



BAC

Bureau d'assurance
du Canada

Mémoire

Projet de Règlement sur l'anonymisation des renseignements personnels

Présenté à

Mme Julie Samuël
Directrice de l'accès à l'information et de la protection
des renseignements personnels
Secrétariat à la réforme des institutions démocratiques,
à l'accès à l'information et à la laïcité
Ministère du Conseil exécutif

Bureau d'assurance du Canada

Février 2024



Table des matières

INTRODUCTION.....	3
SOMMAIRE DES RECOMMANDATIONS.....	4
COMMENTAIRES GÉNÉRAUX.....	5
<i>Ampleur de la tâche.....</i>	5
<i>Obstacles à l’anonymisation et inapplicabilité.....</i>	5
COMMENTAIRES SPÉCIFIQUES ET RECOMMANDATIONS.....	6
SECTION I : CHAMP D’APPLICATION.....	6
Article 2.....	6
SECTION II : CRITÈRES ET MODALITÉS APPLICABLES À L’ANONYMISATION DES RENSEIGNEMENTS PERSONNELS.....	7
Article 3.....	7
Article 4.....	8
Article 5 et 6.....	8
Article 7.....	9
Article 8.....	10
Article 9.....	11
CONCLUSION.....	12

Le Bureau d'assurance du Canada (BAC) est l'association nationale qui représente 90 % des sociétés privées d'assurance habitation, automobile et entreprise au Canada. L'industrie de l'assurance de dommages joue un rôle de premier plan dans l'économie québécoise en permettant à la population de se prémunir contre des sinistres pouvant avoir un impact important sur sa sécurité financière en protégeant son patrimoine.

Le BAC au Québec œuvre auprès des consommateurs, des entreprises, des médias, des groupes d'intérêt et des gouvernements dans le but de les informer et de les sensibiliser sur divers sujets et enjeux qui les touchent de près.



Introduction

Le Bureau d'assurance du Canada (BAC) expose ci-après les commentaires de ses membres, à l'occasion de la publication, par le ministre responsable de l'Accès à l'information et de la Protection des renseignements personnels, du projet de *Règlement sur l'anonymisation des renseignements personnels (Règlement)*. Le BAC remercie le Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité de l'attention qu'il accordera à ses commentaires.

Le présent mémoire vise à informer des problématiques liées à l'application de certains articles du projet de Règlement. Il propose également des recommandations qui permettraient d'assurer une meilleure cohérence entre les dispositions et l'encadrement législatif auquel sont déjà soumises les entreprises.

Johanne Lamanque
Vice-présidente, Québec
Bureau d'assurance du Canada



Sommaire des recommandations

1. Préciser la définition du « critère de corrélation » comme suit :
« le fait de ne pas être en mesure de relier entre eux des ensembles de données distincts, raisonnablement accessibles, qui concernent une même personne. »
Nos soulignés
2. Préciser à l'article 3 qu'il est possible d'anonymiser des renseignements personnels en cours d'utilisation lorsque les fins pour lesquelles ils ont été recueillis ou utilisés ne sont pas encore accomplies.
3. Retirer à l'article 4 la mention précisant « que le processus d'anonymisation doit être réalisé sous la supervision d'une personne compétente », car il est redondant avec ce que prévoit déjà la loi.
4. Combiner les articles 5 et 6 en apportant les modifications suivantes :
 - Retirer l'obligation d'effectuer une analyse préliminaire, car elle vient alourdir inutilement le processus d'anonymisation;
 - Retirer l'expression « espace public », car elle est inappropriée;
 - Préciser à quoi correspondent les identifiants directs;
 - Mettre à la disposition des entreprises l'information nécessaire pour mieux identifier les « meilleures pratiques généralement reconnues »;
 - Établir un critère de matérialité en ce qui concerne les mesures de protection et référer, comme dans le document de préconsultation, à des mesures de protection et de sécurité « raisonnables ».
5. Modifier le troisième paragraphe de l'article 7 en ce qui concerne le risque résiduel de réidentification en retirant les éléments suivants :
 - La nature des renseignements;
 - Les risques que d'autres renseignements disponibles, notamment dans l'espace public, soient utilisés pour identifier directement ou indirectement une personne.
6. À l'article 8, relativement à la mise à jour de l'analyse des risques de réidentification :
 - Ajouter un terme à l'obligation d'effectuer les mises à jour, soit un délai où l'obligation de mise à jour n'est plus requise;
 - Attribuer la responsabilité de la vigie des avancées technologiques à la Commission d'accès à l'information (CAI);
 - Préciser les effets de l'augmentation du risque de réidentification à la suite des développements technologiques.
7. À l'article 9 :
 - clarifier, le délai durant lequel les organisations doivent conserver et alimenter un registre;
 - laisser plus de latitude aux organisations leur permettant de déterminer les méthodes de documentation.



