Centre intégré universitaire de santé et de services sociaux du Nord-de-l'Île-de-Montréal

Québec

Direction de la recherche

Guide de cueillette, d'utilisation et de communication de renseignements personnels à l'intention des chercheurs

Contents

Par Manon Couture, 05 mars 2019

Mise en contexte

Les chercheurs désirent pouvoir utiliser des plateformes électroniques (de type RedCap) pour collecter des données pour fin de recherche via internet. Le présent document vise à donner des outils aux chercheurs dans la planification de son projet afin de respecter l'ensemble de ses responsabilités de confidentialité et de protection des renseignements personnels dans un environnement numérique.

Nous avons conçu ce document comme un outil d'évaluation des risques liés à l'utilisation de plateformes internet pour la collecte, la saisie et la conservation des données collectées pour fins de recherche. La décision finale en ce qui a trait à la meilleure manière de procéder demeure avec le chercheur.

Responsabilités

« La vie privée a trait au droit d'une personne de ne pas subir d'ingérence ou d'interférence de la part d'autrui. Elle fait partie des droits fondamentaux d'une société libre et démocratique. Les personnes ont droit à la protection de leur vie privée en ce qui a trait à leur corps, à leurs renseignements personnels, aux pensées et opinions qu'elles expriment, à leurs communications personnelles et aux lieux qu'elles occupent.

La recherche peut affecter de différentes façons chacun de ces aspects, selon les objectifs du projet de recherche et les méthodes employées. En matière de vie privée, il est important que la personne ait un droit de regard sur l'information qui la concerne personnellement.

La notion de consentement est liée à la vie privée. La vie privée est respectée si la personne a la possibilité d'exercer un certain contrôle sur ses renseignements personnels en donnant ou en refusant son consentement à la collecte, à l'utilisation ou à la divulgation d'informations à son sujet. »[i]

Trois grands plans ont été identifiés dans la recommandation des trois conseils :

1. *Les stratégies de gestion des données des établissements :*
   a. *Fournir à leurs chercheurs un environnement qui favorise des pratiques d'intendance de données de classe mondiale ;*
   b. *Fournir ou appuyer un accès aux dépôts ou autres plateformes où sont conservées et organisées les données et où on peut avoir accès aux données de recherche de façon continue ;*
   c. *Appuyer les chercheurs dans leurs efforts afin d'établir et de mettre en place des pratiques de gestion des données qui sont conformes aux obligations éthiques, juridiques et commerciales et aux exigences des trois organismes qui figurent entre*

Par Manon Couture, 05 mars 2019

autres dans le Cadre de référence des trois organismes sur la conduite responsable de la recherche - 2e édition, le Cadre de référence des trois organismes sur la conduite responsable de la recherche et d'autres politiques pertinentes ;

d. *Fournir à leurs chercheurs affiliés des conseils pour gérer correctement leurs données, conformément aux principes énoncés ci-dessus et aux pratiques exemplaires de la communauté de la recherche, y compris pour élaborer des plans de gestion des données ;*
e. *Reconnaître que les données sont un résultat de recherche important et favoriser l'excellence en matière de gestion des données ;*
f. *Promouvoir, auprès des chercheurs, du personnel et des étudiants, l'importance de la gestion des données ;*
g. *Élaborer leurs propres politiques de gestion des données et s'assurer que ces politiques sont en conformité avec les principes énoncés ci-dessus et avec les lois provinciales et nationales, et qu'elles peuvent s'adapter à l'évolution rapide des pratiques exemplaires des communautés de chercheurs.*

2. *Les plans de gestion des données des chercheurs,*
   a. *La planification de la gestion des données est nécessaire à toutes les étapes du cycle de vie d'un projet de recherche, de la conception jusqu'à la fin.*
   b. *Les plans de gestion de données sont essentiels au processus de gestion des données. Ces plans décrivent le mode de collecte, de formatage, de conservation et de partage des données ; le mode d'utilisation des ensembles de données existantes ; et la nature des nouvelles données qui seront créées. Les plans de gestion aident aussi les chercheurs à déterminer les coûts, les avantages et les défis de la gestion des données. L'élaboration des plans devrait se faire à l'aide d'outils normalisés, lorsqu'ils sont disponibles.*
3. *Le dépôt des données.*

