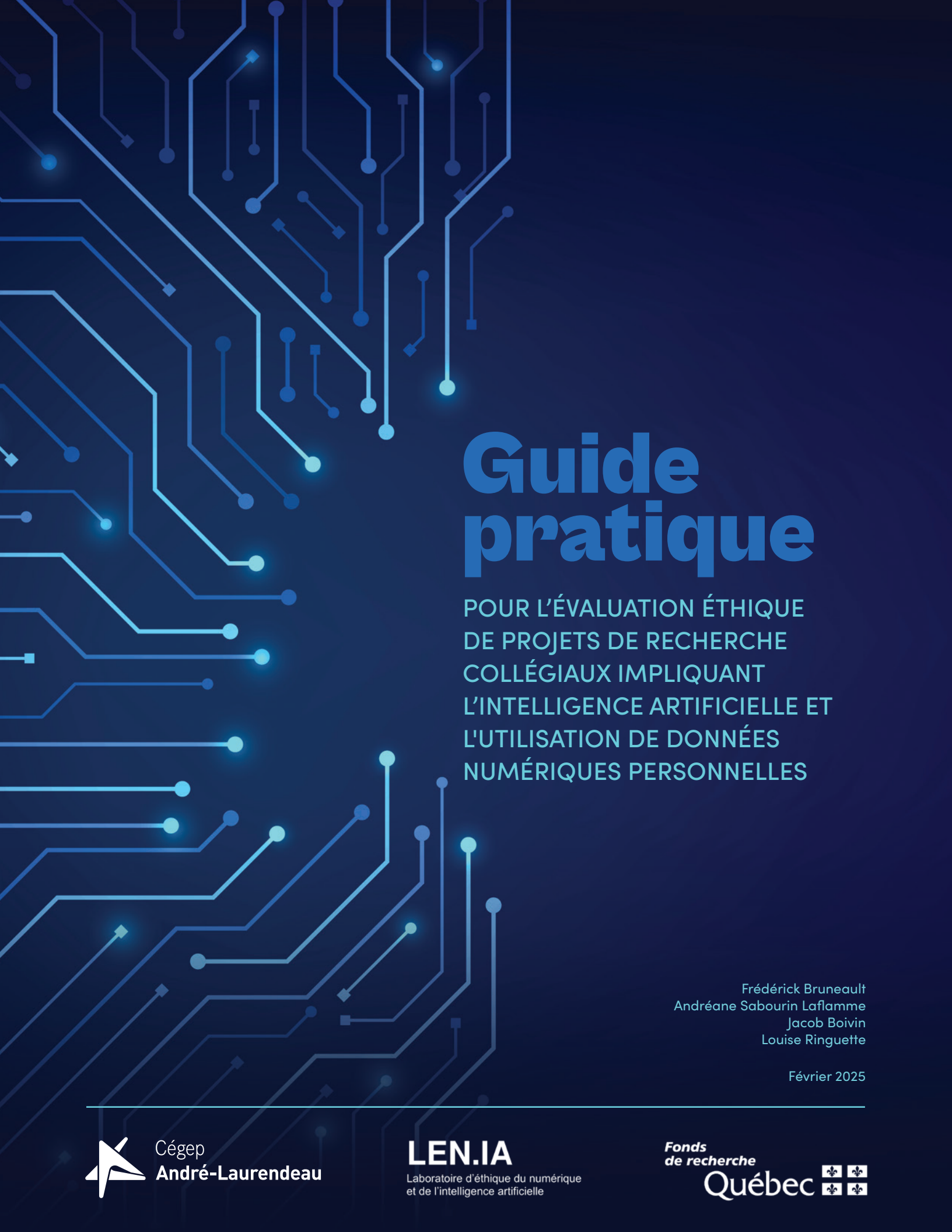




Guide pratique

POUR L'ÉVALUATION ÉTHIQUE
DE PROJETS DE RECHERCHE
COLLÉGIAUX IMPLIQUANT
L'INTELLIGENCE ARTIFICIELLE ET
L'UTILISATION DE DONNÉES
NUMÉRIQUES PERSONNELLES

Frédéric Bruneault
Andréane Sabourin Laflamme
Jacob Boivin
Louise Ringuette

Février 2025



Cégep
André-Laurendeau

LEN.IA

Laboratoire d'éthique du numérique
et de l'intelligence artificielle

Fonds
de recherche

Québec





Table des matières

MEMBRES DU COMITÉ D'EXPERTS.....	4
INTRODUCTION	5
MÉTHODOLOGIE	6
MODE D'EMPLOI	7
REPRÉSENTATION GRAPHIQUE DU GUIDE PRATIQUE	8
SECTION 1 : DONNÉES NUMÉRIQUES PERSONNELLES.....	9
THÉMATIQUE A : PROCESSUS DE CONSENTEMENT	10
THÉMATIQUE B : VIE PRIVÉE ET CONFIDENTIALITÉ	14
THÉMATIQUE C : JUSTICE ET ÉQUITÉ	16
THÉMATIQUE D : CONFLITS D'INTÉRÊTS	18
THÉMATIQUE E : NÉCESSITÉ	20
SECTION 2 : SYSTÈMES D'INTELLIGENCE ARTIFICIELLE.....	21
THÉMATIQUE A : PROCESSUS DE CONSENTEMENT	22
THÉMATIQUE B : VIE PRIVÉE ET CONFIDENTIALITÉ	24
THÉMATIQUE C : JUSTICE ET ÉQUITÉ	26
THÉMATIQUE D : CONFLITS D'INTÉRÊTS	28
THÉMATIQUE E : NÉCESSITÉ	30
BANQUE D'OUTILS	31
CADRES JURIDIQUES.....	33
GLOSSAIRE	34
BIBLIOGRAPHIE	36

Membres du comité d'experts

Nous remercions les membres du comité d'experts en éthique de la recherche qui ont collaboré à la co-construction de ce guide pratique.

Mathieu Andrieux

INEDI, Centre collégial de transfert de technologie
Cégep de Lanaudière à Terrebonne

Sylvain Auclair

Cégep de Sainte-Foy

Michel Bergeron

École nationale de cirque
École de santé publique – Département de
médecine sociale et préventive

Blandine Courcot

École nationale de cirque

Mélissa Gourdeau St-Denis

Cégep de Drummondville

Marc Lamontagne

Cégep Édouard-Montpetit

Emmanuelle Marceau

Cégep du Vieux-Montréal

Anne-Laure Ménard

INEDI, Centre collégial de transfert de technologie
Cégep de Lanaudière à Terrebonne

Danic Ostiguy

Collège de Maisonneuve

Produit avec le soutien financier du Fonds de recherche du Québec



Introduction

Les techniques de collecte et d'analyse de données numériques et les systèmes d'intelligence artificielle (SIA) sont de plus en plus mobilisés en recherche. Si ces avancées sont porteuses de bénéfices notables (analyse et interprétation de données, modélisation complexe, recension des écrits, rédaction, édition, etc.), elles soulèvent également de nouveaux enjeux éthiques (Tiidenberg, 2017; Simonnot, 2019; Mollina et al., 2023; Resnik & Hosseini, 2024). En effet, l'intégration croissante du traitement des données numériques et de l'IA en recherche est susceptible de présenter des risques spécifiques pour les recherches qui comportent la participation d'êtres humains, tout en amplifiant certaines problématiques classiques.

Par exemple, la question de l'obtention d'un consentement libre et éclairé, pierre angulaire de l'éthique de la recherche, doit être interrogée à nouveaux frais lorsqu'on utilise l'IA en recherche. L'imputabilité et la responsabilité de l'équipe de recherche doivent également être redéfinies dans ce nouveau contexte technologique. De plus, l'opacité des algorithmes présente un défi particulier en matière d'explicabilité, alors que la transparence est essentielle pour permettre aux personnes participantes de prendre des décisions éclairées.

