

Anonymiser des données : pas aussi simple qu'il n'y paraît

21 octobre 2025

Auteurs

Eric Lavallée

Associé, Agent de marques de commerce Associé, et Avocat

Ghiles Helli

Avocat

Les angles morts à vérifier lors de l'anonymisation des données

L'anonymisation est devenue une étape essentielle pour valoriser des jeux de données à des fins d'innovation, notamment en intelligence artificielle. À défaut d'un processus d'anonymisation mené selon les règles de l'art, les entreprises peuvent s'exposer à des sanctions financières, à des recours judiciaires et à un risque réputationnel accru et, par le fait même, à des répercussions potentiellement majeures sur leurs activités.

Processus d'anonymisation

Ce qu'en dit la loi

La *Loi sur la protection des renseignements personnels dans le secteur privé* (la « **Loi sur le privé** ») et la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (« **Loi sur l'accès** ») prévoient qu'un renseignement concernant une personne physique est anonymisé lorsqu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne. Puisqu'un renseignement anonymisé ne constitue plus alors un renseignement personnel, cette distinction revêt une importance capitale. Or, mis à part ces critères, les deux lois ne détaillent pas le processus d'anonymisation.

Pour pallier cette lacune, le gouvernement a adopté le *Règlement sur l'anonymisation des renseignements personnels* (le « **Règlement** »), dont l'objet est de définir les critères du processus d'anonymisation et de fixer un cadre qui s'appuie sur des normes élevées de protection de la vie privée.

Ce que les entreprises doivent savoir avant d'amorcer un processus d'anonymisation

Suivant le Règlement, avant d'amorcer un processus d'anonymisation, l'entreprise ou l'organisme désirant anonymiser des renseignements doit définir les fins « sérieuses et légitimes » auxquelles ceux-ci sont destinés. Ces fins doivent demeurer conformes, selon le cas, à la Loi sur le privé ou à la Loi sur l'accès, et toute nouvelle finalité doit être soumise à la même exigence.

Par ailleurs, le processus doit se dérouler sous la supervision d'une personne compétente en la matière, apte à sélectionner et à appliquer les techniques appropriées. Cette supervision vise à garantir non seulement la mise en œuvre adéquate des méthodes retenues, mais aussi à assurer la validation continue des choix technologiques et des mesures de sécurité.

4 étapes clés du processus d'anonymisation des renseignements

1. Dépersonnalisation

Dans un premier temps, il est nécessaire d'entreprendre une dépersonnalisation. Cette opération consiste à retirer ou à remplacer tout renseignement personnel permettant l'identification directe (tels le nom, l'adresse ou le numéro de téléphone) par des pseudonymes. Il importe toutefois de bien prévoir les interactions entre les différents ensembles de données, afin de réduire au maximum les risques de retrouver des renseignements qui permettraient de reconnaître une personne.

2. Analyse préliminaire des risques de réidentification

Une analyse préliminaire des risques de réidentification doit ensuite être menée. Cette deuxième étape repose notamment sur le critère d'individualisation (impossibilité d'isoler une personne), le critère de corrélation (impossibilité de faire le lien entre plusieurs ensembles de données relatifs à une même personne) et le critère d'inférence (impossibilité de déduire des renseignements personnels à partir d'autres informations disponibles). Les outils d'anonymisation les plus couramment utilisés sont l'agrégation, la suppression, la généralisation et la perturbation. Par ailleurs, des mesures de protection adéquates, comme un chiffrement de haut niveau et des contrôles d'accès restrictifs, doivent être prévues afin minimiser la probabilité de réidentification.

3. Approfondissement de l'analyse préliminaire des risques de réidentification

Une fois les deux premières étapes franchies, une analyse approfondie des risques de réidentification doit être effectuée. Force est de reconnaître qu'aucun risque ne peut être nul. Toutefois, ce risque doit être maintenu aussi faible que possible, en prenant en considération la sensibilité des renseignements, la disponibilité d'autres données publiques et la complexité nécessaire pour tenter une réidentification. Afin de maintenir ce très faible niveau de risque, une évaluation périodique doit être effectuée en tenant compte des progrès technologiques susceptibles de faciliter la réidentification.

4. Consignation d'une description des renseignements anonymisés

Enfin, il est essentiel de consigner dans un registre une description des renseignements anonymisés, les fins pour lesquelles ils sont utilisés, les techniques employées et les mesures de sécurité prises, ainsi que les dates des analyses ou des mises à jour effectuées. Cette consignation renforce la transparence et sert à démontrer que l'entreprise ou l'organisme désirant anonymiser des renseignements s'acquitte de ses obligations légales.