensuite une carte virtuelle de l'environnement, utilisée pour suivre les mouvements de l'utilisateur dans cet espace. Cette méthode élimine le besoin de capteurs ou de balises externes, offrant une plus grande liberté de mouvement et un processus d'installation simplifié. Les caméras suivent également la position et l'orientation du casque, permettant à l'environnement virtuel de s'ajuster dynamiquement au fur et à mesure des mouvements de l'utilisateur.

Le suivi des mains est également une fonctionnalité de certains dispositifs comme le Microsoft HoloLens ou le VarjoXR-4. Ces casques n'ont pas besoin de contrôleurs manuels pour fonctionner. Ils s'appuient sur une variété de capteurs et de technologies pour suivre et interpréter les mouvements et les gestes de la main de l'utilisateur. Les capteurs optiques, souvent utilisés, capturent des images ou des vidéos des mains de l'utilisateur. Des algorithmes

avancés traitent ensuite ces images pour identifier et suivre la position, l'orientation et les gestes de la main en temps réel. D'autres types de capteurs peuvent être utilisés pour le suivi des mains et la télémétrie. Les capteurs infrarouges émettent et détectent la lumière infrarouge pour créer une carte de profondeur de l'environnement, aidant à suivre avec précision la position et le mouvement des mains même dans des conditions de faible luminosité. Leap Motion est un exemple bien connu qui utilise des capteurs infrarouges pour le suivi des mains. Les capteurs ultrasoniques émettent des ondes ultrasoniques et mesurent le temps que mettent les ondes pour rebondir sur les mains de l'utilisateur. Ces données aident à déterminer la position et le mouvement des mains. Les unités de mesure inertielle combinent des accéléromètres, des gyroscopes et parfois des magnétomètres pour détecter l'orientation et le mouvement des mains. Bien qu'elles soient plus couramment utilisées dans les contrôleurs traditionnels, elles peuvent également améliorer le suivi des mains en fournissant des données de mouvement supplémentaires. En intégrant ces capteurs, les contrôleurs sans mains dans les environnements XR peuvent offrir une interaction précise et intuitive, améliorant l'expérience immersive.

L'avenir de la technologie XR semble très prometteur, alimenté par des investissements substantiels de géants de la technologie comme Apple, Meta et Microsoft. Ces entreprises sont à la pointe du développement de dispositifs MR de nouvelle génération visant à offrir des expériences encore plus immersives et conviviales. L'introduction des réseaux 5G et la miniaturisation continue des processeurs devraient encore améliorer les capacités de la XR, permettant des interactions plus rapides et plus fluides.

L'IA étant de plus en plus intégrée aux systèmes XR, les capacités des utilisateurs sont améliorées. Les algorithmes d'IA sont utilisés pour créer des environnements virtuels plus réalistes et des éléments interactifs, améliorant l'immersion et la réactivité des applications VR et AR. Par exemple, l'IA peut permettre des interactions entre utilisateurs plus naturelles et intuitives en reconnaissant les gestes et les commandes vocales, ainsi qu'en adaptant l'environnement virtuel en temps réel en fonction du comportement et des préférences de l'utilisateur. De plus, les analyses basées sur l'IA peuvent fournir des informations sur l'engagement des utilisateurs et optimiser la diffusion de contenu. Cela améliore non seulement l'expérience XR globale, mais soulève également des questions en matière de confidentialité.

L'Apple Vision Pro

Pour éviter toute confusion et garantir que toutes les parties prenantes étaient sur la même longueur d'onde, la CIPPIC a utilisé l'Apple Vision Pro comme étude de cas lors de nos entretiens. Nous avons encouragé les participants à penser à cette technologie en répondant à nos questions.

Apple a lancé le Vision Pro aux États-Unis début février 2024. Il s'agit d'un casque qui crée une expérience utilisateur tridimensionnelle grâce à un mélange de capteurs de profondeur, de caméras, de microphones et de gyroscope³. Avec le lancement du casque, Apple a

³ Apple, "[Apple Vision Pro Privacy Overview - Learn how Apple Vision Pro and visionOS protect your data](#)" (2024) at 3, online (pdf).

également introduit un tout nouvel App Store qui donne accès à plus d'un million d'applications compatibles et à plus de six cents nouvelles expériences spatiales⁴.

Une analyse approfondie des politiques de confidentialité du Vision Pro – ce qui n'est pas un processus simple, car ces documents sont dispersés sur plusieurs pages web – révèle un problème préoccupant concernant la manière dont Apple gère la confidentialité des utilisateurs du casque. Dans l'ensemble, le Vision Pro est conçu de manière à minimiser les atteintes à la vie privée ; par exemple, les données sont stockées sur le disque dur du Vision Pro plutôt que dans le « cloud ». Cependant, Apple n'assume pas beaucoup de responsabilités en matière de protection de la vie privée de ses utilisateurs. Le contrat de licence de logiciel dégage Apple de toute responsabilité relative au contenu des applications tierces. Et cela est réitéré dans les meilleures pratiques pour les développeurs d'applications, dans lesquelles Apple déclare clairement que : « il est de votre responsabilité de protéger les données collectées par votre application et de les utiliser de manière responsable et respectueuse de la vie privée⁵. »

Cela peut inquiéter ceux qui sont familiers avec la loi canadienne sur la protection de la vie privée car cela ressemble à l'accord que Facebook avait avec « thisisyourdigitallife », l'application responsable du partage des données de plus de 600 000 Canadiens avec Cambridge Analytica. En 2023, la Cour fédérale a conclu que Facebook ne pouvait pas être tenu responsable de l'incident en vertu de la LPRPDE⁶.

⁴ Apple, “[Apple announces more than 600 new apps built for Apple Vision Pro](#)” (1 February 2024), online: *Apple Newsroom*.

⁵ Apple, “[Adopting best practices for privacy and user preferences](#)”, Online: *Apple Developer*.

⁶ *Canada (Privacy Commissioner) v Facebook Inc*, 2023 FC 533 at para 65. [*Facebook*]

2. Quels sont les impacts de la XR en matière de vie privée ?

Les enjeux que soulève la XR en ce qui concerne la vie privée ne sont pas uniques. Or, ils s'additionnent les uns aux autres d'une manière inédite qui est particulièrement préoccupante. Autrement dit, la XR ne change pas la nature des enjeux, elle change simplement l'ampleur des impacts.

Ce changement de paradigme intervient à deux niveaux :

Premièrement, les casques XR traitent une quantité de données sans précédent et la sensibilité de ces données est inégalée. Les casques XR possèdent de nombreux capteurs qui collectent des données en temps réel. Par exemple, les utilisateurs du Casque Vision Pro d'Apple doivent configurer des capteurs qui suivent les mouvements de leurs yeux et de leur tête⁷. Ces capteurs collectent des données pour offrir une expérience plus fluide et personnalisée. Cependant, ces données peuvent également servir à d'autres fins. Les mouvements de la tête et des mains peuvent être utilisés pour déduire le statut marital, l'orientation sexuelle ou l'origine ethnique d'une personne, par exemple, et la dilatation involontaire des pupilles peut également révéler ce qui intéresse une personne⁸. Cela offre des opportunités commerciales aux entreprises technologiques. Meta, par exemple, prévoit d'améliorer la personnalisation des publicités en suivant les mouvements oculaires et les expressions faciales⁹. Lors de nos entretiens, plusieurs intervenants ont soulevé des inquiétudes quant à cette possibilité. Cela est d'autant plus préoccupant que la XR brouille les lignes entre les expériences virtuelles et réelles d'une manière qui peut être particulièrement efficace pour influencer les consommateurs¹⁰.

