

Chapitre 5

VIE PRIVÉE ET CONFIDENTIALITÉ

Introduction

Tout le monde s'accorde à dire qu'il faut respecter la vie privée des participants à la recherche et que le chercheur a donc le devoir de traiter les renseignements personnels de façon confidentielle. En effet, le respect de la vie privée, dans le contexte de la recherche, constitue à la fois une norme et un principe éthique reconnu à l'échelle internationale. Les tribunaux ont jugé que la protection de la vie privée faisait partie des droits et libertés fondamentaux garantis par la Constitution canadienne. Les droits relatifs à la vie privée sont protégés par diverses lois fédérales, provinciales et territoriales. Des codes types¹ ont en outre été adoptés sur une base volontaire pour régir l'accès aux renseignements personnels et leur protection. Certains organismes professionnels ont établi des codes qui précisent les conditions et les obligations imposées à leurs membres en ce qui a trait à la collecte, à l'utilisation et à la divulgation des renseignements personnels.

En recherche, les risques d'atteinte à la vie privée sont liés à la possibilité d'identifier les participants et aux préjudices que ces derniers ou les groupes auxquels ils appartiennent risquent de subir à la suite de la collecte, de l'utilisation et de la divulgation de renseignements personnels. Ces risques se posent à toutes les étapes de la recherche : collecte initiale des renseignements; utilisation et analyse des renseignements dans l'étude de certaines questions de recherche; diffusion des résultats de la recherche; sauvegarde et conservation de l'information; élimination des dossiers dans lesquels l'information est conservée et des supports connexes.

La Politique repose sur une approche proportionnelle de l'évaluation de l'acceptabilité éthique d'un projet de recherche. Les chercheurs et les comités d'éthique de la recherche (CÉR) reconnaîtront et réduiront au minimum les risques pour la vie privée, en gardant à l'esprit que certaines questions qui ne sont pas de nature délicate ou embarrassante pour le chercheur peuvent l'être pour le participant.

En plus de suivre les orientations de la présente politique, les chercheurs ont la responsabilité de se conformer à toutes les exigences légales et réglementaires en matière de protection de la vie privée des participants et en matière de consentement, pour la collecte, la divulgation ou l'utilisation des renseignements sur les participants. Ces exigences peuvent varier d'une province ou d'un territoire à l'autre, ainsi qu'en fonction des sources de financement et des personnes ou organismes responsables de mener la recherche. Elles peuvent parfois comporter des éléments prescrits par la Constitution (y compris la *Charte canadienne des droits et libertés*), et par les lois et règlements sur la protection de la vie privée au niveau fédéral ou provincial, entre autres.

A. Concepts clés

Vie privée

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. Or, 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 (la question du consentement est abordée plus en détail au chapitre 3).

Confidentialité

Le devoir éthique de confidentialité renvoie à l'obligation qu'ont les personnes ou les organismes de protéger l'information qui leur est confiée. Ce devoir comporte l'obligation de protéger l'information contre l'accès, l'utilisation, la divulgation et la modification non autorisés, d'une part, et contre la perte et le vol, d'autre part. Il est essentiel de s'acquitter de ce devoir éthique de confidentialité pour maintenir tant le lien de confiance entre le chercheur et le participant que l'intégrité du projet de recherche.

Sécurité

La sécurité a trait aux moyens employés pour protéger l'information et comprend les mesures de protection matérielles, administratives et techniques. Les personnes ou les organismes s'acquittent en partie de leur devoir de confidentialité s'ils adoptent et appliquent des mesures de sécurité appropriées. Parmi les mesures de protection matérielles figurent l'utilisation de classeurs verrouillés et l'installation des ordinateurs renfermant les données de recherche dans un lieu non accessible au public. Font partie des mesures de protection administratives l'élaboration et l'application de règles au sein de l'organisme précisant qui a accès aux renseignements personnels concernant les participants. Quant aux mesures de protection techniques, elles comprennent l'utilisation de mots de passe informatiques, de pare-feu, de logiciels antivirus, de clés d'encodage et d'autres mesures destinées à protéger les données contre l'accès non autorisé, la perte et la modification.

Renseignements identificatoires

Dans le contexte de la Politique, des renseignements sont identificatoires s'il y a raisonnablement lieu de croire qu'ils permettraient d'identifier une personne, qu'ils soient utilisés seuls ou en combinaison avec d'autres renseignements accessibles. Dans le présent document, l'expression « renseignements personnels » désigne les renseignements identificatoires.