Les bases de données numériques sont devenues des ressources clés en recherche, mais leur utilisation doit être faite dans le respect de la confidentialité et de la protection de la vie privée, notamment afin de s'assurer que des informations personnelles ou sensibles ne soient pas divulguées ou utilisées de façon à porter préjudice aux personnes participantes. Un autre enjeu important concerne la présence de biais algorithmiques qui peuvent se trouver dans les jeux de données, et qui peuvent être automatisés et même amplifiés dans l'opérationnalisation des SIA. La qualité et la représentativité des données sont donc des enjeux éthiques qui redoublent d'importance en IA.

Afin d'assurer la protection du bien-être des personnes participantes et assurer que leur implication en recherche soit faite de manière libre, éclairée, juste et équitable, il importe de prendre en compte ces nouvelles dynamiques propres aux outils numériques et à l'IA. En effet, pour assurer la conduite éthique de la recherche au 21^e siècle, il convient donc d'intégrer l'évaluation de ces nouveaux enjeux technologiques en éthique de la recherche. Les comités d'éthique de la recherche, tout en poursuivant leur rôle d'évaluation des protocoles au regard des principes éthiques fondamentaux – tels que le respect de la dignité humaine, le consentement libre et éclairé, ainsi que la justice et l'équité – se trouvent aujourd'hui face à de nouveaux défis liés à l'utilisation des données numériques personnelles et de l'IA en recherche. En effet, les principes énoncés dans l'Énoncé de politique des trois conseils – Éthique de la recherche avec des êtres humains (EPTC-2) prennent une nouvelle dimension et doivent être réinterprétés dans ce nouveau contexte.

Or, la rapidité de ces changements entre parfois en conflit avec le temps nécessaire à la réflexion et à la formation. Des études soulignent le manque de ressources auquel font face les comités d'éthique de la recherche (CER) pour appréhender ces nouveaux enjeux (Ferrete et al., 2022; Bouhouita-Guermech et al., 2023).

Le guide pratique proposé ici vise à appuyer les CER collégiaux dans l'évaluation de projets de recherche impliquant la collecte de données numériques personnelles et/ou l'utilisation de SIA. Il s'agit d'un outil qui vise à permettre aux CER collégiaux de cibler plus spécifiquement certains enjeux clés liés à ces développements technologiques et les soutenir dans la réalisation de leur mission.

Les questions soulevées dans ce guide pratique concernent spécifiquement et uniquement les risques associés au traitement des données numériques personnelles et au recours aux SIA en recherche. Celles-ci s'ajoutent aux autres éléments à évaluer par les CER.

Méthodologie

Revue de la littérature

L'élaboration de ce guide pratique repose sur une méthodologie en deux volets. D'abord, une revue de la littérature a permis d'identifier les enjeux éthiques associés à l'utilisation de l'IA et du traitement des données numériques personnelles en recherche. Ces enjeux ont ensuite été croisés avec les principes fondateurs de l'EPTC-2, qui encadre l'éthique de la recherche avec les êtres humains. Les principes de l'EPTC-2 ont ainsi été interprétés à la lumière des enjeux identifiés dans la littérature en éthique de l'IA et du numérique en recherche. Ainsi, les cinq thématiques identifiées dans le guide pratique sont calquées sur les thématiques qui sont au cœur de l'EPTC-2.

Processus de co-construction avec un comité d'experts

Le guide pratique a été élaboré dans le cadre d'un processus de co-construction mobilisant un comité multidisciplinaire d'experts issus du réseau des CER collégiaux. Ce processus d'élaboration collective s'est échelonné sur deux cycles itératifs d'entretiens: un cycle de conception et un cycle de validation. Le cycle de conception avait pour objectif de définir les principaux enjeux et de structurer les premières versions du guide, tandis que le cycle de validation visait à affiner et ajuster le guide en fonction des retours et recommandations du comité d'experts.

Approche

L'approche mobilisée dans le guide vise à engager une démarche réflexive chez les membres des CER. Le guide pratique est construit sous la forme d'une série de questions ouvertes, qui peuvent être adaptées et bonifiées au besoin, et ce, en fonction du projet de recherche évalué. En effet, les interrogations proposées ne constituent pas une liste exhaustive. L'objectif est plutôt d'attirer l'attention des membres des CER et l'équipe de recherche sur un ensemble de problématiques clés associées aux enjeux émergents liés au numérique et à l'IA en éthique de la recherche. Les CER sont ainsi encouragés à s'approprier l'outil et à le bonifier, d'autant plus qu'il s'agit d'un domaine qui évolue rapidement.

Structure du guide pratique

Le guide se divise en deux sections.

La première section du guide permet d'évaluer les projets de recherche quant à la collecte ou le traitement de données numériques personnelles des personnes participantes. La seconde section du guide permet d'évaluer les projets au regard de l'utilisation d'un ou de plusieurs SIA.

Si le projet évalué n'implique pas de SIA, il y a lieu de se référer uniquement à la section 1. Dans le cas où le projet évalué implique au moins un SIA, il y a lieu de se référer d'abord à la section 1 et ensuite à la section 2 du guide.

Selon les caractéristiques du projet évalué, les CER pourraient juger pertinent de se référer à une seule de ces sections ou aux deux, celles-ci pouvant être utilisées de manière complémentaire.

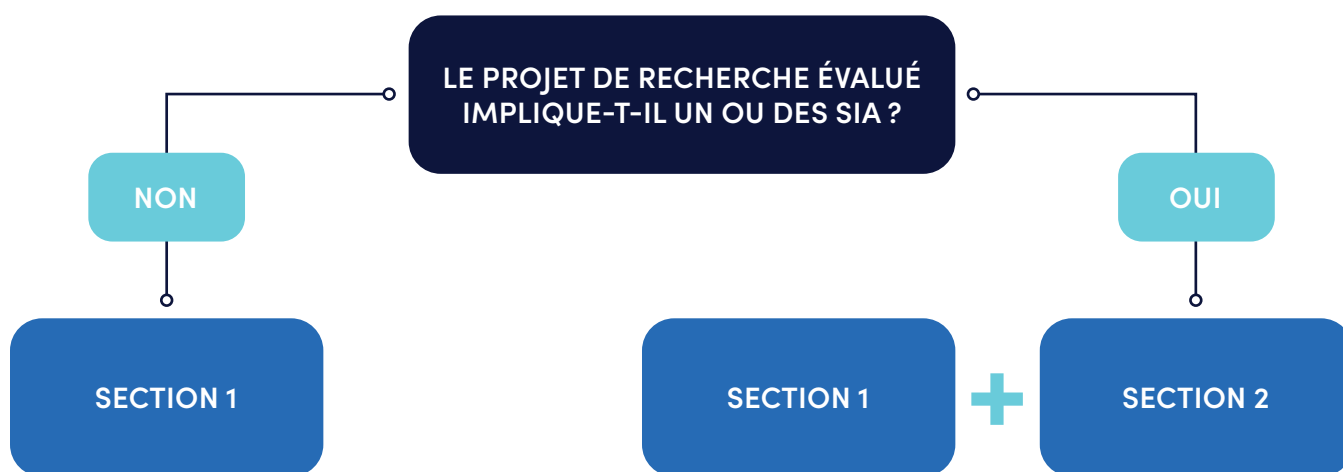
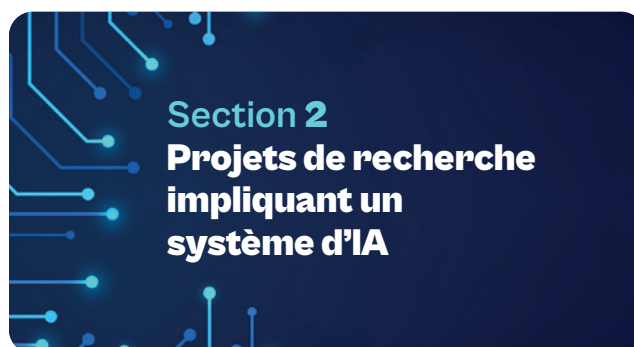
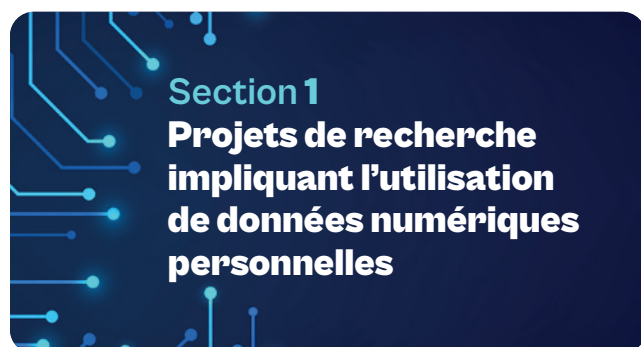
On retrouve dans chacune de ces sections, et pour chacune des cinq thématiques identifiées, une série de questions de réflexion établies à partir des enjeux relevés dans l'EPTC-2 et dans la revue de la littérature.