Deuxièmement, les casques de XR sont intrinsèquement conçus pour traiter des données au sujet de ceux qui se trouvent autour des utilisateurs, bien souvent sans que ces tierces parties n'y aient consenti. Les appareils XR sont équipés de caméras externes et de capteurs qui scannent l'environnement de l'utilisateur pour créer une carte numérique des espaces environnants. Lorsqu'une personne se trouve dans le champ de vision de l'appareil, le casque traite les données sur cette personne, sans prêter attention au fait qu'elle y consente ou non. Dans le cas du casque Vision Pro d'Apple, par exemple, la fonctionnalité de "détection des personnes" détecte activement les personnes dans l'environnement de l'utilisateur et les affiche sur l'écran intégré, de manière à ce que l'utilisateur puisse interagir avec elles sans avoir à retirer le casque Vision Pro. Plusieurs des intervenants interviewés ont soulevé que cela créait une tension relativement inédite, puisque le consentement est la pierre angulaire des lois canadiennes sur la protection des renseignements personnels, et que la prise en compte des tierces parties est une composante essentielle des systèmes de XR.

⁷ Apple, "[Redo Eye and Hand Setup on your Apple Vision Pro](#)", online: *Apple Vision Pro User Guide*.

⁸ Brittan Heller, "[Revisiting Code as Law: Regulation and Extended Reality](#)" (1 September 2023) at 6, online.

⁹ Nelson Reed & Katie Joseff, "[Kids and the Metaverse: What Parents, Policymakers, and Companies Need to Know](#)" (2022) at 1, online (pdf): *Common Place*.

¹⁰ Clifford Nass, BJ Fogg & Youngme Moon, "[Can Computers Be Teammates?](#)" (December 1996) 45:6 Intl J Human-Computer Studies 669.

3. Le droit canadien protège-t-il bien les utilisateurs de XR?

En matière de vie privée et de protection des renseignements personnels, le droit canadien a des allures de courtepoinette. Plusieurs lois différentes peuvent s'appliquer selon le contexte. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) régit le traitement des données dans le secteur privé. Or, l'Alberta, la Colombie-Britannique et le Québec ont des lois provinciales qui s'appliquent à sa place dans certains contextes. Par ailleurs, la LPRPDE est vraisemblablement sur le point d'être remplacée par la *Loi sur la protection de la vie privée des consommateurs* (LPVPC), qui est en quelque sorte une version mise à jour de la LPRPDE.

Il s'agit d'un processus de réforme qui est en cours depuis plusieurs années déjà.

En septembre 2020, le gouvernement a déposé le projet de loi C-11, qui aurait promulgué la *Loi sur la protection de la vie privée des consommateurs* et la *Loi sur le Tribunal de la protection des renseignements personnels et des données*. Or, le projet de loi est mort au feuilletton après qu'une élection ait été déclenchée. Plus tard, en novembre 2022, le gouvernement a récidivé avec le projet de loi C-27 édictant la LPVPC et la *Loi sur le Tribunal de la protection des renseignements personnels et des données*. Le Comité permanent de l'industrie et de la technologie de la Chambre des communes a tenu plusieurs séances d'études du projet de loi en 2024. Toutefois, compte tenu du contexte politique actuel, il est possible que le C-27 tombe lui aussi dans la désuétude.

Le présent rapport se concentre principalement sur deux textes législatifs : la LPRPDE et la LPVPC. Ce sont les deux instruments juridiques les plus pertinents en ce qui a trait à la XR car les principaux fournisseurs de XR sont des entreprises privées basées à l'étranger qui relèvent donc du régime fédéral régissant le secteur privé. Comme la plupart des lois modernes sur la protection des données, la LPRPDE et la LPVPC tirent leur origine des "Fair Information Practices". Elles appartiennent donc à une famille de lois sur la protection des renseignements personnels qui définissent la vie privée comme étant la capacité d'un individu à contrôler la manière dont circulent ses renseignements personnels. Par conséquent, comme la plupart des lois modernes sur la protection des données, ces deux lois accordent une importance cruciale au principe du consentement.

En effet, le consentement est le pilier du régime fédéral actuel du secteur privé. Tant qu'elles ne traitent pas des renseignements personnels à des fins inappropriées, les organisations soumises à la LPRPDE peuvent collecter, utiliser et partager des informations personnelles comme elles le souhaitent si elles ont obtenu un consentement éclairé pour le faire¹¹. Si la LPVPC venait à remplacer la LPRPDE, le principe du consentement demeurerait la règle par défaut pour légitimer le traitement des renseignements personnels. Son importance serait toutefois un peu diluée par l'introduction de deux exceptions au principe du consentement :

¹¹ *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c 5, s 5 [PIPEDA].

l'exception relative aux « intérêts légitimes » et l'exception relative aux « activités commerciales¹². » Si la LPVPC venait à être adoptée, les organisations pourraient collecter ou utiliser les renseignements personnels des utilisateurs sans leur consentement si elles arrivaient à s'inscrire dans ces deux exceptions. Dans le cas de la XR, on pourrait penser à des traitements nécessaires pour faire fonctionner le casque, ou encore à des traitements nécessaires pour assurer la sécurité de l'information. Une organisation pourrait aussi traiter les renseignements personnels d'un utilisateur sans son consentement si cela est fait dans l'intention d'atteindre un objectif pour lequel l'organisation a un « intérêt légitime » qui l'emporte sur les effets néfastes potentiels pour l'utilisateur¹³. La collecte ne peut toutefois pas être utilisée pour influencer le comportement de l'utilisateur dans le cadre de cette exception. Il importe également de souligner que la LPVPC change la façon dont le consentement est interprété et appliqué. La nouvelle loi exigerait l'utilisation du « langage clair » dans les formulaires de consentement, par exemple. Tout d'abord, cet ajout semble être une avancée. Or dans les faits, cette nouvelle obligation est moins stricte que ce que la LPRPDE exige. Maintenant que nous avons brièvement brossé le portrait du paysage législatif en matière de protection des renseignements personnels au Canada, nous pouvons amorcer de notre analyse de LPRPDE et de la LPVPC afin de mieux déterminer si elles arrivent à bien protéger la vie privée des personnes interagissant avec la XR.

3.1. La LPRPDE – La loi qui régit actuellement le traitement des données dans le secteur privé

La LPRPDE n'est plus en phase avec les réalités technologiques d'aujourd'hui. Elle ne parvient pas à réglementer correctement l'univers numérique. Pour s'en convaincre, il suffit de se rappeler du refus de la cour fédérale de sanctionner Facebook pour son rôle dans le scandale Cambridge Analytica¹⁴. Ou encore de penser à l'incapacité de tenir Clearview AI responsable pour les activités de surveillances de masse dans lesquelles la compagnie s'est engagée¹⁵. Ce sont deux exemples qui témoignent de l'insuffisance de la LPRPDE. Puisque le Parlement travaille actuellement à réformer la loi fédérale régissant la protection des renseignements personnels dans le secteur privé, nous avons choisi de ne pas trop mettre l'accent sur les lacunes de la LPRPDE dans ce rapport. Nous nous servirons plutôt de la loi actuelle comme d'un étalon de mesure pour évaluer la LPVPC. Il s'agira ainsi de déterminer si la réforme proposée permet véritablement d'assurer une meilleure protection de la vie privée des Canadiens.

