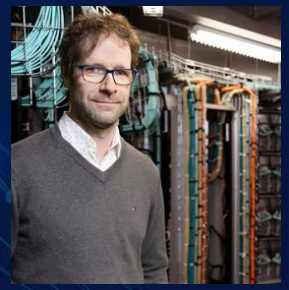
Anonymisation des données de santé en droit québécois

18 juin 2025 12h@13h

Pierre-Luc Déziel
Professeur titulaire
Faculté de droit
Université Laval
Chaire de recherche du Canada sur la protection et la valorisation des données de santé



Philippe Després
Professeur titulaire
Faculté des sciences et de génie
Université Laval

CONSORTIUM SANTÉ NUMÉRIQUE

Université de Montréal

DOSA

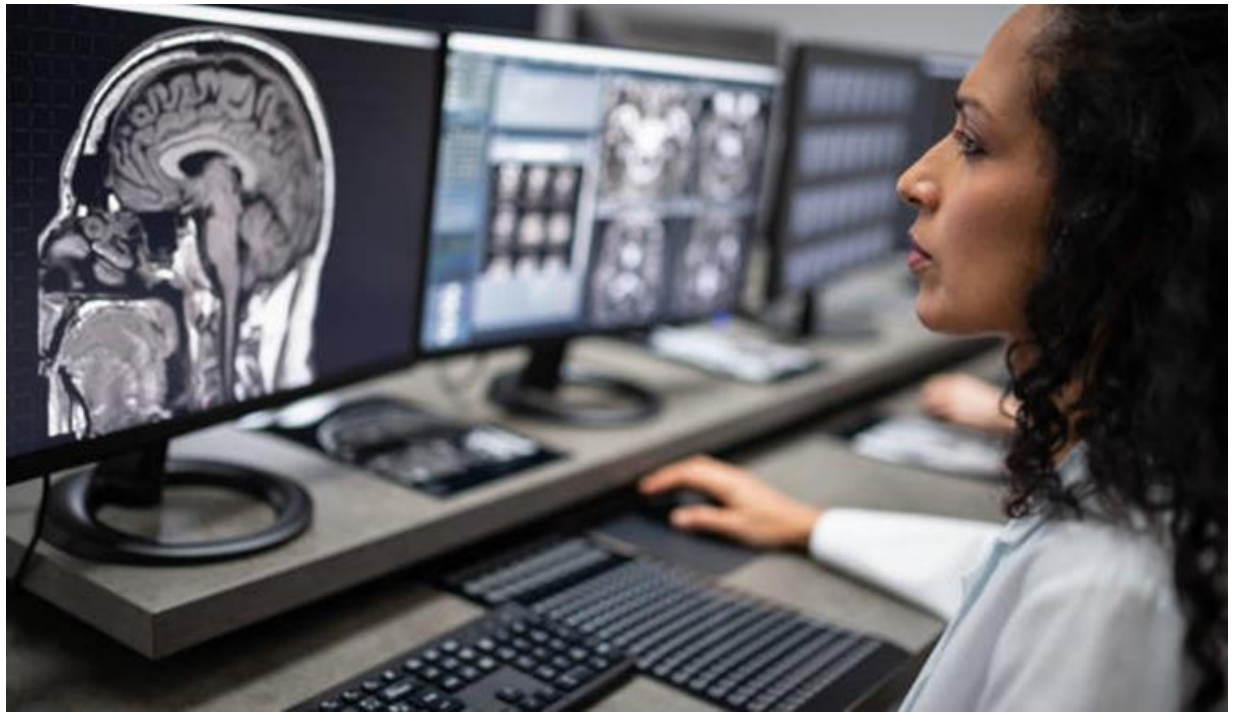
Chaire de recherche du Canada sur la protection et la valorisation des données de santé

