Analyse vidéo anonyme : un avenir incertain

04 novembre 2020

Les autorités canadiennes de protection de la vie privée enquêtent sur l'utilisation de l'AVA par une société de gestion immobilière

Le 28 octobre 2020, le commissaire à la protection de la vie privée du Canada et ses homologues provinciaux de l'Alberta et de la Colombie-Britannique ont publié les conclusions de leur enquête conjointe sur les pratiques de traitement des renseignements personnels d'une société de gestion immobilière qui utilisait la technologie de l'analyse vidéo anonyme (AVA) pour générer des données démographiques sur le comportement des consommateurs dans ses centres commerciaux selon une méthode qui, aux dires de cette société, permettait d'obtenir des données anonymes sommaires.

Dans le cas qui nous occupe, des capteurs avaient été installés dans les bornes d'information numériques de divers centres commerciaux un peu partout au Canada. Les capteurs utilisaient une technologie de caractérisation faciale – une autre façon de désigner la technologie d'analyse vidéo anonyme – pour évaluer la tranche d'âge et le sexe des consommateurs se trouvant à proximité des capteurs. Même si la société soutenait que les lois canadiennes sur la protection des renseignements personnels ne s'appliquaient pas à l'utilisation qu'elle faisait de la technologie d'AVA puisque cette technologie ne lui permettait pas de recueillir des renseignements personnels au sens de ces lois, les commissaires n'étaient pas de cet avis et ont tiré un certain nombre de conclusions importantes au sujet de l'AVA.

Les commissaires ont conclu que compte tenu de la nature des renseignements recueillis grâce à la technologie d'AVA en l'espèce, la société devait obtenir le consentement positif et explicite des consommateurs, étant donné que certains des renseignements recueillis étaient de nature délicate et que leur collecte à l'insu des consommateurs dans ce contexte allait au-delà de leurs attentes raisonnables. La société a été invitée à limiter la conservation des renseignements personnels ainsi obtenus et à mettre à jour ses politiques et ses procédures en matière d'obtention d'un consentement valable. Bien que dans cette décision, les commissaires aient également abordé l'utilisation par la société de technologies de géolocalisation d'appareils mobiles, nous nous en tiendrons dans le présent document aux conclusions relatives à l'AVA.

Contexte

Dans un récent Rapport de conclusions d'enquête, le Commissariat à la protection de la vie privée du Canada a, en collaboration avec ses homologues de l'Alberta[1] et de la Colombie-Britannique[2] (les commissaires), rendu une décision déroutante sur la légalité de la technologie d'analyse vidéo anonyme (AVA) au regard de la *Loi sur la protection* des renseignements personnels et les documents électroniques (« LPRPDE ») du Canada et de lois essentiellement similaires sur la protection des renseignements personnels dans le secteur privé de l'Alberta et de la Colombie-Britannique (collectivement les lois canadiennes sur la protection des renseignements personnels). Cette décision risque de chambarder le recours à une technologie relativement nouvelle qui, pour beaucoup, favorisait la protection des renseignements personnels[3].

Les commissaires avaient ouvert une enquête conjointe sur les pratiques de traitement des renseignements personnels d'une société de gestion immobilière à la suite de nombreux reportages dans les médias qui avaient révélé que des renseignements personnels des consommateurs étaient recueillis à leur insu et sans leur consentement dans des centres commerciaux canadiens au moyen de bornes d'orientation numériques interactives contenant le répertoire électronique de magasins, en l'occurrence des systèmes de cartes numériques à écran tactile.

L'enquête avait révélé que les capteurs avaient recueilli et utilisé des images faciales (images) qui avaient été converties en représentations numériques des traits faciaux (représentations numériques des traits faciaux) en vue de générer des renseignements permettant d'évaluer la tranche d'âge et le sexe des consommateurs (données démographiques).

La société faisait toutefois valoir que la technologie d'AVA utilisée – qui avait été installée et était gérée par un fournisseur de services – n'avait pas permis de recueillir, d'utiliser ou de communiquer des « renseignements personnels » au sens des lois canadiennes sur la protection des renseignements personnels. Elle affirmait plutôt que les renseignements recueillis grâce aux capteurs étaient anonymes, en ce qu'ils ne pouvaient être utilisés seuls ou conjointement avec d'autres renseignements pour identifier une personne. La société faisait valoir que comme elle ne recueillait aucun renseignement personnel au moyen de la technologie d'AVA, elle n'était pas tenue de se conformer aux exigences en matière d'avis et de consentement.

Qu'est-ce que l'analyse vidéo anonyme ou AVA?