Ceci réfère aux critères des IRSC pour le dépôt des données, tels que définis dans la Politique des trois organismes sur le libre accès aux publications (2015)[ii]

Risques pour les participants

Deux risques majeurs sont identifiés :

- Être reconnus
- Vol d'identité

Les deux risques peuvent avoir des conséquences très sérieuses sur la vie d'une personne. Il se peut par exemple que les données, de toutes sortes de manières, soient vendues ou volées et se retrouvent dans les mains des compagnies d'assurances, d'employeurs notamment ou pire encore.

C'est pourquoi nous devons protéger les renseignements personnels des participants à nos recherches.

L'identité

On définit l'identité comme suit :

« L'identité d'un individu peut être définie comme étant la somme de toutes les caractéristiques qui font de cette personne qui elle est, par exemple son nom, sa date de naissance, son lieu de résidence ou d'autre information. Ces caractéristiques sont appelées attributs d'identité.

Un attribut d'identité peut également être un identifiant. Par exemple, on peut désigner une personne en utilisant son nom ou le numéro qui lui a été attribué. Il peut s'agir d'un identifiant commun (p. ex., plusieurs personnes peuvent avoir la même date de naissance) ou unique, dans la mesure où il s'applique à une seule personne. » [iii]

Il y a deux catégories d'identifiants : les identifiants directs et indirects. Il n'y a pas de liste formelle d'identifiants directs ou indirects dans aucun document officiel (sauf pour les identifiants indirects de l'HIPPA aux USA). Ces listes ne sont pas mutuellement exclusives et le jugement doit être exercé selon le contexte.

Identifiants directs :

Il s'agit de tous les attributs qui identifie une personne directement tel que :

Nom, prénom, adresse (toutes les subdivisions géographiques inférieures à l'état, y compris le numéro civique, la province, la ville et le code postal), tous les éléments (sauf les années) des dates liées à un individu (date de naissance, date d'admission, date de sortie, date du décès), numéros de téléphone, numéro de fax, adresse électronique, numéro de d'assurance sociale, numéro du dossier médical, numéro d'assurance maladie, numéro de compte de banque, numéro de permis de conduire, tout numéro de série de véhicule ou autre appareil, Adresse URL, protocole Internet (IP), empreinte digitale ou vocale, image photographique (les images photographiques ne se limitent pas au visage), toute autre caractéristique permettant d'identifier de manière unique l'individu.

Identifiants indirects : Il s'agit de variables qui, lorsqu'elles sont utilisées conjointement, deviennent redoutablement efficace à identifier les personnes.

Par exemples (liste provenant principalement de l'HIPPA des USA) : l'âge, le genre, des renseignements sur les habitudes de navigation sur internet, des renseignements géographiques détaillés, caractéristiques inhabituelles de l'individu (p. ex., état de santé rare, nombre d'enfants), caractéristiques très visibles de l'individu (p. ex., ethnicité, race), organisations auxquelles la

personne appartient, établissements d'enseignement où la personne a gradué, année de graduation, titres professionnels détaillés, lieu où une personne a grandi, revenu détaillé, etc.

Renseignements sensibles.

Tous les renseignements peuvent devenir sensibles selon le contexte.

Certaines données sont toujours sensibles comme les dossiers médicaux (les diagnostiques, les médicaments consommés, les effets indésirables, les valeurs de laboratoire, les images de toutes sortes provenant de scans ou autres, les questionnaires (e.g. sur la qualité de la vie), etc.etc.).

La loi sur les renseignements personnels du Québec parle des renseignements sur la santé comme étant des renseignements sensibles.

Les données sur les finances comme le revenu, vos dettes, vos actifs peuvent s'avérer très sensibles tout dépendant du contexte.

Ou encore les opinions politiques, les convictions religieuses, l'appartenance syndicale, les antécédents judiciaires, les données biométriques, l'orientation sexuelle, etc.