Il est important de se poser la question puisque, selon Chantale Bernier, les principes de PIPEDA sont généralement adéquats. Ils sont suffisamment larges pour s'appliquer à la XR. Bien sûr, il serait pertinent de moderniser certains principes pour les rendre plus spécifiques à certains aspects techniques qui ont évolué depuis l'adoption de la loi—la biométrie par exemple. Or, de manière générale, les principes de la LPRPDE sont rédigés de manière

¹² Bill C-27, *The Consumer Privacy Protection Act*, 1st Sess, 44th Parl. 2022, s 18(2) (first reading 16 June 2022) [CPPA].

¹³ *Ibid.*, at s 18(3).

¹⁴ *Facebook*, *supra* note 6.

¹⁵ *Doan v Canada (Attorney General)*, 2023 FC 236.

technologiquement neutre, ce qui permet à la loi de rester pertinente malgré les évolutions technologiques.

Pour illustrer l'applicabilité de la LPRPDE à la XR, Bernier donne deux exemples concrets. Elle met aussi de l'avant quelques modifications mineures qui amélioreraient la protection offerte par PIPEDA aux Canadiens interagissant avec les technologies XR.

Le premier exemple concerne l'utilisation de la réalité virtuelle pour traiter le trouble de stress post-traumatique. En vertu de PIPEDA, une entreprise offrant ce type de service serait soumise à des exigences accrues en matière de consentement et de mesures de sécurité, car les renseignements personnels de santé sont sensibles¹⁶. Par conséquent, le consentement pour le traitement des données devrait être exprès, et les mesures pour assurer la sécurité des données devraient être plus élevées que ce qui serait normalement requis pour d'autres types de renseignements personnels¹⁷. De plus, comme toute autre entreprise traitant des données, une organisation qui offrirait des services de thérapie mobilisant la réalité virtuelle devrait également limiter sa collecte, sa rétention et son utilisation de renseignements personnels à ce qui est strictement nécessaire pour atteindre ses objectifs.¹⁸

Dans la mesure où ces principes étaient respectés, la LPRPDE serait en mesure d'offrir une protection adéquate de la vie privée des Canadiens. Or, c'est là où le bât blesse avec la LPRPDE. Ce n'est pas nécessairement que les règles de fond ne sont pas suffisantes, mais plutôt que les principes sont difficiles à faire respecter. Pour garantir que les entreprises soient transparentes sur la sécurité, la rétention et l'utilisation des données qu'elles traitent, Bernier suggère de donner des pouvoirs d'audit au gouvernement. Elle recommande également d'inscrire plus clairement dans la législation la relation entre la sensibilité des données et la rigueur des exigences légales, afin que les entreprises connaissent clairement leurs obligations.

Le deuxième exemple abordé par Bernier porte sur les mineurs et l'utilisation de XR à des fins de divertissements. Bernier n'est pas opposée à ce que les entreprises comme Apple traitent des renseignements personnels concernant les enfants utilisant cette technologie. Cependant, puisque les enfants ont une capacité réduite à donner un consentement éclairé, elle suggère que les entreprises devraient demander le consentement des parents pour traiter les données de leurs enfants. D'ailleurs, c'est plus ou moins ce que PIPEDA exige déjà. En effet, dans ses lignes directrices pour obtenir un consentement valable, le Commissariat à la protection de la vie privée du Canada (CPVP) dit que, sauf circonstances exceptionnelles, les enfants de moins de 13 ans ne peuvent pas consentir au traitement de leurs données¹⁹. En ce qui concerne les mineurs entre 13 et 18 ans, les lignes directrices prévoient que les organisations traitant des informations personnelles doivent adapter leur demande de consentement au niveau de maturité

¹⁶ *Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96, being Schedule 1 to PIPEDA, supra note 11, at ss 4.3, 4.7.

¹⁷ *Ibid.*, at ss 4.3.6, 4.7.2.

¹⁸ *Ibid.*, at s 4.4.

¹⁹ Office of the Privacy Commissioner of Canada, "[Guidelines for obtaining meaningful consent](#)" (2021) online: *Office of the Privacy Commissioner of Canada*.

des utilisateurs avec lesquels elles interagissent²⁰. Selon Bernier ces exigences devraient être clarifiées et intégrées explicitement dans la loi.

Étant donné que l'enfance est une période charnière où l'on forge sa personnalité, Bernier suggère également que les entreprises qui offrent des services de XR évitent de stocker les informations qu'elles collectent sur leurs jeunes utilisateurs sur leurs propres serveurs. Elles ne devraient stocker seulement les données qui sont véritablement nécessaires au fonctionnement du système XR, et elles devraient supprimer les données dès qu'elles ne servent plus les objectifs pour lesquels elles ont été collectées.

Enfin, certains types de traitement de données associés à la XR qui ne sont ni nécessaires ni proportionnés ne devraient tout simplement pas être autorisés pour les enfants. Bien que la LPRPDE ne contienne aucune disposition explicite à ce sujet, la manière dont elle a été appliquée au fil des ans est cohérente avec cette idée. Par exemple, le Commissariat à la protection de la vie privée a jugé que Nexopia ne s'était pas conformé adéquatement à la LPRPDE puisqu'elle avait programmé son réseau social pour que les profils de ses utilisateurs soient « visibles de tous » par défaut. Le CPVP a considéré que cela n'était inapproprié pour un réseau social destiné aux jeunes²¹. En résumé, l'intervention de Bernier permet de mettre en lumière le fait que la LPRPDE n'est pas aussi insatisfaisante qu'on tend à le croire. Du moins, sur le plan des principes substantifs. Il n'en demeure pas moins que certains éléments – l'âge du consentement et les zones interdites – pourraient bénéficier de clarifications.

3.2. La LPVPC – La loi proposée pour régir le traitement des renseignements personnels dans le secteur privé

La LPVPC n'est pas une refonte complète de la LPRPDE, il s'agit plutôt d'une version modernisée des principes qui sont déjà en vigueur. Par exemple, si le projet de loi édictant la LPVPC est adopté, le consentement restera la base du régime de protection des données au Canada. Or, certaines modifications seront apportées pour faciliter son application et son exécution. Cette mise à jour du régime de protection des renseignements personnels nous incite à nous interroger à savoir si la nouvelle version de la loi protégera adéquatement la vie privée des Canadiens. Pour la plupart des intervenants que nous avons interviewés, la réponse est non.