L'AVA est une technologie conçue pour recueillir des renseignements de valeur sur les consommateurs se trouvant à un endroit déterminé – notamment sur leur tranche d'âge, leur sexe et même leur état émotionnel face à un affichage numérique donné – en créant des rapports sommaires anonymisés à l'aide d'algorithmes de détection des formes des visages qui balaient les images en temps réel de caméra vidéo[4].

Contrairement à la reconnaissance faciale, qui crée un modèle des caractéristiques physiques ou comportementales d'une personne aux fins d'authentification ou d'identification, l'AVA n'est pas conçue pour identifier ou authentifier des individus, de sorte que les images recueillies grâce à la technologie d'AVA sont généralement traitées à l'interne et conservées pendant une très courte période de temps (voire pas du tout). En principe, aucun modèle unique et permanent des traits du visage de l'individu n'est créé ou conservé[5]. Compte tenu de ces différences importantes, l'AVA est appelée « détection faciale » ou « caractérisation faciale ». On la considère souvent

à tort comme une technique de surveillance ou un système biométrique, car elle repose sur les caractéristiques biométriques et fait usage de matériel similaire[6].

Bien qu'elle ne soit pas utilisée exclusivement dans le secteur de la vente au détail, la technologie d'AVA est de plus en plus associée aux magasins physiques, d'autant plus que ceux-ci cherchent à se réinventer pour concurrencer le commerce électronique, un secteur qui a connu une croissance spectaculaire au détriment des détaillants traditionnels.

L'essor inexorable du commerce électronique peut être attribué, du moins en partie, à la capacité des entreprises qui font du commerce en ligne à exploiter divers outils de collecte de renseignements et de suivi afin d'adapter leur publicité en fonction de leur clientèle, et de personnaliser l'expérience d'achat des consommateurs, leur permettant ainsi de recueillir de précieuses données en cours de route. L'AVA s'est révélée la réponse du secteur de la vente au détail « hors ligne » à une situation de plus en plus inégale, promettant de corriger le déséquilibre qui existe entre les commerces traditionnels et les magasins en ligne en ce qui concerne les renseignements dont ils disposent. Plus précisément, l'AVA est utilisée pour produire en temps réel diverses données sur les consommateurs, qui peuvent être exploitées pour créer une expérience d'achat plus fluide, améliorer la gestion des produits et les décisions commerciales et mesurer la réaction des consommateurs face à des communications visuelles et à l'affichage, tout en promettant de mieux protéger les renseignements personnels des consommateurs grâce à une protection dite « dès la conception »[7].

Décision

Dans leur décision, les commissaires s'appuient sur un certain nombre de conclusions clés concernant les caractéristiques de la technologie d'AVA utilisée en l'espèce, sur le type de renseignements recueillis et sur la durée de conservation de ces renseignements par le fournisseur de services. Bien que la décision traite aussi des renseignements recueillis au cours de la phase pilote du projet d'implantation de l'AVA, notre analyse est axée sur le déploiement subséquent de l'AVA dans les centres commerciaux de la société.

D'entrée de jeu, les commissaires soulignent que la technologie d'AVA utilisée en l'espèce « ne fonctionnait pas entièrement en temps réel » et qu'il était nécessaire de conserver en mémoire les images saisies « quoique pendant une très courte période »[8]. Sans analyser davantage la question, les commissaires estiment que cette pratique représente une collecte de renseignements personnels au sens des lois canadiennes sur la protection des renseignements personnels, malgré le fait que les images étaient conservées pendant à peine « quelques millisecondes », pour reprendre l'expression de la société.

Anticipant peut-être qu'à l'avenir, la technologie permette de rendre ce stockage d'images éphémères encore plus imperceptible, les commissaires ont également fait observer qu'il n'était pas nécessaire de stocker les renseignements pour que ceux-ci soient considérés comme une collecte de renseignements personnels au sens des lois canadiennes sur la protection des renseignements personnels. En pratique, la plupart des types de technologies d'AVA seront probablement assujettis aux lois canadiennes sur la protection des renseignements personnels, étant donné que l'AVA nécessite l'utilisation de capteurs visuels.

S'agissant des particularités de la technologie d'AVA utilisée en l'espèce, les commissaires ont également conclu que les images étaient utilisées pour générer des « représentations numériques biométriques de visages de personnes » (décrites plus loin) et des données démographiques, ce qui constituait effectivement une collecte et une utilisation distinctes de renseignements personnels. Par un procédé d'intégration, les images étaient converties en représentations numériques uniques de visages, ce que les commissaires ont appelé des « renseignements biométriques », une nuance importante compte tenu du caractère relativement délicat de ce type de renseignements. Les commissaires ont par ailleurs qualifié de « biométriques » ces représentations numériques de traits faciaux, en ce qu'elles étaient créées à partir d'une série de mesures de traits faciaux et pouvaient être utilisées aux fins d'identification ou d'authentification, c'est-à-dire pour la reconnaissance faciale.

