

[Chapitre 3]

VIE PRIVÉE ET CONFIDENTIALITÉ DES DONNÉES

Le souci de l'autonomie et de la dignité humaine constitue le fondement éthique du respect de la vie privée des sujets de recherche. Le respect de la vie privée est une valeur fondamentale, vue par beaucoup comme essentielle à la protection et à la promotion de la dignité humaine. En conséquence, l'accès aux renseignements personnels, ainsi que le contrôle et la diffusion de telles informations ont une importance considérable pour l'éthique de la recherche.

Les renseignements privés dévoilés dans le contexte d'une relation professionnelle ou de recherche doivent rester confidentiels. Les chercheurs auxquels des sujets confient des informations d'ordre privé ne doivent en aucun cas les révéler sans le consentement libre et éclairé des sujets à cet effet. Tout bris de confidentialité risque de nuire à la relation de confiance entre le chercheur et le sujet, d'autres personnes ou groupes, ou encore à la réputation du milieu de la recherche. La protection des renseignements personnels s'applique aux renseignements obtenus soit directement des sujets, soit d'autres chercheurs ou organismes tenus par la loi de protéger la confidentialité des dossiers personnels. À cet égard, les chercheurs soucieux de mieux concevoir et mener leurs travaux peuvent trouver utile d'adopter une perspective centrée sur les sujets lorsqu'ils évaluent la nature et la finalité de leurs projets ou encore la possibilité que ceux-ci n'empiètent sur des intérêts délicats. Par exemple, telle question vue comme publique dans la culture du chercheur pourra être envisagée comme privée dans la culture d'un sujet pressenti.

Le droit des sujets pressentis au respect de leur vie privée et les devoirs correspondants des chercheurs de traiter les renseignements personnels de façon confidentielle et respectueuse font l'objet d'un vaste consensus. Le respect de la vie privée constitue en recherche à la fois une norme et un principe éthique reconnu dans de nombreux pays. Au Canada, ce droit est inséré dans la Constitution comme un droit fondamental et est protégé autant par les lois provinciales que fédérales. Par ailleurs, plusieurs codes types ont été volontairement adoptés pour réglementer la protection des renseignements personnels et l'accès à ce type d'informations¹.

Toutefois, les valeurs qui sous-tendent le respect et la protection de la vie privée et des renseignements personnels ne sont pas absolues. Des intérêts publics incontestables et précisément cernés — protection de la santé, de la vie, de la sécurité, etc. — justifient parfois des bris de confidentialité et des ingérences dans la vie privée. Ainsi, les lois obligeant à rapporter les cas de mauvais traitements infligés à des enfants, les maladies sexuellement transmissibles ou les intentions d'homicide se fondent sur ce raisonnement, comme le sont les lois et les règlements protégeant les dénonciateurs. Cependant, dans certaines disciplines (épidémiologie, histoire, génétique, politique, etc.), la recherche a permis d'enrichir considérablement le savoir et d'améliorer la qualité de vie et il serait difficile, voire impossible, de mener à bien d'importants projets de recherche sociétaux sans avoir accès à des renseignements personnels. En conséquence, l'intérêt public justifie parfois que l'on autorise les chercheurs à avoir accès à des renseignements personnels afin d'approfondir les connaissances et d'atteindre divers objectifs sociaux, telle la création de programmes de santé publique adéquats.

L'utilisation confidentielle de données personnelles en recherche a produit par le passé d'importants bienfaits, comme l'illustre, par exemple, l'association entre l'exposition au tabac et le cancer du poumon ou encore l'utilisation de dossiers pédagogiques ou d'emploi pour évaluer les avantages et les inconvénients de divers facteurs sociaux. Depuis une vingtaine d'années, l'essor des banques de données et les percées technologiques permettent aux chercheurs de mieux concevoir et évaluer la prestation de services ou les conséquences de multiples produits et procédures. De telles études ont favorisé la prestation de services plus adaptés et plus efficaces dans de nombreux domaines — santé, éducation, sécurité, environnement, etc.