Lors de nos entretiens, plusieurs personnes ont exprimé des préoccupations concernant une loi qui demeurerait trop axée sur le principe du consentement. Selon Jane Bailey et Jacquelyn Burkell, le consentement est mal adapté pour régir les technologies XR compte tenu de la nature relationnelle de l'information. Le fait qu'une personne consente n'est pas suffisant pour bien protéger la vie privée de tous, car le consentement d'une personne a des répercussions sur la vie privée des autres également. En effet, comme mentionné précédemment, les casques de XR collectent des données sur ceux qui se trouvent autour des utilisateurs. Et ceux-ci n'ont aucun réel moyen de s'opposer à la collecte de leurs informations—ils peuvent même ne pas en être conscients. Cela affecte leur autonomie et leur dignité en les privant de la capacité de contrôler la manière dont leurs renseignements personnels sont collectés et partagés. Par ailleurs, étant

²⁰ *Ibid.*

²¹ *Nexopia*, (February 2013) PIPEDA Report of Findings #2012-001, online.

donné le progrès rapide des technologies et de la nature permanente des données²², il est devenu presque impossible de donner un consentement véritablement éclairé, puisque personne ne sait vraiment ce que l'avenir nous réserve. Bailey illustre le problème avec un exemple frappant : jusqu'à tout récemment, les gens publiaient des photos de leurs enfants sans être trop craintifs. Publier une photo de son enfant sur Facebook n'était pas considérée comme une activité particulièrement risquée. Or, de nos jours, les risques sont plus grands. Une photo d'enfance peut être réutilisée à des fins qui étaient impensables il y a quelques années. Un acteur malveillant pourrait réutiliser cette photo pour créer un "deep fake" pornographique, par exemple. Dans un monde où les technologies évoluent à un rythme effréné et où le futur est difficile à imaginer, les lois de protection des renseignements personnels fondée sur le consentement ne sont plus suffisantes.

C'est également la conclusion de Valérie Steeves, qui suggère de délaisser les approches fondées sur le consentement au profit d'approches axées sur les droits de la personne, qui sont plus ancrées dans les valeurs sociales et démocratiques de la vie privée. Elle croit que la vie privée serait mieux protégée avec des instruments juridiques qui mobilisent le langage des droits fondamentaux car cela permettrait aux tribunaux d'interpréter ces textes souples lorsqu'ils seraient confrontés à de nouvelles situations. Ainsi, elle suggère que la LPRPDE inclue des engagements clairs en matière de droits de la personne.

Poursuivant dans la même veine, Leslie Regan Shade offre des illustrations concrètes de ce à quoi pourrait ressembler l'inclusion d'engagements clairs en matière de droits de la personne dans la LPVPC. Premièrement, elle souligne que la vie privée est un droit humain protégé par les instruments internationaux de droit des droits de l'homme, et elle devrait être reconnue comme telle à la fois dans le préambule de la loi, et dans la disposition qui prévoit quel est son objet²³. Deuxièmement, le Canada a le devoir d'incorporer l'intérêt supérieur de l'enfant dans la législation et les politiques en vertu de la Convention relative aux droits de l'enfant. Pour se conformer à cette obligation, le gouvernement devrait modifier la disposition sur les mineurs²⁴ pour indiquer que l'intérêt supérieur de l'enfant est une considération primordiale pour toutes les questions affectant les mineurs.

Cela renforcerait le reste de la loi. Par exemple, le fait d'intégrer clairement l'intérêt supérieur de l'enfant dans la loi aurait un impact sur la manière dont les tribunaux interprètent la disposition relative aux « fins acceptables »²⁵ de la LPVPC. Cela constituerait une véritable avancée par rapport à l'article 5(3) de la LPRPDE qui ne peut bénéficier d'une interprétation large et libérale car l'objet de la loi actuelle est d'établir l'équilibre entre les intérêts commerciaux et la protection des droits des utilisateurs²⁶. Concrètement, une mention de l'intérêt supérieur de l'enfant faciliterait la tâche du CPVP dans des situations où il aurait à juger de la légitimité de certaines utilisations de renseignements personnels concernant les

²² Coined by Wendy Wong. It illustrates that once the data is collected, it's never truly possible to get rid of it. Wendy Wong, *We, the Data, Human Rights in the Digital Age* (Cambridge, Ma: MIT University Press, 2023).

²³ CPPA, *supra* note 12 at s 5.

²⁴ *Ibid*, at at s2(2).

²⁵ *Ibid*, at s 12.

²⁶ *Facebook*, *supra* note 6 at [para 50](#).

enfants par exemple, interdire le traitement des renseignements personnels des enfants à des fins de publicités ciblées.

Les interdictions totales de certains types de traitement de données sont parfois appelées "zones interdites". Presque tous nos interviewés ont mentionné que ces interdictions seraient une addition bienvenue à la LPVPC. Certains ont suggéré que cela soit fait par le biais de dispositions générales soutenues par des principes interprétatifs ancrés dans les principes de droits fondamentaux, d'autres ont plutôt suggéré une liste codifiée énonçant clairement quels sont les types de traitement de renseignements personnels interdits. Or, la plupart des intervenants rencontrés étaient en faveur de l'idée d'interdire certains types d'utilisation renseignements personnels traités dans le contexte de la XR.

Avoir des « zones interdites » s'inscrirait bien dans le virage préventif que le gouvernement prend avec la LPVPC. Plutôt que de s'en remettre uniquement aux sanctions a posteriori, la LPVPC met en place des mesures pour prévenir les dommages. Principalement, la nouvelle loi exigerait que les entreprises documentent les choix qu'ils font en matière de protection des renseignements personnels. Par exemple, pour traiter des informations personnelles sans consentement en vertu de l'exception de « fins acceptables »²⁷, les organisations doivent établir et consigner l'objectif pour lequel elles souhaitent traiter les données. Pour collecter des informations en vertu des exceptions « d'intérêt légitime »²⁸, les organisations doivent réaliser une évaluation des impacts sur la vie privée. En obligeant les organisations à réfléchir explicitement aux choix qu'ils font en matière de vie privée, et en les incitant à les documenter par écrit, la loi cherche à inciter les organisations à agir de manière plus responsable. Le fait d'avoir des traces écrites permet également de faciliter les enquêtes et d'agir plus efficacement lorsque vient le moment de sanctionner les organisations qui sont négligentes en matière de vie privée.

Ce genre de mesure qui s'inscrit dans une logique de « privacy-by-design » semblait rallier la plupart des intervenants interviewés. Par exemple, selon Chantale Bernier, les évaluations des impacts sur la vie privée peuvent être très utiles pour déterminer l'étendue des protections de la vie privée nécessaires pour une certaine technologie. Elles permettent également de s'assurer que les impacts négatifs d'une technologie ne dépassent pas ses avantages. À ce propos, Valérie Steeves souligne qu'il serait intéressant que des chercheurs développent des méthodes claires qui pourraient aider les acteurs de l'industrie à réfléchir aux impacts des technologies qu'ils développent sur les droits fondamentaux. Il semble que les acteurs de l'industrie seraient d'ailleurs preneurs de telles méthodes. En effet, lors de nos entrevues avec les acteurs impliqués dans le développement de technologie XR, Caroline Dupuis et Matthew Sherdown ont mentionné qu'ils apprécieraient avoir plus de directives de la part du Commissaire à la protection de la vie privée quant à la manière d'aborder les enjeux de vie privée découlant de nouvelles technologies comme la XR.

²⁷ CPPA, *supra* note 12 at s 12(1).

²⁸ *Ibid*, at s 18(3).

