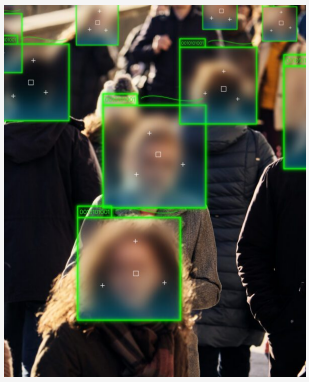
OSLER

La Commission d'accès à l'information du Québec interdit à un détaillant d'utiliser la reconnaissance faciale comme outil de prévention des pertes



25 MARS 2025 12 MIN DE LECTURE

Expertises Connexes

- Litiges relatifs à la protection de la vie privée et des données
- Respect de la vie privée et gestion de l'information

Auteurs(trice): François Joli-Coeur, Joanna Fine, Andy Nagy, Gregory Corosky

Le 18 février 2025, la Commission d'accès à l'information du Québec (la CAI) a rendu une décision interdisant à une grande chaîne d'épiceries et de pharmacies de lancer son projet pilote de reconnaissance faciale, qui visait à prévenir le vol à l'étalage et la fraude dans ses établissements.

Alors que l'utilisation de la vidéosurveillance est une pratique courante dans les commerces de détail au Québec, cette décision constitue un rappel important que, pour extraire des données biométriques à partir d'images brutes captées par un système de vidéosurveillance, les entreprises faisant affaire au Québec doivent respecter les exigences sévères prévues aussi bien par la *Loi concernant le cadre juridique des technologies de l'information* (la Loi sur les TI) que par la *Loi sur la protection des renseignements personnels dans le secteur privé* (la Loi sur le privé) du Québec.

L'enquête s'est concentrée principalement sur la question de savoir si l'entreprise respectait les exigences de la Loi sur les TI relatives à l'utilisation de données biométriques aux fins de la vérification ou de la confirmation de l'identité. Par conséquent, la décision n'a pas abordé des questions générales de conformité touchant la Loi sur le privé, y compris la question de savoir si la collecte de données biométriques au moyen de la technologie de reconnaissance faciale répondait au critère de nécessité dans le contexte particulier de l'affaire[1], et si la collecte était effectuée pour un « motif légitime »[2]. La CAI a analysé récemment le critère de nécessité dans une autre décision concernant une entreprise qui utilisait la technologie de reconnaissance faciale pour contrôler l'accès de ses employés à ses locaux (pour plus de détails, consultez notre précédent bulletin d'actualités Osler, intitulé « La Commission d'accès à l'information du Québec maintient la sévérité des exigences applicables au traitement des renseignements biométriques : leçons pour les entreprises »).

Les faits en bref

Metro Inc., grande chaîne d'épiceries et de pharmacies du Canada, prévoyait de lancer dans certains de ses établissements un projet pilote permettant d'évaluer la faisabilité de la mise en place de la technologie de reconnaissance faciale comme outil de prévention des pertes,

en vue d'un déploiement éventuel à grande échelle. Le projet visait à contrer le vol à l'étalage et la fraude dans les établissements Metro au moyen de l'identification des personnes précédemment impliquées dans de telles activités. La CAI a lancé son enquête peu après avoir reçu de l'entreprise sa déclaration l'informant de son intention de mettre en place une banque de données biométriques, conformément aux obligations d'information concernant les banques de données biométriques prévues à l'article 45 de la Loi sur les TI.

Dans le cadre de ce projet pilote, Metro aurait utilisé son système de vidéosurveillance existant pour constituer une banque d'images de référence au moyen du captage des images faciales des délinquants présumés et de la création de modèles biométriques. Lorsqu'un client serait entré dans un établissement participant, le système aurait capté son image faciale, généré un nouveau modèle biométrique, puis comparé celui-ci à ceux déjà emmagasinés dans la banque d'images. En cas de correspondance, les responsables de l'établissement en cause auraient reçu une alerte leur permettant de prendre les mesures qui s'imposent dans les circonstances.

Le cadre juridique en matière de respect de la vie privée au Québec

Les articles 44 et 45 de la Loi sur le privé prévoient des exigences précises relativement au traitement des données biométriques. Les entreprises faisant affaire au Québec qui utilisent des données biométriques aux fins de la vérification ou de la confirmation de l'identité d'une personne doivent respecter aussi bien la Loi sur le privé, qui établit des exigences générales relativement au traitement des renseignements personnels, que la Loi sur les TI, qui prévoit, aux articles 44 et 45, des exigences particulières relativement au traitement des données biométriques.