Le processus d'évaluation éthique est essentiel pour résoudre ce conflit de valeurs sociétales. Le rôle des CÉR, qui doivent équilibrer la nécessité de la recherche avec les éventuelles violations de la vie privée et la réduction des ingérences inévitables, est capital. Les personnes qui ont fourni des renseignements personnels alors qu'elles estimaient avoir droit au respect de leur vie privée et au bénéfice de la confidentialité devraient être protégées contre tout inconvénient lié à une utilisation non autorisée de cette information.

Il peut arriver qu'un tiers tente d'avoir accès à des dossiers de recherche — ce qui aurait pour résultat de rompre la promesse de confidentialité à laquelle s'est engagé le chercheur lorsque son projet a été approuvé par le CÉR. Le chercheur est tenu par l'honneur de protéger la confidentialité promise lors du processus de consentement libre et éclairé, tout en restant dans les limites de la loi. D'une façon générale, l'établissement, qui doit entre autres protéger l'intégrité de son CÉR, devrait appuyer son chercheur. Les chercheurs et les établissements qui reçoivent une demande de comparution en vue de remettre des données de recherche peuvent à bon droit vouloir plaider la cause devant les tribunaux. En pareil cas, les dossiers des CÉR et les documents relatifs au consentement peuvent s'avérer utiles pour contrer l'argumentation des parties cherchant à avoir accès aux données. Toutefois, en cas d'assignation, le chercheur n'aura vraisemblablement comme seul recours légal que d'interjeter appel pour protéger la confidentialité des données.

Les chercheurs devraient préciser, dans le processus du consentement libre et éclairé, l'étendue de la protection pouvant être assurée aux sujets pressentis qui fournissent des renseignements personnels et, en conséquence, connaître les lois applicables.

Les règles ci-dessous expriment l'obligation universelle de protéger la vie privée et les renseignements personnels en avisant les personnes qui donnent des informations privées et en obtenant leur consentement. Au sens de cette politique, les données personnelles permettant une identification ultérieure font référence aux renseignements concernant une personne pouvant raisonnablement être identifiée alors que celle-ci a raisonnablement pu penser avoir droit au respect de sa vie privée. Cette information englobe aussi bien des caractéristiques personnelles (âge, culture, religion, situation sociale) que des expériences de vie ou des antécédents dans divers domaines (éducation, emploi, santé). Toutefois, l'alinéa c) de la règle 1.1 stipule que les CÉR n'ont pas à approuver les projets reposant uniquement sur des informations accessibles au public — définition qui englobe des dossiers, des documents, des spécimens et du matériel provenant d'archives publiques, des ouvrages publiés, etc. auxquels le public a un droit d'accès.

D'une façon générale, la meilleure façon de protéger la confidentialité des renseignements personnels passe par l'anonymat. Si les données conservées sont véritablement anonymes, la recherche ne fera l'objet que d'une évaluation minimale du CÉR.

A. Accès aux renseignements personnels : les entrevues privées

Règle 3.1

Sous réserve des exceptions mentionnées à l'alinéa c) de la règle 1.1, les chercheurs qui souhaitent interroger un sujet en vue d'obtenir des renseignements personnels pouvant mener à une identification ultérieure feront approuver par le CÉR le protocole de leurs entrevues et s'assureront, tel que le requiert la règle 2.4, d'obtenir le consentement libre et éclairé des sujets interrogés. Tel que le mentionne l'alinéa c) de la règle 1.1, les CÉR n'ont pas à approuver les projets nécessitant un accès à du matériel ou à des documents publiquement accessibles, y compris à des documents d'archives, à des dossiers d'entrevues ou à des représentations publiques.