4. Recommandations – Que propose CIPPIC ?

L'évolution rapide des technologies XR nécessite un cadre robuste qui protège la vie privée des utilisateurs, notamment celle des groupes vulnérables tels que les enfants et les adolescents. L'intégration des technologies XR dans la vie quotidienne présente des défis et des opportunités uniques pour la protection de la vie privée. Pour naviguer dans ce terrain complexe, ce rapport propose un ensemble complet de recommandations visant à renforcer les garanties de confidentialité, à améliorer les mesures réglementaires et à favoriser un environnement d'utilisation informée et consciente des technologies XR. Nous offrons ces recommandations pour aborder la nature multifacette des préoccupations en matière de vie privée dans les XR, et ce, depuis sa phase de développement jusqu'à son utilisation quotidienne. Notre approche protège la vie privée et maintient les normes plus élevées pour les utilisateurs canadiens sans freiner l'innovation dans la technologie XR.

La technologie XR pose des problèmes de confidentialité multifacettes et la seule réglementation juridique ne suffit probablement pas à les résoudre. La CIPPIC recommande plutôt une approche multimodale, comme décrite par Lawrence Lessig dans son livre publié en 2006, *Code : Version 2.0*²⁹. Dans *Code*, Lessig identifie quatre types de régulation comportementale dans le cyberspace : la loi, les normes sociales, le marché et la technologie³⁰. Ces quatre types de régulation jouent des rôles différents dans le cyberspace.

La loi menace des conséquences pour ceux qui la défient³¹. **Les normes sociales** menacent des sanctions communautaires pour ceux qui transgressent les normes acceptables³². **Le marché** limite l'accès par les structures de prix et l'économie³³. **La technologie** limite les logiciels et le matériel pour rendre certains comportements possibles ou impossibles³⁴.

Aucune approche réglementaire unique ne peut pleinement résoudre les problèmes de confidentialité posés par les technologies XR. Des approches qui traitent toutes les quatre régulateurs comportementaux, en s'appuyant fortement sur les normes sociales et les approches juridiques, sont nécessaires³⁵. L'éducation et l'autonomisation peuvent influencer la façon dont les gens perçoivent la confidentialité individuelle et la collecte acceptable de données, créant des normes sociales qui soutiennent une régulation plus stricte. Les utilisateurs cherchant à acheter de la technologie XR doivent être conscients des applications et des dispositifs qui respectent le mieux leurs droits en matière de vie privée, afin qu'ils puissent choisir l'entreprise qui répond le mieux à leurs attentes en matière de confidentialité. Bien qu'Apple ait déjà commencé à intégrer des limites technologiques sur les capacités des appareils XR avec son

²⁹ Lawrence Lessig, *Code: Version 2.0*, 2nd ed (New York: Basic Books, 2006) at 123; see also Brittan Heller, *supra* note 8.

³⁰ *Ibid* at 123.

³¹ *Ibid* at 124.

³² *Ibid*.

³³ *Ibid*.

³⁴ *Ibid* at 125.

³⁵ *Ibid*; see also Heller, *supra* note 8.

Vision Pro, des directives plus strictes doivent être mises en œuvre et être plus largement acceptées pour affecter le marché.

4.1. La Loi - Adopter une lecture intentionnelle de la LPRPDE et amender la LPVPC

Il est clair que les XR nécessitent une réglementation plus stricte. La CIPPIC propose trois approches juridiques directes pour traiter l'implication des technologies XR dans la collecte, l'utilisation et le partage des renseignements personnels : (1) interpréter l'exigence actuelle du consentement éclairé de la loi pour inclure des versions actives et informées du consentement opt-in; (2) convoquer une consultation pour le développement d'un document de lignes directrices coréglementaires qui informera l'application de la loi actuelle ; ou (3) amender le projet de loi C-27 pour tenir compte des défis spécifiques des technologies XR.

(1) L'interprétation de la LPRPDE : Le Commissariat à la protection de la vie privée (CPVP) pourrait interpréter la LPRPDE de manière à exiger un consentement explicite avec une explication détaillée de l'utilisation prévue des données par la plateforme. La LPRPDE est un cadre basé sur le consentement. Dans ce modèle, les organisations doivent obtenir le consentement éclairé des utilisateurs pour collecter, utiliser et divulguer leurs renseignements personnels. Les dispositifs XR accumulent de grands volumes de données de leur utilisateur, leur environnement et des tiers observateurs pour fonctionner à un niveau de base. Étant donné l'ampleur et les types de données collectées par la technologie XR, obtenir un consentement éclairé est impossible selon l'interprétation actuelle de la LPRPDE. Cependant, comme l'a déclaré Chantal Bernier, la LPRPDE est une loi basée sur des principes qui peut être interprétée dans son contexte. Les technologies XR collectent des informations sensibles au temps, soit intrinsèquement (enfants, biométriques, etc.) ou soit par leur contexte inattendu (effet observateur). Le CPVP pourrait, par un Bulletin d'interprétation, signaler que le Commissaire planifie interpréter la LPRPDE de manière à exiger un consentement explicite et opt-in. Cela exigerait la présence d'une explication détaillée de l'intention de la plateforme permettant une évaluation réfléchie de cette dernière (et non, par exemple, pendant le jeu). Cette approche éliminerait effectivement la collecte d'informations sur les observateurs puisqu'il est impossible d'obtenir leur consentement éclairé. Cela nécessiterait également des approches réfléchies pour engager les enfants, puisqu'il est impossible d'obtenir un consentement éclairé de ceux-ci.

(2) Lignes directrices coréglementaires : En vertu de la loi actuelle, le CPVP pourrait adopter ce qui est en fait un modèle « coréglementaire ». Le CPVP pourrait convoquer une consultation parmi les parties prenantes dans l'espace technologique XR pour trouver un consensus face aux exigences actuelles de la loi pour les acteurs commerciaux dans ce contexte. Le CPVP pourrait alors utiliser cette consultation pour préparer des lignes directrices d'interprétation qui instruiraient les fabricants de technologies XR et les développeurs d'applications sur la façon dont le Commissaire entend appliquer la LPRPDE. Cette approche pourrait résoudre plusieurs des problèmes de confidentialité légale identifiés.

(3) Amendements du projet de loi C-27 : Les problèmes de confidentialité liés aux technologies XR pourraient également être abordés par l'amendement du projet de loi C-27, la LPVPC. Bref, des recommandations similaires ont été soumises au Parlement concernant le

projet de loi C-27. La LPVPC devrait définir les « renseignements sensibles » comme étant des informations pour lesquelles un individu aurait des attentes de confidentialité accrues ou dont la divulgation aurait des risques de nuire à l'individu. Cela peut inclure des données de santé, biométriques et génétiques, ainsi que les renseignements personnels des mineurs. En procédant ainsi, elle couvre la large gamme d'informations que les dispositifs XR collectent sur les utilisateurs. Cela devrait être couplé à des mesures de protection substantielles pour garantir que les organisations prennent en compte les risques de confidentialité inhérents à la collecte et à l'utilisation de ces informations³⁶.

Les amendements à la LPVPC devraient également mettre les individus au centre du consentement et de ses exceptions. Cela pourrait être exécuté en garantissant que le consentement des utilisateurs soit significatif, et ce, en légiférant une exigence visant à s'assurer qu'il soit raisonnable que les utilisateurs comprennent directement ce qui leur est demandé. Il convient de noter que la LPRPDE prévoyait une telle norme dans l'article 6.1, mais la LPVPC semble appliquer une norme moins stricte dans l'article 15(4), qui oblige seulement l'organisation à fournir l'information dans un « langage clair » dont l'individu serait raisonnablement censé comprendre. Cela pourrait également être réalisé en supprimant la capacité d'imputer le consentement et en augmentant la transparence autour des exceptions entourant le consentement. Cela permettrait de répondre aux préoccupations accrues concernant la collecte et le partage des données avec les technologies XR.