Types de renseignements

Il arrivera que les chercheurs souhaitent recueillir et utiliser différents types de renseignements sur les participants, les partager et y accéder. Citons à titre d'exemple des renseignements portant sur des caractéristiques personnelles ou autres qu'une personne s'attend raisonnablement à garder confidentiels (âge, ethnicité, études, antécédents professionnels, antécédents de santé, religion, expériences de vie, statut social).

Dans le contexte de la Politique, les chercheurs et le CÉR doivent se demander si les renseignements qu'ils souhaitent utiliser pour leur projet de recherche permettraient d'identifier des personnes. Les catégories suivantes peuvent aider à évaluer les renseignements en fonction de cette possibilité.

- *Renseignements qui permettent l'identification directe.* Renseignements servant à l'identification de la personne par des identificateurs directs (le nom, le numéro d'assurance sociale ou le numéro personnel du régime de santé, par exemple).
- *Renseignements qui permettent l'identification indirecte.* Renseignements dont on présume qu'ils peuvent aider à identifier une personne par une combinaison d'identificateurs indirects (par exemple, la date de naissance, le lieu de résidence et des caractéristiques personnelles distinctives).
- *Renseignements codés.* Renseignements dont on a retiré les identificateurs directs pour les remplacer par un code. Selon le degré d'accès à ce code, on sera en mesure de réidentifier des participants (par exemple, dans le cas où le chercheur principal conserve une liste associant le nom de code des participants à leur nom véritable, ce qui permet de les relier à nouveau au besoin).
- *Renseignements rendus anonymes.* Renseignements dont les identificateurs directs sont irrévocablement retirés et pour lesquels aucun code permettant une future réidentification n'est conservé. Le risque de réidentification des personnes à partir des identificateurs indirects restants est faible ou très faible.
- *Renseignements anonymes.* Renseignements auxquels aucun identificateur n'a jamais été associé (enquêtes anonymes, par exemple). Le risque d'identification des personnes est faible ou très faible.

Les préoccupations éthiques à l'égard de la vie privée s'atténuent en fonction de la difficulté, sinon de l'impossibilité, d'associer l'information à une personne donnée. Ces préoccupations varient aussi selon la nature délicate de l'information et selon le risque de préjudice auquel l'accès à ces renseignements, de même que l'utilisation ou la divulgation des renseignements, exposent les personnes ou les groupes visés.

La façon la plus simple de protéger les participants consiste à recueillir et à utiliser des données anonymes ou rendues anonymes, bien que ce ne soit pas toujours possible ni souhaitable. Par exemple, une fois l'information rendue anonyme, il n'est plus possible d'établir un lien entre les nouveaux renseignements et les personnes associées à un ensemble de données, ni de transmettre les résultats aux participants. Une autre solution consiste à utiliser des données dépersonnalisées : les données sont fournies aux chercheurs après avoir retiré les renseignements qui permettent d'identifier des personnes, et le code existant n'est accessible qu'à un dépositaire ou à une tierce partie fiable indépendants des chercheurs. La dernière solution pour les chercheurs consiste à recueillir des données identificatoires et de prendre des mesures pour les dépersonnaliser dès que possible. Bien que ces mesures constituent des moyens efficaces de protéger l'identité des participants, l'utilisation, à des fins de recherche, de renseignements codés ou rendus anonymes, mais qui sont indirectement identificatoires, peut quand même présenter des risques de réidentification.

De nouvelles technologies facilitent la consultation, la sauvegarde et l'analyse de grandes quantités de données. Ces activités augmentent le risque de réidentification, par exemple par suite du couplage d'ensembles de données (comme il en est question à la section E du présent chapitre), ou lorsqu'un ensemble de données comprend des renseignements sur la population d'une aire géographique restreinte ou sur des personnes ayant des caractéristiques très spécifiques (par exemple, s'il s'agit d'un domaine de spécialisation professionnelle peu commun ou du diagnostic d'une maladie très rare). Divers facteurs interviennent à l'égard des risques de réidentification; aussi les chercheurs et les CÉR doivent-ils faire preuve de vigilance pour reconnaître ces risques et les réduire. Le couplage de données de deux ensembles de données ou plus comprenant des renseignements anonymes peut présenter des risques d'identification (voir l'article 2.4 et l'article 9.22).

Dans les cas où il est impossible d'utiliser des données anonymes ou rendues anonymes dans le projet de recherche — et il y a une foule de raisons pour lesquelles il faut parfois recueillir et conserver les données sous une forme identificatoire —, le devoir éthique de confidentialité et l'application de mesures efficaces de protection des renseignements revêtent une importance capitale. La présente politique exige, de façon générale, un surcroît de rigueur à l'égard de la protection des renseignements identificatoires. Les chercheurs consulteront leur CÉR s'ils ne sont pas certains que les renseignements qu'ils se proposent d'utiliser sont identificatoires (par exemple, lorsqu'ils se proposent de coupler des ensembles de données codées ou rendues anonymes).

