

La Commission d'accès à l'information du Québec maintient la sévérité des exigences applicables au traitement des renseignements biométriques : leçons pour les entreprises



22 JANVIER 2025 14 MIN DE LECTURE

Expertises Connexes

- [Droit du travail et de l'emploi](#)
- [Intelligence artificielle](#)
- [Respect de la vie privée et gestion de l'information](#)

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

À la fin de l'année dernière, la section de surveillance de la Commission d'accès à l'information du Québec (CAI) a rendu sa première décision depuis l'entrée en vigueur des changements considérables apportés par la Loi 25. Elle a rendu sa [décision](#) (datée de septembre 2024) après avoir fait enquête sur les pratiques d'une imprimerie qui lui avait déclaré son utilisation d'un système biométrique, comme l'exigent les lois du Québec. La CAI a ordonné à l'entreprise de cesser d'utiliser la reconnaissance faciale pour contrôler l'accès des employés à ses locaux et a conclu que, l'utilisation de renseignements biométriques aux fins de la reconnaissance faciale n'était pas suffisamment nécessaire et proportionnelle pour justifier l'atteinte grave atteinte à la vie privée des employés que représente cette pratique selon la CAI.

Tout en étant cohérente avec les ordonnances et lignes directrices antérieures de la CAI, la décision souligne la sévérité des obligations à respecter pour pouvoir utiliser la reconnaissance faciale et d'autres technologies d'identification biométrique au Québec en vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé* (la Loi sur le privé) et des dispositions connexes de la *Loi concernant le cadre juridique des technologies de l'information* (la Loi sur les TI).

La décision reflète également une tendance observée au Québec ces dernières années, où la CAI – conformément aux exigences particulières de la province concernant la constitution de banques de caractéristiques ou de mesures biométriques^[1] – a pris des mesures d'application de la loi contre les entreprises qui utilisaient ces technologies et a exprimé son scepticisme quant à la nécessité et à la proportionnalité de ces outils. Cette tendance est évidente non seulement dans la récente décision de la CAI, mais aussi dans ses récentes lignes directrices^[2], ainsi que dans ses interactions avec les entreprises qui déclarent des systèmes biométriques^[3].

La position de la CAI sur l'utilisation de la biométrie est particulièrement intéressante pour

les entreprises, compte tenu des lourdes sanctions pécuniaires prévues en cas de non-respect des lois du Québec en matière de protection de la vie privée. En vertu de la Loi sur le privé, les sanctions administratives pécuniaires peuvent atteindre 10 millions de dollars ou 2 % du chiffre d'affaires mondial, le montant le plus élevé étant retenu.

Dans le présent bulletin, nous présentons les principales obligations légales régissant les systèmes de vérification de l'identité au moyen de la biométrie au Québec, l'application par la CAI de ces obligations aux faits de cette décision, ainsi que de précieuses indications à l'intention des entreprises.

Cadre juridique et lignes directrices réglementaires

Au Québec, les entreprises du secteur privé sont soumises à la Loi sur le privé, qui définit les règles et les principes régissant la collecte, l'utilisation, la communication et la conservation des renseignements personnels, y compris les renseignements biométriques.

Les renseignements biométriques constituent des renseignements personnels sensibles en vertu de la Loi sur le privé^[4]. De plus, la CAI a souligné que leur caractère unique et immuable les rendait particulièrement sensibles.

En outre, les renseignements biométriques sont visés par des exigences de déclaration particulières au Québec. Outre l'obtention d'un consentement explicite, les entreprises doivent déclarer à la CAI qu'elles prévoient d'utiliser un système biométrique aux fins d'identification et doivent lui déclarer la création d'une banque de renseignements biométriques au moins 60 jours avant son déploiement ([un formulaire de déclaration standard \[PDF\]](#) est disponible à cette fin sur le site Web de la CAI). Selon l'interprétation que la CAI a toujours donnée aux dispositions applicables de la Loi sur les TI, les entreprises qui utilisent la biométrie aux fins d'identification ont l'obligation d'offrir aux personnes concernées une solution de rechange ne faisant pas appel à la biométrie.