Déterminer les mesures de sécurités appropriées[iv]

Cette section a été largement inspirée par les travaux de Josée Coté[v] et de Lain Hrynaszkievicz[vi], tous les deux cités en références sur la collecte et l'analyse des données par sondage en ligne dans un cadre de recherche.

Les mesures à prévoir pour préserver la confidentialité des participants concernent principalement deux aspects :

- Les modalités de collecte et de conservation des données et
- La diffusion des résultats de recherche.

De plus, il faut savoir qu'au Québec la donnée appartient à l'individu, le dossier médical à l'institution et les résultats de recherche au chercheur.

Assurer la confidentialité et la sécurité demeure un défi de taille. Le chercheur a la responsabilité de s'outiller de :

- Logiciels pour chiffrer les données sensibles,
- Logiciels antivirus (établissement et chercheur),
- Pare-feu (établissement),
- Clés et disques de sauvegarde de données cryptés (établissement et chercheur).

Il est recommandé de développer des outils gérés par l'institution de recherche.

- Les chercheurs accéderaient aux données à l'aide de mots de passe et de procédures d'identification, mais les données demeureraient hébergées sur les serveurs de l'institution plutôt que sur des serveurs tiers ou des ordinateurs personnels.

En dehors des exceptions, plus l'interaction est importante, plus la recherche comporte de risques pour les participants. Le chercheur tentera de les minimiser lors du recrutement, du consentement et de la collecte de données.

1. Liste de distributions par courriel : Quatre précautions sont à prévoir :
   - La première consiste à utiliser une liste de courriels dont l'accès est autorisé (par consentement).
   - La seconde concerne l'usage de la fonction copie conforme invisible (CCI).
   - La troisième s'attarde à l'exactitude des adresses courriel. Le Boston Children's Hospital (2011) recommande aux chercheurs d'indiquer la personne à contacter en cas d'erreur et de vérifier que les communications ont effectivement été reçues.
   - La quatrième concerne l'utilisation d'une connexion Internet protégée avec un protocole de communication sécurisé (British Psychological Society, 2007). (https?)

2. Pour les sondages en ligne :
   - Le fait de répondre au questionnaire d'enquête manifeste implicitement le consentement.
   - La British Psychological Society (2007) recommande d'indiquer aux participants de contacter un professionnel de la santé en cas de détresse. Fournir un site Web de référence, un formulaire en ligne sécurisé ou un numéro de téléphone sans frais pourrait être des atouts. Le Boston Children's Hospital (2011) précise toutefois qu'un questionnaire susceptible de provoquer de l'anxiété ne serait pas convenable pour une recherche par Internet.
     - Le chercheur est invité à réfléchir à cette éventualité pour déterminer s'il devra intervenir et de quelle façon. En outre, il est de mise de vérifier si la politique de confidentialité du site utilisé confirme la possibilité de transmettre aux autorités concernées les coordonnées et autres informations utiles dans l'éventualité d'un signalement de harcèlement dont le chercheur aurait été informé.
     - Le questionnaire d'enquête doit permettre à la personne de se retirer à mi-chemin et de sauter des questions en prévoyant les options « poursuivre », « préfère ne pas répondre », « quitter » (British Psychological Society, 2007 ; Buchanan et Ess, 2009). De plus, la stratégie devrait permettre d'identifier les contributions individuelles des participants de sorte qu'un participant désirant après coup soustraire ses données de l'étude puisse le faire (British Psychological Society, 2007).

