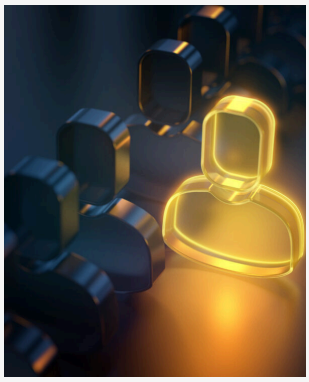
OSLER

Les exigences du Québec en matière d'anonymisation un an plus tard : leçons et questions en suspens pour les entreprises



8 MAI 2025 19 MIN DE LECTURE

Expertises Connexes

- Cybersécurité et intervention en cas d'incident lié à la sécurité
- Respect de la vie privée et gestion de l'information

Auteurs(trice): Éloïse Gratton, Ad. E., Katelyn Smith, Catherine Hart

Entré en vigueur le 30 mai 2024[1], le *Règlement sur l'anonymisation des renseignements personnels* [PDF] du Québec (le *Règlement sur l'anonymisation*) prévoit des exigences particulières pour l'anonymisation des renseignements personnels en vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé* (la *Loi sur le privé* ou la *Loi*)[2]. Près d'un an plus tard, demeurent en suspens des questions clés concernant la portée et l'application du *Règlement sur l'anonymisation* et les mesures pratiques que les organisations cherchant à anonymiser des renseignements personnels en vertu de la *Loi sur le privé* devraient prendre pour mettre en œuvre les exigences qui les concernent.

Qu'est-ce que l'« anonymisation » ?

Comme la plupart des lois en matière de protection des renseignements personnels, la *Loi sur le privé* réglemente les « renseignements personnels », c'est-à-dire les renseignements concernant une personne identifiable. Par conséquent, tout renseignement qui ne correspond pas à la définition de renseignements personnels n'est pas (ou n'est plus) soumis à la *Loi*.

L'« anonymisation » est un processus de modification des renseignements personnels visant à réduire le risque qu'une personne soit identifiée, directement ou indirectement, à partir des renseignements résiduels, en-deçà du seuil prévu par la loi (voir ci-dessous pour plus de détails à ce sujet). Les renseignements anonymisés conformément à ce seuil ne constituent plus des « renseignements personnels » et tombent, par conséquent, en dehors du champ d'application de la *Loi*.

Les renseignements « anonymisés » se distinguent des renseignements « dépersonnalisés » (ou « pseudonymisés »), que la *Loi sur le privé* définit comme des renseignements personnels qui « ne permettent plus d'identifier *directement* la personne concernée » [soulignement ajouté]. Puisque les renseignements dépersonnalisés peuvent encore permettre d'identifier une personne de manière indirecte, ils conservent leur statut de « renseignements personnels » et demeurent assujettis à la *Loi*. Loin d'être théorique, cette distinction a des conséquences juridiques importantes, en particulier pour les organisations qui souhaitent utiliser ou communiquer des renseignements anonymisés sans consentement. Toute organisation qui utilise ou communique, sans consentement ou autre fondement juridique valable, des renseignements qui n'ont pas été anonymisés correctement risque d'enfreindre

la loi et de s'exposer à des mesures d'application de la loi de la part de la Commission d'accès à l'information (CAI)[3].

Il convient de noter que ces termes ne sont pas toujours employés de manière cohérente d'un territoire à l'autre et d'un texte législatif à l'autre. Par exemple, si, quant au fond, le terme « anonymiser » est défini de la même manière dans la *Loi sur le privé*, le *Règlement général sur la protection des données* (*RGPD*) de l'Union européenne et le règlement correspondant du Royaume-Uni, et l'ancien projet de loi C-27 du gouvernement fédéral du Canada (qui est mort au feuilleton en janvier 2025), le terme « *de-identify*[4] » utilisé dans la version anglaise de la *Loi de 2004 sur la protection des renseignements personnels sur la santé* (*LPRPS*) de l'Ontario renvoie à un concept dont la fonction est équivalente. Pour s'assurer que tous comprennent bien les termes employés, il convient de les utiliser avec prudence, en particulier dans les ententes commerciales, où l'absence de définition claire peut créer de l'incertitude et exposer l'une ou l'autre des parties (voire les deux) à un risque de non-conformité règlementaire, par exemple s'il est question de « renseignements anonymisés » mais que le seuil d'anonymisation prévu par la loi applicable n'est pas satisfait.