Plus précisément, pour utiliser des données biométriques aux fins d'identification, les entreprises sont tenues, en vertu de la Loi sur les TI, de faire ce qui suit :

- obtenir le consentement exprès des personnes avant d'utiliser leurs données biométriques pour vérifier ou confirmer leur identité;
- informer les personnes de manière adéquate du traitement de leurs données biométriques et leur proposer un autre moyen de vérification de l'identité ne recourant pas aux données biométriques;
- déclarer l'utilisation de données biométriques aux fins d'identification, y compris la création d'une banque de données biométriques, dans les délais prescrits par la Loi sur les TI[3].

L'entreprise qui ne respecte pas ces exigences, entre autres, s'expose à des mesures d'application de la loi, y compris des ordonnances de suspension, de destruction ou d'interdiction du déploiement d'une banque de données biométriques, ou à des ordonnances exigeant la modification des pratiques de traitement des données biométriques. En outre, en vertu de la Loi sur le privé, une telle entreprise pourrait s'exposer à des amendes ou à des sanctions administratives pécuniaires, y compris des sanctions pouvant aller jusqu'à 10 millions de dollars ou 2 % du chiffre d'affaires mondial de l'exercice précédent, le montant le plus élevé étant retenu.

Principales constatations et conclusions

La CAI a évalué si le processus projeté de traitement des données biométriques de Metro était soumis à la Loi sur les TI et, si tel était le cas, si son projet pilote garantirait l'obtention d'un consentement exprès des personnes avant que leurs données biométriques ne soient utilisées aux fins de vérification de l'identité, comme l'exige l'article 44 de la Loi sur les TI.

La CAI a conclu que le projet pilote de l'entreprise contreviendrait à la Loi sur les TI du fait que le consentement exprès requis ne serait pas obtenu. La CAI a souligné la nature automatique et systématique de la collecte de données biométriques auprès de toutes les personnes entrant dans l'établissement et a noté que l'entreprise elle-même admettait qu'il ne serait pas possible d'obtenir le consentement exprès de chaque visiteur.

Arrivant à la conclusion que, sans consentement, la banque de données biométriques projetée par l'entreprise constituait une « atteinte au respect de la vie privée » importante au sens de l'article 45 de la Loi sur les TI, la CAI a rendu une ordonnance interdisant à l'entreprise de déployer la banque de données dans le contexte actuel. Il est à noter que c'est la première fois que la CAI s'appuie sur ce fondement juridique pour rendre une telle ordonnance.

Bien que la CAI ait conclu d'emblée que le consentement exprès n'aurait pas été obtenu dans le cadre du projet pilote, son analyse des arguments de l'entreprise contestant l'applicabilité de cette exigence apporte des éclaircissements importants sur la portée des dispositions relatives au traitement des données biométriques de la Loi sur les TI et sur leur interaction avec la Loi sur le privé :

- **Étendue de la vérification ou de la confirmation de l'identité en vertu de la Loi sur les TI :** L'entreprise a fait valoir que l'utilisation projetée de données biométriques aux fins d'identification ne constituerait pas « une confirmation ou une vérification » de l'identité au sens de l'article 44 de la Loi sur les TI. Rejetant cet argument, la CAI a adopté une interprétation large et téléologique de la disposition. Plus précisément, la CAI a précisé que la vérification et la confirmation de l'identité englobent à la fois l'authentification (comparaison d'un à un) et l'identification (comparaison d'un à plusieurs) et ne nécessitent pas de relier une personne à son nom, à sa date de naissance ou à d'autres attributs de base de l'identité. Ainsi, l'utilisation de la reconnaissance faciale projetée par l'entreprise aux fins de l'identification des personnes impliquées dans des vols à l'étalage ou des fraudes antérieurs est considérée comme un processus de vérification de l'identité au sens de la Loi sur les TI.
- **Moment de l'extraction des données biométriques et de l'identification :** L'entreprise a fait remarquer que l'exigence de consentement exprès ne s'applique que lorsque l'identité est vérifiée « au moyen » d'un procédé permettant de saisir des données biométriques[4], ce qui, selon elle, signifie que le procédé doit simultanément recueillir des données biométriques et les utiliser pour vérifier l'identité d'une personne. Puisque, dans le cadre du projet, a fait valoir l'entreprise, la collecte et l'utilisation de données biométriques auraient eu lieu à des moments différents, la disposition ne s'appliquait pas. La CAI a rejeté cet argument, car, selon elle, il faut considérer l'effet combiné de l'ensemble des opérations du système d'identification et considérer les différentes phases comme étant

interdépendantes. En conséquence, l'exigence de consentement exprès s'applique même si la collecte des données biométriques et la vérification de l'identité ont lieu à des moments différents.