B. Le devoir éthique de confidentialité

Article 5.1 Les chercheurs doivent protéger les renseignements qui leur sont confiés et éviter de les utiliser ou de les divulguer à tort. Les établissements doivent aider les chercheurs à tenir leurs engagements de confidentialité.

Application Recueillir des renseignements en contrepartie d'une promesse de confidentialité confère aux chercheurs un devoir éthique qui est essentiel au maintien du respect des participants et à la préservation de l'intégrité du projet de recherche. Tout manquement à la confidentialité peut nuire au participant, à la relation de confiance entre le chercheur et le participant, à d'autres personnes ou à d'autres groupes, ou encore à la réputation du milieu de la recherche. La recherche portant sur des sujets de nature délicate (des activités illégales, par exemple) exige habituellement de solides promesses en matière de confidentialité pour qu'un rapport de confiance soit établi avec les participants.

Le devoir éthique de confidentialité s'applique à l'information obtenue directement soit des participants soit d'autres chercheurs ou d'organismes qui ont l'obligation juridique, professionnelle ou autre de préserver la confidentialité.

Il faut parfois concilier le devoir éthique de confidentialité avec des considérations d'ordre éthique ou des impératifs juridiques ou professionnels qui exigeraient la divulgation de renseignements constitués ou obtenus dans le cadre de travaux de recherche. Dans certaines circonstances exceptionnelles et impérieuses, par exemple, les chercheurs ont parfois l'obligation de divulguer des renseignements aux autorités afin de protéger la santé, la vie ou la sécurité d'un participant ou d'un

tiers. Les chercheurs devraient être au courant des codes d'éthique ou des lois susceptibles d'exiger la divulgation de renseignements qu'ils obtiennent dans le contexte de la recherche — par exemple les codes de déontologie professionnelle ou encore les lois qui obligent à signaler les situations où des enfants ont besoin de protection. Dans d'autres situations, il arrive qu'un tiers cherche à accéder à des renseignements constitués ou recueillis à titre confidentiel dans le cadre d'un projet de recherche. L'objet de la demande d'accès peut être la divulgation volontaire de l'information ou même sa divulgation forcée, au nom de la loi (au moyen d'un bref d'assignation, par exemple). La section C du chapitre 1 aborde la relation entre l'éthique de la recherche et le droit.

Certains domaines de recherche (comme la recherche auprès d'enfants susceptibles de faire l'objet de mauvais traitements ou les études sur le comportement criminel) sont particulièrement propices à la création, chez les chercheurs, de tensions entre le devoir éthique de confidentialité et l'obligation de divulguer des renseignements à des tiers. Les chercheurs doivent respecter la promesse de confidentialité qu'ils ont faite aux participants, dans les limites permises des principes de l'éthique et par la loi. Cela veut dire qu'il leur arrivera parfois de résister à des demandes d'accès, par exemple en s'opposant à des requêtes déposées devant les tribunaux pour obtenir la divulgation de renseignements. Dans les situations de ce genre, les chercheurs détermineront leur ligne de conduite au cas par cas et consulteront, selon le cas, des collègues, les organismes professionnels pertinents, le CÉR ou un avocat.

Dans certains cas, il est possible que des participants renoncent à leur anonymat, par exemple, quand ils demandent à être identifiés pour leur contribution à la recherche. Dans ces cas, les chercheurs devraient obtenir le consentement de ces participants et négocier avec eux des accords sur la façon de les identifier ou de les reconnaître pour leur contribution à la recherche. Par contre, si un participant en particulier renonce à l'anonymat, mais que d'autres membres au sein du groupe s'y opposent parce que l'identification pourrait nuire au groupe, le chercheur doit maintenir l'anonymat de tous les membres du groupe (voir l'alinéa 3.2 f) et l'article 10.4).

Article 5.2 Les chercheurs doivent décrire les mesures qu'ils prendront pour s'acquitter de leurs obligations en matière de confidentialité et doivent expliquer les exigences de divulgation raisonnablement prévisibles :

- a) dans la documentation accompagnant la demande qu'ils présentent au CÉR;
- b) au cours des discussions visant à obtenir le consentement des participants éventuels à la recherche.