La règle 3.1 stipule que les chercheurs désireux de recueillir des renseignements par l'entremise d'entrevues privées doivent obtenir l'accord de leur CÉR. Les méthodes de ces entrevues devant permettre de documenter des études biographiques, des recherches sur des personnalités précises, etc., sont variées et englobent aussi bien des rencontres en personne que des appels téléphoniques ou des communications électroniques ou encore des questionnaires personnalisés. Pour faciliter l'évaluation de telles activités, les CÉR peuvent inciter les facultés et les départements utilisant très souvent ces méthodes d'entrevues personnelles à élaborer des protocoles normalisés s'inspirant des règles 2.3 et 3.1 ainsi que des exigences des corporations professionnelles. L'approbation préalable de tels protocoles d'entrevues pourrait énormément simplifier l'évaluation ultérieure de semblables procédures, malgré les dangers manifestes à vouloir s'efforcer de mettre en vigueur dans un établissement complexe une seule procédure d'entrevue pour des situations variées.

Il incombe aux CÉR de s'assurer que les sujets pressentis pour des entrevues reçoivent toute l'information exigée en vertu de cette politique avant de donner leur consentement libre et éclairé. Il est évident que ces personnes ont le droit de refuser de participer à une entrevue.

Cette règle ne signifie en aucun cas que les CÉR devraient censurer de façon préalable les projets concernant des personnalités actives sur la scène publique, artistique ou littéraire (voir alinéa c) de la règle 1.1).

B. Accès aux renseignements personnels : enquêtes, questionnaires et collecte de données

Règle 3.2

Sous réserve de la règle 3.1, les chercheurs qui souhaitent obtenir des renseignements personnels pouvant mener à l'identification ultérieure des sujets devront obtenir l'autorisation de leur CÉR, qui tiendra compte de ce qui suit :

- a) type des données devant être recueillies,**
- b) utilisation prévue des données,**
- c) limites restreignant l'utilisation, la divulgation et la conservation des données,**
- d) balises garantissant la sécurité et la confidentialité des données,**
- e) méthode d'observation (photographie, vidéo, etc.) ou d'accès à l'information (enregistrement sonore) permettant d'identifier des sujets précis,**
- f) utilisation secondaire prévue des données de la recherche permettant une identification ultérieure,**
- g) fusion prévue des données de la recherche avec d'autres données concernant les sujets — que celles-ci soient conservées dans des dossiers publics ou privés,**
- h) mesures visant à protéger la confidentialité des données résultant de la recherche.**

La règle 3.2 stipule que les projets où des renseignements personnels permettant une identification ultérieure sont recueillis, entre autres, grâce à des entrevues, des questionnaires ou des observations, ou encore grâce à un accès à des dossiers publics ou privés, devraient être évalués par un CÉR avant d'être mis en œuvre.

Les chercheurs devraient s'assurer que les données obtenues sont conservées avec toutes les précautions nécessaires particulières dues à la nature délicate des renseignements. Les données publiées ne devraient contenir ni nom, ni initiale, ni aucune autre sorte de renseignement pouvant mener à une identification. Il peut s'avérer important de conserver certains types d'identificateurs (par exemple, région de résidence), mais ceux-ci devraient être dissimulés le mieux possible, selon un protocole normalisé, avant que les données ne soient communiquées aux fins de la recherche. Toutefois, il peut arriver que de telles informations soient légitimement cruciales pour le projet. En conséquence, les renseignements permettant d'identifier des personnes ou des groupes devraient être conservés dans des banques de données différentes, avec des identificateurs distincts. Les chercheurs devraient prendre les mesures raisonnables visant à prévenir toute identification accidentelle de personnes ou de groupes et résoudre cette question à la satisfaction des CÉR.