- Certains sites commerciaux offrant des sondages en ligne ou des services infonuagiques donnent peu d'informations quant à la conservation, la sécurité et la confidentialité des données qui leur sont confiées (Aldrige, Medina et Ralph, cités par Buchanan et al., 2011 : 77).
    - De plus, des sites tel Survey Monkey conservent les informations sur des serveurs américains où les données peuvent être accessibles selon les termes de la Patriot Act. Certains fournisseurs de services vendent les données, d'autres en sous-traitent la conservation, si bien qu'elles peuvent dès lors se retrouver hébergées à travers le monde sous des législations différentes en l'absence de règles internationales claires sur le droit applicable, qui est ainsi laissé aux mains des corporations.
    - De plus, à l'instar de Google, les fournisseurs ne semblent pas prendre en compte les lois des pays où ils ne sont pas implantés, bien que leurs services y soient accessibles (Bloche et Verchère, 2011). Buchanan et al. (2011) conseillent donc aux chercheurs de se documenter sur les sites commerciaux utilisés et d'inclure ces informations à leur devis :
        - Durée et lieu de conservation, politique de destruction des données, responsabilités à l'égard de la perte ou la fuite des données, mécanismes pour en aviser les participants et le chercheur. Le chercheur se souciera de savoir si les administrateurs de ces sites sollicitent des renseignements personnels en échange de l'accès à leurs services et s'ils envoient des courriels non sollicités aux usagers.

3. Protection des données :
    a. La dénominalisation : La dénominalisation est réversible. Les recherches sur les algorithmes de ré-identification montrent qu'à l'ère des réseaux sociaux, la dénominalisation constitue une faible protection, car la ré-identification demeure possible même sans les identifiants directs en utilisant les préférences de consommation, les transactions commerciales, le parcours de navigation, l'historique de recherche, etc. Il suffit que les informations soient passablement stables dans le temps et les contextes, et que les attributs correspondants soient suffisamment nombreux et distinctifs afin qu'aucune autre personne ne soit similaire, excepté dans une faible probabilité.
        - Il est recommandé que les banques de données soient accompagnées de mécanismes de contrôle d'accès (utilisateur et mot de passe) et autres méthodes de protection, tels que le consentement éclairé et des modalités d'utilisation des données.
        - La dénominalisation des dossiers médicaux désigne la suppression ou le remplacement d'identificateurs personnels dans le but de rendre difficile le

rétablissement d'un lien entre un participant et les données à son sujet. On parle alors de confidentialité.

b. Anonymisation : L'anonymisation est la suppression irréversible du lien entre un participant et les données de son dossier de recherche, de manière qu'il soit pratiquement impossible de les associer de nouveau.
   - L'anonymat implique une démarche supplémentaire qui rend absolument impossible l'accès à l'identité du participant parce que la liste associant le nom des participants et des codes a été détruite (dénominalisation irréversible ou anonymisation). On parle d'anonymat.
   - C'est la raison pour laquelle les formulaires de consentement font généralement référence à la confidentialité plutôt qu'à l'anonymat.

c. Dans les cas où il est essentiel pour la validité scientifique de l'étude d'inclure des dates, telles que les dates de traitement (identifiant direct), les données doivent être présentées de manière à ne pas affecter les statistiques dans les analyse mais doit préserver l'anonymat. Par exemple, vous pouvez ajouter ou soustraire un petit nombre de jours choisi au hasard à toutes les dates, de sorte que les dates vraies ne soient pas publiées. Dans les cas où il est nécessaire d'inclure des dates, ce fait et toute information à l'appui doivent être divulgués lors de leur soumission pour publication.

Préparer un plan de gestion des données

La planification de la gestion des données est nécessaire à toutes les étapes du cycle de vie d'un projet de recherche, de la conception jusqu'à la fin. De plus les plans de gestion aident aussi les chercheurs à déterminer les coûts, les avantages et les défis de la gestion des données.

Décrivez chacun des éléments avec autant de précision que possible :

a. Le mode de collecte *:*

i. *Comment allez-vous obtenir les données que vous utiliserez ?*

ii. *Décrivez toutes les étapes du processus :*

iii. Quels seront les sites commerciaux utilisés ? De plus il est fortement conseillé d'inclure ces informations à votre devis. Quelles sont les politiques du site commercial choisi (RedCap) en matière de :

iv. Durée et lieu de conservation, politique de destruction des données, responsabilités à l'égard de la perte ou la fuite des données, mécanismes pour en aviser les participants et le chercheur. Le chercheur se souciera de savoir si les administrateurs de ces sites sollicitent des renseignements

personnels en échange de l'accès à leurs services et s'ils envoient des courriels non sollicités aux usagers.