Application Le présent article souligne que certains projets de recherche exposeront vraisemblablement les chercheurs à une situation où ils seront tenus de divulguer des renseignements à des tiers. On peut évaluer la probabilité que l'on soit obligé de divulguer des renseignements en tenant compte de la nature et des objectifs des travaux de recherche. Prenons l'exemple d'un projet de recherche au sujet de la violence intergénérationnelle, et comportant des entrevues avec des familles à risque. Il est raisonnablement prévisible, en ce cas, que les chercheurs recueilleront,

au cours de leurs travaux, des renseignements indiquant qu'un enfant fait l'objet de mauvais traitements. Les chercheurs qui ont tout lieu de croire que leur étude les obligera, pour des raisons d'ordre éthique ou juridique, à divulguer de l'information recueillie dans le cadre de leurs travaux doivent informer le CÉR et les participants éventuels de la possibilité qu'ils soient tenus de procéder à une divulgation. Le fait d'informer les participants de l'existence d'obligations de divulgation raisonnablement prévisibles est un aspect important du processus de consentement.

Il arrive que des chercheurs recueillent, de façon inattendue, de l'information dont la divulgation à un tiers serait justifiée. Dans d'autres situations, ils reçoivent d'un tiers une demande de divulgation. Dans un cas comme dans l'autre, le fait d'informer un participant de la divulgation revêt sans doute de l'importance dans l'optique de la relation de confiance avec le participant et de la préservation de la validité de son consentement. Dans leur processus de décision d'informer un participant d'une divulgation et afin de choisir les moyens et le moment de le faire, les chercheurs tiendront compte des normes en vigueur dans leur discipline; ils consulteront aussi, selon le cas, le CÉR, des collègues, l'organisme professionnel compétent ou un avocat.

Les chercheurs doivent aussi informer les participants et solliciter leur consentement sur la possibilité que des renseignements personnels soient transmis à des ministères ou à des organismes gouvernementaux, à des partenaires communautaires du projet de recherche, au personnel d'un organisme chargé de surveiller les travaux de recherche, à un commanditaire du projet de recherche (une société pharmaceutique, par exemple), au CÉR ou à un organisme de réglementation.

Les chercheurs doivent éviter les situations qui les amèneraient à agir comme des informateurs pour les autorités ou les dirigeants d'organismes. Ainsi, lorsque des dossiers personnels sont utilisés à des fins de recherche — qu'il s'agisse de prisonniers, d'employés, d'étudiants ou autres —, les chercheurs ne doivent pas communiquer aux autorités des résultats susceptibles de permettre l'identification des personnes à moins que les participants aient donné au préalable leur consentement écrit. Toutefois, les chercheurs peuvent fournir aux organes administratifs des données agrégées qu'il est impossible d'associer à des personnes, par exemple en vue d'élaborer des politiques ou d'évaluer des programmes. En cherchant à obtenir le consentement des participants éventuels, les chercheurs doivent les informer de la possibilité que des données agrégées tirées du projet de recherche soient divulguées, en particulier dans les cas où cette divulgation comporte un risque pour les participants. À titre d'exemple, fournir aux autorités des données agrégées sur la consommation illégale de drogues dans un pénitencier risque de donner lieu à des représailles visant les détenus, même s'ils ne sont pas identifiés individuellement.

Au moment de planifier leur étude, les chercheurs veilleront à intégrer tout principe de droit ou autre principe de nature juridique qui s'applique et est susceptible de contribuer à la protection de la vie privée des participants et à la confidentialité des renseignements obtenus dans le cadre du projet de recherche.

C. La protection de l'information

Article 5.3 Les chercheurs doivent fournir au CÉR des précisions sur les mesures de protection prévues pour toute la durée utile des renseignements. Sont ainsi visées la collecte, l'utilisation, la diffusion, la conservation et la suppression éventuelle de ces renseignements.

Application Les chercheurs doivent évaluer les risques d'atteinte à la vie privée et les menaces pour la sécurité de l'information touchant tous les stades du cycle de vie de la recherche. Ils doivent aussi mettre en place des mesures adéquates pour protéger l'information. La protection de l'information contribue au respect de la vie privée des participants; elle aide en outre les chercheurs à s'acquitter de leurs obligations en matière de confidentialité. Les mesures de protection de l'information qu'ils adoptent doivent être conformes aux normes et aux pratiques en usage dans la discipline des chercheurs en ce qui concerne la collecte et la protection des renseignements recueillis à des fins de recherche. Certains établissements exigent une évaluation en bonne et due forme des facteurs affectant la vie privée; cette obligation peut aussi découler de règles légales ou administratives, provinciales ou territoriales. Les mesures de sécurité tiendront compte de la nature, du type et de l'état des renseignements : le support (documents sur papier ou données informatiques), le contenu (informations renfermant ou non des identificateurs directs ou indirects), la mobilité (données conservées à un endroit ou soumises à un transfert physique ou électronique), et la vulnérabilité du mode de protection d'accès (cryptage ou protection par mot de passe). Les mesures relatives à la protection de l'information s'appliquent tant aux originaux qu'aux copies.