Troisièmement, certaines préoccupations en matière de confidentialité autour des XR peuvent également être abordées en renforçant les protections pour la confidentialité des enfants dans la LPVPC. L'intérêt supérieur de l'enfant devrait être la principale préoccupation des entreprises fournissant des services en ligne aux enfants. Cela pourrait se refléter dans la section des définitions de la législation. De plus, il devrait y avoir une exigence selon laquelle les paramètres de confidentialité soient par défaut « élevés » pour les enfants. Cela adresserait spécifiquement leur vulnérabilité et les protégerait contre la collecte, l'utilisation et la divulgation de leurs données biométriques. La LPVPC n'a pas été promulguée au moment de la rédaction. L'occasion est propice pour apporter des amendements conséquents qui traiteront des préoccupations de confidentialité liées aux technologies XR émergentes et protégeront les données des Canadiens.

4.2. Les normes sociales – Besoin de plus d'éducation face à la confidentialité

L'éducation face à la confidentialité est essentielle pour réguler la vie privée dans les espaces XR. Le CPVP peut aider en préparant des matériels éducatifs axés sur les utilisateurs, mais aussi sur les fabricants de technologies XR et les développeurs d'applications, ce que les parties prenantes de l'industrie privée ont déclaré être utile lors des entretiens avec le CIPPIC.

Les utilisateurs sont souvent décontractés lorsqu'il s'agit de confidentialité avec les plateformes XR. Des documents dédiés du CPVP éduquant les utilisateurs sur leur droit à la vie privée dans les XR et les mesures qu'ils peuvent prendre pour limiter les intrusions des entreprises XR

³⁶ The House of Commons INDU committee appears to have passed a similar amendment during its clause-by-clause review of the legislation at its May 22 meeting. This is a positive development as the definition includes information about an individual that reveals core characteristics, such as race, political opinions, sexual orientation, genetic data, government identifiers, etc. The definition includes information on individuals' health conditions and any treatment or prescriptions they are receiving. -- House of Commons, Standing Committee on Industry and Technology, *Evidence*, 44-1, No 124 (22 May 2024) at 16:03 (Joël Lightbound)

peuvent aider à répondre à cette préoccupation. Des documents distincts pour les adultes ainsi que les enfants et leur incapacité à fournir un consentement éclairé seraient particulièrement utiles. L'Institution d'Ingénierie et de Technologie estime que parmi les parents dont les enfants interagissent déjà avec la VR, plus de 25% ne savent pas dans quels types de mondes leurs enfants se trouvent, et plus de 60% ne comprennent rien au métavers³⁷. Cela étant dit, même les utilisateurs matures ont besoin de plus de ressources dédiées et dignes de confiance ce dont le CPVP est le mieux placé pour en fournir. Les acteurs commerciaux ont également besoin d'une éducation à la confidentialité et la charge ne doit pas reposer complètement sur les utilisateurs. Le CPVP peut fournir cette orientation éducative sous forme de bulletins d'interprétation, de documents d'orientation, de fiches techniques, ainsi que par des engagements publics dans les médias, lors de conférences et même devant les législateurs. Les initiatives éducatives du CPVP peuvent influencer à la fois la conception et le déploiement des technologies XR.

Enfin, l'application de la LPRPDE elle-même contre les contrevenants a une influence puissante sur les normes sociales et les comportements sur le marché. En vertu de la LPRPDE, le Commissaire à la protection de la vie privée est à la fois un ombudsman, promouvant la conformité à la loi et un exécuter, enquêtant et se prononçant sur les violations, les portant même devant les tribunaux pour application. L'application peut être un outil efficace pour promouvoir la conformité et changer les normes. Lorsque la société dans son ensemble voit le CPVP prendre des mesures contre les contrevenants à la LPRPDE et appliquer des conséquences réelles pour les violations, ils sont plus susceptibles de suivre la loi et de se conformer à la législation. Cela crée une nouvelle norme sociale où ceux du marché sont plus enclins à protéger la vie privée des utilisateurs, car ils voient que les échecs entraînent des conséquences.

4.3. Le marché - Introduire un système de notation de la confidentialité

Le CPVP pourrait envisager introduire un système de notation pour les dispositifs et applications XR. Cela permettrait aux utilisateurs de décider comment dépenser leur argent. Les utilisateurs de XR n'ont actuellement aucune norme à suivre et il existe une grande variété de choix sur le marché. Le Commissariat à la protection de la vie privée publie actuellement des lignes directrices sur de nombreuses technologies de confidentialité, mais n'évalue pas les concurrents du marché quant à leur conformité à ces lignes directrices. Le faire donnerait plus de pouvoir à ces documents, promouvrait la concurrence sur la confidentialité, et faciliterait aux consommateurs l'exercice de leur pouvoir de confidentialité sur le marché. Des programmes similaires existent déjà dans d'autres industries. Par exemple, l'*Environmental Working Group* a son propre système de notation pour savoir à quel point un produit de beauté est « naturel » afin d'aider les utilisateurs à identifier les problèmes tels que les matériaux cancérigènes, les allergènes et diverses toxicités³⁸. Dans ce système, les utilisateurs qui priorisent la beauté naturelle peuvent investir leur argent dans des produits qui répondent à une certaine norme. Certaines entreprises dans les XR sont plus orientées vers la confidentialité

³⁷ The Institution of Engineering and Technology, Press Release, "[Generation VR](#)" (19 April 2022) online.

³⁸ The Environmental Working Group, "[Understanding Skin Deep® Ratings](#)", online: *EWG's Skin Deep*.

que d'autres. Par exemple, le Vision Pro d'Apple stocke autant de données que possible sur l'appareil de l'utilisateur sans les partager avec des tiers. En revanche, Meta stocke les données des utilisateurs sur la sauvegarde « cloud » de l'Oculus, une approche du stockage des données moins respectueuse de la vie privée puisque l'utilisateur a moins de contrôle sur les données et qu'elles sont plus vulnérables à une violation. Un système de notation de la confidentialité peut aider les consommateurs à décider rapidement quel produit est le meilleur pour eux. En fin de compte, si les individus achètent des produits auprès d'entreprises XR ayant des normes de confidentialité plus élevées, d'autres entreprises sur le marché peuvent adopter des normes de confidentialité plus élevées en réponse.