La règle 3.2 indique que les sujets ont le droit de savoir qui aura accès aux renseignements permettant de les identifier et quel genre de renseignements sera accessible. Les chercheurs devraient notamment leur indiquer si les renseignements seront transmis à un gouvernement, à un organisme gouvernemental, au personnel de l'organisme chargé de contrôler la recherche, au commanditaire de la recherche (par exemple, une compagnie pharmaceutique), au CÉR ou à un organisme de réglementation. Par ailleurs, il peut arriver que des données fassent l'objet de déclarations obligatoires (lois obligeant à rapporter les cas d'enfants maltraités, les maladies infectieuses, les intentions d'homicide, etc.). Les CÉR et les chercheurs devraient être attentifs aux intérêts des personnes et groupes pouvant être stigmatisés. Ainsi, les chercheurs qui utilisent des dossiers de détenus, d'employés, d'étudiants ou d'autres personnes ne devraient pas transmettre aux autorités des résultats permettant d'identifier ces personnes à moins d'avoir préalablement obtenu leur consentement libre et éclairé par écrit. Toutefois, ils peuvent communiquer à des instances administratives, à des fins d'élaboration de politiques, des données globalisées anonymes ne pouvant être reliées à des personnes.

La règle 3.2 fait non seulement référence à l'utilisation secondaire des données, mais aussi à d'autres genres d'utilisations, dont l'utilisation subséquente de vidéos de recherche à des fins pédagogiques. Il est essentiel que ces utilisations soient précisées de façon suffisamment détaillée afin que les sujets pressentis puissent donner leur consentement libre et éclairé; il ne convient guère de solliciter une autorisation « pour l'ensemble de la recherche ». L'importance de l'alinéa g) de la règle 3.2 tient à ce que certains renseignements pouvant être considérés comme inoffensifs par des sujets peuvent prendre un sens radicalement différent lorsqu'ils sont fusionnés à d'autres données (voir règle 3.6).

C. Utilisation secondaire des données

En recherche, l'expression « utilisation secondaire des données » signifie l'utilisation de données obtenues dans un autre but que celui de la recherche. Parmi les exemples courants, citons les dossiers médicaux ou scolaires ou encore les spécimens biologiques produits au départ à des fins thérapeutiques ou pédagogiques, mais proposés cette fois-ci à des fins de recherche. La question ne se pose vraiment que lorsque les données peuvent être reliées à des personnes; elle devient cruciale lorsque des sujets risquent d'être identifiés dans des rapports publiés.

Règle 3.3

Les CÉR approuveront les projets où une utilisation secondaire des données permet d'identifier des sujets. Les chercheurs peuvent avoir accès à de telles données à condition d'avoir démontré à la satisfaction des CÉR ce qui suit :

- a) **les données permettant une identification ultérieure sont essentielles à la recherche,**
- b) **des précautions appropriées permettront de protéger la vie privée des sujets, d'assurer la confidentialité des données et de réduire les inconvénients pouvant être subis par les sujets, et**

- c) **les personnes auxquelles se réfèrent les données ne s'opposent pas à ce que celles-ci soient réutilisées.**

La possibilité d'identification variant considérablement d'une banque de données à l'autre, les CÉR devraient utiliser une méthode d'évaluation proportionnelle adaptée au caractère délicat des informations conservées dans les banques et moduler leurs exigences en conséquence. Les chercheurs devraient être autorisés à avoir accès aux banques contenant des dossiers personnels ne permettant aucune identification. Les CÉR devraient soigneusement évaluer toute possibilité d'identification, et notamment l'étendue des inconvénients ou de l'opprobre pouvant en résulter. Les chercheurs et les CÉR devraient également connaître les clauses juridiques régissant les banques de données applicables à la recherche.

Les chercheurs et les CÉR devraient également tenir compte du contexte de la création de ces banques de données (par exemple, relation de confiance) et des attentes des groupes et des personnes concernant l'utilisation, la rétention et la divulgation des données au moment où celles-ci ont été fournies. Les chercheurs qui s'interrogent sur le caractère privé de certains renseignements devraient consulter leur CÉR. L'information confidentielle obtenue de cette manière ne devrait pas être transmise aux autorités — sauf si elle est requise par la loi, par les tribunaux ou par d'autres organismes légalement constitués.