Les thématiques ne suivent pas un ordre de progression linéaire. Il est donc possible de naviguer de thématique en thématique selon la nature spécifique du projet de recherche à évaluer. Il est également possible que certaines questions se révèlent moins pertinentes en fonction des particularités de chaque projet.

Le guide pratique contient également une banque d'outils accessibles en ligne qui peuvent être mobilisés par les CER ou par les équipes de recherche. Il inclut aussi des références liées aux enjeux juridiques de l'utilisation des données numériques en recherche.

Enfin, l'outil comprend un glossaire afin de faciliter la compréhension de certains termes plus techniques dans le domaine des technologies numériques et de l'IA.

Mode d'emploi



Usage non déclaré ou informel de l'IA générative en recherche (*Shadow AI*)

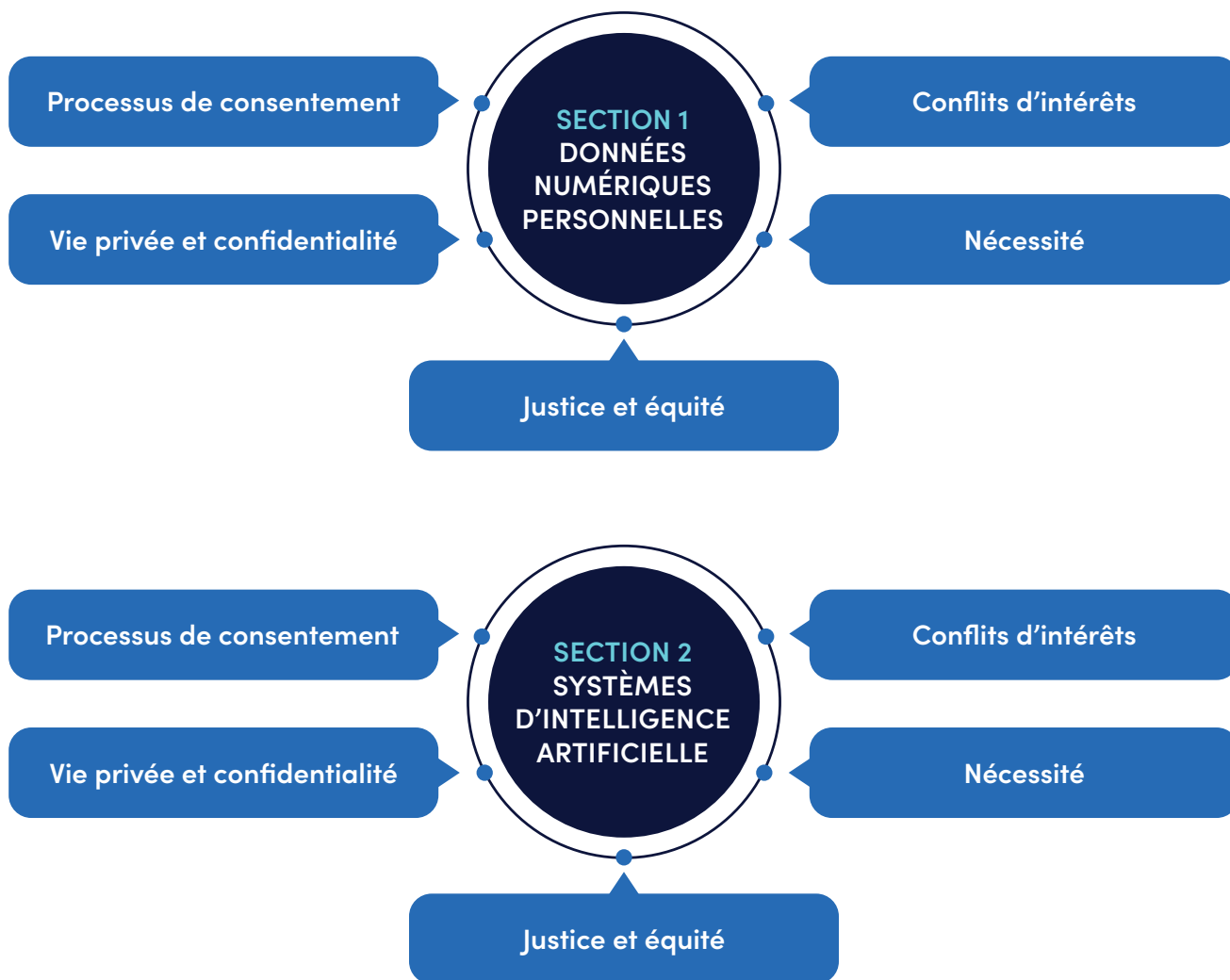
Même si un projet de recherche ne prévoit pas explicitement l'utilisation d'un SIA spécifique, des outils d'IA générative peuvent néanmoins être employés pour la réalisation de certaines tâches liées au projet (ex : transcription, résumé, synthèse, traduction, rédaction, etc.).

L'utilisation non déclarée ou informelle de l'IA générative en recherche (*Shadow AI in Research*) soulève plusieurs enjeux liés à la protection des personnes participantes. Lorsque des outils d'IA sont utilisés sans être explicitement intégrés au protocole de recherche, cela peut notamment compromettre l'obtention du consentement éclairé et la protection des données de recherche.

Afin de protéger les personnes participant au projet de recherche, il faut indiquer explicitement toutes les utilisations prévues de l'IA générative, qu'elles soient formelles ou informelles, au protocole de recherche et se référer à la section 2 du guide pratique quant à ces utilisations, le cas échéant.



Représentation graphique du guide pratique



Données numériques personnelles

Une donnée numérique personnelle est une information portée par un support technologique numérique, qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier. Par exemple, des informations numériques telles que l'adresse IP, la date de naissance, le code postal ou la photo d'une personne sont des données numériques personnelles.

Systèmes d'intelligence artificielle (SIA)

Un système d'intelligence artificielle (SIA) désigne un système automatisé utilisant des algorithmes d'intelligence artificielle, c'est-à-dire l'ensemble des techniques permettant de simuler certains traits de l'intelligence humaine, tels que le raisonnement, l'apprentissage, la prédiction, la prise de décision, la perception du monde environnant et la génération de contenu. Par exemple, les systèmes à base de connaissances (systèmes experts) et ceux fondés sur l'apprentissage automatique qui permettent notamment la reconnaissance de la parole, le traitement du langage naturel, la vision artificielle et les agents conversationnels sont des systèmes d'IA.