Commentaires généraux

Ampleur de la tâche

L'analyse d'impact réglementaire concernant le projet de règlement sur l'anonymisation des renseignements personnels (analyse d'impact)¹ affirme notamment qu'« étant donné le caractère facultatif de l'anonymisation, les critères et les modalités prévus au projet de règlement ne représentent pas des contraintes et entraînent donc des coûts nuls ». En ce qui concerne spécifiquement les activités des assureurs de dommages, cet énoncé n'est pas fidèle à la réalité.

Certes, l'anonymisation est facultative, mais elle est essentielle pour les assureurs de dommages, car elle contribue à l'amélioration des scénarios et des simulations, à l'établissement de comparatifs et à l'agrégation de données, le tout au bénéfice de la clientèle. L'anonymisation est également une technique permettant de protéger efficacement les renseignements personnels.

Les entreprises qui désirent utiliser l'anonymisation, conformément aux modalités prévues actuellement par le projet de règlement, devront assumer des coûts disproportionnés par rapport aux bénéfices de son utilisation. Le processus d'anonymisation tel qu'il est proposé aura aussi pour effet d'alourdir déraisonnablement la charge de conformité des assureurs, sans compter les impacts sur la réorganisation administrative.

À titre d'exemple, les organisations devront recruter et former des équipes détenant une expertise précise sur l'anonymisation, revoir leurs procédures et politiques, effectuer l'inventaire complet de leurs bases de données ainsi que celles des plateformes et applications externes, revoir les contrats avec leurs fournisseurs, s'équiper de puissants serveurs pour effectuer les algorithmes de vérification de réidentification, etc. Ces modifications entraîneront des coûts importants.

L'analyse d'impact réglementaire indique que le projet de règlement a été conçu de manière à ne pas trop alourdir les tâches pour les entreprises qui feront le choix de l'anonymisation. Malheureusement, le BAC n'est pas de cet avis. Les entreprises qui décideront d'anonymiser certains renseignements personnels devront mobiliser un nombre important de ressources à cette fin et possiblement créer un secteur attiré uniquement à l'anonymisation. Considérant toutes les obligations découlant de la Loi et du projet de règlement, certaines entreprises pourraient décider tout simplement de ne pas utiliser l'anonymisation et opter pour la destruction des renseignements personnels.

Obstacles à l'anonymisation et inapplicabilité

Le Règlement semble déterminer que des renseignements anonymisés peuvent redevenir des renseignements personnels encadrés par la Loi lorsqu'il y a un changement au niveau du

¹ Analyse d'impact réglementaire, Projet de règlement sur l'anonymisation des renseignements personnels, 20 novembre 2023

https://www.google.ca/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&cad=rja&uact=8&ved=2ahUKEwio0JKr4eKDAxWDpokEHZ4XCoIQFnoECAkOAO&url=https%3A%2F%2Fcdn-contenu.quebec.ca%2Fcdn-contenu%2Fgouvernement%2FMCE%2Fdossiers-soumis-conseil-ministres%2F2023-0252_air.pdf&usq=AOvVaw2DmXllaFf9KOMwPunIPyXx&opi=89978449



risque de réidentification. Cette épée de Damoclès pourrait décourager l'utilisation de l'anonymisation.