b. Les identifiants :
   i. Quelles sont les identifiants personnels directs et indirects qui seront collectés ?
   ii. Un groupe de données comprenant deux identifiants directs ou trois identifiants indirects ou plus devrait être justifié par le chercheur :
   iii. *Comment allez-vous protéger les renseignements personnels (dénominalisation ou anonymisation) ?*
      1. *Décrivez en détail ce qui sera fait pour chacune des données ou son ensemble :*

c. Les renseignements sensibles – *quels sont les renseignements sensibles que vous entendez collecter ? Sont-ils tous nécessaire ? Qu'allez-vous pouvoir conclure des renseignements sensibles que vous collectez ?*

d. Le formatage *(formater signifie organiser, ou encore mettre dans un format. Préparer (un support de stockage) à recevoir des données.) – Quel sont les outils logiciels ou informatiques que vous utiliserez pour demander, recevoir, analyser et conserver les données ?*

e. Le partage des données. (Les chercheurs devraient être encouragés à prendre en compte le partage ou la publication des données lors de la préparation des protocoles d'étude) – *quelles données seront disponibles pour le partage des connaissances ? Quelles données seront utilisées pour la publication des résultats ?*

f. Le mode d'utilisation des ensembles de données existantes – *Si vous utilisez des données ou un ensemble de données qui est déjà existant, comment allez-vous utiliser ce sous-groupe ?*

g. La nature des nouvelles données qui seront créées – *Décrivez le nouvel ensemble de données que vous allez créer par ce projet ?*

Le formulaire de consentement :

Si vous anticipez des limites à la confidentialité, vous devez en informer explicitement les participants. Même si l'information est publique, vous ne pouvez pas collecter et utiliser des renseignements personnels sans le consentement de la personne.

Le consentement, qu'il soit implicite, verbal ou signé doit inclure une section sur la méthode employée pour dénominaliser ou anonymiser les données. Cette section doit décrire précisément les risques encourus par le participant.

De plus il est recommandé d'inclure la possibilité que les données puissent être utilisées dans le cadre de méta-analyses ultérieures.

Une clause sur la publication des résultats devrait être également explicite.

Autres considérations éthiques

L'Université Laval a créé un guide d'évaluation à l'intention des comités d'éthiques. Il est accessible ici : Les enjeux éthiques de l'utilisation d'Internet en recherche

Il arrivera que des chercheurs souhaitent publier un ensemble de données de manière rétrospective. Cela peut provenir d'une recherche clinique en cours menée sans consentement explicite pour le partage de données ou la publication par les participants (en raison de l'absence d'exigences spécifiques des bailleurs de fonds ou des régulateurs) ou de l'utilisation de données issues d'une recherche historique réalisée avant la mise en place de politiques de partage de données Dans de tels cas, les chercheurs peuvent publier des données brutes s'il est clair et démontrable qu'il n'existe aucune menace pour l'anonymat - par exemple, si le jeu de données ne comprend aucun identificateur direct et moins de trois identificateurs indirects

Dans de tels cas, les chercheurs peuvent publier des données brutes s'il est clair et démontrable qu'il n'existe aucune menace pour l'anonymat - par exemple, si l'ensemble de données ne comprend aucun identifiant direct et moins de trois identificateurs indirects. S'il n'est pas certain que les données soient complètement anonymes et que le consentement de tous les participants ne soit pas possible, vous devez procéder à une évaluation minutieuse au cas par cas - en tenant compte de l'intérêt public et de l'impératif scientifique de la publication - avant de publier les données.

Lorsqu'il existe un risque d'identification, nous recommandons aux auteurs de consulter les comités d'éthique locaux pour indiquer s'ils souhaitent publier leurs données brutes de manière librement accessible avant de les soumettre pour publication.

Enfin, Buchanan et al. (2011) proposent qu'un spécialiste des TIC siège aux CÉR pour évaluer les recherches au plan de la sécurité informatique.