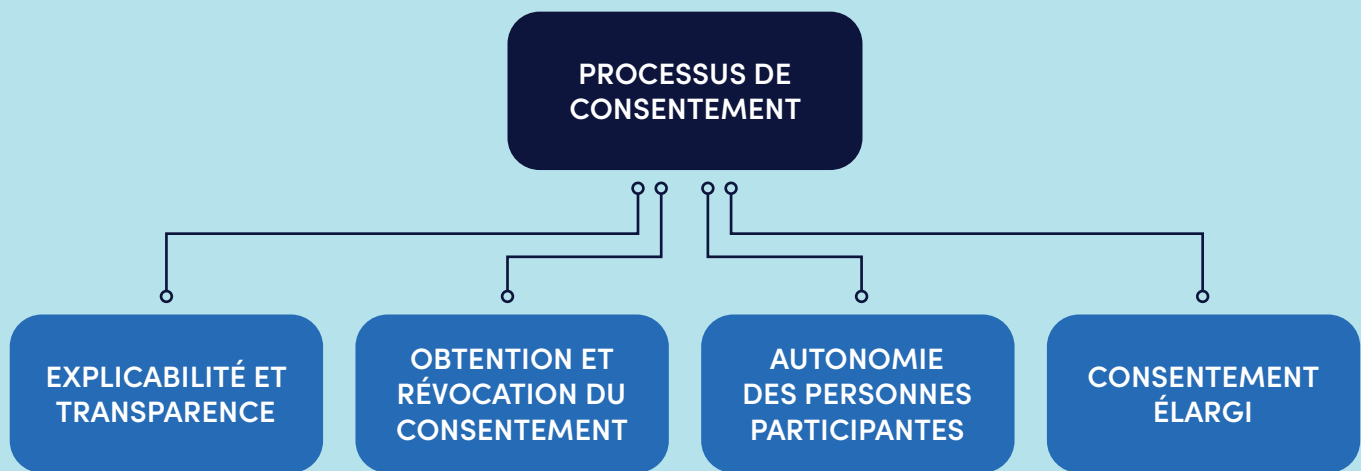
An abstract graphic of a circuit board pattern in light blue on a dark blue background. The pattern consists of numerous lines, dots, and small squares, some of which are glowing with a bright blue light. The lines are of varying thickness and form a complex, interconnected network. The dots and squares are scattered throughout the pattern, some appearing as nodes or components. The overall effect is a sense of digital connectivity and technology.

Section 1

Projets de recherche impliquant l'utilisation de données numériques personnelles

Données numériques personnelles

Thématique A : processus de consentement



L'utilisation de données numériques personnelles, notamment dans le cas de données massives (big data), complexifie la question du consentement en recherche. Les données numériques peuvent souvent être utilisées ultérieurement dans d'autres contextes (analyse secondaire, traitement ultérieur par un SIA) qui ne sont pas toujours clairement définis au moment de l'obtention du consentement. Cela présente un défi en matière d'**explicabilité et de transparence** puisqu'une description adéquate des finalités du projet doit être présentée aux personnes participantes pour obtenir un consentement éclairé. Ainsi, il faut notamment s'assurer que le **consentement** est **élargi** à l'ensemble du cycle de vie des données, que les personnes participantes reçoivent suffisamment d'information sur l'utilisation de leurs données numériques personnelles, y compris pour les usages ultérieurs, et que la **révocation du consentement** soit assurée le cas échéant. Un tel élargissement des préoccupations permet de s'assurer que l'**autonomie des personnes participantes** est respectée conformément aux exigences de l'EPTC-2.

Le consentement des participant(e)s est-il manifeste, libre, éclairé et donné à des fins spécifiques ?

- Quelle information est fournie aux personnes participantes concernant le traitement et l'usage qui est fait de leurs données numériques personnelles (type d'information, utilisation, type d'analyse réalisée, etc.) et les finalités recherchées ?
- Le consentement est-il demandé pour chacune des fins prévues, en termes simples et clairs, en précisant la durée de la validité de ce consentement ?
- De quelle manière les personnes participantes sont informées des utilisations possibles de leurs données numériques personnelles à long terme, et quelle forme de contrôle leur est offerte sur ces utilisations futures ?
- Lorsqu'une personne le requiert, une procédure est-elle prévue pour lui prêter assistance afin de l'aider à comprendre la portée du consentement demandé ?

Comment la possibilité de révocation du consentement des personnes participantes est assurée tout au long du projet ?

- Les limites de la révocation ont-elles été expliquées aux personnes participantes ?
- Quelles sont les mesures prises pour supprimer les données numériques personnelles ou cesser leur utilisation lorsque le consentement est révoqué ?

Quelle procédure permet d'assurer que toute utilisation ultérieure des données numériques personnelles reste conforme aux attentes des personnes participantes et aux buts de la recherche ?

En l'absence de consentement des personnes participant à la recherche, une demande d'autorisation à l'organisme public ou à l'entreprise privée qui détient les données numériques personnelles a-t-elle été déposée afin d'avoir accès à ces informations ?

- Une évaluation des facteurs relatifs à la vie privée (EFVP) a-t-elle été réalisée ?
- Une entente de communication avec l'organisme ou l'entreprise privée pour avoir accès aux données numériques personnelles a-t-elle été signée ?
- Le détenteur des données numériques personnelles (ex. organisme public ou entreprise privée) a-t-il été identifié, afin de déterminer la loi qui encadre ces données ?
- Le type de données numériques personnelles (ex. renseignements personnels ou renseignements de santé et de services sociaux) a-t-il été identifié, afin de déterminer la loi qui encadre ces données ?



Données numériques personnelles obtenues sans consentement

Dans certaines circonstances exceptionnelles, une équipe de recherche peut avoir besoin d'utiliser des données numériques personnelles à des fins d'étude, de recherche ou de production de statistiques, sans le consentement des personnes concernées par ces données. Dans ce contexte particulier, l'EPTC-2 identifie des règles à suivre lorsqu'une équipe de recherche souhaite collecter et utiliser des données numériques personnelles sans le consentement des personnes participantes (art. 5.5A). À ces règles s'ajoutent également des obligations légales, que les données proviennent d'un organisme public ou d'une entreprise privée. Ces obligations sont décrites aux articles 67.2.1 à 67.2.3 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Loi sur l'accès) et aux articles 21 à 21.0.2 de la *Loi sur la protection des renseignements personnels dans le secteur privé* (Loi secteur privé). Elles comprennent, notamment, l'exigence de démontrer qu'il est déraisonnable d'exiger le consentement des personnes, que les données numériques personnelles collectées sont nécessaires pour répondre aux objectifs de la recherche et que les critères prévus à la loi pour l'évaluation des facteurs relatifs à la vie privée sont respectés. De plus, l'organisme public ou l'entreprise qui donne accès à des données numériques personnelles et qui communiquent de telles données doit, avant de permettre une telle utilisation ou communication des données, conclure une entente de communication avec l'équipe de recherche.

Données de santé obtenues sans consentement

Depuis juillet 2024, les renseignements de santé et de services sociaux sont encadrés par un régime juridique particulier. Ainsi, les membres de l'équipe de recherche qui souhaitent collecter et utiliser des données numériques personnelles relatives à la santé des personnes, sans leur consentement, doivent respecter les obligations prévues à la *Loi sur les renseignements de santé et de services sociaux* (LRSSS). Ces obligations sont similaires à celles citées précédemment, mais avec l'ajout de règles particulières lorsque les membres de l'équipe de recherche ne sont pas liés à un établissement de santé ou à un organisme public visé par la LRSSS.