Comme la CAI le souligne dans son [guide d'accompagnement pour les entreprises](#) (voir note 2 plus haut), la Loi sur le privé prévoit que la collecte de renseignements personnels doit être effectuée pour un motif sérieux et légitime et se limiter aux renseignements nécessaires aux fins déterminées préalablement^[5]. Pour évaluer le respect de ces exigences, la CAI exige des entreprises qu'elles démontrent que la collecte de renseignements personnels remplit les deux critères suivants :

1. **objectif légitime, important et réel** : l'entreprise doit établir que l'objectif poursuivi par la collecte est légitime, important et réel;
2. **proportionnalité** : l'entreprise doit établir la proportionnalité entre l'atteinte à la vie privée qui est commise par la collecte et l'objectif poursuivi, ce qui, à son tour, veut dire de démontrer ce qui suit :
 - la collecte est rationnellement liée à l'objectif poursuivi;
 - l'atteinte à la vie privée est minimisée;
 - la collecte est nettement plus utile à l'entreprise que préjudiciable aux personnes concernées.

En appliquant ces critères, les entreprises doivent prendre en considération des facteurs tels que (i) la nature sensible des renseignements personnels visés, (ii) les autres moyens à leur disposition pour atteindre l'objectif poursuivi et (iii) les conséquences de l'atteinte à la vie privée pour les personnes concernées. Il est important de noter que le consentement d'une personne à la collecte de ses renseignements personnels n'est pas suffisant pour justifier la

collecte si celle-ci ne répond pas aux critères indiqués ci-dessus^[6].

Aperçu de la décision

Dans cette décision, un employeur du secteur de l'imprimerie a mis en place un système de reconnaissance faciale pour contrôler l'accès de ses employés à ses locaux. L'ayant initialement introduit comme mesure de santé et de sécurité du travail devant limiter la propagation de la COVID-19, l'employeur a continué à utiliser le système pour contrôler les accès de manière générale après le pic de la pandémie.

Aux fins de la vérification de son identité par le système biométrique, l'employé devait se présenter devant le lecteur biométrique à l'entrée des locaux de l'employeur. Le système prenait alors une photo du visage de l'employé, la convertissait en une représentation numérique irréversible (également appelée « modèle biométrique »), puis la comparait au modèle créé lors de l'inscription initiale de l'employé. S'il était établi que les modèles correspondaient, l'accès aux locaux était accordé. Le système comprenait à l'origine une fonction de vérification de la température, mais cette fonctionnalité a été supprimée par la suite et n'a pas été prise en compte dans la décision de la CAI.

Il est à noter que l'employeur avait obtenu le consentement des employés relativement à la collecte et au traitement de leurs renseignements biométriques et avait déclaré la création d'une banque de renseignements biométriques à la CAI, comme la loi l'exige.

En appliquant aux faits les critères relatifs à la nécessité susmentionnés, la CAI a conclu que la collecte de renseignements biométriques par l'employeur aux fins du contrôle des accès ne répondait pas aux exigences de la Loi sur le privé.

Plus précisément, l'employeur n'a pas rempli le premier des deux critères, car il n'a pas pu démontrer que l'objectif poursuivi, soit contrôler les accès au moyen de la reconnaissance faciale, était « réel » ou « important », même si, en soi, l'objectif de sécurité était considéré comme « légitime ».

La CAI a également estimé que l'employeur n'avait pas rempli le deuxième critère. Bien qu'elle ait reconnu que la collecte était rationnellement liée à l'objectif poursuivi, la CAI a déterminé que l'atteinte à la vie privée des employés n'était pas suffisamment minimisée, et que les avantages du système ne l'emportaient pas clairement sur les préjudices que pourraient subir les employés.