Cadre Légal

Canada :

La loi canadienne[vii] (LRPDE - **Loi sur la protection des renseignements personnels et les documents électroniques**) en matière de confidentialité et de renseignements personnels décrit le cadre de référence comme suit :

- *L'identité d'un individu peut être définie comme étant la somme de toutes les caractéristiques qui font de cette personne qui elle est, par exemple son nom, sa date de*

naissance, son lieu de résidence ou d'autre information. Ces caractéristiques sont appelées attributs d'identité.

- *Un attribut d'identité peut également être un identifiant. Par exemple, on peut désigner une personne en utilisant son nom ou le numéro qui lui a été attribué. Il peut s'agir d'un identifiant commun (p. ex., plusieurs personnes peuvent avoir la même date de naissance) ou unique, dans la mesure où il s'applique à une seule personne.*

- *Il faut garder à l'esprit ces concepts et leurs caractéristiques lorsque l'on réfléchit à la façon d'élaborer et de mettre en œuvre des processus d'identification et d'authentification appropriés.*

Québec :

La charte des droits et libertés de la personne. Charte Québécoise chapitre C-12 : article 5. Toute personne a droit au respect de sa vie privée.

Au Québec, les renseignements personnels des individus sont protégés par deux lois différentes. C'est principalement la seconde qui nous concerne.

1. selon qu'ils sont détenus par une entreprise privée (Loi sur la protection des renseignements personnels dans le secteur privé[viii])
2. ou par un organisme public (Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels[ix]).

Ces lois encadrent notamment : la cueillette, la conservation, l'utilisation, la communication et la destruction des renseignements personnels.

Extraits pertinents :

- 63.1. Un organisme public doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.
- 63.2. Un organisme public, à l'exception du Lieutenant-gouverneur, de l'Assemblée nationale et d'une personne qu'elle désigne pour exercer une fonction en relevant, doit protéger les renseignements personnels en mettant en œuvre les mesures édictées à cette fin par règlement du gouvernement.
- 83. Toute personne a le droit d'être informée de l'existence, dans un fichier de renseignements personnels, d'un renseignement personnel la concernant.
  Elle a le droit de recevoir communication de tout renseignement personnel la concernant.

  Toutefois, un mineur de moins de 14 ans n'a pas le droit d'être informé de l'existence ni de recevoir communication d'un renseignement personnel de nature médicale ou sociale le

concernant, contenu dans le dossier constitué par l'établissement de santé ou de services sociaux visé au deuxième alinéa de l'article 7.

La loi traite spécifiquement des renseignements sensibles comme suit :

- Un organisme public devrait également porter une attention particulière à la sensibilité des renseignements personnels qui feront l'objet de la communication.
- Sont généralement considérés comme sensibles les renseignements qui concernent la santé, les opinions politiques, la religion, l'orientation sexuelle. Des renseignements d'une autre nature peuvent également revêtir ce caractère sensible.
- Même si la Loi sur l'accès ne traite pas plus sévèrement les renseignements personnels qui ont un caractère sensible, chaque organisme public devrait sérieusement s'interroger sur la nécessité de communiquer ce type de renseignements aux fins de la réalisation d'un sondage. Un questionnement de même nature devrait également être fait au sujet des renseignements sensibles que pourrait être amené à colliger un organisme public ou son mandataire lors de la réalisation d'un sondage.

L'organisme qui est chargé de veiller au respect de ces lois est la Commission d'accès à l'information du Québec :

- Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier.

La loi sur les services de santé et les services sociaux du Québec[x] comporte aussi des dispositions importantes concernant les renseignements personnels sur la santé.

> 19. Le dossier d'un usager est confidentiel et nul ne peut y avoir accès, si ce n'est avec le consentement de l'usager ou de la personne pouvant donner un consentement en son nom.
>
> 19.1. Le consentement de l'usager à une demande d'accès à son dossier à des fins d'étude, d'enseignement ou de recherche doit être donné par écrit ; il doit être libre et éclairé, et accordé pour une activité précise. À défaut, il est sans effet.
>
> Le consentement ne vaut que pour le temps nécessaire à l'accomplissement de l'activité pour laquelle il a été accordé ou, dans le cas d'un projet de recherche approuvé par un comité d'éthique, pour la durée fixée, le cas échéant, par ce dernier.
>
> 19.2. Le directeur des services professionnels d'un établissement ou, à défaut d'un tel directeur, le directeur général peut autoriser un professionnel à prendre connaissance du dossier d'un usager, à des fins d'étude, d'enseignement ou de recherche.