Cela étant, les commissaires ont reconnu que ni la société ni son fournisseur de services n'avaient utilisé ces renseignements pour confirmer ou authentifier l'identité d'une personne. Il est pertinent de signaler que la technologie d'AVA n'est pas normalement conçue pour générer ce type de « modèle » unique et permanent des traits faciaux d'individus, étant donné qu'elle n'est pas conçue pour la reconnaissance faciale[9]. Toutefois, dans le cas qui nous occupe, les commissaires ont conclu que la technologie d'AVA reposait sur un logiciel qui pouvait être utilisé pour la reconnaissance faciale, même si cette fonction particulière était désactivée.

Tout en reconnaissant que les données démographiques – c'est-à-dire les évaluations de l'âge et du sexe – ne pouvaient constituer en soi des renseignements personnels au sens des lois canadiennes en matière de protection des renseignements personnels, les commissaires ont estimé qu'elles devenaient des « renseignements personnels » dans le présent contexte, étant donné qu'elles étaient conservées avec d'autres renseignements qui pouvaient être utilisés pour identifier un individu. Plus précisément, et à l'insu de la société, le fournisseur de services avait stocké les données démographiques avec des représentations numériques de traits faciaux et d'autres renseignements circonstanciels, en l'occurrence la date, l'heure et le lieu où la photo avait été prise, et ce, sans la moindre justification.

Les commissaires ont donc non seulement estimé que les renseignements en question répondaient à la définition de « renseignements personnels », mais aussi que la société avait manqué à ses obligations en matière de conservation de données en conservant des renseignements personnels – c'est-à-dire des représentations numériques de traits faciaux – au-delà de la période nécessaire pour atteindre le but dans lequel ils avaient été recueillis, en l'occurrence, pour générer des données démographiques, et non pour repérer ou autrement identifier des individus.

Compte tenu des conclusions des commissaires suivant lesquelles la société de gestion immobilière avait recueilli des renseignements personnels, cette dernière devait obtenir un consentement valable avant de pouvoir recueillir et utiliser les renseignements personnels des consommateurs au moyen de la technologie d'AVA. Toutefois, en l'espèce, la société devait obtenir le consentement positif et explicite des consommateurs, étant donné que la collecte et l'utilisation des renseignements biométriques recueillis étaient considérées comme étant de nature délicate et allant au-delà des attentes raisonnables des consommateurs, qui n'avaient guère de raison de soupçonner que leur image était saisie et utilisée à de telles fins alors qu'ils consultaient le répertoire d'un centre commercial.

Les commissaires ont par ailleurs invité la société à revoir sa politique sur les renseignements personnels et son affichage en la matière, étant donné qu'ils n'indiquaient pas assez précisément les objectifs poursuivis, le type de renseignements recueillis et l'utilisation qu'on entendait en faire. Comme la méthode suivie allait au-delà des attentes raisonnables des consommateurs, il incombait à la société de leur expliquer clairement et de façon explicite et aisément accessible ses méthodes de gestion de la communication de renseignements personnels lorsque les consommateurs consultaient ses bornes d'information numériques (c'est-à-dire au moment de la collecte). Pour ces motifs, les commissaires ont conclu que la société avait manqué à son obligation d'obtenir un consentement valable et éclairé.

Points à retenir pour les entreprises

On peut dégager des conclusions des commissaires sur l'utilisation de la technologie d'AVA par la société quatre points importants pour les entreprises qui utilisent des technologies similaires :