RSN

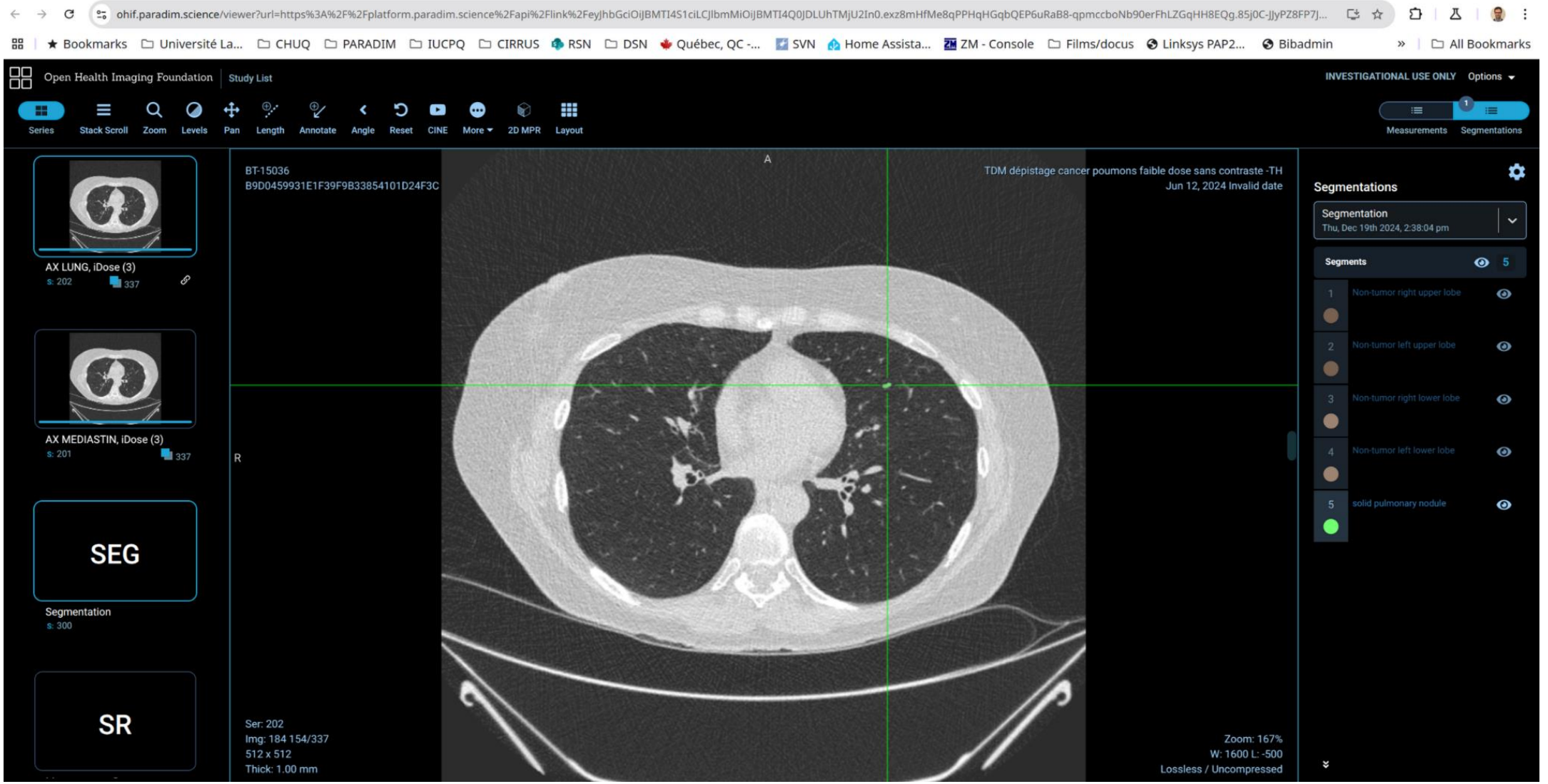
Perspective de la recherche

Perspective de la recherche

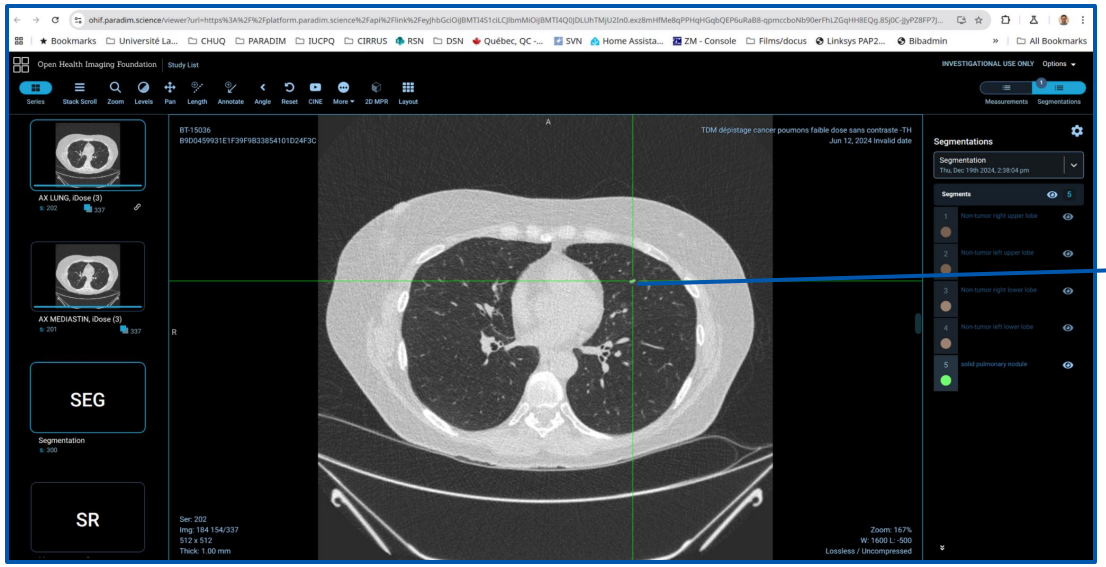
- Constitution de grands ensembles de données annotées
  - Matière première pour l'IA (entraînement ou évaluation de modèles)
- Coûteux en temps, expertise disciplinaire (par ex. médecine, technologie)



Ensembles de données annotées (vérités terrain)



Dépersonnalisation (sous la supervision d'une personne compétente en la matière)



Imaging Measurement Report (126000 - DCM)

InstanceCreationDate - 20230323
InstanceCreationTime - 112315
InstanceCreatorUID - 1.2.276.0.7230010.3.0.3.6.6
SOPClassUID - 1.2.840.10008.5.1.4.1.1.88.22
SOPInstanceUID - 1.2.276.0.7230010.3.1.4.2005612997.5464.1679584995.29
StudyDate - 20060719
SeriesDate - 20230323
ContentDate - 20230323
StudyTime - 082926.000000
SeriesTime - 112315
ContentTime - 112315
AccessionNumber -
Modality - SR
Manufacturer - QIICR
ReferringPhysicianName -
StudyDescription - Taco thorax et abdomen avec contraste
SeriesDescription - Measurement Report
ManufacturerModelName - https://github.com/QIICR/dcmqi.git
PatientName - 2172
PatientID - 2172
PatientBirthDate - 20000101
PatientSex - O
PatientWeight - 0
DeviceSerialNumber - 0
SoftwareVersions - 7f45450
StudyInstanceUID - 1.2.826.0.1.3680043.6.61224.62555.20170322082033.4760.12.5713
SeriesInstanceUID - 1.2.276.0.7230010.3.1.3.2005612997.5464.1679584995.31
StudyID -
SeriesNumber - 103
InstanceNumber - 1
ValueType - CONTAINER
CodeValue - 126000