Cadre législatif de l'anonymisation au Québec

Dans la *Loi sur le privé*, il est peu question d'anonymisation ; seules les trois dispositions suivantes la mentionnent :

- L'article 23 est la disposition qui introduit le concept de renseignement anonymisé. Selon l'article 23, un renseignement est anonymisé « lorsqu'il est, en tout temps, raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne ». En vertu de l'article 23, les renseignements anonymisés doivent également l'être « selon les meilleures pratiques généralement reconnues » et « selon les critères et modalités déterminés par règlement ».
    - L'article 23 constitue essentiellement une obligation de minimisation des données. Il prévoit que, lorsque les fins auxquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, l'organisation doit « le détruire ou l'anonymiser pour l'utiliser à des fins sérieuses et légitimes ». En d'autres termes, l'article 23 autorise les organisations à anonymiser un renseignement personnel au lieu de le détruire ; cependant, de façon générale, il ne traite pas de l'anonymisation effectuée au cours du cycle de vie du renseignement personnel, avant le moment où l'organisation est tenue de le détruire. Pour plus de précisions sur ce sujet, voir la rubrique *Questions clés en suspens* ci-dessous.
- L'alinéa 3.2 de l'article 90 confère au gouvernement du Québec le pouvoir d'adopter des règlements *aux fins de l'article 23* (c'est-à-dire en lien avec l'obligation de détruire ou d'anonymiser un renseignement personnel).
- L'alinéa 5 de l'article 91 prévoit que commet une infraction quiconque procède ou tente de procéder à l'identification d'une personne à partir de renseignements anonymisés.

Exigences prévues par le Règlement sur l'anonymisation

En vertu du *Règlement sur l'anonymisation,* lorsqu'elle procède à l'anonymisation de renseignements personnels en application de l'article 23 de la *Loi sur le privé,* une organisation doit respecter les huit exigences suivantes :

1. Elle doit établir les fins « sérieuses et légitimes » auxquelles elle entend utiliser les renseignements anonymisés[5].
2. Elle doit réaliser le processus d'anonymisation sous la supervision d'une « personne compétente en la matière »[6].
3. Elle doit retirer des renseignements qu'elle entend anonymiser tous les renseignements personnels qui permettent d'identifier directement la personne concernée (comme son nom, ses coordonnées ou son numéro d'assurance sociale)[7].
4. Elle doit effectuer une analyse préliminaire des risques de réidentification, enconsidérant les éléments prévus par règlement, notamment :
   - le critère d'individualisation, le critère de corrélation et le critère d'inférence
   - les risques que d'autres renseignements raisonnablement disponibles, notamment dans l'espace public, soient utilisés pour identifier une personne[8]
5. Elle doit établir des techniques d'anonymisation et des mesures de sécurité appropriées, conformes aux meilleures pratiques généralement reconnues, pour diminuer les risques de réidentification[9].
6. Elle doit ensuite effectuer une analyse des risques de réidentification qui démontre que les risques résiduels de réidentification sont « très faibles » (il n'est pas nécessaire de démontrer un risque nul), en tenant compte des éléments prévus par règlement, notamment :
   - les fins et les circonstances de l'anonymisation
   - la nature des renseignements
   - le critère d'individualisation, le critère de corrélation et le critère d'inférence
   - les risques que d'autres renseignements raisonnablement disponibles, notamment dans l'espace public, soient utilisés pour identifier une personne
   - les efforts, les ressources et le savoir nécessaires pour réidentifier la personne[10]
7. Elle doit périodiquement réévaluer les risques de réidentification pour s'assurer que les risques résiduels de réidentification demeurent « très faibles » (il n'est pas nécessaire que le risque soit nul), en considérant, notamment, les progrès technologiques. La périodicité à laquelle elle doit évaluer ces renseignements est déterminée en fonction des risques résiduels identifiés dans la dernière analyse des risques de réidentification qu'elle a effectuée[11].
8. Elle doit tenir un « registre » d'anonymisation contenant les renseignements prévus par règlement, notamment :
   - une description des renseignements personnels qui ont été anonymisés
   - les fins pour lesquelles ces renseignements anonymisés sont utilisés
   - les techniques d'anonymisation utilisées et les mesures de sécurité établies
   - les dates auxquelles la première analyse des risques et les suivantes ont été complétées[12]