- **Les lois canadiennes sur la protection des renseignements personnels s'appliquent à la technologie d'AVA.** Cette décision représente une affirmation claire et sans ambages de la part des autorités de réglementation que la technologie d'AVA est de manière générale assujettie aux lois canadiennes sur la protection des renseignements personnels, car on peut supposer que la plupart des technologies d'AVA permettent de capter temporairement l'image du visage d'une personne avant d'en extraire des données anonymes sommaires. Les commissaires ont également pris soin de préciser que les lois canadiennes sur la protection des renseignements personnels n'exigent pas que les renseignements soient « consignés » pour être considérés comme des renseignements personnels et, en tout état de cause, qu'il y a collecte de renseignements personnels même lorsqu'une image est conservée en mémoire pendant une fraction de seconde seulement.
- **Vérification et examen périodiques des pratiques des fournisseurs de services en matière de traitement des renseignements.** Les commissaires insistent dans leur décision sur l'importance de vérifier et d'examiner périodiquement les pratiques de traitement des renseignements des fournisseurs de services pour s'assurer que ces derniers respectent leurs obligations contractuelles, y compris celles relatives à la collecte, à la conservation et à l'utilisation de renseignements personnels qu'ils font au nom d'une entreprise. Les lois canadiennes sur la protection des renseignements personnels obligent en général les entreprises à conclure avec leurs fournisseurs de services qui traitent des renseignements personnels en leur nom – y compris les sociétés affiliées agissant en cette qualité – des ententes écrites formelles prévoyant des mesures de sécurité adéquates adaptées à la nature, à la portée et au caractère sensible des renseignements traités. En pratique, ces ententes renferment souvent des exigences concernant la durée maximale de conservation des renseignements personnels et accordant à l'entreprise le droit de vérifier et d'examiner les activités du fournisseur de services. Par conséquent, il est essentiel que ces droits soient bien respectés pour réduire les risques liés à la conservation et au stockage non autorisés de renseignements personnels.
- **Évaluation des fonctions et des caractéristiques de la technologie d'AVA et tenue d'une évaluation des facteurs relatifs à la vie privée avant sa mise en œuvre.** Les entreprises qui utilisent la technologie d'AVA pour recueillir des

renseignements sur les consommateurs doivent examiner et évaluer attentivement les fonctions et les caractéristiques de cette technologie pour s'assurer qu'elle ne génère pas d'identificateurs uniques et permanents qui pourraient être utilisés pour identifier une personne. Comme nous l'avons déjà expliqué, la technologie d'AVA n'est pas conçue pour conserver des images pendant une période de temps prolongée ni pour générer des « modèles » uniques des traits faciaux d'une personne en vue de les utiliser aux fins d'identification faciale. Les commissaires auraient pu tirer des conclusions différentes si un autre type de technologie d'AVA avait été utilisé, mais il n'en demeure pas moins important que les entreprises fassent preuve de diligence raisonnable pour évaluer comment la technologie qu'ils utilisent recueille, utilise, conserve ou divulgue des renseignements afin de réduire les risques d'atteinte à la protection des renseignements personnels. D'ailleurs, les entreprises devraient envisager de procéder à une évaluation des incidences de ces technologies sur la protection des renseignements personnels avant de les mettre en œuvre afin de bien identifier, évaluer et atténuer ces risques.

- **Examen des politiques et des procédures existantes pour garantir la transparence et le consentement.** En ce qui concerne les exigences relatives à l'avis et au consentement, cette décision indique clairement que les entreprises devront faire preuve de plus de transparence avant d'utiliser l'AVA, d'autant plus qu'il existe actuellement une méfiance et des craintes élevées de la part des citoyens à l'égard de cette technologie. Les entreprises ont donc intérêt à revoir leurs pratiques de communication existantes pour s'assurer que les consommateurs sont bien informés de l'utilisation de la technologie d'AVA lorsqu'ils utilisent des écrans numériques qui en sont équipés. En d'autres termes, avant de recueillir des images des consommateurs dans le but de générer des données exploitables, les entreprises doivent leur fournir de l'information claire, non ambiguë et accessible concernant les buts de la collecte de renseignements, le type de renseignements recueillis et l'utilisation que l'entreprise entend en faire. Cette information peut être fournie par divers moyens de communication – affichage, brochures, pages consacrées à cette fin sur le site Web officiel de l'entreprise, vidéos, etc. Même si les commissaires recommandent aux entreprises d'obtenir un consentement positif explicite, il vaut la peine de signaler qu'ils n'écartent pas expressément le recours au consentement implicite pour d'autres formes de technologies d'AVA qui ne recueillent pas des renseignements biométriques ou d'autres types de renseignements de nature délicate. Comme nous l'expliquons plus en détail dans la section suivante, la décision des commissaires est fortement influencée par leur conclusion suivant laquelle la collecte de représentations numériques de traits faciaux par la société constituait une collecte de « renseignements biométriques », ce qui permet de penser que les technologies d'AVA qui ne recueillent pas de tels renseignements ne requièrent pas nécessairement un consentement positif explicite. Cela étant, comme il est primordial de s'assurer la confiance du public avant de recourir à ce type de mesure, les entreprises devraient faire preuve de prudence et bien réfléchir à la façon dont elles communiquent des renseignements sur les pratiques de traitement des renseignements.