- **Exceptions à l'exigence de consentement prévues par la Loi sur le privé :** L'entreprise a également tenté d'invoquer les exceptions prévues à l'article 12 de la Loi sur le privé, qui autorisent l'utilisation de renseignements personnels sans consentement à certaines fins secondaires, telles que la prévention et la détection de la fraude, et à des fins compatibles avec celles pour lesquelles les renseignements ont été recueillis. En concluant que les exceptions à l'exigence de consentement ne pouvaient être invoquées pour le projet pilote, la CAI a estimé que l'extraction de données biométriques à partir d'images faciales brutes captées par le système de vidéosurveillance constituerait une nouvelle collecte de renseignements personnels plutôt qu'une utilisation secondaire. L'entreprise ne pouvait donc pas invoquer les exceptions à l'exigence de consentement applicables à l'utilisation secondaire de renseignements personnels pour passer outre l'exigence de consentement exprès prévue par la Loi sur les TI lorsqu'elle recueille des données biométriques pour vérifier ou confirmer l'identité d'une personne.

Principaux points à retenir pour les entreprises

Alors que l'utilisation de la vidéosurveillance est une pratique courante dans les commerces de détail au Québec, cette décision constitue un rappel important que, pour extraire des données biométriques à partir d'images brutes captées par un système de vidéosurveillance, les entreprises faisant affaire au Québec doivent respecter des exigences sévères en matière de collecte et d'utilisation de données biométriques aux fins de vérification ou de confirmation de l'identité.

En outre, les entreprises faisant affaire au Québec doivent savoir que les exigences de la Loi sur les TI en matière de biométrie, y compris l'obligation d'obtenir un consentement exprès, ont préséance sur celles de la Loi sur le privé du fait qu'elles sont plus sévères. En outre, les exceptions à l'obligation de consentement applicables à des fins secondaires, telles que la prévention de la fraude ou d'autres fins commerciales légitimes, ont peu de chances de s'appliquer lorsque les données biométriques sont utilisées pour vérifier ou confirmer l'identité d'une personne.

Les entreprises qui envisagent de mettre en place une technologie de reconnaissance faciale ou d'autres technologies biométriques devraient, avant leur déploiement, examiner attentivement les obligations qui leur incombent en vertu de la Loi sur les TI et de la Loi sur le privé afin de garantir leur respect et de réduire le risque d'être visées par des mesures d'application de la loi.

---

[1] Au Québec, le « critère de nécessité » fait référence aux obligations prévues aux articles 4 et 5 de la Loi sur le privé, suivant lesquels les entreprises qui, en raison d'un intérêt sérieux et légitime, recueillent des renseignements personnels ne doivent recueillir que ceux qui sont nécessaires.

[2] Sur ce point, la CAI renvoie au préavis d'ordonnance qu'elle a adressé à l'entreprise, selon

lequel le fait que le processus projeté soit basé sur les interventions policières pour vol à l'étalage et fraude plutôt que sur des jugements reconnaissant la culpabilité des personnes impliquées dans ces événements pourrait contrevenir au droit d'être présumé innocent et avoir ainsi une incidence sur le test de la légitimité prévu à l'article 4 de la Loi sur le privé.

[3] Selon les articles 44 et 45 de la Loi sur les TI, la déclaration doit être soumise à la CAI au plus tard 60 jours avant la mise en service de la banque de données ou, si aucune banque de données n'est créée, à tout moment avant que les données biométriques ne soient utilisées aux fins d'identification.

[4] La décision ne traite pas expressément d'une divergence entre les versions anglaise et française de l'article 44 de la Loi sur les TI. Dans la version française de cette disposition, le législateur a eu recourt au terme « saisir » pour décrire le processus biométrique visé, ce qui suggère que l'accent est mis sur la phase de la collecte. En revanche, dans la version anglaise du passage en question, qui se lit comme suit : « *a process that allows biometric characteristics or measurements to then be used* » (librement traduit par « processus qui permet alors d'utiliser les caractéristiques ou les mesures biométriques »), le législateur a mis l'accent sur une phase ultérieure du processus biométrique. Bien que cette divergence n'ait pas fait l'objet d'une discussion particulière, elle confirme la conclusion de la CAI selon laquelle il faut considérer les phases du traitement des données biométriques dans leur ensemble lorsqu'il s'agit de déterminer si l'article 44 s'applique.