GOWLING WLG

Règlement sur l'anonymisation de renseignements personnels au Québec : Modélisation et commentaires

La présente contribution vise à commenter le projet de Règlement sur l'anonymisation des renseignements personnels (Gazette no 51 du 20-12-2023, page 5877) (le « Règlement »), notamment dans le cadre de la consultation du Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité.

Le Règlement vise à déterminer les critères et modalités applicables à l'anonymisation de renseignements personnels comme alternative à la destruction découlant de l'article 23 de la Loi sur la protection des renseignements personnels dans le secteur privé (RLRQ c P-39.1) (la « Loi sur le secteur privé ») et de l'article 73 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ c A-2.1) (la « Loi sur l'accès »).

Typologie des commentaires :

⚠ Clarification
● Modification
✕ Suppression

Lorsque les fins auxquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, la personne qui exploite une entreprise doit le détruire ou l'anonymiser pour l'utiliser à des fins sérieuses et légitimes, sous réserve d'un délai de conservation prévu par une loi.

Pour l'application de la présente loi, un renseignement concernant une personne physique 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.

Les renseignements anonymisés en vertu de la présente loi doivent l'être **selon les meilleures pratiques généralement reconnues et selon les critères et modalités déterminés par règlement.**

Art. 23 de la Loi sur le secteur privé

Étape 1 : Déterminer la nature de l'organisation

Déterminer la nature de l'« organisation », soit une personne exploitant une entreprise au Québec (notamment en fonction de la présence physique et/ou du marché ciblé), un organisme public ou un ordre professionnel en vertu de la loi.

Art. 1 du Règlement

⚠ L'article 23 ne s'applique pas aux partis politiques, députés indépendants et candidats indépendants en vertu de l'article 127.22 de la Loi électorale ; une telle disparité demeure surprenante.

Étape 2 : Établir les finalités d'anonymisation

Établir le caractère « sérieux et légitime » (pour les entreprises) ou l'« intérêt public » (pour les organismes publics) des fins d'utilisation des « renseignements personnels anonymisés ».

Art. 3 du règlement

⚠ La notion de fins « sérieuses et légitimes » ne fait l'objet d'aucune définition dans la loi ou le règlement. Il faut donc s'en remettre au sens courant des mots et, dans une certaine mesure, aux règles de droit commun (notamment l'exigence d'avoir un intérêt sérieux et légitime pour constituer un dossier sur autrui) ; cette notion ne veut toutefois pas dire qu'il s'agit d'une autre étape du cycle de vie des renseignements personnels.

● L'expression « renseignements personnels anonymisés » est trompeuse puisqu'un renseignement personnel ne peut pas être anonyme par définition (puisqu'il ne permettrait plus d'identifier directement ou indirectement la personne concernée). Il conviendrait plutôt de parler de « renseignements personnels que l'organisation entend anonymiser ».

Étape 3 : Superviser par une personne compétente

Réaliser un processus d'anonymisation implique la « supervision d'une personne compétente en la matière ».

Art. 4 du Règlement

✕ Il conviendrait de supprimer cette obligation de moyen qui n'apporte pas plus de garanties quant à la qualité de l'anonymisation tout en ne répondant pas à la diversité des pratiques et intervenants au sein des organisations.

Étape 4 : Retirer les renseignements personnels

Retirer des renseignements que l'organisation entend anonymiser tous les renseignements personnels permettant d'identifier directement la personne concernée des renseignements.

Art. 5 al. 1 du Règlement

⚠ Un tel processus est équivalent au fait de « dépersonnaliser » les renseignements personnels pour qu'ils ne permettent plus d'identifier directement la personne concernée en vertu de l'article 12 de la Loi sur le secteur privé et de l'article 65.1 de la Loi sur l'accès. En pratique, sur le plan séquentiel, il n'est toutefois pas toujours nécessaire de passer par la dépersonnalisation pour atteindre l'anonymisation.

Étape 5 : Préanalyser les risques de réidentification

Effectuer une analyse préliminaire des risques de réidentification en tenant notamment compte des critères d'individualisation, de corrélation et d'inférence ainsi que la disponibilité d'autres renseignements (notamment dans l'espace public).

Arts. 2 et 5 al. 2 du Règlement

✕ Il conviendrait de supprimer cette étape préliminaire qui est redondante avec l'analyse principale (voir étape 7) et risque d'alourdir les processus existants des organi sations.

● Les critères d'individualisation, de corrélation et d'inférence s'évaluent sur la base d'un standard très élevé, soit « le fait de ne pas être en mesure de ». Il conviendrait plutôt d'assouplir cette formulation, par exemple « la faible probabilité de », pour mieux coller à l'esprit du règlement et des standards internationaux.