Analyse des questions en suspens

Les conclusions des commissaires remettent en question la viabilité de l'AVA dans le secteur de la vente en détail « hors ligne » au Canada, car elles semblent obliger les entreprises à obtenir le consentement explicite des consommateurs. Cette exigence n'est pas toujours réaliste ni applicable, d'autant plus que le fait de demander le consentement du consommateur risque de compromettre la valeur et l'exactitude des données recueillies. Pourtant, il peut être possible d'établir une distinction entre les circonstances à l'origine de la présente décision et d'autres types de technologies d'AVA, dont la portée pourrait être considérée comme moins attentatoire, afin de rendre plus raisonnable dans certaines situations le recours au consentement implicite. Nous examinons ci-dessous quelques-uns de ces arguments potentiels et proposons certaines balises pour la mise en œuvre de ces technologies.

Portée de la définition des « renseignements personnels »

Bien que les commissaires donnent une interprétation large de l'expression « renseignements personnels » et concluent sans hésiter que la simple saisie d'une image, même pour une milliseconde, constitue une collecte de renseignements personnels, ces arguments risquent d'être remis en question au fur et à mesure que les technologies d'AVA se développent et rendent de plus en plus imperceptible la conservation des données.

Les renseignements sont des « renseignements concernant un individu identifiable » lorsqu'il y a « de fortes possibilités que l'individu puisse être identifié par l'utilisation de ces renseignements, seuls ou en combinaison avec des renseignements d'autres sources[10] ».

La Cour fédérale a récemment expliqué que la norme minimale des « fortes possibilités » correspondait à « une possibilité qui dépasse une spéculation ou une "simple possibilité", sans être "plus susceptible de se produire que l'inverse" (c.-à-d. qui ne doit pas être "probable" selon la prépondérance des probabilités)[11] ». Ainsi, pour pouvoir conclure que les renseignements suscitent de fortes possibilités que l'individu puisse être identifié, on préconise une évaluation contextuelle dans le cadre de laquelle on tient compte de l'ensemble des faits, « y compris le type de renseignements en question, le contexte dans lequel ces renseignements sont consignés dans le dossier en question et la nature des autres renseignements qui sont disponibles[12] ».

Dans le cas qui nous occupe, il peut y avoir lieu de se demander si une image conservée de façon purement temporaire donne lieu à de « fortes possibilités » que l'on puisse identifier la personne concernée. Il n'existe aucune possibilité réaliste que l'entreprise ou le fournisseur de services accède à ces renseignements, et encore moins qu'il les utilise pour identifier une personne avant qu'ils soient supprimés. Même si tout dépend des capacités et des caractéristiques de sécurité particulières de la technologie d'AVA utilisée, il sera probablement de plus en plus difficile d'ignorer ce raisonnement, car il semble illusoire d'affirmer qu'une image « saisie » dans ces conditions puisse être mise sur le même pied que celles qui sont saisies par des caméras de surveillance. Non seulement une telle façon de voir ferait-elle fi de la réalité, elle contribuerait aussi à la fausse croyance selon laquelle la technologie d'AVA et la surveillance sont une seule et même chose. En tout état de cause, la conservation pour un temps limité de renseignements est une stratégie évidente d'atténuation des risques

qui devrait réduire le caractère délicat des renseignements recueillis et rendre le consentement implicite plus acceptable dans ces circonstances.

Portée des « renseignements biométriques »

Un autre aspect important de cette décision est l'interprétation que les commissaires font de l'expression « renseignements biométriques », interprétation qui a joué un rôle déterminant dans leur conclusion selon laquelle la société en cause devait obtenir le consentement explicite des consommateurs avant de recueillir leurs renseignements personnels. Pourtant, de nombreux aspects du raisonnement des commissaires pourraient potentiellement donner matière à discussion à l'avenir, notamment leurs conclusions sur le caractère relativement délicat des renseignements biométriques utilisés à d'autres fins que l'authentification ou l'identification.

La conclusion des commissaires suivant laquelle les représentations numériques des traits du visage répondent à la définition de « renseignements biométriques » était fondée sur le fait que ces renseignements provenaient uniquement de l'identification des traits physiques d'une personne identifiable particulière et « pourraient servir à faire la distinction entre différentes personnes ». Cette définition n'est cependant pas tout à fait conforme aux Orientations sur les renseignements biométriques du commissaire fédéral à la protection de la vie privée, qui parle toujours de ces renseignements dans le contexte de systèmes permettant à des machines « de reconnaître des personnes ou de confirmer ou d'authentifier leur identité[13] ». En d'autres termes, on ne sait pas avec certitude si les renseignements provenant de caractéristiques physiques doivent inévitablement être qualifiés de renseignements « biométriques » – et, partant, de nature délicate – par nature s'ils ne sont pas utilisés dans le contexte de systèmes d'identification ou d'authentification.