4.4. La technologie – Promouvoir la confidentialité par conception

La technologie fonctionne comme un régulateur en permettant ou en interdisant certains comportements par les capacités de la technologie elle-même. Bien que le CPVP ne soit pas un développeur de technologie, il peut influencer la manière dont la technologie se développe et comment les entreprises la déploient en développant des documents de meilleures pratiques, des documents d'orientation et des bulletins d'interprétation. Par exemple, une orientation exigeant l'adoption de règles de confidentialité par conception dans le développement et le déploiement de technologies pourrait aider à résoudre les préoccupations en matière de confidentialité, et ce, même au niveau du dispositif. Identifier les normes de confidentialité auquel le marché canadien devrait adopter pourrait également encourager l'adoption de technologies plus respectueuses de la vie privée. Les entreprises XR sont dans une position unique pour répondre aux préoccupations de confidentialité des utilisateurs. Bien que les programmes XR nécessitent certaines données pour fonctionner, les entreprises peuvent contrôler qui a accès à ces données et comment elles sont stockées. Elles peuvent contrôler les circonstances dans lesquelles un utilisateur satisfait des demandes de collecte, d'utilisation et de partage des données. Par exemple, Apple a déjà des limites intégrées sur l'accès des tiers aux données des utilisateurs avec son Vision Pro, mais peut encore améliorer ses normes de confidentialité, en particulier en ce qui concerne les jeux destinés aux enfants. En raison des préoccupations uniques qui surviennent avec les enfants, Apple pourrait mettre en œuvre un mécanisme de contrôle parental spécifique permettant aux parents de contrôler les jeux que leurs enfants peuvent télécharger sur l'appareil et limiter les données que les tiers peuvent demander dans le jeu.

Le CPVP pourrait également envisager d'adopter un modèle d'application « se conformer ou expliquer », obligeant les entreprises à justifier pourquoi elles ne respectent pas une norme de confidentialité. Le modèle pourrait être similaire à celui du Commissaire aux valeurs mobilières, qui oblige les entreprises à se conformer aux normes de divulgation de la diversité du commissaire, ou à expliquer leurs échecs de conformité et à risquer une action coercitive³⁹.

³⁹ Andrew Pollock, "[Canadian Securities Administrators Propose Enhanced Diversity Disclosure](#)", Norton Rose Fulbright (19 April 2023).

Conclusions

Le développement et le déploiement des technologies XR présentent des défis uniques en matière de confidentialité, mais offrent également une opportunité de développer un cadre réglementaire innovant qui répond aux défis actuels en matière de confidentialité tout en accommodant l'innovation technologique. Ce type de cadre nécessite un dialogue entre les décideurs politiques, les leaders de l'industrie, les défenseurs de la confidentialité et les consommateurs pour s'assurer qu'un engagement envers la confidentialité, les considérations éthiques et le respect de l'autonomie individuelle guide la régulation.

Avec les technologies XR franchissant les frontières internationales, le Canada pourrait fournir un cadre de protection de la confidentialité que d'autres juridictions pourraient répliquer. L'éducation et la sensibilisation sont également des composants clés de notre approche proposée. Le Canada peut cultiver une société plus consciente de la confidentialité en informant le public des implications des technologies XR sur la vie privée et en équipant les individus des outils nécessaires pour naviguer dans ce nouveau terrain numérique. Cela inclut le développement de ressources pour les parents et les éducateurs afin de protéger la confidentialité des enfants dans les environnements XR. Investir dans la recherche et le développement pour explorer les technologies améliorant la confidentialité et les méthodes pour XR est une autre étape cruciale. Ce mouvement stratégique pourrait ouvrir la voie à des innovations permettant de profiter des XR de manière plus sécurisée et respectueuse de la vie privée, sans compromettre les données personnelles. Un cadre complet de confidentialité pour les technologies XR nécessite une législation proactive, un engagement solide entre les secteurs public et privé, une éducation publique et une innovation continue.

Annexe

Entretiens avec les parties prenantes – Processus de recrutement

La CIPPIC a contacté plusieurs chercheurs universitaires canadiens dont les travaux se concentrent sur la confidentialité des données des utilisateurs en préparation de cette étude. La CIPPIC a également contacté Chantal Bernier, ancienne commissaire à la protection de la vie privée du Canada et conseillère actuelle en matière de confidentialité et de sécurité chez Dentons⁴⁰, en raison de son expertise approfondie en matière de confidentialité et de cyber sécurité dans les secteurs public et privé. Un résumé de l'expertise professionnelle de tous les participants se trouve en annexe 1, page 43 ci-dessous. Tout nouveau partenaire mentionné par les personnes interrogées sélectionnées a été ajouté à la collecte d'entretiens si leurs collègues croyaient qu'ils pourraient apporter une expertise pertinente à ce projet. En conséquence, la CIPPIC a contacté deux autres chercheurs universitaires dont les travaux portent sur les aspects techniques des technologies XR (éthique et ingénierie ; technologies améliorant la confidentialité). Malheureusement, les tentatives de programmer des entretiens avec ces personnes supplémentaires n'ont pas abouti.

La collecte de personnes interrogées comprenait également des techniciens, des juristes et des responsables de la politique publique travaillant dans des entreprises fabriquant des technologies XR. Dix professionnels ont été contactés par courriel ou LinkedIn. Sur les dix professionnels contactés, trois ont répondu et ont été interrogés simultanément.

Enfin, la CIPPIC a contacté quatre organisations dédiées à la sécurité des enfants sur Internet. La CIPPIC a choisi ces organisations, car elles avaient publié des documents spécifiquement liés à la sécurité des enfants lors de l'utilisation des technologies XR. Parmi ces quatre organisations, une seule a répondu. L'organisation s'est engagée à une réunion initiale pour discuter de l'orientation et des objectifs du projet, mais ses priorités organisationnelles ne lui ont pas permis de répondre aux questions avant la date limite de ce rapport.

La CIPPIC a contacté les parties prenantes et les a informées que le Commissariat à la protection de la vie privée du Canada avait accordé une subvention au CIPPIC pour étudier les implications en matière de confidentialité des données collectées par les technologies XR, avec un accent particulier sur la confidentialité des enfants. La CIPPIC a informé les parties prenantes qu'il existait peu d'études évaluant la pertinence ou la suffisance des lois sur la confidentialité régissant les XR, et aucune étude n'avait abordé cette question d'un point de vue canadien. La CIPPIC a également informé les parties prenantes que la CIPPIC considérerait les lacunes potentielles des lois existantes ou proposées et identifierait les protections légales potentielles. La CIPPIC a informé les parties prenantes que le casque Vision Pro d'Apple était l'étude de cas principale pour la recherche de la CIPPIC.

⁴⁰ Pour plus d'informations, voir la [biographie](#) de Chantal Bernier publiée par l'Université d'Ottawa.

Le CIPPIC a sélectionné les parties prenantes pour participer à la recherche du CIPPIC car la littérature les identifiait comme un ensemble diversifié de spécialistes juridiques canadiens, de développeurs d'applications et d'autres personnes pouvant fournir une compréhension complète des implications de confidentialité des technologies XR. Les parties prenantes ont été informées que les informations recueillies lors de leurs entretiens joueraient un rôle essentiel dans la formation de l'analyse du CIPPIC, garantissant que le CIPPIC pourrait fournir une opinion complète sur les considérations de confidentialité associées aux technologies XR. Les parties prenantes ont été informées que les résultats de la recherche du CIPPIC seraient présentés au Commissariat à la protection de la vie privée du Canada, aux décideurs politiques, aux universitaires et au public avant leur participation. Ils ont également été informés que l'équipe de recherche du CIPPIC mènerait tous les entretiens par vidéoconférence et que l'entretien durerait environ une heure.

Lorsque les parties prenantes ont accepté de participer, elles ont reçu les détails de la réunion par vidéoconférence et un document contenant des informations sur le CIPPIC, un résumé du sujet et des objectifs du projet, la manière dont leurs réponses seraient utilisées et les questions auxquelles elles pourraient s'attendre à répondre pendant l'entretien.