Consentement élargi

L'EPTC-2 définit le consentement élargi comme un consentement à des recherches futures non déterminées, mais sous réserve des lois applicables. Ce type de consentement inclut toujours des restrictions précises (par exemple limité à un domaine d'étude en particulier, à une maladie, etc.) et il s'applique au stockage, à la conservation et à l'utilisation secondaire des données numériques personnelles.

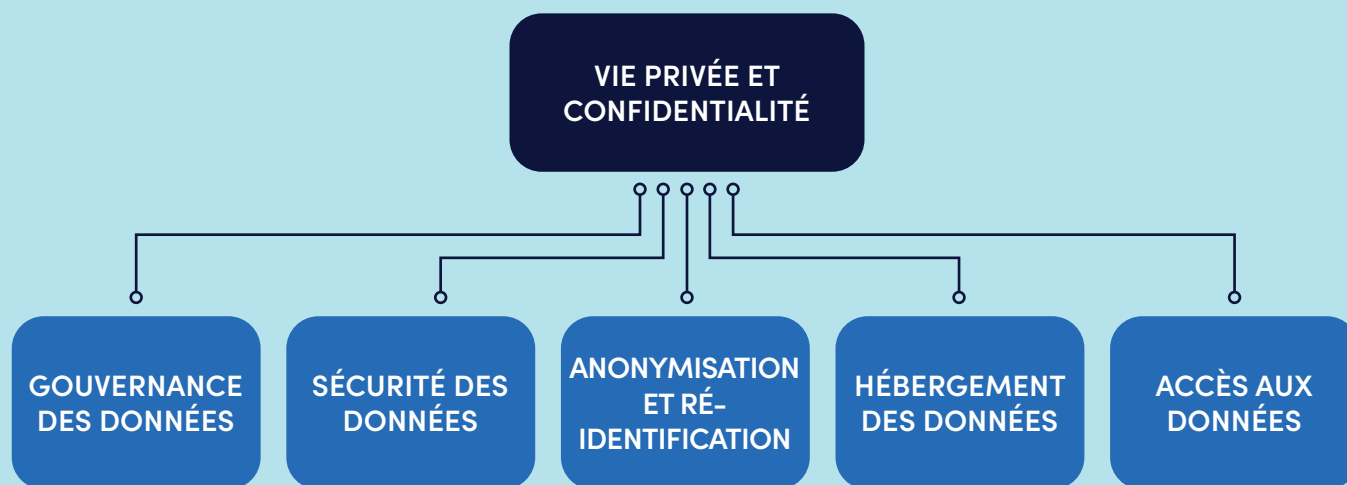
Au Québec, la notion de consentement élargi a aussi été introduite dans la *Loi sur les renseignements de santé et de services sociaux* (LRSSS, en vigueur depuis le 1^{er} juillet 2024). Dans cette loi, tout consentement à l'utilisation ou à la communication d'un renseignement de santé et de services sociaux détenu par un organisme visé par la LRSSS doit être manifeste, libre, éclairé et être donné à des fins spécifiques. “ *En matière de recherche, il peut viser des thématiques de recherche, des catégories d'activités de recherche ou des catégories de chercheurs* ” (art. 6, al.1 de la LRSSS)

Évaluation des facteurs relatifs à la vie privée

La Commission d'accès à l'information du Québec définit l'évaluation des facteurs relatifs à la vie privée (EFVP) comme une forme d'analyse d'impact qui vise à protéger les données numériques personnelles et à respecter la vie privée des personnes, et ce, avant même de débiter un projet et pendant celui-ci. L'EFVP est donc évolutif et elle doit être revue tout au long d'une recherche. Elle comprend, notamment, cinq critères essentiels énumérés dans la Loi sur l'accès (art. 67.2.1) et dans la Loi du secteur privé (art. 21). La réalisation d'une EFVP doit être proportionnée à la sensibilité des données numériques personnelles concernées, à la finalité de leur utilisation, à leur quantité, à leur répartition et à leur support.



Thématique B : vie privée et confidentialité



L'usage de données numériques personnelles en recherche soulève différentes problématiques spécifiques en ce qui a trait à la vie privée et à la confidentialité. D'abord, il est essentiel que le projet de recherche prévoie une bonne **gouvernance des données numériques**. Il est en effet important de pouvoir assurer une bonne gestion des données numériques personnelles au moyen d'un protocole clair et explicite quant à l'**accès aux données**, le lieu d'hébergement des données, le degré de sensibilité de l'information recueillie, les méthodes et/ou infrastructures utilisées en matière de **sécurité** ainsi que les techniques de dépersonnalisation ou d'**anonymisation** utilisées pour assurer que les personnes participantes ne sont pas facilement réidentifiables. Ces enjeux doivent être discutés de façon claire et explicite. Il est à cet effet particulièrement important d'intégrer la perspective des personnes participantes dans l'anticipation de ces problématiques dans le but de maintenir un lien de confiance avec l'équipe de recherche. À cet effet, il faut s'assurer qu'une utilisation secondaire ou commerciale des données numériques personnelles soit, le cas échéant, explicitement indiquée dans le formulaire de consentement et dans le protocole de recherche puisque cela peut nuire à la protection de la vie privée. Il faut en dernière instance s'assurer que le protocole de recherche soit conforme aux cadres législatifs en vigueur en matière de protection de la vie privée (voir la section à la fin du document concernant les cadres législatifs en contexte canadien et québécois). Cela s'applique également aux infrastructures mobilisées.

Quel est le protocole établi en matière de gestion des données numériques personnelles recueillies, et ce, tout au long de leur cycle vie ?

- Comment ces données sont collectées, utilisées, communiquées, conservées et éventuellement détruites ?
- Qui dans l'équipe de recherche a accès à ces données ?
- Comment le partage de ces données est encadré ?
- Quelles mesures sont mises en place pour assurer la sécurité de ces données ?

Les données numériques personnelles des personnes participantes sont-elles dépersonnalisées ou anonymisées et, le cas échéant, à partir de quelles techniques ?

- Ces techniques sont-elles éprouvées et robustes ?
- Les risques de réidentification ont-ils été évalués et mitigés ?

Quel est le protocole prévu en cas d'incident affectant la sécurité des données numériques personnelles ?

- Advenant un incident lié à la confidentialité, qui dans l'équipe de recherche sera responsable de déclarer cet incident auprès du CER ?
- Comment le CER et l'équipe de recherche ont-ils prévu d'inscrire l'incident de confidentialité au registre des incidents de l'organisation ?
- Comment ces protocoles de sécurité sont communiqués auprès des personnes participantes ? Est-ce que cela est fait dans un langage simple et clair ?

À quelles réglementations sont soumises les infrastructures mobilisées (notamment pour l'hébergement des données numériques personnelles) si elles ne sont pas situées à l'endroit où se déroule la recherche ? Est-ce que ces réglementations assurent une protection adéquate des personnes participantes ?