Bien que les commissaires confondent ces questions – il a été révélé que le logiciel sous-jacent utilisé pour la technologie d'AVA pouvait également être utilisé pour la reconnaissance faciale, de sorte que les représentations numériques de traits faciaux pouvaient servir à identifier des gens –, on peut se demander si le résultat aurait été le même si la technologie d'AVA n'avait aucune capacité de reconnaissance faciale. D'ailleurs, selon le Future of Privacy Forum, la technologie d'AVA [traduction] « ne crée et ne conserve pas systématiquement des modèles de visages identifiables personnellement », ce qui donne à penser que les mesures du visage saisies au moyen de technologies AVA plus traditionnelles ne présentent pas le degré d'« unicité » et de « permanence » suffisant pour permettre la reconnaissance faciale[14].

De façon plus générale, on peut également se demander si les mesures du visage sont effectivement « de nature délicate » dans d'autres circonstances. Selon les commissaires, les renseignements faciaux biométriques sont de nature plus délicate, puisque « la possession d'un modèle de reconnaissance faciale peut permettre l'identification d'une personne par comparaison à une vaste gamme d'images facilement accessibles sur Internet ou par surveillance clandestine[15] ».

Pourtant, dans ses orientations, le commissaire fédéral à la protection de la vie privée déclare que les traits physiques sont d'une nature moins délicate que d'autres types de renseignements biométriques, comme les empreintes digitales, l'iris ou l'ADN, parce que les traits du visage sont moins distinctifs, peuvent changer au fil des années et peuvent aussi être modifiés « par le maquillage, les déguisements ou la chirurgie ». Le

commissaire fédéral à la protection de la vie privée déclare aussi dans ses Orientations sur les renseignements biométriques que le recours à des « modèles » ou à l'enregistrement de « renseignements résumés » des caractéristiques biométriques protège davantage la vie privée, parce qu'on limite ainsi la quantité de renseignements conservés et parce que des méthodes d'extraction des caractéristiques exclusives peuvent être nécessaires pour réussir à jumeler les renseignements.

S'il est vrai que le « vaste éventail d'images facilement accessibles en ligne ou par surveillance clandestine » peut faciliter encore plus l'identification des individus par rapport à leurs informations biométriques, ce risque ne doit pas être surestimé ni prévaloir sur les arguments contraires, comme ceux que nous avons déjà évoqués. En tout état de cause, toute possibilité sérieuse d'identification semble particulièrement limitée si les caractéristiques faciales sont conservées uniquement aux fins d'extraction de données démographiques et si elles sont immédiatement supprimées de la mémoire du système.

Recours au « consentement implicite » pour l'analyse vidéo anonyme comme solution pour l'avenir

Selon les Lignes directrices pour l'obtention d'un consentement valable du commissaire fédéral, le consentement peut être explicite ou implicite selon les circonstances. Il faut toutefois obtenir le consentement explicite de l'intéressé dans les cas suivants :

- les renseignements sont sensibles;
- la collecte, l'utilisation ou la communication des renseignements ne répond pas aux attentes raisonnables de l'intéressé;
- la collecte, l'utilisation ou la communication des renseignements crée un risque résiduel important de préjudice grave.

Pourtant, sans analyser longuement la question[16], les commissaires concluent que le consentement explicite doit être obtenu lorsque la technologie d'AVA est utilisée, étant donné que les renseignements recueillis au moyen de cette technologie sont des renseignements biométriques dont la collecte, l'utilisation ou la communication ne répond pas aux attentes raisonnables des consommateurs. Il est possible de mettre en doute ces conclusions pour au moins deux raisons, ce qui ouvre la porte au « consentement implicite » dans d'autres situations. Tout d'abord, on peut contester ces conclusions en invoquant la portée et le caractère délicat des renseignements biométriques par rapport aux technologies d'AVA traditionnelles, comme nous l'avons déjà expliqué. Deuxièmement – et c'est le sujet de la présente section –, on peut les contester en fonction des « attentes raisonnables » des consommateurs dans les lieux publics.