● La notion d'« espace public » est inédite et ne fait l'objet d'aucune définition. Il conviendrait de plutôt faire référence à un concept existant, comme le caractère public d'un renseignement en vertu de la loi, ou alors de limiter la portée de cette exigence en la rendant facultative plutôt qu'impérative.

Étape 6 : Établir les techniques d'anonymisation

Établir les techniques d'anonymisation, lesquelles « doivent être conformes aux meilleures pratiques généralement reconnues », et les mesures de protection et sécurité pour diminuer les risques de réidentification en fonction du niveau de risque issu de l'analyse préliminaire (voir étape 5).

Art. 6 du Règlement

⚠ La notion de « meilleures pratiques généralement reconnues » découle de la loi, mais devrait faire l'objet de clarifications sous forme de lignes directrices ou de code découlant de concertation étroite avec l'industrie.

Étape 7 : Analyser les risques de réidentification

Analyser les risques de réidentification comme suite à la mise en œuvre des techniques d'anonymisation (voir étape 6) qui doit mener à des résultats démontrant que les renseignements personnels « ne permettent plus, de façon irréversible, d'identifier directement ou indirectement une personne ». Particulièrement, le « risque résiduel de réidentification doit être très faible » au regard de plusieurs éléments dont ceux précédemment énoncés (voir étapes 2 et 5) ainsi que « les moyens nécessaires pour réidentifier les personnes, notamment en considérant les efforts, les ressources et le savoir-faire requis pour mettre en œuvre ces moyens ».

Art. 7 du Règlement

⚠ Le risque résiduel de réidentification peut être faible sans pour autant être nul ou irréversible, ce qui laisse une flexibilité salutaire aux organisations.

● Les mesures de protection et sécurité précédemment énoncées (voir étape 6 ci-dessus) devraient être ajoutées aux éléments à prendre en compte pour évaluer le risque de réidentification.

Étape 8 : Mettre à jour l'analyse des risques de réidentification

Mettre à jour de façon régulière l'analyse des risques de réidentification (voir étape 7 ci-dessus), notamment en considérant les « avancées technologiques », afin d'assurer que les résultats demeurent inchangés. Le cas échéant, les renseignements ne sont plus considérés comme anonymisés.

Art. 8 du Règlement

⚠ Il n'existe pas de délai prescrit pour cette mise à jour régulière qui doit donc répondre à un standard de raisonnabilité en fonction des processus internes de l'organisation.

Étape 9 : Maintenir un registre d'anonymisation

Maintenir un registre d'anonymisation contenant les éléments suivants : (i) une description des renseignements personnels (voir étape 2 ci-dessus) ; (ii) les fins d'utilisation (voir étape 2 ci-dessus) ; (iii) les techniques d'anonymisation et les mesures de protection et sécurité (voir étape 6 ci-dessus) ; (iv) une synthèse des résultats de l'analyse des risques de réidentification (voir étapes 7 et 8 ci-dessus) ; et (v) les dates d'approbation ou de mise à jour des analyses.

Art. 9 du règlement

✕ Il conviendrait de supprimer cette exigence de maintenir un registre qui ajoute une couche de complexité à un processus d'anonymisation déjà largement documenté (voir toutes les étapes ci-dessus).

● Le délai de conservation du registre d'anonymisation devrait être précisé (par exemple, six mois) en tout état de cause.

Mécanismes de sanction

En plus des mécanismes de sanction généraux pour non-conformité à la Loi sur le secteur privé, l'article 91 précise que toute organisation qui procède ou tente de procéder à l'identification d'une personne physique à partir de renseignements anonymisés est susceptible d'une amende de 15 000 $ à 25 000 000 $ ou du montant correspondant à 4 %du chiffre d'affaires mondial de l'exercice financier précédent si ce dernier montant est plus élevé.

Antoine Guilmain
Associé et Co-chef, Groupe de pratique national Cybersécurité et protection des données
Montréal
+1 514 392 9521 Ext 69521
antoine.guilmain@gowlingwlg.com

Justin Boileau
Avocat, Groupe de pratique national Cybersécurité et protection des données
Montréal
+1 514 877 3988
justin.boileau@gowlingwlg.com

Dernière mise à jour : février 2024

Si vous avez des questions ou souhaitez recevoir une version anglaise des documents cités plus haut, n'hésitez pas à communiquer avec les auteurs ou un autre membre du groupe national de cybersécurité et de protection des données de Gowling WLG