Le BAC s'interroge quant à la possibilité que des renseignements ayant été anonymisés et utilisés légalement à d'autres fins puissent redevenir des renseignements personnels. Il est pertinent de rappeler les propos de M. Jean-Philippe Miville-Deschênes lors des débats parlementaires du projet de loi 64² :

« En fait, actuellement, là, une loi... un renseignement qui est anonyme n'est pas soumis à la Loi sur l'accès puis à la Loi sur la protection des renseignements personnels. Puis je vais même citer le RGPDV qui le prévoit spécifiquement, là. Il dit : " Le présent règlement ne s'applique pas au traitement de telles informations > anonymes ".

Ça fait que c'est une notoriété, je dirais... Les entreprises qui veulent utiliser des renseignements à d'autres fins, bien, elles peuvent les anonymiser, et là être exclues de l'application de la loi et les utiliser à d'autres fins, parce que ce ne sont plus des renseignements qui sont, au sens de la définition ' renseignements personnels ', qui sont identificatoires directement ou indirectement, etc. »

L'un des attraits de l'anonymisation est justement l'inapplication de la Loi aux renseignements anonymisés. Toutefois, cette inapplicabilité devient purement théorique si, à la suite d'avancées technologiques, les renseignements peuvent redevenir des renseignements personnels.

Conséquemment, le BAC est d'avis que le projet de Règlement nécessite certaines modifications afin que l'anonymisation puisse être utilisée par les organisations dans le cadre de leurs activités.

Commentaires spécifiques et recommandations

Section I : champ d'application

Article 2

Le BAC est préoccupé par la définition de « critère de corrélation » présente dans le projet de règlement. Suivant la définition actuelle, il ne doit y avoir aucune corrélation avec l'ensemble des informations disponibles, tant dans les systèmes de l'entreprise qui procède à l'anonymisation, que sur le Web (voire le *Dark Web*) ou dans toutes autres plateformes et applications. Cette définition rend impossible le travail de vérification des entreprises pour s'assurer de l'impossibilité de réidentification par corrélation puisqu'elle ne comprend aucune limite quant à l'étendue des informations à vérifier. L'application du critère de corrélation devrait être limitée aux données raisonnablement accessibles pour l'entreprise en question.

Recommandation n° 1

Préciser la définition du « critère de corrélation » comme suit : « le fait de ne pas être en mesure de relier entre eux des ensembles de données distincts, raisonnablement accessibles, qui concernent une même personne. »

(nos soulignés)

² [Journal des débats de la Commission des institutions - Assemblée nationale du Québec \(assnat.qc.ca\)](http://Journal%20des%20d%C3%A9bats%20de%20la%20Commission%20des%20institutions%20-%20Assemblée%20nationale%20du%20Québec%20(assnat.qc.ca))



Section II : critères et modalités applicables à l'anonymisation des renseignements personnels

Article 3

Cet article impose qu'avant même de commencer un processus d'anonymisation, une organisation doit établir les fins pour lesquelles elle entend utiliser les renseignements personnels anonymisés et que ces fins soient conformes à l'article 23 de la Loi dans le secteur privé et à l'article 73 de la Loi sur l'accès.

Loi sur la protection des renseignements personnels dans le secteur privé (« Loi dans le secteur privé »)

23. 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.

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (« Loi sur l'accès »)

73. Lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, l'organisme public doit le détruire, ou l'anonymiser pour l'utiliser à des fins d'intérêt public, sous réserve de la Loi sur les archives (chapitre A-21.1) ou du Code des professions (chapitre C-26).

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.

Considérant que l'article 3 réfère à ces deux articles, doit-on comprendre qu'il est impossible d'utiliser l'anonymisation pour d'autres fins que celles qui y sont prévues lorsque les fins pour lesquelles ils ont été recueillis ou utilisés ne sont pas encore toutes accomplies ? Bien qu'il n'y ait pas de précisions sur ce point dans le Règlement, le BAC considère que l'anonymisation des renseignements personnels en cours d'utilisation est possible suivant l'article 12 al. 2 (1) de la Loi dans le secteur privé ainsi que l'article 65.1 al. 2 (1) de la Loi sur l'accès.