Bien que les consommateurs aient droit à un certain respect de leur vie privée dans les lieux publics, leur attente en la matière est probablement assez faible, surtout dans les lieux où ils savent déjà qu'ils sont filmés par des caméras de surveillance. Dans les décisions concernant l'utilisation de systèmes de surveillance, les tribunaux mentionnent le caractère public des lieux qui sont filmés comme facteur contribuant à diminuer les attentes des particuliers quant au respect de leur vie privée[17]. Ainsi, la collecte et l'utilisation d'images ne devraient pas justifier d'emblée l'obligation d'obtenir un consentement explicite, surtout si les renseignements en question sont conservés

pendant très peu de temps, ne font pas l'objet d'une surveillance constante, ne sont pas consultés d'une autre manière et ne sont pas utilisés aux fins de reconnaissance faciale. En ce sens, la technique d'AVA n'est généralement pas plus attentatoire qu'une enquête menée sur place. À la différence de la technique d'AVA, ces enquêtes sont beaucoup plus coûteuses et ne sont pas nécessairement aussi précises.

Il vaut la peine de signaler que ce qui constitue une « attente raisonnable » pour un consommateur est une appréciation qui fait nécessairement intervenir certaines valeurs susceptibles d'évoluer au fil du temps. Prenons, par exemple, les renseignements recueillis en ligne sur les utilisateurs lorsqu'ils naviguent sur Internet. D'une part, les outils de suivi en ligne sont beaucoup plus attentatoires et persistants que la technique d'AVA, car ils permettent de suivre, de profiler et de cibler les utilisateurs. Pourtant, le public connaît bien ces technologies et semble les accepter. En revanche, il se peut que les consommateurs ne soient pas pleinement conscients de ce qu'est la technique d'AVA ou de l'utilisation qu'on peut en faire, ce qui crée beaucoup de confusion et de méfiance envers cette technologie, qui est souvent assimilée à la reconnaissance faciale. Cette méfiance constitue peut-être un argument plus convaincant pour améliorer la transparence et fournir aux consommateurs des renseignements de meilleure qualité, plus clairs et plus accessibles concernant l'utilisation qu'une entreprise fait de l'AVA.

Conclusion

Dans l'ensemble, les faits à l'origine de cette décision étaient loin d'être idéaux pour évaluer le bien-fondé de la technique d'AVA, car la technologie utilisée dans cette affaire présentait vraisemblablement certaines caractéristiques communes avec des technologies portant davantage atteinte à la vie privée, comme la reconnaissance faciale. Les conclusions des commissaires laissent planer un doute sur la légalité de la technique d'AVA au regard des lois canadiennes sur la protection des renseignements personnels, et on ne sait pas avec certitude si le résultat aurait été différent si les commissaires s'étaient penchés sur un autre type d'AVA.

Bien qu'il soit possible de se fonder sur le consentement implicite des consommateurs dans certaines circonstances, cette décision insiste sur l'importance de s'éloigner d'un modèle de protection des renseignements personnels axé sur le consentement au profit d'un modèle qui reconnaît divers fondements juridiques pour le traitement des renseignements personnels – une solution que le commissaire fédéral à la vie privée a adoptée lors de sa récente comparution devant la Commission québécoise chargée de moderniser les dispositions législatives en matière de protection des renseignements personnels. Cette approche n'est ni nouvelle ni radicale, d'autant plus que c'est précisément la solution retenue par l'Union européenne dans son Règlement général sur la protection des données, qui prévoit six bases juridiques distinctes permettant le traitement des données à caractère personnel, y compris les intérêts légitimes des entreprises, sous réserve de solides garanties de transparence et de droits reconnus aux personnes concernées.

Dans le contexte actuel, il peut être tout simplement irréaliste et inutile d'obtenir le consentement explicite des consommateurs en ce qui concerne la technologie d'AVA, en particulier lorsque cette technologie est utilisée pour recueillir passivement des renseignements sur les consommateurs. Par exemple, l'AVA peut être utilisée pour mesurer le regard et l'expression faciale de passants afin de déterminer l'efficacité

d'une publicité numérique. Dans ce scénario, les consommateurs ne s'intéressent que passivement à l'affichage. En pareil cas, il est beaucoup plus difficile d'invoquer le consentement, explicite ou implicite, sans déformer le sens de ce concept.

Pour le secteur de la vente au détail hors ligne, cette décision peut finalement être considérée comme un coup dur porté à ses efforts en vue de concurrencer le commerce électronique, car elle risque de limiter indûment sa capacité d'obtenir des renseignements précieux sur les consommateurs et d'adapter ses pratiques pour rendre l'expérience d'achat en magasin plus fluide et plus pratique. Comme la numérisation du commerce au détail ne devrait que s'accélérer, notamment en raison de l'impact de la COVID-19 sur le comportement des consommateurs – impact qui, selon certains, devrait se maintenir pour un certain temps[18] –, il est évident que les magasins ayant pignon sur rue devraient disposer des outils appropriés pour innover afin de demeurer compétitifs.