CodingSchemeDesignator - DCM
CodeMeaning - Imaging Measurement Report
ContinuityOfContent - SEPARATE
VerifyingOrganization - QIICR
VerificationDateTime - 20230323112315
VerifyingObserverName -
ReferencedSOPClassUID - 1.2.840.10008.5.1.4.1.1.66.4
ReferencedSOPInstanceUID - 1.2.276.0.7230010.3.1.4.2005612997.3772.1679584993.777
SeriesInstanceUID - 1.2.276.0.7230010.3.1.3.2005612997.3772.1679584993.776
ReferencedSOPClassUID - 1.2.840.10008.5.1.4.1.1.2

Collections enrichies en continu avec de nouvelles annotations, de nouvelles issues cliniques, de nouvelles images, de nouvelles données.

Anonymisation à ce stade est impossible (lien unidirectionnel vers données dépersonnalisées est essentiel).

Perspective de la recherche

- Tension entre destruction et principes FAIR (Politique des trois organismes sur la gestion des données de recherche)

  - *“Les organismes subventionnaires sont d’avis que les données recueillies par la recherche au moyen de fonds publics doivent être gérées de manière responsable et sûre. Elles doivent aussi, lorsque les obligations éthiques, juridiques et commerciales le permettent, être disponibles pour être réutilisées par d’autres.”*

- **Anonymisation comme alternative à la destruction**

Perspective juridique: la *Loi sur les renseignements de santé et de services sociaux*

Plan de la section

1. **Définition :** définir le renseignement anonymisé en fonction du contexte terminologique plus large de la loi (renseignement personnel, sensible, dépersonnalisé).