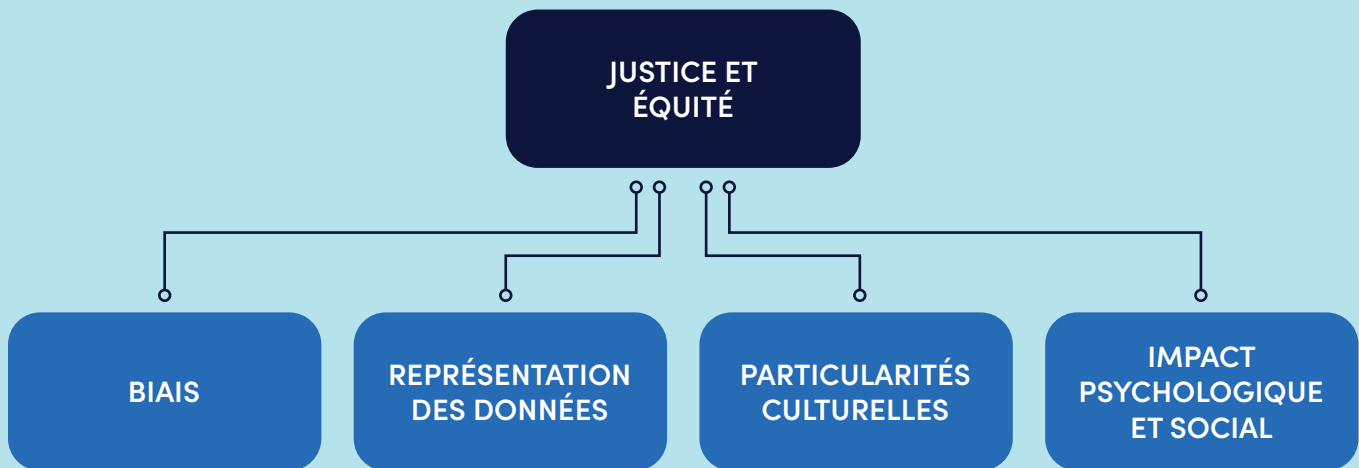
- Avant de communiquer des données numériques personnelles à l'extérieur du Québec, la personne responsable du projet de recherche a-t-elle réalisé une évaluation des facteurs relatifs à la vie privée ?
- Cette évaluation tient-elle compte de la sensibilité des données, la finalité de leur utilisation, les mesures de protection prévues et le régime juridique applicable dans l'État où les données seront communiquées ?



Plan de gestion des données

Depuis 2021, les organismes subventionnaires à l'origine de l'EPTC-2 ont lancé la *Politique des trois organismes sur la gestion des données de recherche*. Cette politique encourage les membres de l'équipe de recherche à mettre en place un plan de gestion pour leurs données de recherche. Ce plan de gestion des données est un document évolutif permettant de décrire comment seront gérées les données recueillies pour la recherche, et ce, tout au long de leur cycle de vie (de leur collecte jusqu'à leur destruction). Le contenu, la forme et l'ampleur de ce plan varient en fonction de la nature du projet de recherche.

Thématique C : justice et équité



L'utilisation de données personnelles numériques massives demande l'évaluation de certains risques spécifiques en ce qui a trait à la justice et l'équité. Un des principaux enjeux est la question des **biais** que peuvent présenter les données massives. Bien que les CER n'aient pas la charge d'évaluer la qualité des données, ces derniers peuvent demander que l'équipe ait évalué le risque que des jeux de données biaisés ou non représentatifs puissent mener à une répartition inéquitable des avantages et des inconvénients liés à la participation à la recherche. L'équipe de recherche pourrait être appelée à démontrer qu'elle a pris en compte le risque de biais dans les données numériques personnelles pour minimiser les risques d'interprétations ou de décisions erronées. On pourrait, par exemple, demander de justifier l'adéquation des bases de données avec leurs objectifs et de s'assurer que les biais potentiels ont été identifiés, atténués, ou, si ce n'est pas possible, documentés. La collecte et le traitement de données numériques personnelles peuvent également avoir un impact **psychologique et social** important. La collecte, lorsqu'elle s'étend dans le temps, peut entraîner un sentiment de surveillance susceptible d'affecter le bien-être des personnes participantes. L'utilisation et la divulgation de **données numériques sensibles** (par exemple liées à la santé mentale, l'orientation sexuelle ou la situation socio-économique) peuvent également mener à de la stigmatisation et même à de la discrimination. À cet effet, il est nécessaire de considérer les **particularités culturelles** des personnes participantes dans la collecte, le traitement et l'analyse des données numériques personnelles. Un intérêt tout particulier doit également être porté à la juste répartition des retombées de la recherche pour ne pas reproduire une forme d'exploitation des données numériques personnelles des populations vulnérables au sein de la recherche.

Comment les membres du groupe de recherche démontrent avoir pris en compte le risque des biais dans les données numériques personnelles qui seront récoltées et/ou analysées ?

- Les risques de stigmatisation ou de discrimination envers des individus, communautés ou groupes susceptible d'être en situation de vulnérabilité sont-ils anticipés et mitigés ?
- Les particularités locales, culturelles et linguistiques des personnes participantes sont-elles prises en compte dans la collecte, le traitement et l'analyse des données numériques personnelles ?

Des mesures ont-elles été prises pour prévenir d'éventuels impacts psychologiques ou sociaux préjudiciables résultant de la divulgation de l'utilisation des données numériques personnelles ou sensibles des personnes participantes ?

- Le cas échéant, quel est le protocole pour accompagner les personnes participantes dans ce processus ?

Les données numériques personnelles utilisées vont-elles permettre une répartition juste des avantages et des inconvénients associés à la recherche ?

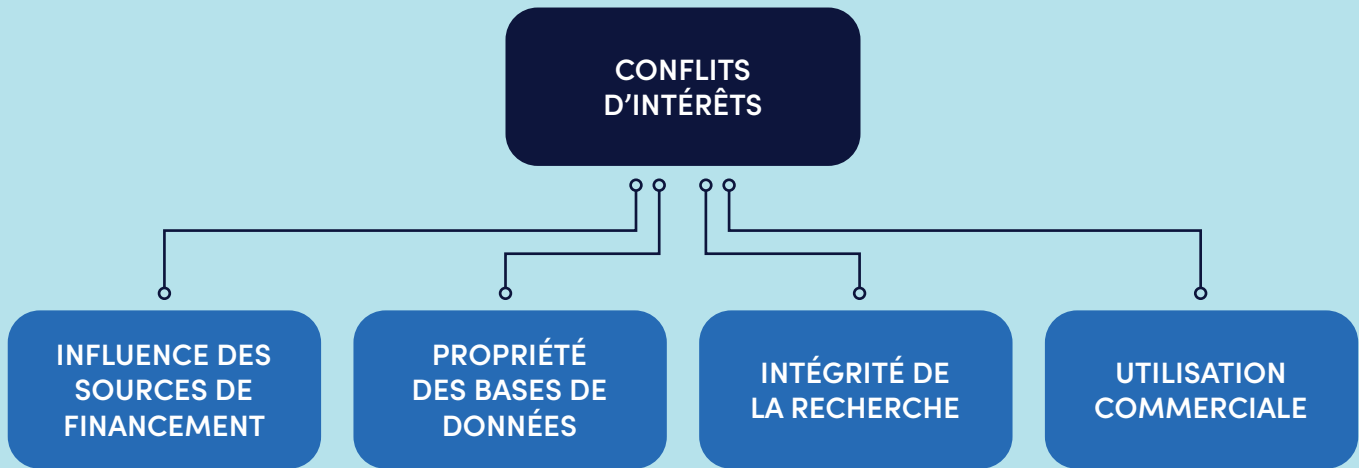
- Comment est-il prévu que les personnes participantes puissent bénéficier des résultats du projet de recherche ?
- Des mesures particulières seront-elles prises à cet effet lors de la publication et de la diffusion des résultats de la recherche ?



Données numériques sensibles

Une donnée numérique personnelle est dite sensible lorsque, de par sa nature (notamment médicale, biométrique, intime, politique, culturelle, religieuse, etc.) ou en raison du contexte de son utilisation ou de sa communication, elle suscite un haut degré d'attente raisonnable en matière de vie privée.