Le BAC souligne que l'anonymisation peut être utile pour protéger des renseignements personnels alors que les fins pour lesquelles ils ont été recueillis ou utilisés ne sont pas encore accomplies. Par exemple, nous pouvons penser à l'utilisation de l'anonymisation comme



mesure de protection de certains renseignements sensibles, pour le partage de renseignements dans des cas de vérifications diligentes en matière de vente d'entreprise, pour des comparatifs de marché, etc. Ainsi, l'anonymisation des renseignements personnels n'est pas seulement une alternative à la destruction visant la conservation des données au-delà de la durée où ils sont nécessaires à la réalisation des fins pour lesquelles ils ont été recueillis.

De surcroît, la détermination des finalités devrait être faite au fur et à mesure de l'utilisation de l'anonymisation et non de façon globale au début. En effet, il sera difficile et beaucoup trop contraignant d'établir à l'avance toutes les finalités pour lesquelles les renseignements personnels anonymisés pourront éventuellement être utilisés.

Recommandation n° 2

Préciser à l'article 3 qu'il est possible d'anonymiser des renseignements personnels en cours d'utilisation lorsque les fins pour lesquelles ils ont été recueillis ou utilisés ne sont pas encore accomplies.

Article 4

Cette disposition exige que le processus d'anonymisation soit réalisé sous la supervision d'une personne compétente en la matière. Or, c'est au responsable de la protection des renseignements personnels, nommé conformément à la loi, de veiller au respect et à la mise en œuvre de la Loi et de déléguer au besoin cette tâche à des personnes compétentes. Le BAC est donc d'avis que cette disposition est superflue en plus de porter à interprétation quant à la nature et l'étendue des compétences nécessaires pour superviser l'anonymisation.

Recommandation n° 3

Retirer à l'article 4 la mention précisant « *que le processus d'anonymisation doit être réalisé sous la supervision d'une personne compétente* », car il est redondant avec ce que prévoit déjà la loi.

Articles 5 et 6

En ce qui concerne l'article 5, avant même de commencer le processus d'anonymisation, il est précisé à la première étape de retirer tous les renseignements personnels qui permettent d'identifier directement la personne concernée. Cette étape est nécessaire, mais il serait nécessaire de préciser à quoi correspondent les identifiants directs. Certes, les renseignements tels que le nom et prénom, l'adresse personnelle et les numéros d'identification (ex. numéro d'assurance sociale, numéro d'assurance maladie, numéro de permis de conduire) sont des identifiants directs. Toutefois, il est parfois difficile de tracer la ligne entre les identifiants directs et indirects et des précisions à cet égard faciliteraient l'application de cette disposition.

Suivant l'alinéa 2, l'étape suivante est une analyse préliminaire des risques de réidentification en considérant notamment le critère d'individualisation, le critère de corrélation et le critère d'inférence, ainsi que les risques que d'autres renseignements disponibles, notamment dans l'espace public, soient utilisés pour identifier directement ou indirectement une personne. Le BAC considère que l'expression « espace public » est inappropriée et qu'elle doit être retirée.



Sur ce point, le BAC réitère ses commentaires relatifs à l'article 2 du présent mémoire soit, qu'il est difficile, voire impossible de faire une vérification aussi large.

Considérant qu'une analyse des risques de réidentification est prévue à l'article 7, une analyse préliminaire vient alourdir inutilement le processus d'anonymisation. Ainsi, l'obligation de procéder à une telle analyse devrait être retirée.

En ce qui concerne l'article 6, il est fait mention qu'une organisation doit établir les techniques d'anonymisation conformément aux meilleures pratiques généralement reconnues et doit également établir des mesures de protection pour diminuer les risques de réidentification.