Parmi les facteurs dont le CÉR doit tenir compte lorsqu'il évalue le caractère adéquat des mesures proposées par les chercheurs pour protéger les renseignements, mentionnons les suivants :

- a) le type de renseignements devant être recueillis;
- b) les fins auxquelles ces renseignements serviront, ainsi que celles de toute utilisation secondaire des renseignements identificatoires;
- c) les restrictions relatives à l'utilisation, à la divulgation et à la conservation des renseignements;
- d) les risques pour les participants en cas de violation de la sécurité des données, y compris les risques de réidentification des personnes;
- e) les mesures de sécurité appropriées pour l'ensemble de la durée utile des renseignements;
- f) les modes d'enregistrement des observations (par exemple, les photos, les vidéos et les enregistrements sonores) employés au cours des travaux de recherche qui risquent de permettre l'identification de participants en particulier;
- g) les utilisations prévues des renseignements personnels tirés de la recherche;

- h) les couplages prévus des données recueillies dans le cadre du projet de recherche, avec d'autres données sur les participants, que celles-ci soient conservées dans des registres publics ou privés (voir aussi la section E de ce chapitre).

Dans son évaluation du caractère adéquat des mesures de protection proposées pour l'ensemble de la durée utile des renseignements, le CÉR n'imposera pas automatiquement au chercheur l'obligation de détruire les données de recherche. L'information conservée peut servir à bien d'autres fins, dans le futur. Les périodes appropriées de conservation des données varient selon la discipline, l'objet de la recherche et la nature des données. Dans certaines situations, il peut y avoir communication officielle de données aux participants — par exemple, si l'on remet aux différents participants, en guise de remerciement, soit une copie d'un enregistrement, soit une transcription, copie ou transcription qu'ils conserveront à des fins personnelles, familiales ou autres. De même, certains organismes subventionnaires tels que le Conseil de recherches en sciences humaines du Canada et les Instituts de recherches en santé du Canada disposent de politiques sur l'archivage et le partage de données². Les chercheurs aborderont la question du traitement des renseignements recueillis sur un participant qui décide de se retirer du projet de la recherche.

Lors de la diffusion des résultats de la recherche, les chercheurs doivent éviter de dévoiler des renseignements identificatoires sans le consentement des participants. Dans le cas de la recherche comportant une démarche critique, des renseignements identificatoires concernant les personnes qui font l'objet de la recherche seront parfois divulgués puisque ces personnes ne sont normalement pas considérés comme des participants (voir l'article 3.6). Les chercheurs devront prendre des mesures raisonnables pour prévenir l'identification par mégarde de personnes ou de groupes dans des publications ou lorsqu'ils utilisent d'autres moyens de diffusion. Les chercheurs doivent traiter cette question à la satisfaction du CÉR.

L'examen des utilisations futures des renseignements personnels ne vise pas uniquement le projet de recherche à l'étude. Il s'étend aussi aux autres fins, comme l'utilisation éventuelle de documents de recherche à des fins didactiques.

Il pourrait être nécessaire de coder, à l'aide d'un logiciel de cryptage ou d'anonymisation, les données de recherche transmises par Internet, afin de prévenir l'interception de ces données par des personnes non autorisées ou de soustraire ces données à d'autres risques touchant la sécurité. En règle générale, il faut crypter les données identificatoires obtenues au cours de travaux de recherche et conservées sur un ordinateur branché à Internet.

Article 5.4 Les établissements et les organismes où sont conservées des données de recherche ont la responsabilité d'établir des mesures de sécurité appropriées pour protéger ces données.

Application En plus des mesures adoptées par les chercheurs pour protéger les données, les dispositifs de sécurité mis en place au sein de l'établissement ou de l'organisme en

question offrent aussi une protection importante. Ces dispositifs comprendront des mesures matérielles, administratives et techniques convenables. Les mesures viseront en outre l'ensemble du cycle de vie de l'information. Elles comprendront les mesures de protection institutionnelles ou organisationnelles applicables à l'information pendant l'exécution des travaux de recherche, ainsi qu'à la conservation à long terme de l'information.