Le directeur doit cependant, avant d'accorder une telle autorisation, s'assurer que les critères établis par l'article 125 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1) sont satisfaits. Il doit refuser d'accorder son autorisation s'il est d'avis que le projet du professionnel ne respecte pas les normes d'éthique ou d'intégrité scientifique généralement reconnues.

L'autorisation doit être limitée dans le temps et elle peut être assortie de conditions. Elle peut être révoquée en tout temps si le directeur a des raisons de croire que le professionnel autorisé ne respecte pas le caractère confidentiel des renseignements ainsi obtenus ou ne se conforme pas aux conditions imposées ou aux normes d'éthique ou d'intégrité scientifique généralement reconnues.

Règlement général sur la protection des données (RGPD – Europe)

Le **Règlement général sur la protection des données** (RGPD)[xi] est la nouvelle réglementation européenne qui est entrée en vigueur le 25 mai 2018. Il vient remplacer la directive européenne sur la protection des données personnelles datant de 1995.

Le RGPD reprend bon nombre de principes de protection des renseignements personnels (PRP) universellement reconnus et qui se retrouvent dans les lois québécoises de PRP, tels que le consentement de la personne concernée, la nécessité de la collecte ou le droit d'accéder à ses données personnelles.

Cependant, le RGPD suscite beaucoup d'intérêt à travers le monde, car il crée de nouveaux droits pour les personnes, notamment le droit au déréférencement et le droit à la portabilité des données, et de nouvelles obligations pour les entreprises et organismes, en particulier l'obligation de démontrer la conformité de leurs pratiques avec le nouveau règlement.

Bien que ce texte soit européen, les entreprises et organismes québécois pourraient devoir s'y conformer s'ils sont établis :

- Au sein de l'Union européenne ;
- Hors de l'Union européenne, **mais** qu'ils offrent des biens ou des services aux personnes qui se trouvent sur le territoire de l'Union européenne ou surveillent le comportement de ces mêmes personnes.

Cadre règlementaire

L'Énoncé Politique des Trois Conseils (EPTC2) dit ceci :

La gestion des données doit être effectuée en conformité avec l'Énoncé de politique des trois Conseils : Éthique de la recherche avec des êtres humains - 2e édition. L'énoncé fournit des conseils sur les aspects de gestion des données de recherche utilisant des êtres humains, tels que le

consentement, le respect de la vie privée et de la confidentialité, les droits des Autochtones, l'utilisation secondaire des données et le couplage des données. La gestion des données doit également être effectuée en conformité avec le Cadre de référence des trois organismes sur la conduite responsable de la recherche.

- Dans le contexte de la Politique, recherche « à risque minimal » renvoie à la recherche où la probabilité et l'ampleur des préjudices éventuels découlant de la participation à la recherche ne sont pas plus grandes que celles des préjudices inhérents aux aspects de la vie quotidienne du participant qui sont associés au projet de recherche.

- Équilibre entre bénéfices potentiels et risques : L'analyse, la recherche de l'équilibre et la répartition des bénéfices potentiels et des risques revêtent une importance cruciale pour l'éthique de tout projet de recherche avec des êtres humains. Le principe de préoccupation pour le bien-être impose une obligation éthique : celle d'élaborer, d'évaluer et d'exécuter le projet en veillant à protéger les participants contre tout risque inutile ou évitable. Dans leur examen, les CÉR chercheront à vérifier si l'évaluation des résultats éventuels et des bénéfices potentiels de la recherche justifie les risques.