Règle 3.4

Les CÉR peuvent aussi exiger des chercheurs ayant recours à une utilisation secondaire des données le respect des conditions suivantes :

- a) **obtention du consentement libre et éclairé des personnes ayant fourni les données ou des tiers autorisés,**
- b) **établissement d'une stratégie adéquate d'information des sujets,**
- c) **consultation avec les représentants des sujets ayant fourni les données.**

La règle 3.4 repose sur le concept de la méthode proportionnelle d'évaluation éthique de la recherche. En conséquence, les CÉR devraient examiner avec plus de soin les projets comportant un risque plus que minimal et adapter leurs exigences et la protection des sujets en fonction de l'importance des inconvénients et de leur probabilité — y compris de la possibilité que des données publiées puissent être reliées à des personnes. L'alinéa a) stipule que de telles délibérations et un tel équilibre peuvent mener les CÉR, lorsque la situation s'avère particulièrement délicate, à demander à ce que les personnes ayant fourni les données consentent à ce que celles-ci soient réutilisées. C'est le cas, par exemple, lorsque des données permettant une identification ultérieure seront publiées, ou qu'il existe un risque important de bris de confidentialité.

Il est parfois impossible, difficile ou économiquement irréaliste de prendre contact avec tous les sujets d'un groupe d'étude pour obtenir le consentement libre et éclairé de chacun, notamment lorsqu'ils sont nombreux ou que certains membres sont décédés, géographiquement dispersés ou difficiles à retracer. En conséquence, l'alinéa b) stipule que les chercheurs doivent proposer une méthode appropriée d'information des parties concernées, et l'alinéa c) que ceux-ci consultent les membres représentant le groupe en question (par exemple, dans le cas d'une étude sur le sida, un ou plusieurs groupes de pression sur le sida) ou obtiennent un échantillonnage des opinions des membres de ce groupe.

Règle 3.5

Les chercheurs qui souhaitent communiquer avec des personnes ayant fourni des données obtiendront l'autorisation préalable de leur CÉR.

Dans certains cas, le but de la recherche ne peut être atteint que grâce à un suivi et à des entrevues avec des personnes. De toute évidence, les personnes ou les groupes qui découvrent qu'une recherche a été réalisée à partir de leurs propres données sans qu'ils en aient été avertis peuvent réagir vivement; certains peuvent refuser tout autre contact. Cet éventuel inconvénient souligne à quel point il est important que les chercheurs fassent tout en leur pouvoir pour permettre aux sujets de choisir de consentir à ce que leurs données et renseignements personnels soient intégrés à l'étude.

D. Fusion des données

Règle 3.6

Les CÉR évalueront les conséquences des fusions de données pouvant mener à une identification ultérieure.

Les progrès concernant la fusion de banques de données ouvrent de nouvelles perspectives de recherche et s'accompagnent de nouvelles menaces d'ingérence dans la vie privée. Par ailleurs, ces techniques peuvent offrir des réponses à des questions jusque-là irrésolues et générer des informations plus complètes sur la santé et sur la société. Les valeurs qui sous-tendent le devoir d'ordre éthique du respect de la vie privée imposent aux chercheurs et aux CÉR de faire preuve de prudence lorsqu'il y a création et utilisation de données de ce genre. Les CÉR devraient également être au courant des cadres statutaires appropriés ainsi que des critères gouvernementaux autorisant l'utilisation des données conservées dans des banques gouvernementales². Seul un nombre restreint de personnes devrait être autorisé à effectuer des fusions de banques de données. Les chercheurs devraient soit détruire les dossiers fusionnés immédiatement après les avoir utilisés, soit renforcer les mesures de sécurité s'ils veulent les conserver. Quelle que soit l'utilisation faite de ces données (statistique ou autre), leur caractère privé doit être protégé par tous les membres de l'équipe de recherche. Lorsque des banques fusionnées permettent d'identifier des personnes ou des groupes susceptibles d'être exposés à un risque important d'inconvénients, il peut s'avérer judicieux de communiquer avec ceux-ci ou avec les autorités concernées. Il convient également d'avertir le CÉR et l'établissement dépositaire du dossier.

Notes

1. Association canadienne de normalisation, *Code type sur la protection des renseignements*, CSA, 1996.
2. Voir la *Loi sur la statistique*, L.R.C., 1985, ch. S-19.