En conséquence, la CAI a conclu que la collecte de renseignements biométriques aux fins de la reconnaissance faciale contrevenait à la Loi sur le privé et a ordonné à l'employeur de cesser de collecter de tels renseignements, de cesser d'utiliser le système de reconnaissance faciale aux fins du contrôle des accès et de détruire tous les renseignements biométriques qui avaient déjà été collectés.

Enseignements pour les entreprises

Cette décision illustre l'approche rigoureuse adoptée par la CAI lorsqu'elle évalue la légalité de la collecte de renseignements biométriques et d'autres renseignements personnels sensibles en vertu de la Loi sur le privé. La décision peut également avoir des répercussions générales à l'échelle du Canada, compte tenu de l'intérêt que suscite la reconnaissance faciale et les technologies similaires pour les autorités réglementaires, ainsi que de la consultation publique en cours lancée par le Commissariat à la protection de la vie privée du Canada avec son *Document d'orientation provisoire à l'intention des organisations sur le traitement des renseignements biométriques*.

Bien que les conclusions de la CAI dans cette décision soient cohérentes avec les lignes directrices et les décisions antérieures, son analyse et son application aux faits en l'espèce de chacun des critères relatifs à la nécessité fournissent des enseignements précieux pour les entreprises qui cherchent à mettre en œuvre des solutions d'identification biométrique :

- **fournir une preuve objective d'un objectif réel et important** : pour démontrer qu'un système biométrique sert un objectif important et réel, les entreprises doivent fournir des preuves objectives et bien documentées de l'existence d'un problème réel. À moins qu'une entreprise n'exerce ses activités dans un secteur où des exigences réglementaires ou de sécurité accrues imposent l'utilisation de systèmes biométriques (par exemple, infrastructures critiques ou environnements hautement sensibles), des allégations généralisées ou des risques spéculatifs sont généralement insuffisants. Les entreprises doivent donc soigneusement documenter la nature, la gravité et la fréquence du problème que le système biométrique est censé résoudre.
- **éviter les justifications générales ou basées sur la commodité** : il est peu probable que les enjeux opérationnels communs à la plupart des entreprises répondent au critère relatif à l'« importance », car ils sont souvent considérés comme des questions de commodité plutôt que de nécessité. De même, les exigences des programmes volontaires ou des certifications n'apportent qu'un soutien limité, en particulier lorsque l'identification biométrique est facultative ou présentée comme une solution potentielle parmi d'autres plutôt que comme une exigence devant être respectée.
- **démontrer un niveau élevé de proportionnalité** : la collecte de renseignements biométriques représente une grave atteinte à la vie privée en raison de la nature sensible des renseignements, du fait de leurs caractéristiques intimes, uniques et immuables. Pour cette raison, les entreprises doivent démontrer un niveau élevé de proportionnalité.
- **ne pas seulement miser sur les mesures de sécurité, car elles ne minimisent pas l'atteinte à la vie privée** : si des mesures de sécurité solides, telles que le cryptage, sont importantes pour protéger les renseignements biométriques, elles ne réduisent pas le niveau d'atteinte à la vie privée inhérent à la collecte de ces renseignements. Par conséquent, la mise en œuvre de contrôles de sécurité rigoureux ne peut à elle seule remplir le critère relatif à la proportionnalité.
- **documenter les solutions de rechange envisagées** : les entreprises doivent fournir des preuves documentées des solutions de rechange envisagées et expliquer pourquoi ces solutions ont été jugées insuffisantes pour atteindre l'objectif poursuivi. Par exemple, lorsque des systèmes biométriques sont utilisés pour contrôler l'accès à des installations, d'autres solutions telles que des badges, des cartes, des codes ou des clés doivent généralement être envisagées. Les affirmations selon lesquelles les solutions biométriques sont plus efficaces ou que les autres solutions présentent des risques hypothétiques (par exemple, le partage de badges ou le « buddy punching ») ont peu de chances d'être convaincantes si elles ne sont pas étayées par des preuves réelles et documentées.