D. Consentement et utilisation secondaire de renseignements identificatoires à des fins de recherche

On entend par utilisation secondaire l'utilisation, dans un projet de recherche, de renseignements recueillis à l'origine à des fins autres que celles visées par les travaux de recherche en cours. Cette situation se présente souvent dans le domaine des sciences sociales ou de la santé, lorsque des ensembles de données constitués à partir d'enquêtes destinées à un projet de recherche particulier ou à la production de statistiques, servent par la suite à élucider d'autres questions étudiées dans le contexte d'un projet distinct. Ainsi des renseignements recueillis pour une évaluation de programme peuvent devenir utiles pour des travaux de recherche ultérieurs. Mentionnons également les dossiers médicaux, des spécimens biologiques, des dossiers scolaires, les registres d'état civil, ou encore les registres de chômage, tous constitués ou recueillis à l'origine à des fins thérapeutiques, didactiques ou administratives, mais que l'on pourrait vouloir utiliser ultérieurement à des fins de recherche. Le chapitre 12 fournit des indications supplémentaires qui s'appliquent aux travaux de recherche comportant l'utilisation secondaire de matériel biologique humain prélevé antérieurement.

Il existe plusieurs raisons d'effectuer des analyses secondaires des données : éviter de répéter la collecte de données primaires et, partant, réduire le fardeau imposé aux participants; corroborer ou critiquer les conclusions du projet original; comparer l'évolution d'un échantillon d'un projet de recherche au fil du temps; appliquer de nouveaux tests d'hypothèses dont on ne disposait pas au moment de la première collecte de données; confirmer l'authenticité des données. Sur le plan de la vie privée, les situations suivantes soulèvent néanmoins des préoccupations quant à la nécessité d'obtenir le consentement : d'une part, lorsqu'il est possible de relier aux personnes visées les renseignements destinés à une utilisation secondaire pour les besoins d'un projet de recherche; d'autre part, lorsqu'il y a risque que l'on puisse identifier des personnes lors de la publication des résultats d'une étude ou grâce au couplage de données. Les lois portant sur la protection des renseignements personnels reconnaissent ces préoccupations et permettent l'utilisation secondaire à certaines conditions.

Article 5.5 Les chercheurs qui n'ont pas obtenu le consentement des participants en vue de l'utilisation secondaire de renseignements identificatoires peuvent uniquement utiliser ces renseignements à cet effet si les conditions suivantes sont rencontrés à la satisfaction du CÉR :

- a) les renseignements identificatoires sont essentiels à l'objet de la recherche;
- b) à défaut de consentement des participants l'utilisation des renseignements identificatoires risque peu d'avoir des conséquences négatives sur le bien-être de la personne concernée par les renseignements;

- c) les chercheurs prendront des mesures appropriées pour protéger la vie privée des personnes ainsi que l'information identificatoire;
- d) les chercheurs respecteront les préférences connues et exprimées précédemment par les personnes à propos de l'utilisation de l'information les concernant;
- e) il est impossible ou pratiquement impossible de solliciter le consentement de la personne concernée par les renseignements;
- f) les chercheurs ont obtenu toute autre permission nécessaire à l'utilisation secondaire de renseignements à des fins de recherche.

Si un chercheur satisfait à toutes les conditions énoncées aux alinéas 5.5 a) à f), le CÉR peut approuver le projet de recherche sans exiger le consentement des personnes concernées par les renseignements.

Application La Politique n'exige pas que les chercheurs obtiennent le consentement des personnes pour l'utilisation secondaire de renseignements non identificatoires. Dans le cas de l'utilisation secondaire de renseignements identificatoires, les chercheurs doivent obtenir le consentement conformément à la loi à moins de satisfaire à toutes les exigences énoncées à l'article 5.5.

L'exception à l'obligation de solliciter le consentement dans le présent article est applicable expressément aux situations de l'utilisation secondaire de renseignements identificatoires. Les conditions énoncées à l'article 3.7 visent la modification du consentement applicable à d'autres situations que la présente.

Les articles 9.20 à 9.22³ abordent la question de l'utilisation secondaire des renseignements identificatoires provenant d'une communauté autochtone particulière, ou d'une partie de l'ensemble de la communauté autochtone.

« L'impossibilité pratique » renvoie à une difficulté tellement grande ou excessive que la conduite des travaux de recherche est menacée. Cela ne renvoie pas à un simple inconvénient. Il est parfois impossible ou pratiquement impossible de solliciter le consentement si le groupe est important ou si ses membres sont probablement décédés, dispersés géographiquement ou difficiles à retrouver. Les efforts faits pour retrouver les membres d'un groupe et les contacter pourraient faire surgir d'autres préoccupations sur le plan de la vie privée. Les ressources financières, humaines et autres requises pour joindre ces personnes et solliciter leur consentement peuvent imposer au chercheur un fardeau indu qui met en péril le projet de recherche. Dans certaines provinces ou certains territoires, les lois sur la protection des renseignements personnels peuvent empêcher les chercheurs d'utiliser ces renseignements pour entrer en contact avec des personnes afin de solliciter leur consentement à l'utilisation secondaire d'information les concernant⁴.