Thématique D : conflits d'intérêts



Puisque les bases de données numériques mobilisées en recherche peuvent être issues d'entreprises du secteur privé, il est possible que la recherche bénéficie de leurs services, de leurs infrastructures et même de leur financement. Ainsi, la recherche peut être soumise à une **influence issue des sources de financement**, ce qui pourrait en orienter la réalisation et les finalités. Dans cette perspective, il faut notamment s'assurer que **la propriété des bases de données** et leur accès n'impliquent pas de conflits d'intérêts et qu'une éventuelle **utilisation commerciale** de ces dernières est explicitement divulguée aux personnes participantes. Il faut donc s'assurer que les données numériques personnelles des personnes participantes ne seront utilisées que dans le cadre de ce qui a été explicitement établi par l'équipe de recherche. De façon générale, l'**intégrité de la recherche** doit être assurée en faisant preuve de **transparence** sur le plan des **objectifs de la recherche** et des liens d'intérêts qu'on y retrouve, notamment entre les membres de l'équipe de recherche et les sources de financement. Les différents niveaux de conflits d'intérêts (au niveau des institutions de recherche, de l'équipe de recherche ou des entreprises) doivent donc être anticipés, d'autant plus que le domaine du numérique mobilise souvent ces différents milieux.

Quels types de lien existent entre les membres de l'équipe de recherche, les institutions de recherches et les entreprises impliquées dans le projet de recherche, notamment en ce qui concerne l'infrastructure numérique du projet ?

- Les récompenses ou les incitatifs pour encourager la participation à la recherche à la source des bases de données numériques sont-ils modestes ou de nature non contraignante ?

Si les données numériques collectées et traitées ont un potentiel d'utilisation commerciale, comment évite-t-on les conflits d'intérêts dans l'atteinte des objectifs du projet de recherche ?

- La propriété des bases de données numériques peut-elle avoir un impact sur la neutralité et l'accessibilité des recherches réalisées ? Comment s'assure-t-on que les intérêts des bailleurs de fonds ou les fournisseurs de bases de données numériques n'influencent pas indûment la conception, la méthodologie, l'analyse et la publication des résultats de la recherche ?
- De quelle manière assure-t-on une communication transparente de l'utilisation des données numériques personnelles et de leur objectif dans de la recherche, tant auprès des personnes participantes que de la communauté scientifique ?

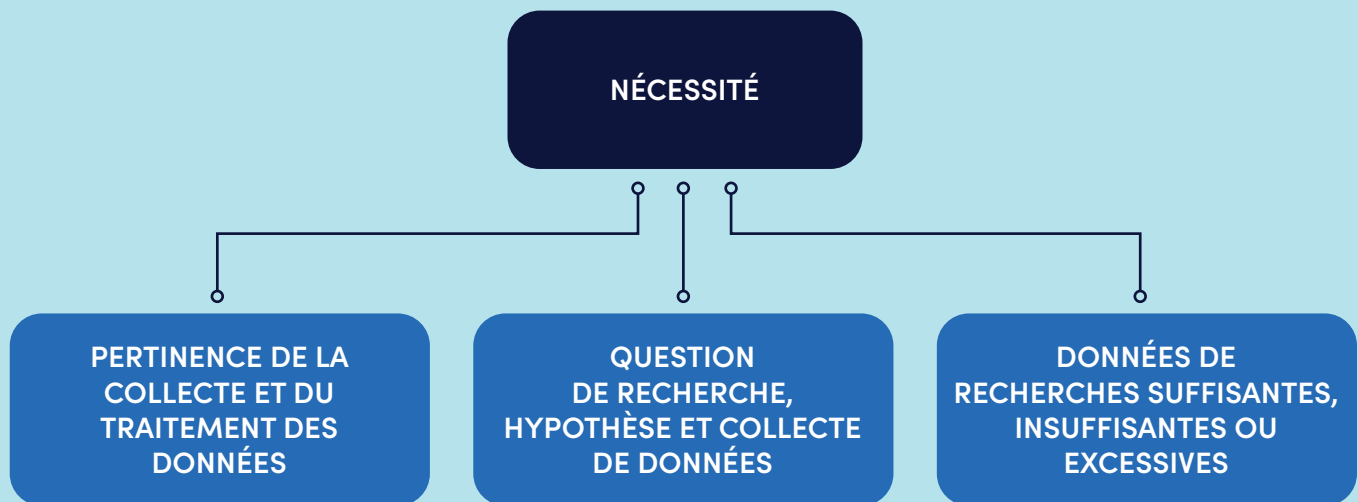


Conflit d'intérêts

L'ETPC-2 définit le conflit d'intérêts comme une « incompatibilité entre au moins deux devoirs, responsabilités ou intérêts (personnels ou professionnels) d'une personne ou d'un établissement dans l'optique de la conduite éthique de la recherche faisant en sorte qu'un ou l'autre sera compromis » (EPTC-2, p. 301).



Thématique E : nécessité



L'un des avantages de la collecte et du traitement de données numériques personnelles, et notamment de données massives (*big data*), est qu'elle rend possible l'identification de corrélations ou de tendances qui seraient plus difficiles à détecter à partir d'un volume de données plus limitées. Or, la **nécessité de la collecte et du traitement des données** n'est pas toujours justifiée en elle-même pour autant. Afin de minimiser les risques pour les personnes participantes, il faut donc évaluer la pertinence de la collecte et du traitement des données au regard des objectifs de la recherche.

La collecte de données numériques personnelles est-elle nécessaire et pertinente pour atteindre les objectifs de la recherche ?

- Comment la collecte et le traitement des données numériques personnelles servent-ils les objectifs spécifiques de la recherche ?
- Le volume de données numériques personnelles collecté ou traité est-il justifié par la nature de la recherche, et comment évite-t-on le risque de collecte excessive ?
- Les données numériques personnelles collectées sont-elles suffisantes (pour être représentatives par exemple), insuffisantes ou au contraire excessives ?



Évaluation de la nécessité

Selon la Commission d'accès à l'information du Québec, l'évaluation de la nécessité de collecter des données numériques personnelles prévaut en toute circonstance, et ce, en dépit de l'obtention du consentement de la personne. L'évaluation de la nécessité permet de minimiser l'atteinte à la vie privée des personnes, en ne collectant que les données nécessaires pour répondre aux objectifs de la recherche.

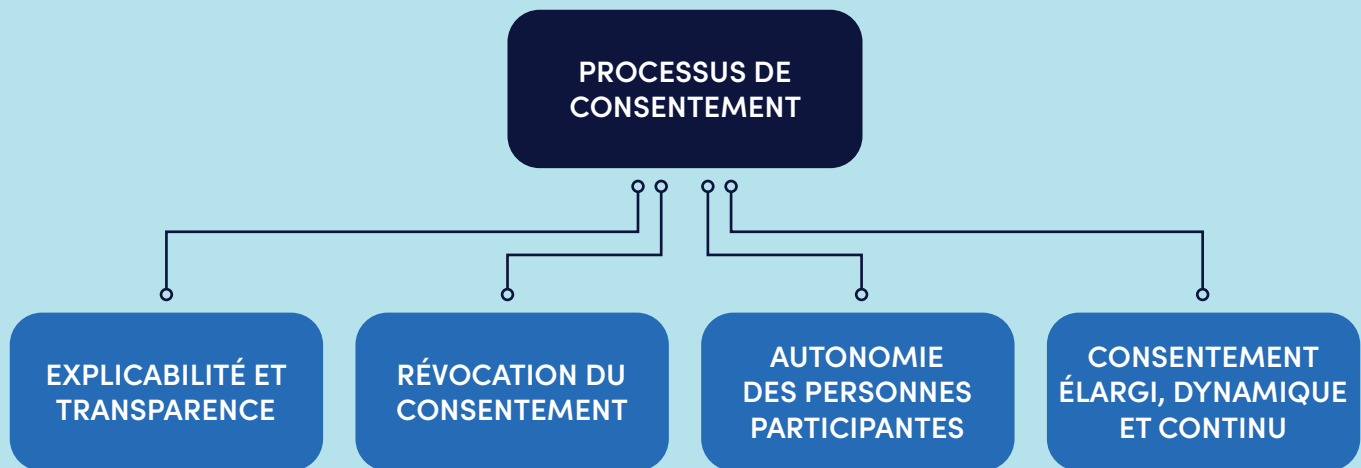
An abstract graphic of a circuit board pattern in light blue lines on a dark blue background. The lines form a complex, interconnected network of paths, with some lines ending in small circles or squares, suggesting components or data points. The pattern is more dense on the left side and fades towards the right.