Bien que la protection des renseignements personnels des consommateurs demeure essentielle pour assurer la viabilité de ces mesures, ces intérêts doivent être évalués de façon réaliste et soupesés par rapport à la portée, à la nature et aux conséquences des activités de traitement de l'information.

Les avocats de BLG spécialisés en cybersécurité, en respect de la vie privée et en protection des renseignements personnels sont à votre disposition pour répondre à toutes les questions que vous pourriez vous poser au sujet de l'analyse vidéo anonyme au Canada. Si vous avez des questions, n'hésitez pas à communiquer avec votre avocat de BLG ou l'une des personnes-ressources ci-dessous.

[1] Office of the Information and Privacy Commissioner of Alberta.

[2] Office of the Information and Privacy Commissioner for British Columbia.

[3] Commissariat à l'information et à la protection de la vie privée de l'Ontario, « White Paper: Anonymous Video Analytics (AVA) technology and privacy », [Livre blanc : la technologie d'analyse vidéo anonyme (AVA) et la vie privée] (disponible en anglais seulement), avril 2011.

[4] Commissariat à l'information et à la protection de la vie privée de l'Ontario, « White Paper: Anonymous Video Analytics (AVA) technology and privacy », [Livre blanc : la technologie d'analyse vidéo anonyme (AVA) et la vie privée] (disponible en anglais seulement), avril 2011, page 3.

[5] Future of Privacy Forum, « Privacy Principles for Facial Recognition Technology in Commercial Applications », septembre 2018, page 1 (en anglais seulement).

[6] Future of Privacy Forum, « Understanding Facial Detection, Characterization and Recognition Technologies » (disponible en anglais seulement), mars 2018.

[7] Commissariat à l'information et à la protection de la vie privée de l'Ontario, « White Paper: Anonymous Video Analytics (AVA) technology and privacy », [Livre blanc : la technologie d'analyse vidéo anonyme (AVA) et la vie privée] (disponible en anglais seulement), avril 2011.

[8] Commissariat à la protection de la vie privée du Canada, « Rapport de conclusions d'enquête en vertu de la LPRPDE no 2020-004 », paragraphe 62.

[9] Future of Privacy Forum, « Privacy Principles for Facial Recognition Technology in Commercial Applications », septembre 2018 (en anglais seulement).

[10] *Gordon* c. Canada (Santé), 2008 CF 258.

[11] Canada (Commissaire à l'information) c. Canada (Sécurité publique et Protection *civile)*, 2019 CF 1279, par. 53.

[12] Canada (Commissaire à l'information) c. Canada (Sécurité publique et Protection *civile)*, 2019 CF 1279, par. 67.

[13] Voir également Commission d'accès à l'information du Québec, « Biométrie : principes à respecter et obligations légales des organisations », juillet 2020, page iv.

[14] Future of Privacy Forum, « Privacy Principles for Facial Recognition Technology in Commercial Applications », septembre 2018 (en anglais seulement).

[15] Commissariat à la protection de la vie privée du Canada, Rapport de conclusions d'enquêtes en vertu de la LPRPDE no 2020-004, par. 79.

[16] Commissariat à la protection de la vie privée du Canada, Rapport de conclusions d'enquêtes en vertu de la LPRPDE no 2020-004, par. 79 à 81.

[17] Eastmond c. Canadien Pacifique Ltée, 2004 CF 852, par. 180.

[18] Les ventes du commerce électronique américain devraient atteindre 1 000 milliards de dollars en 2022, soit environ deux ans plus tôt que les estimations précédentes, en partie à cause de la COVID-19.

Par

Andy Nagy

Services

Cybersécurité, respect de la vie privée et protection des renseignements personnels, Protection de la vie privée et atteintes à la sécurité, Technologies

BLG | Vos avocats au Canada

Borden Ladner Gervais S.E.N.C.R.L., S.R.L. (BLG) est le plus grand cabinet d'avocats canadien véritablement multiservices. À ce titre, il offre des conseils juridiques pratiques à des clients d'ici et d'ailleurs dans plus de domaines et de secteurs que tout autre cabinet canadien. Comptant plus de 725 avocats, agents de propriété intellectuelle et autres professionnels, BLG répond aux besoins juridiques d'entreprises et d'institutions au pays comme à l'étranger pour ce qui touche les fusions et acquisitions, les marchés financiers, les différends et le financement ou encore l'enregistrement de brevets et de marques de commerce.

blg.com

Bureaux BLG

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000, rue De La Gauchetière Ouest
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749