Il est possible que les lois régissant la protection des renseignements personnels imposent des règles précises concernant la divulgation des renseignements en vue d'une utilisation secondaire à des fins de recherche. Ces lois peuvent obliger la personne ou l'organisme qui a la garde ou le contrôle des renseignements

personnels demandés à obtenir l’approbation du commissaire à la protection de la vie privée ou d’un autre organisme avant de divulguer l’information aux chercheurs. Elles peuvent aussi imposer des exigences supplémentaires telles que des ententes sur la communication de renseignements décrivant les conditions de divulgation. Ces exigences peuvent inclure des dispositions empêchant expressément le chercheur de publier une information identificatoire ou de contacter des individus reliés à cette information.

Au moment de la collecte initiale des renseignements les concernant, il se peut que les personnes visées aient eu l’occasion d’exprimer leurs préférences quant aux utilisations futures de ces renseignements, y compris à des fins de recherche (voir le paragraphe d) de l’application de l’article 3.2). Les détenteurs des données ont l’obligation de respecter les préférences exprimées par la personne. Par exemple, si une personne ne souhaite pas que les renseignements la concernant soient utilisés pour d’autres projets de recherche à venir, les détenteurs des données doivent supprimer ces renseignements de tous les ensembles de données utilisés ou rendus accessibles à des fins de recherche.

Si les travaux envisagés s’appuient sur des renseignements de nature plus délicate (des renseignements génétiques, des renseignements sur les personnes qui cherchent de l’aide dans des foyers contre la violence familiale ou encore des renseignements concernant des pratiques sexuelles, par exemple), il se peut que le CÉR demande aux chercheurs d’engager un dialogue avec les personnes dont les points de vue peuvent contribuer à dégager les implications éthiques du projet de recherche, et de proposer des moyens de réduire les risques qui y sont associés. La discussion ne doit pas être considérée comme un consentement par procuration. Son but est plutôt de recueillir des suggestions sur le projet de recherche proposé, par exemple, en ce qui a trait à l’élaboration du projet, aux mesures de protection de la vie privée ou à l’utilisation potentielle des résultats. Ce dialogue peut aussi servir à déterminer si le projet de recherche aura ou non des incidences négatives sur le bien-être des personnes concernées par les renseignements. Les chercheurs doivent informer le CÉR des résultats de ces échanges. Le CÉR pourrait demander aux chercheurs d’apporter des modifications au projet de recherche proposé à la suite de ce dialogue.

Article 5.6 Si l’utilisation secondaire de données identificatoires a été approuvée sans qu’il y ait eu obligation de solliciter le consentement en vertu de l’article 5.5, les chercheurs qui souhaitent prendre contact avec les personnes en cause pour recueillir des renseignements supplémentaires doivent faire approuver la procédure envisagée, par le CÉR avant toute tentative de prise de contact.

Application Dans certains cas, l’un des buts de la recherche n’est atteint que par un contact de suivi avec les personnes concernées pour obtenir des renseignements supplémentaires. Aux termes de l’article 5.5, le CÉR peut avoir approuvé l’utilisation secondaire sans avoir exigé l’obtention du consentement, après en avoir conclu, entre autres, qu’il était impossible ou pratiquement impossible de solliciter le consentement de toutes les personnes dont on entendait utiliser les

renseignements dans le contexte du projet de recherche. Dans les situations où la communication avec un sous-groupe est réalisable, les chercheurs pourraient vouloir par la suite prendre contact avec certaines personnes pour collecter des renseignements supplémentaires. Cependant, le fait d'entrer en contact avec des personnes dont les renseignements personnels préalablement collectés sont utilisés à des fins secondaires dans la recherche soulève en soi des préoccupations sur le plan de la vie privée. Il se peut que certaines personnes ne veuillent pas être contactées par des chercheurs ou n'apprécient pas que des renseignements identificatoires aient été divulgués à des chercheurs sans leur consentement. Les avantages possibles d'un contact ultérieur avec les personnes visées, doivent être manifestement supérieurs aux risques pour les personnes concernées. De plus, le CÉR doit être convaincu que le mode de suivi envisagé auprès de ces personnes réduit au minimum les risques qu'elles pourraient subir. Le plan proposé doit indiquer qui communiquera avec les personnes pour les inviter à participer à la recherche (par exemple, un représentant de l'organisme qui détient les renseignements à leur sujet) et la nature de sa relation avec ces personnes. Les chercheurs doivent également faire en sorte que le plan de contact de suivi soit conforme aux lois applicables en matière de protection de la vie privée. Par exemple, certaines lois de protection de la vie privée interdisent aux chercheurs d'avoir des contacts avec les personnes, sauf si le détenteur de l'information a d'abord sollicité et obtenu le consentement de ces personnes à cet égard. Lorsque cela est possible, il est préférable que ce soit le détenteur de l'information qui reprenne contact avec les participants. Les chercheurs devront obtenir le consentement de chaque participant pour toute nouvelle collecte de données. L'article 3.1 donne des indications supplémentaires sur le consentement et les modalités du recrutement.