Questions clés en suspens

Pour les organisations faisant affaire au Québec, la *Loi sur le privé* fournit un cadre utile pour

l'anonymisation et apporte plusieurs clarifications importantes, notamment le fait qu'il n'est pas nécessaire de démontrer un *risque nul* de réidentification pour que les critères d'anonymisation soient satisfaits. Toutefois, il n'en reste pas moins que des questions clés demeurent en suspens, notamment les suivantes :

Portée et application du Règlement sur l'anonymisation

Comme il est indiqué ci-dessus, les dispositions habilitantes de la *Loi sur le privé* (à savoir l'article 23 et l'alinéa 3.2 de l'article 90), qui introduisent l'anonymisation et confèrent au gouvernement du Québec le pouvoir d'adopter des règlements, sont fondées sur une obligation de minimisation des données qui autorise le recours à l'anonymisation comme solution de rechange à la destruction.

Comme la *Loi sur le privé* est muette sur l'anonymisation au cours du cycle de vie d'un renseignement personnel avant le moment où l'organisation est tenue de le détruire, il reste à savoir si les exigences prévues par le *Règlement sur l'anonymisation* s'appliquent uniquement à l'anonymisation du renseignement personnel effectuée au moment où l'organisation a l'obligation de le détruire ou si elles s'appliquent également à l'anonymisation du renseignement personnel effectuée plus tôt au cours de son cycle de vie (c'est-à-dire, hors du champ d'application de l'article 23).

Le libellé des deuxième et troisième paragraphes de l'article 23, qui renvoient à l'anonymisation effectuée « [p]our l'application de la présente loi » et « en vertu de la présente loi », pourrait appuyer cette interprétation plus large. Ce libellé laisse entendre que le *Règlement sur l'anonymisation* pourrait s'appliquer de façon générale à toute anonymisation de renseignements personnels effectuée en vertu de la *Loi*, et non seulement à l'anonymisation effectuée à la fin du cycle de vie du renseignement. Cette interprétation cadre avec la façon dont le législateur a utilisé, ailleurs dans la *Loi*, un libellé similaire pour signaler un élargissement du champ d'application, alors que, en règle générale, il utilise l'expression « en vertu du présent article » lorsqu'il a l'intention de limiter l'effet d'une disposition à un article particulier.

Cette question d'interprétation soulève d'importantes considérations pratiques. Il convient de noter que la CAI a précédemment indiqué sur son site Web qu'en l'absence d'un règlement établissant des exigences précises en matière d'anonymisation, il n'était pas possible d'anonymiser des renseignements en vertu de la *Loi*. Si on devait interpréter le *Règlement sur l'anonymisation* comme un règlement ne s'appliquant qu'à la fin du cycle de vie des renseignements personnels, il pourrait en résulter une incertitude pour les organisations quant à la position de la CAI sur la question de savoir si l'anonymisation est permise plus tôt dans le cycle de vie des renseignements (voir la rubrique *Autorisation légale d'anonymiser des renseignements personnels* ci-après).

Autorisation légale d'anonymiser des renseignements personnels

La déclaration de la CAI selon laquelle, en l'absence de règlement, il n'était pas possible d'anonymiser des renseignements personnels soulève également des questions concernant l'autorisation légale d'en anonymiser en premier lieu. En d'autres termes, si des renseignements bel et bien anonymisés n'entrent pas dans le champ d'application de la *Loi*, certains se demandent si une autorisation légale est nécessaire pour mener à bien le processus d'anonymisation en premier lieu.