Tout d'abord, l'expression « meilleures pratiques généralement reconnues » est subjective. Il ne semble pas y avoir de « pratiques généralement reconnues » en matière d'anonymisation ou de standards qui définissent ces « meilleures pratiques » comme les normes ISO, NIST ou autres normes similaires. Le BAC recommande que la CAI vienne mettre à la disposition des entreprises l'information nécessaire pour mieux identifier ces « meilleures pratiques ».

De plus, le BAC est d'avis qu'un critère de matérialité devrait être ajouté en ce qui concerne les mesures de protection et recommande de référer, comme dans le document de préconsultation, à des mesures de protection et de sécurité « raisonnables ».

Recommandation n° 4

Combiner les articles 5 et 6 en apportant les modifications suivantes :

- Retirer l'obligation d'effectuer une analyse préliminaire, car elle vient alourdir inutilement le processus d'anonymisation;
- Retirer l'expression « *espace public* », car elle est inappropriée;
- Préciser à quoi correspondent les identifiants directs;
- Mettre à la disposition des entreprises l'information nécessaire pour mieux identifier les « *meilleures pratiques généralement reconnues* »;
- Établir un critère de matérialité en ce qui concerne les mesures de protection et recommande de référer, comme dans le document de préconsultation, à des mesures de protection et de sécurité « *raisonnables* ».

Article 7

La prochaine étape du processus d'anonymisation correspond à l'analyse des risques de réidentification. Une fois les techniques et les mesures de protection et de sécurité établies, l'entreprise devra effectuer une analyse des risques de réidentification. Les résultats de l'analyse doivent démontrer qu'il est, en tout temps, raisonnable de prévoir dans les circonstances que les renseignements produits à la suite du processus d'anonymisation ne permettent plus, de façon irréversible, d'identifier directement ou indirectement une personne. Le risque résiduel de réidentification doit être démontré comme étant très faible.

Le BAC considère que certains éléments énumérés à cet article pour démontrer un risque résiduel très faible sont inappropriés et recommande leur retrait.

Au paragraphe 2 du troisième alinéa, on réfère à la nature des renseignements, mais puisque celle-ci peut être sensible (ex. biométrie, renseignements médicaux, etc.), elle n'a pas d'impact



sur les risques de réidentification. La nature des renseignements entraîne un risque plus ou moins élevé dans le cas où il y a réidentification, mais n'a pas d'incidence sur la possibilité qu'il y ait ou non réidentification. Le BAC recommande ainsi le retrait du paragraphe 2 du troisième alinéa.

Comme expliqué précédemment, le BAC est en désaccord avec l'utilisation de la notion d'espace public puisqu'il est déraisonnable et potentiellement impossible de vérifier tous les renseignements qui se trouvent dans l'espace public. Ainsi, il serait adéquat d'enlever le paragraphe 4.

Recommandation n° 5

Le BAC recommande de modifier le troisième paragraphe de l'article 7 afin qu'il se lise comme suit :

« [...] Pour l'application du deuxième alinéa, il n'est pas nécessaire de démontrer un risque nul. Cependant, les résultats de l'analyse doivent démontrer, en tenant compte notamment des éléments suivants, que le risque résiduel de réidentification est très faible :

- 1° les circonstances liées à l'anonymisation des renseignements personnels, notamment les fins pour lesquelles elle entend utiliser les renseignements anonymisés;
- 2° le critère d'individualisation, le critère de corrélation et le critère d'inférence;
- 3° 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. »

Article 8

L'article 8 indique qu'une organisation doit régulièrement évaluer les renseignements qu'elle a anonymisés afin de s'assurer qu'ils le demeurent. Pour ce faire, elle doit mettre à jour l'analyse des risques de réidentification qu'elle a effectuée et doit notamment considérer les avancées technologiques qui peuvent contribuer à réidentifier une personne.