E. Couplage de données

Article 5.7 Les chercheurs qui se proposent de procéder à un couplage de données doivent obtenir l'autorisation préalable du CÉR, à moins que les travaux de recherche s'appuient exclusivement sur des renseignements accessibles au public tels qu'ils sont définis à l'article 2.2. Dans la demande d'approbation, ils doivent décrire les données qui seront couplées et évaluer la probabilité que des renseignements identificatoires ne soient créés à la suite du couplage de données.

Si le couplage de données vise des renseignements identificatoires ou a de bonnes chances de produire des renseignements de ce genre, les chercheurs doivent démontrer à la satisfaction du CÉR que :

- a) le couplage de données est essentiel à l'objet de la recherche;
- b) des mesures de sécurité adéquates seront mises en œuvre pour protéger l'information.

Application Le nombre croissant de bases de données et les progrès de la technologie permettant de coupler des bases de données créent de nouvelles possibilités pour la recherche, mais aussi de nouveaux risques d'atteinte à la vie privée. Il se peut, en particulier,

que le couplage de bases de données dépersonnalisées ou rendus anonymes permette de réidentifier des personnes. Dans cette perspective, le présent article donne des indications aux chercheurs qui se proposent d'effectuer des couplages de données; il exige de plus qu'ils évaluent et réduisent au minimum les risques de réidentification. Seul un nombre restreint de personnes effectueront la fusion de bases de données. Les chercheurs renforceront les mesures de sécurité s'ils veulent conserver les dossiers fusionnés.

Si les chercheurs entendent accéder à des ensembles de données détenus par un autre organisme, il est préférable que le détenteur effectue lui-même le couplage de données et supprime les identificateurs avant de transmettre l'ensemble de données fusionnées.

Les lois et les politiques des organismes réglementent parfois le couplage de données dans ces circonstances précises. Par exemple, certaines lois sur la protection des renseignements personnels exigent que soient conclus des accords sur la communication de données fixant les conditions auxquelles il est permis de procéder au couplage de données. Il se peut aussi que les détenteurs de données, comme les organismes de statistique, se soient dotés de politiques sur le couplage de données⁵.

Les exigences énoncées à la section D s'appliquent dans les cas où des chercheurs entendent accéder à des ensembles de données comprenant des renseignements identificatoires, et effectuer un couplage entre ces ensembles en vue d'une utilisation secondaire à des fins de recherche.

Notes

¹ Voir, par exemple, Association canadienne de normalisation, *Code type sur la protection des renseignements* (1996).

² Voir la *Politique du Conseil de recherches en sciences humaines sur l'archivage des données de recherche* : www.sshrc-crsh.gc.ca/site/apply-demande/policies-politiques/edata-donnees_electroniques_fra.aspx, et la *Politique sur l'accès aux résultats de la recherche* des Instituts de recherche en santé du Canada (septembre 2007) : www.cihr-irsc.gc.ca/f/34846.html, voir aussi, *Accès aux résultats de la recherche : principes directeurs*, du Conseil de recherches en sciences humaines du Canada, du Conseil de recherches en sciences naturelles et en génie du Canada, des Instituts de recherche en santé du Canada : www.science.gc.ca/default.asp?Lang=Fr&n=9990CB6B-1.

³ Voir aussi les Instituts de recherche en santé du Canada, les *Lignes directrices des IRSC pour la recherche en santé chez les peuples autochtones* (mai 2007) : www.cihr-irsc.gc.ca/f/29134.html.

⁴ Au sujet des facteurs à considérer pour évaluer le besoin de lever l'obligation de consentement, voir les Instituts de recherche en santé du Canada, les *Pratiques exemplaires des IRSC en matière de protection de la vie privée dans la recherche en santé*, Section 3.3, Utilisation secondaire (septembre 2005) : www.cihr.ca/f/29072.html#Element3.

⁵ Voir, par exemple, Statistique Canada, *Politique relative au couplage d'enregistrements* : www.statcan.gc.ca/record-enregistrement/policy4-1-politique4-1-fra.htm.