Par exemple, en vertu de la *LPRPS* de l'Ontario et du *RGPD* de l'UE et du Royaume-Uni, les organismes de réglementation de la protection des renseignements personnels considèrent l'anonymisation de renseignements personnels comme une « utilisation » (*use*) ou une « opération de traitement » (*processing operation*) qui nécessite un fondement juridique valide

en vertu du cadre de protection des données applicable[13]. Cependant, contrairement à la *Loi sur le privé*, qui est un régime fondé sur le consentement, la *LPRPS* de l'Ontario comprend une autorisation légale expresse d'anonymiser[14] et le *RGPD* de l'UE et du Royaume-Uni reconnaît de multiples fondements juridiques au-delà du consentement (tels que les intérêts légitimes)[15].

À l'instar de la *Loi sur la protection des renseignements personnels et les documents électroniques* du Canada, la *Loi sur le privé* n'autorise pas expressément les organisations à anonymiser des renseignements personnels hors du champ d'application de l'article 23 (c'est-à-dire comme solution de rechange à la destruction). Bien que ni le Commissariat à la protection de la vie privée du Canada ni la CAI n'aient pris de position claire sur cette question à ce jour, il semble y avoir un consensus parmi de nombreux intervenants – bien qu'il soit généralement fondé sur des considérations pratiques plutôt que sur une interprétation juridique établie – sur le fait qu'une autorisation légale distincte n'est pas nécessaire. Cette position est généralement fondée sur la notion que l'anonymisation de renseignements personnels sert à modifier des renseignements personnels en vue de protéger à la fois leur caractère confidentiel et le droit à la vie privée de la personne concernée, et est souvent utilisée comme mesure de sécurité (pour laquelle le consentement n'est manifestement pas nécessaire). En effet, la *Loi sur le privé* prévoit une exception au consentement à l'utilisation de renseignements personnels à des fins de production de statistiques *si les renseignements sont dépersonnalisés*[16]. De l'avis de nombreuses personnes, il serait absurde que, en pareil contexte, la dépersonnalisation nécessite une autorisation légale distincte.

Pour atténuer l'incertitude sur ce point, un nombre croissant d'organisations au Québec et dans l'ensemble du Canada prennent des mesures proactives pour améliorer la transparence de leurs pratiques d'anonymisation, notamment en mettant à jour leurs politiques externes de protection des renseignements personnels.

Obligation d'établir les « fins sérieuses et légitimes »

L'obligation d'établir les « fins sérieuses et légitimes » auxquelles les renseignements anonymisés seront utilisés est propre à la *Loi sur le privé* et n'a pas d'équivalent connu dans les lois en matière de protection des renseignements personnels ailleurs au pays ou à l'étranger. Pour les raisons exposées à la rubrique « Qu'est-ce que l'« anonymisation » ? » ci-dessus, de façon générale, les renseignements qui ont été anonymisés peuvent être utilisés sans restriction, car ils ne sont plus régis par les lois en matière de protection des renseignements personnels.

Le terme « fins sérieuses et légitimes » n'est pas défini dans la *Loi sur le privé* ni dans le *Règlement sur l'anonymisation*. Toutefois, dans le contexte de la *collecte* de renseignements personnels en vertu de l'article 4 de la *Loi sur le privé*, la CAI a considéré que des fins étaient « sérieuses et légitimes » lorsqu'elles étaient « légitimes, importantes et réelles » et que l'atteinte au droit à la vie privée était « proportionnelle aux objectifs poursuivis », en tenant compte, entre autres, de la sensibilité des renseignements, de la légalité de l'objectif poursuivi et de sa conformité au droit, à la justice et à l'équité[17].