2. **L’anonymisation en droit québécois :** situer l'anonymisation dans le contexte juridique actuel et identifier sa fonction et ses possibles utilisations.

3. **Le processus d’anonymisation :** présenter le *Règlement sur l’anonymisation* et les étapes prévues pour qualifier un renseignement d’anonymisé.

Plan de la section

1. **Définition :** définir le renseignement anonymisé en fonction du contexte terminologique plus large de la loi (renseignement personnel, sensible, dépersonnalisé).

2. **L'anonymisation en droit québécois :** situer l'anonymisation dans le contexte juridique actuel et identifier sa fonction et ses possibles utilisations.

3. **Le processus d'anonymisation :** présenter le *Règlement sur l'anonymisation* et les étapes prévues pour qualifier un renseignement d'anonymisé.

Qu’est-ce qu’un renseignement ***personnel*** ?

« **Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent, directement ou indirectement, de l’identifier.** » (Art. 54, *Loi sur l’accès*)

- Notion d’identification, directe ou indirecte.
- Ne précise pas de **seuil** (quantitatif ou qualitatif) d’identification, donc définition très **large**.
- Ne porte pas non plus sur le niveau de **sensibilité** : n’a pas besoin d’être sensible pour être un RP.

Qu'est-ce qu'un renseignement *de santé* ?

« Au sens de la présente loi, est un renseignement de santé et de services sociaux tout renseignement qui permet, même indirectement, d'identifier une personne et qui répond à l'une des caractéristiques suivantes:

1° il concerne l'état de **santé physique ou mentale** de cette personne et ses facteurs déterminants, y compris les antécédents médicaux ou familiaux de la personne;

2° il concerne tout **matériel** prélevé sur cette personne dans le cadre d'une évaluation ou d'un traitement, incluant le matériel biologique, ainsi que tout implant ou toute orthèse, prothèse ou autre aide suppléant à une incapacité de cette personne;

3° il concerne **les services** du domaine de la santé et des services sociaux offerts à cette personne, notamment la nature de ces services, leurs **résultats**, les lieux où ils ont été offerts et l'identité des personnes ou des groupements qui les ont offerts;

4° il a été obtenu dans l'exercice d'une fonction prévue par la Loi sur la santé publique ;

5° toute autre caractéristique déterminée par règlement du gouvernement. »

(Art. 4 , *Loi sur les renseignements de santé et des services sociaux*)

Qu’est-ce qu’un renseignement ***dépersonnalisé*** ?

« Un renseignement personnel est dépersonnalisé lorsque ce renseignement ne permet plus d’identifier directement la personne concernée. » (Art. 65.1 , *Loi sur l’accès*)

- **Exception** au principe de limitation de l’utilisation “ lorsque son utilisation est nécessaire à des fins d’étude, de recherche ou de production de statistiques et qu’il est dépersonnalisé”.
- Renseignement dépersonnalisé reste un renseignement personnel.

Qu’est-ce qu’un renseignement *anonymisé* ?

« Pour l’application de la présente loi, 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, même indirectement, la personne qu’il concerne.

Un renseignement ainsi anonymisé doit l’être selon les meilleures pratiques généralement reconnues et selon les critères et modalités déterminés par un règlement pris en vertu de l’article 73 de la Loi sur l’accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1), avec les adaptations nécessaires. » (Art. 111 , *LRSSS*)

- Définition plus **stricte**, critère plus exigeant.
- Expression un peu **contradictoire** “ en tout temps/dans les circonstance”
- Art. 73 - > *Règlement sur l’anonymisation* (mai 2024)

Plan de la section

1. **Définition :** définir le renseignement anonymisé en fonction du contexte terminologique plus large de la loi (renseignement personnel, sensible, dépersonnalisé).

2. **L’anonymisation en droit québécois :** situer l'anonymisation dans le contexte juridique actuel et identifier sa fonction et ses possibles utilisations.