- Il est possible que les bénéfices potentiels et les risques ne soient pas perçus de la même façon par différentes personnes et différents groupes au sein de la société. Les chercheurs et les CER en tiendront compte dans l'élaboration et l'évaluation du projet de recherche. Ils reconnaîtront aussi le fait que les chercheurs et les participants n'envisagent pas nécessairement de la même façon les bénéfices potentiels et les risques d'un projet de recherche. Dans l'évaluation des bénéfices potentiels et des risques pour certaines populations, les chercheurs et les CER devraient comprendre le rôle de la culture, des valeurs et des croyances des populations à l'étude.

Les trois organismes fédéraux de financement de la recherche — les Instituts de recherche en santé du Canada (IRSC), le Conseil de recherches en sciences naturelles et en génie du Canada (CRSNG) et le Conseil de recherches en sciences humaines du Canada (CRSH) — ont élaboré une ébauche de politique sur la gestion des données de recherche, laquelle vise l'excellence dans la recherche au Canada en favorisant de bonnes pratiques de gestion des données numériques et d'intendance des données.[xii]

Étant financés avec des deniers publics, ces organismes militent pour la démocratisation de l'accès aux résultats de la recherche qu'ils subventionnent, afin de faire progresser les connaissances, d'éviter la duplication de la recherche, d'encourager la réutilisation des résultats, de maximiser les avantages de la recherche pour les Canadiens et de mettre en valeur les réalisations des chercheurs canadiens.

La capacité de stocker, de consulter, de réutiliser et de mettre à profit les données numériques de la recherche est devenue essentielle à l'avancement de la science et des connaissances et au développement de solutions novatrices aux défis économiques et sociaux, et offre d'énormes possibilités d'améliorer la productivité, la compétitivité et la qualité de vie au Canada.

Université de Montréal

Lignes directrices pour la protection des renseignements personnels

Le stockage des renseignements personnels : Les renseignements personnels, qu'ils soient conservés en format numérique ou sur support papier, doivent être conservés dans des endroits sécurisés.

- *Les renseignements personnels stockés en format numérique doivent être conservés sur des serveurs gérés par l'Université de Montréal. Lors du remplacement d'un ordinateur, et afin d'assurer la protection des renseignements qui y sont stockés, vous devez communiquer avec la Division des archives (archives@archiv.umontreal.ca) qui verra avec vous, à traiter ces renseignements, par leur élimination ou leur archivage, en conformité avec le calendrier de conservation des documents de l'Université.*
- *Pour leur part, les renseignements personnels consignés sur support papier doivent être conservés, selon le cas, dans des classeurs fermés à clés ou dans des locaux sécurisés et dont l'accès est limité aux personnes pour qui ils sont nécessaires dans l'exercice de leurs fonctions.*

[i] http://www.ger.ethique.gc.ca/fra/policy-politique/initiatives/tcps2-eptc2/chapter5-chapitre5/

[ii] http://www.science.gc.ca/eic/site/063.nsf/fra/h_F6765465.html

[iii] https://www.priv.gc.ca/media/1708/id_paper_f.pdf

[iv] Les enjeux éthiques de l'utilisation d'Internet en recherche ( ) (Côté, Deleury)

[v] https://journals.openedition.org/ethiquepublique/997

[vi] https://trialsjournal.biomedcentral.com/articles/10.1186/1745-6215-11-9

[vii] https://www.priv.gc.ca/media/1708/id_paper_f.pdf

[viii] http://www.legisquebec.gouv.qc.ca/fr/showdoc/cs/P-39.1

[ix] http://legisquebec.gouv.qc.ca/fr/showdoc/cs/A-2.1/20180320

[x] http://legisquebec.gouv.qc.ca/fr/showdoc/cs/S-4.2

[xi] Commission Européenne :
Réforme des règles de l'UE en matière de protection des données 2018;

Lignes directrices du G29* (G29 : groupe des autorités européennes de protection des renseignements personnels).
Commission nationale de l'informatique et des libertés (CNIL) : l'autorité française de protection des renseignements personnels.

[xii] http://www.science.gc.ca/eic/site/063.nsf/fra/h_83F7624E.html