Le BAC est d'avis que la vigie des avancées technologiques ne devrait pas être une obligation qui incombe aux organisations, mais plutôt à la Commission d'accès à l'information (CAI). Ceci est d'autant plus vrai considérant que dans l'analyse d'impact, il est fait mention que « le projet de règlement proposera un encadrement permettant aux entreprises d'uniformiser leurs pratiques quant à l'anonymisation des renseignements personnels ». Au bénéfice des citoyens, il est primordial que les pratiques d'anonymisation soient uniformes et considérant l'évolution rapide des technologies, il est nécessaire qu'un organisme, comme la CAI, effectue cette vigie et donne des directions aux entreprises.

Par ailleurs, si cette proposition n'est pas retenue, le BAC recommande que l'alinéa 1 soit modifié comme suit :

« Cette mise à jour doit notamment considérer les avancées technologiques largement reconnues et qui rendraient inefficaces les techniques d'anonymisation mises en place à la suite d'une analyse des risques de réidentification. »

(nos soulignés)

En outre, les membres du BAC souhaitent avoir des précisions sur la période durant laquelle ces mises à jour devront être effectuées. Les entreprises pourront-elles arrêter de faire ces



mises à jour, après 5, 10 ou 20 ans ? Le BAC est d'avis que cette obligation doit être limitée dans le temps.

Le deuxième alinéa indique que lors de la mise à jour, les résultats de l'analyse doivent toujours démontrer un risque résiduel très faible suivant les critères énumérés à l'article précédent. Dans le cas où le niveau de risque deviendrait plus élevé que « très faible » soit « faible » ou « moyen », les renseignements ne sont plus considérés comme anonymisés. Il y a lieu de préciser si le risque de réidentification lié aux nouvelles technologies constitue un incident de confidentialité bien que le risque ne se soit pas encore matérialisé.

Les mesures de sécurité mises en place à la suite d'une augmentation du risque de réidentification dans ces circonstances seront mises en œuvre pour les nouvelles anonymisations, mais pourraient difficilement l'être pour celles effectuées précédemment. Pensons par exemple à des renseignements ayant été transférés à des fournisseurs. Une telle situation apporterait une instabilité au niveau des affaires et des opérations. En effet, une organisation aurait un fardeau administratif important l'obligeant à auditer les processus d'anonymisation de tiers avec qui elle pourrait ne plus avoir de lien contractuel.

Recommandation n° 6

À l'article 8, relativement à la mise à jour de l'analyse des risques de réidentification :

- Préciser un terme à l'obligation d'effectuer les mises à jour, soit un délai où l'obligation de mise à jour n'est plus requise.
- Attribuer la responsabilité de la vigie des avancées technologiques à la Commission d'accès à l'information.
- Préciser les effets de l'augmentation du risque de réidentification à la suite de développements technologiques.

Article 9

L'article 9 précise qu'une organisation qui procède à l'anonymisation de renseignements personnels doit consigner dans un registre certains renseignements.

Le BAC convient que la documentation de l'anonymisation fait partie d'une bonne pratique de gouvernance. Néanmoins, il est pertinent de souligner qu'un registre apporte aussi son lot de risques puisque l'on vient centraliser toute l'information concernant l'anonymisation. Afin de minimiser ce risque, le BAC recommande de laisser la liberté aux organisations de déterminer les méthodes de documentation. En sus, le BAC croit qu'il serait approprié de venir indiquer le délai de conservation de ce registre.

Recommandation n° 7

- Clarifier le délai pendant lequel les organisations doivent conserver et alimenter un registre.
- Laisser aux organisations la liberté de déterminer les méthodes de documentation.



Conclusion

Le BAC reconnaît l'importance d'établir les critères et les modalités de l'anonymisation. Cependant, il est d'avis qu'il est nécessaire d'apporter certaines modifications au Règlement afin que les dispositions soient applicables et réalisables.

Les demandes de précision et de simplification qui précèdent permettront aux assureurs d'utiliser l'anonymisation des renseignements personnels essentiels à leurs activités dans un cadre réaliste tout en assurant la protection des consommateurs.

Nous vous remercions de l'opportunité qui est offerte aux assureurs de dommages de commenter ce projet de Règlement et nous demeurons disponibles pour en discuter plus amplement.

Fin du document