3. **Le processus d’anonymisation :** présenter le *Règlement sur l’anonymisation* et les étapes prévues pour qualifier un renseignement d’anonymisé.

L’anonymisation dans la *Loi sur les renseignements de santé*

- Le terme anonymisation apparaît à un (seul) endroit où il est pertinent dans un contexte de recherche, soit comme alternative à la ***destruction*** des renseignements;
- Jeu sur le principe de **limitation de la conservation** en droit québécois ;
- Alternative de l’anonymisation introduite par les **réformes récentes,** pour encourager la **valorisation** ;
- En quoi est-ce que cet **emplacement** dans l’architecture globale de la loi nous permet d’interpréter l’anonymisation ?
  - N’est plus un renseignement personnel (comme s’il était détruit)
- Peut collecter, utiliser ou communiquer un renseignement anonymisé sans réelles contraintes.

La position de la CAI

Un renseignement anonymisé cesse d'être qualifié de renseignement personnel et n'est plus soumis aux règles applicables en cette matière. Il peut donc être utilisé, communiqué, diffusé et conservé sans autre obligation.

- Donc même si risque de ré-identification, n'est pas un renseignement personnel
- Source: Site Web de la CAI, onglet "Conservation et destruction des renseignements personnels"

La position de la CAI

L’avis de la Commission sur l’anonymisation

À la lumière des avancées technologiques actuelles et futures, la Commission estime qu’il est quasi impossible de certifier que des renseignements anonymisés ne pourraient pas éventuellement être réidentifiés.

Certains renseignements sont tellement distinctifs par nature qu’ils ne peuvent pas être adéquatement anonymisés. Pensons, par exemple, aux renseignements génétiques, biométriques ou encore à ceux relatifs à la géolocalisation.

L’anonymisation des renseignements personnels présuppose des risques d’incidents de confidentialité. Des sanctions sont prévues pour toute personne qui tente d’identifier une personne à partir de renseignements anonymisés.

Plan de la section

1. **Définition :** définir le renseignement anonymisé en fonction du contexte terminologique plus large de la loi (renseignement personnel, sensible, dépersonnalisé).

2. **L'anonymisation en droit québécois :** situer l'anonymisation dans le contexte juridique actuel et identifier sa fonction et ses possibles utilisations.

3. **Le processus d'anonymisation :** présenter le *Règlement sur l'anonymisation* et les étapes prévues pour qualifier un renseignement d'anonymisé.

1. Avant l'anonymisation
Identification des finalités

3. Avant de débuter un processus d'anonymisation, une organisation **doit établir les fins** pour lesquelles elle entend **utiliser** les renseignements anonymisés. L'organisation doit s'assurer que ces fins sont conformes, selon le cas, à l'article 73 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1) ou à l'article 23 de la Loi sur la protection des renseignements personnels dans le secteur privé (chapitre P-39.1).

- Art. 23 & 73 - l'utiliser à des fins d'intérêt public
- ** Principe de limitation de l'utilisation (régime PRP)

2. Au début de l'anonymisation
Dépersonnalisation et analyse des risques

4. Une organisation doit, au début d'un processus d'anonymisation, retirer tous les renseignements personnels qui permettent d'identifier **directement** la personne concernée des renseignements qu'elle entend anonymiser. (i.e. *dépersonnalisation*)

Elle doit ensuite effectuer 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 raisonnablement disponibles, notamment dans l'espace public, soient utilisés pour identifier directement ou indirectement une personne.

2. Au début de l'anonymisation
Les critères d'analyse du risque de ré-identification

3. Dans le présent règlement, on entend par:

« **critère de corrélation** » : le fait de ne pas être en mesure de relier entre eux des ensembles de données qui concernent une même personne;

« **critère d'individualisation** » : le fait de ne pas être en mesure d'isoler ou de distinguer une personne dans un ensemble de données;

« **critère d'inférence** » : le fait de ne pas être en mesure de déduire des renseignements personnels à partir d'autres renseignements disponibles;

3. Le processus d'anonymisation
Les meilleures pratiques

6 . En fonction des risques de réidentification déterminés conformément au deuxième alinéa de l'article 5, une organisation doit **établir les techniques d'anonymisation à utiliser, lesquelles doivent être conformes aux meilleures pratiques généralement reconnues.** Elle doit également établir des mesures de **protection** et de sécurité raisonnables pour diminuer les risques de réidentification.