Principales étapes pour assurer la conformité

Afin d'atténuer les risques réglementaires et de respecter les normes élevées établies par la

CAI pour le traitement légal des renseignements biométriques, les entreprises qui envisagent de mettre en œuvre des solutions d'identification biométrique au Québec devraient prendre en considération les étapes suivantes :

- **procéder à une évaluation des facteurs relatifs à la vie privée (EFVP)** avant la mise en œuvre de la solution biométrique afin d'évaluer et d'atténuer les risques d'atteinte à la vie privée et de démontrer le respect de toutes les obligations pertinentes en matière de protection des renseignements personnels (par exemple, notification et transparence, consentement valable, minimisation, conservation et destruction des renseignements, sécurité de l'information, transferts transfrontaliers de renseignements et externalisation, droits individuels à la protection de la vie privée) en cas de plainte ou d'enquête. Il convient de noter qu'en vertu de la Loi sur le privé, une entreprise est tenue de procéder à une EFVP de tout projet d'acquisition, de développement et de refonte d'un système biométrique^[7].
- **évaluer la nécessité et la proportionnalité du traitement des renseignements biométriques**, en tenant compte des lignes directrices et décisions réglementaires pertinentes, y compris les conclusions de la récente décision de la CAI présentées ci-dessus (cette évaluation devrait être documentée dans l'EFVP mentionnée ci-dessus).
- **rassembler des preuves, des faits et des statistiques pertinents pour documenter et étayer votre dossier**, y compris toute affirmation concernant la nécessité, la proportionnalité, l'efficacité et le caractère peu intrusif de la solution biométrique proposée.
- **préparer soigneusement la déclaration relative au système biométrique devant être produite à la CAI**, en tenant compte des obligations légales et réglementaires pertinentes et en collaborant avec les parties prenantes internes et externes concernées (par exemple, les fournisseurs de solutions biométriques), au besoin, afin de garantir l'exactitude et l'exhaustivité des renseignements.

Les abonnés d'AccessPrivacy peuvent obtenir des précisions supplémentaires sur le cadre juridique applicable aux renseignements biométriques, notamment dans les pôles thématiques sur la biométrie. Pour en savoir plus, consultez le site d'AccessPrivacy [en anglais seulement].

[1] Articles 44-45 de la Loi sur les TI.

[2] Dans son guide de 2022, « Biométrie : principes à respecter et obligations légales des organisations », la CAI s'inquiète du recours accru à la biométrie et met en garde contre la banalisation de ses implications potentiellement importantes en matière de protection des renseignements personnels. De même, dans un rapport publié en 2023, intitulé « Horodateurs et pointeuses biométriques – constats », la CAI a conclu que la plupart des pointeuses biométriques en milieu de travail qu'elle a examinées ne respectaient pas les obligations légales strictes de nécessité et de proportionnalité prévues par la Loi sur le privé. Cette position est généralement conforme aux décisions antérieures de la CAI (voir Auberge du lac Sacacomie inc., CAI 1014137-S, 7 avril 2022; Enquête à l'égard de Compagnie Selenis Canada, CAI 1016217-S, 14 janvier 2022; Plainte à l'endroit du « Marché d'alimentation Marcanio et fils inc. »).

[3] Dans le contexte des dossiers portant sur la biométrie et d'autres interactions réglementaires, la CAI s'est montrée de plus en plus disposée à remettre en question la légalité des pratiques biométriques. En particulier, les entreprises qui déclarent à la CAI qu'elles utilisent un système biométrique reçoivent souvent des lettres de réponse concernant une *éventuelle* non-conformité. Bien que ces lettres ne constituent pas des décisions officielles ou contraignantes, elles relèvent généralement diverses violations *potentielles* sur la base de l'examen par la CAI de la documentation soumise et, dans certains cas, mettent en garde contre des amendes potentiellement lourdes en cas de non-respect de ces questions si une enquête officielle était menée.

[4] Article 12, par. 5, alinéa (2) de la Loi sur le privé.

[5] Articles 4 et 5 de la Loi sur le privé.

[6] Voir le par. 59 de la décision.

[7] Article 3.3 de la Loi sur le privé.