Même si la CAI pourrait chercher à appliquer un critère similaire lorsqu'elle évalue le caractère sérieux et légitime des fins poursuivies par une organisation dans le cadre de l'utilisation de renseignements anonymisés, il serait difficile d'appliquer aux renseignements anonymisés les éléments clés habituellement utilisés pour évaluer la proportionnalité (par exemple, la sensibilité des renseignements et l'incidence sur le droit à la vie privée des personnes). Une fois les critères d'anonymisation satisfaits, l'utilisation ultérieure des renseignements anonymisés n'aurait pas, en pratique, d'incidence sur le droit à la vie privée, car, pour que les critères d'anonymisation soient satisfaits, il faut déjà que les risques

résiduels de réidentification (et, par conséquent, le risque d'atteinte au droit à la vie privée) soient « très faibles ».

Cela soulève une question importante : quel exercice de mise en balance, s'il y en a un, peut-on ou doit-on effectuer en vertu du critère susmentionné lorsque les renseignements en question n'identifient plus une personne ? Une fois que les risques de réidentification sont manifestement très faibles, l'incidence sur le droit à la vie privée de toute utilisation ultérieure est, par définition, minime. À notre avis, les organisations devraient simplement confirmer que la finalité est légale et repose sur un intérêt réel et non négligeable.

Forme du registre d'anonymisation

Ni la *Loi sur le privé* ni le *Règlement sur l'anonymisation* ne prescrivent la forme du registre d'anonymisation que les organisations doivent tenir en vertu de l'article 9 du *Règlement sur l'anonymisation*. De même, aucune période de conservation n'est précisée. Certaines organisations ont indiqué leur intention de s'appuyer sur leur processus actuel d'évaluation des facteurs relatifs à la vie privée pour satisfaire à l'exigence relative au registre.

Supervision du processus d'anonymisation par une « personne compétente en la matière »

Le *Règlement sur l'anonymisation* exige expressément qu'une « personne compétente en la matière » supervise le processus d'anonymisation ; toutefois, il ne précise pas les qualifications, l'expertise ou les attestations que cette personne doit posséder, ni ne définit l'étendue de ses responsabilités ou son niveau de participation. Par conséquent, les organisations conservent une marge de manœuvre pour déterminer les intervenants à faire participer, à quelles étapes et dans quelle mesure.

Selon le contexte, les organisations pourraient avoir besoin de la participation d'une série d'intervenants dans le cadre du processus d'anonymisation, qu'il s'agisse des responsables de la protection des renseignements personnels, des spécialistes des technologies de l'information, des dirigeants des unités opérationnelles ou d'experts externes. Ces décisions doivent être guidées par des facteurs tels que la nature, la sensibilité et le volume des renseignements personnels anonymisés, la complexité des techniques d'anonymisation et des mesures de sécurité employées, et l'utilisation prévue des renseignements anonymisés. En pratique, les organisations devraient évaluer soigneusement leurs ressources internes et, au besoin, faire appel à des experts externes pour s'assurer que le processus d'anonymisation est supervisé de manière adéquate et répond aux attentes réglementaires.

Prochaines étapes pour les entreprises

De nombreuses organisations constateront que leurs pratiques d'anonymisation existantes satisfont à plusieurs des exigences prévues par le *Règlement sur l'anonymisation*, en particulier celles qui, de manière générale, cadrent avec les éléments fondamentaux d'autres normes bien établies, notamment les Lignes directrices sur l'anonymisation des données structurées [PDF] [en anglais seulement] du Commissaire à l'information et à la protection des renseignements personnels de l'Ontario et le cadre d'anonymisation de l'ISO [en anglais seulement]. Certaines autres exigences, notamment l'obligation d'établir et de documenter les fins auxquelles les renseignements anonymisés seront utilisés, et de s'assurer que les fins sont « sérieuses et légitimes », sont propres à la *Loi sur le privé* et peuvent exiger à certains égards la mise à jour ou l'amélioration des pratiques existantes.