• Analyse contextuelle, en fonction des risques identifiées

- Conformité aux meilleures pratiques : "*Le choix de la solution optimale doit être évalué au cas par cas et nécessite généralement une combinaison de techniques différentes*." Site Web du GQ, onglet "anonymisation"

• **Compétence singulière** en la matière : "Un processus d'anonymisation doit être réalisé sous la supervision d'une personne compétente en la matière" (art. 4 - LRSSS)

- Le Secrétariat à la réforme des institutions démocratiques, à l'accès à l'information et à la laïcité "*invite les organismes publics qui envisagent de procéder à l'anonymisation de certains renseignements personnels à se tenir au courant des meilleures techniques existantes et à détenir une expertise dans ce domaine.*"

4. Analyse des risques de ré-identification
Post-anonymisation

7. Après avoir mis en œuvre les techniques d'anonymisation établies pour le processus d'anonymisation et les mesures de protection et de sécurité conformément à l'article 6, une organisation doit 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 d'un processus d'anonymisation ne permettent plus, **de façon irréversible**, d'identifier directement ou indirectement une personne.

- Critères exigeants ;
- Difficilement interprétables ;
- Difficilement réalisable.

4. Analyse des risques de ré-identification
Post-anonymisation

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 les risques résiduels de réidentification sont très faibles:

1° les **circonstances** liées à l'anonymisation des renseignements personnels, notamment les fins pour lesquelles elle entend utiliser les renseignements anonymisés;

2° la **nature** des renseignements;

3° le **critère** d'individualisation, le critère de corrélation et le critère d'inférence;

4° les risques que **d'autres renseignements** raisonnablement disponibles, notamment dans l'espace public, soient utilisés pour identifier directement ou indirectement une personne;

5° les **moyens nécessaires pour réidentifie**r les personnes, notamment en considérant les efforts, les ressources et le savoir-faire requis pour mettre en œuvre ces moyens.

5. Processus en continue
Documentation

8. Une organisation doit périodiquement évaluer les renseignements qu'elle a anonymisés afin de s'assurer **qu'ils le demeurent**. Pour ce faire, **elle doit mettre à jour** la dernière analyse des risques de réidentification qu'elle a effectuée. Cette mise à jour doit notamment considérer les avancées technologiques qui peuvent contribuer à réidentifier une personne.

Les résultats de la mise à jour de cette analyse doivent être conformes au deuxième alinéa de l'article 7. Dans le cas contraire, ** **les renseignements ne sont plus considérés comme anonymisés *****

- Un travail exigeant, mérite une attention à travers le temps.
- Possible de considérer que des renseignements *anonymisés* redeviennent *personnels*.
- Que faire si on les a communiqués ou échangés ? ***

6. Responsabilités pour la conservation
Documentation

9. Une organisation qui procède à l'anonymisation de renseignements personnels doit consigner dans un **registre** les renseignements suivants:

1° une **description** des renseignements personnels qui ont été anonymisés;

2° les **fins pour lesquelles** elle entend utiliser ces renseignements anonymisés;

3° les **techniques d'anonymisation** utilisées et les mesures de protection et de sécurité établies conformément à l'article 6;

4° la date à laquelle l'analyse des risques de réidentification effectuée conformément à l'article 7 a été complétée et, le cas échéant, la date à laquelle la mise à jour de l'analyse effectuée conformément à l'article 8 a été complétée.

Conclusion

Un travail exigeant, long et complexe :

- Deux analyses de risques, des processus d'anonymisation, compétences particulières, un travail en continu et exigences de documentation

Un cadre juridique et réglementaire complexe :

- Loi et règlement, un vocabulaire parfois ambigu, contre-intuitif ;
- Une absence de précision sur les pratiques à suivre (neutralité technologique) ;
- Flexibilité du cas par cas.

Des questions en suspens

- Risques sur la possibilité de voir les renseignements anonymisés comme n'étant plus des renseignements personnels ;
- Peut échanger et utiliser sans trop de contraintes (CAI), mais exigences de finalités, de documentation, de surveillance et de monitoring.

Merci !

CONSORTIUM SANTÉ NUMÉRIQUE

Université de Montréal

DOSA

Chaire de recherche du Canada
sur la protection et la valorisation
des données de santé

RSN