Entretiens avec les parties prenantes – Biographies des participants

Partenaires académiques

Les quatre partenaires académiques participent au projet eQuality du Conseil de recherches en sciences humaines. Le professeur Steeves et le professeur Bailey codirigent l'organisation, et le professeur Shade et le professeur Burkell sont des chercheurs. Le projet « est dédié à la création de nouvelles connaissances sur l'utilisation des espaces connectés par les jeunes, avec un accent particulier sur les questions de confidentialité et d'égalité⁴¹. »

Professeur Jacquie Burkell est vice-présidente associée de la recherche à l'Institut de philosophie Rotman et professeure associée à la Faculté des études de l'information et des médias de l'Université Western. Ses recherches portent sur l'impact social de la technologie et examinent comment la médiation technologique modifie les interactions sociales et les comportements informationnels.

Professeur Leslie Regan Shade est professeure à la Faculté des informations de l'Université de Toronto. Depuis le milieu des années 1990, ses recherches se concentrent sur les aspects sociaux et politiques des technologies de l'information et de la communication, avec un accent particulier sur les questions de genre, de jeunesse et d'économie politique. Elle est récipiendaire de la subvention Insight du CRSH sur la relation entre les jeunes adultes et la confidentialité numérique.

Professeur Jane Bailey est membre de la faculté du Centre de droit, de technologie et de société de l'Université d'Ottawa et professeure titulaire de droit à la section de common law de la Faculté de droit. Ses recherches portent sur les implications sociétales et culturelles des contrôles technologiques privés émergents, en particulier en ce qui concerne les membres des communautés socialement défavorisées.

⁴¹ The eQuality Project, "[Research Projects](#)."

Ses recherches se concentrent également sur le harcèlement, la haine, la confidentialité et les préoccupations d'égalité découlant du ciblage comportemental en ligne des jeunes.

Professeuse Valérie Steeves est membre de la faculté du Centre de droit, de technologie et de société et professeure titulaire au Département de criminologie de la Faculté des sciences sociales de l'Université d'Ottawa. Ses recherches portent sur l'impact des nouvelles technologies sur les droits de la personne. Elle a été experte témoin devant des comités parlementaires concernant la législation sur la confidentialité et a développé des programmes d'éducation à la confidentialité pour des départements gouvernementaux. Elle est la chercheuse principale du projet de recherche "Les jeunes Canadiens dans un monde branché" de MediaSmart.

Partenaires de l'industrie privée

Chantal Bernier a consacré près de six ans à la tête du Commissariat à la protection de la vie privée du Canada. Pendant son mandat au CPVP, elle a dirigé des enquêtes nationales et internationales sur la confidentialité dans les secteurs public et privé, des audits de confidentialité, des évaluations d'impact sur la vie privée, des analyses technologiques, ainsi que le développement et la recherche de politiques de confidentialité. Elle est maintenant coprésidente du groupe mondial de confidentialité et de cybersécurité chez Dentons, où elle conseille des entreprises nationales et internationales de pointe lors de leur expansion au Canada et en Europe, de leur entrée dans le commerce électronique, de l'adoption de l'analyse des données et du déploiement d'initiatives de marché basées sur les données. Ses clients incluent des entreprises de technologie publicitaire, des institutions financières, des entreprises de biotechnologie, des entreprises d'analyse de données et des institutions gouvernementales.

Caroline Dupuis est vice-présidente principale des produits XR du Learning Network. Ses spécialités incluent la compréhension du cadre du cycle de vie du développement logiciel et l'établissement de relations solides avec les parties prenantes. Auparavant, elle a travaillé chez ICOM Productions en tant que chef de projet AR/VR, travaillant avec des concepteurs pédagogiques, des artistes et des développeurs de contenu pour créer et exécuter les spécifications des clients pour les technologies XR.

Matthew Sheardown est directeur de la conception pédagogique des produits XR du Learning Network. Il supervise et gère la conception et le développement pédagogique des projets XR et 3D pour les clients sur diverses plateformes XR. Il a précédemment travaillé en tant que concepteur principal de produits XR chez ICOM Productions, dirigeant la conception pédagogique et les principes d'apprentissage pour tous les projets XR.

Alex Gimson est développeur de jeux et chef de projet XR chez ICOM Productions. Il est titulaire d'un baccalauréat en nouveaux médias de l'Université de Lethbridge. Il travaille dans l'industrie XR depuis presque quatre ans et développe depuis plus d'une décennie. Son travail de développement le plus récent est "Ocnus Theory", un jeu de plateforme sandbox en 3D qui teste la résolution créative de problèmes en ramassant des blocs pour grimper une tour très haute après une chute douloureuse.

Entretien avec les parties prenantes – Questionnaire

Impact des technologies XR sur la vie privée :

1. Pensez-vous que les technologies XR peuvent affecter la vie privée des gens ?
2. Pensez-vous que les personnes de différents groupes démographiques sont impactées de manière égale ?
3. Pensez-vous que ces préoccupations en matière de confidentialité sont uniques aux technologies XR ? Si oui, en quoi diffèrent-elles ? Veuillez expliquer.
4. Comment ces préoccupations en matière de confidentialité pourraient-elles être mieux traitées ?

Risques de la collecte de données biométriques :

5. Les données biométriques sont la collecte d'informations sur les caractéristiques physiques ou comportementales des personnes. Selon vous, quels sont les avantages et les inconvénients de la collecte de données biométriques par le biais des technologies XR ?
6. Pensez-vous que cette collecte de données biométriques est éthique ? Sinon, quelles sont vos préoccupations ?

Implications de l'IA sur les technologies XR :

7. Comment l'ajout potentiel de l'IA générative aux technologies XR modifie-t-il, ou peut-il modifier, la portée et la nature de ces préoccupations en matière de confidentialité ?
8. Pensez-vous que les entreprises devraient être autorisées à analyser les données collectées à partir des technologies XR avec l'IA ?
9. L'anonymisation des données améliore les protections de la vie privée des utilisateurs en supprimant les identifiants qui relient les données stockées à l'utilisateur. Pensez-vous que l'intégration de l'IA peut augmenter le risque que les utilisateurs puissent être identifiés en dehors de l'environnement XR ?

Adéquation de la législation canadienne sur la confidentialité pour les technologies XR :

10. Comment les protections de la vie privée pourraient-elles être mieux intégrées dans le processus de développement des technologies XR ?
11. Pensez-vous que les cadres juridiques et politiques existants, tels que la *Loi sur la protection des renseignements personnels et les documents électroniques* et la *Loi sur la protection de la vie privée des consommateurs* (proposée dans le cadre du projet de loi C-27), répondent adéquatement aux préoccupations en matière de confidentialité des XR ? De nouveaux statuts ou règlements sont-ils nécessaires ?
12. Quel est le meilleur forum pour les consommateurs pour exprimer leurs préoccupations ou problèmes de confidentialité liés aux technologies XR ?

Confidentialité des enfants dans les XR :

13. Les préoccupations en matière de confidentialité sont-elles différentes pour les adultes et les enfants ?
14. Pensez-vous que le stockage des données des enfants nécessite des protocoles de sécurité différents ? Pouvez-vous expliquer ?
15. L'IA pourrait-elle exposer les enfants à un risque accru de manipulation ou compromettre leur autonomie ?