Les organisations qui souhaitent anonymiser des renseignements personnels en vertu de la *Loi sur le privé* doivent se familiariser avec les exigences prévues par le *Règlement sur l'anonymisation* et revoir leur processus d'anonymisation pour s'assurer qu'il les respecte. Il peut s'agir notamment :

- de mettre à jour les politiques et procédures internes de sorte qu'elles reflètent l'approche de l'organisation en matière d'anonymisation
- d'attribuer des rôles et des responsabilités clairs quant au moment, à la manière et aux conditions dans lesquelles les renseignements personnels sont anonymisés
- d'élaborer une méthode pratique permettant de documenter les pratiques d'anonymisation, y compris le registre d'anonymisation
- de former les employés aux exigences pertinentes en matière de protection des renseignements personnels et de sécurité des données, y compris les restrictions relatives à la réidentification des renseignements anonymisés
- de revoir les ententes pour s'assurer que les droits accordés à des tiers (par exemple, des fournisseurs de services) en matière d'anonymisation des renseignements personnels sont conformes aux exigences prévues par le *Règlement sur l'anonymisation* et que ces tiers sont soumis à des mesures de sécurité robustes prévues par contrat, y compris l'interdiction de réidentifier les renseignements anonymisés et des droits d'audit permettant de vérifier la conformité à ces mesures et d'en assurer le respect
- de mettre à jour les avis ou politiques de confidentialité destinés au public afin qu'ils traitent de l'anonymisation des renseignements personnels, dans la mesure où cela est pertinent et approprié

De manière générale, les organisations devraient soigneusement documenter leur processus d'anonymisation, demander l'avis d'experts externes le cas échéant, et établir des périodes de conservation claires et des procédures de réévaluation périodique des risques de réidentification. Elles devraient revoir régulièrement de telles mesures, entre autres, pour s'assurer qu'elles respectent, en matière d'anonymisation, les normes juridiques et réglementaires en constante évolution et les progrès technologiques rapides, en particulier à l'ère de l'IA et de l'informatique quantique.

---

[1] À l'exception de l'obligation prévue à l'article 9 de consigner dans un registre certains renseignements concernant les activités d'anonymisation, qui est entrée en vigueur le 1er janvier 2025.

[2] Le *Règlement sur l'anonymisation* s'applique également aux organismes publics en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*; toutefois, dans le présent bulletin d'actualités Osler, nous nous concentrons sur les conséquences pour les organisations du secteur privé visées par la *Loi sur le privé*.

[3] En vertu de la *Loi sur le privé*, la CAI a le pouvoir d'imposer d'importantes sanctions administratives pécuniaires pouvant aller jusqu'à 10 millions de dollars ou 2 % du chiffre d'affaires mondial, selon le montant le plus élevé, pour un large éventail d'infractions. Pour les infractions prévues par la loi, les amendes pénales peuvent atteindre 25 millions de dollars ou 4 % du chiffre d'affaires mondial, selon le montant le plus élevé.

[4] Il convient de noter que le terme anglais « de-identify » est rendu par « anonymiser » dans la version française de la *LPRPS* de l'Ontario.

[5] Article 23 de la *Loi sur le privé* et article 3 du *Règlement sur l'anonymisation*.

[6] Article 4 du *Règlement sur l'anonymisation*.

[7] Article 5 du *Règlement sur l'anonymisation*.

[8] Article 5 du *Règlement sur l'anonymisation*.

[9] Article 6 du *Règlement sur l'anonymisation*.

[10] Article 7 du *Règlement sur l'anonymisation*.

[11] Article 8 du *Règlement sur l'anonymisation*.

[12] Article 9 du *Règlement sur l'anonymisation*.

[13] Voir le Commissaire à l'information et à la protection de la vie privée de l'Ontario, Décision 175 relative à la LPRPS, 25 mars 2022 ; Information Commissioner's Office (ICO), *Anonymisation* (consultée le 3 mai 2025).

[14] Alinéa 37(1)f) de la *LPRPS*.

[15] Paragraphe 6(1) du *RGPD*.

[16] Paragraphe 12(5) de la *Loi sur le privé*.

[17] Voir les Conclusions en vertu de la LPRPDE n° 2021-001, par. 71–73; 1023158-S, par. 96–107