Section 2

Projets de recherche qui impliquent un système d'IA

Systemes d'intelligence artificielle

Thématique A : processus de consentement



La mobilisation de SIA en recherche, notamment ceux basés sur l'apprentissage automatique (*machine learning*), peut complexifier l'obtention d'un consentement libre et éclairé, notamment en raison du phénomène de « boîte noire ». L'opacité du fonctionnement interne des SIA soulève des enjeux d'**explicabilité et de transparence**. En effet, compte tenu de la complexité des modèles d'IA, il s'avère difficile de comprendre comment ces systèmes prennent des décisions et traitent les données, et ce, même pour les spécialistes. Le fonctionnement opaque des SIA peut donc nuire à l'obtention de l'information nécessaire au consentement éclairé. Bien que cette opacité représente un défi, il faut tout de même tenter de rendre les processus décisionnels des SIA aussi explicables et intelligibles que possible pour les personnes participantes. De plus, étant donné que les SIA peuvent évoluer au fil du temps et donner lieu à des analyses ultérieures, il peut être nécessaire d'obtenir un **consentement élargi, continu et dynamique**, ce qui implique que les personnes participantes soient informées en continu de l'évolution du SIA et des utilisations des résultats ou des données. Une telle prise en compte de l'aspect évolutif des SIA permet notamment d'assurer l'**autonomie des personnes participantes**. Il faut également noter que la possibilité de **révocation du consentement** pose des défis particuliers en IA. En effet, une fois qu'un modèle a été entraîné à partir de données, leur suppression s'avère complexe, voire impossible, sans entraîner à nouveau le modèle. L'**interaction avec un SIA** peut prendre différentes formes, allant de la collecte des données à des échanges directs avec des agents conversationnels ou des systèmes de recommandation, mais il demeure dans tous les cas nécessaire d'informer les personnes participantes lorsqu'elles interagissent avec un SIA. Dans les cas où les personnes participantes sont en contact avec un SIA capable d'interagir en **langage naturel**, tel un robot conversationnel, celles-ci doivent être clairement informées qu'elles ne sont pas en train d'interagir avec un humain, mais bien avec un système automatisé.

Lors de la phase d'entraînement d'un SIA, il est possible d'utiliser des données numériques personnelles déjà existantes (disponibles sur internet, partagées par un tiers ou issues de bases de données publiques ou privées), et ce, possiblement sans le consentement des personnes concernées par ces données. La collecte et l'utilisation de ces données doit être faite en conformité avec les lois en vigueur (voir section 1A). Ces obligations comprennent, notamment, le devoir de démontrer pourquoi il est déraisonnable d'exiger le consentement des personnes et la démonstration qu'une évaluation des facteurs relatifs à la vie privée a été réalisée.

Quelles mesures sont prises pour s'assurer que les personnes participantes comprennent au moins minimalement l'objectif de l'utilisation du SIA dans le projet ainsi que son fonctionnement ?

- Une explication vulgarisée est-elle fournie concernant les capacités et les limites du SIA utilisé ?
- Existe-t-il une procédure d'assistance pour aider les personnes participantes à comprendre l'impact du SIA sur leur participation au projet ?

Comment le consentement libre, éclairé et continu est obtenu et garanti tout au long du projet, et ce, compte tenu de l'évolution possible du SIA utilisé ?

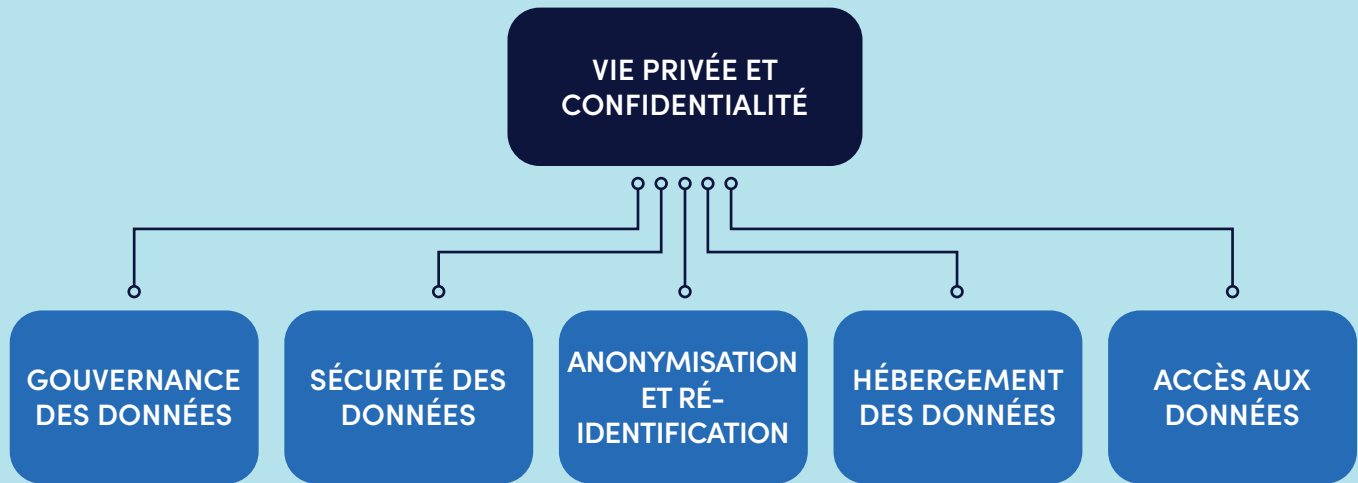
- Quelles informations sont fournies aux personnes participantes concernant l'usage immédiat et ultérieur de leurs données au sein du SIA ?
- Comment la capacité de révocation du consentement est-elle assurée tout au long du projet, y compris si les données des personnes participantes ont été utilisées dans l'entraînement d'un SIA ?
- Les limites de la révocation ont-elles été expliquées aux personnes participantes, en particulier si leurs données ont été utilisées pour entraîner un SIA et qu'elles ne peuvent plus être extraites rétroactivement du modèle ?

Est-ce que les personnes participantes interagiront directement avec un SIA dans le cadre du projet ?

- Si oui, ces dernières en ont-elles été clairement informées ?
- L'utilisation du SIA est-elle explicitement mentionnée dans le formulaire de consentement ?
- Quelles mesures sont prises pour s'assurer que le SIA ne compromette pas l'autonomie des personnes participantes dans leur capacité à prendre des décisions éclairées ?



Thématique B : vie privée et confidentialité



Les SIA reposent sur le traitement de vastes quantités de données, ce qui peut soulever des enjeux liés à la protection de la vie privée. Même lorsque des données sont dépersonnalisées ou anonymisées, l'IA peut faciliter la **réidentification**, notamment parce que les SIA permettent de croiser différents ensembles de données. La question de la **sécurité des données** est également primordiale en ce qui a trait aux données massives associées aux SIA. Par ailleurs, comme les SIA nécessitent d'énormes quantités de données, une puissance de calcul élevée et une consommation énergétique importante, il est probable que les équipes de recherche fassent appel à des SIA développés par un tiers. Dans ce cas, il faut évaluer les risques et enjeux spécifiquement liés à l'utilisation de produits, services ou modèles d'IA externes et adopter des stratégies appropriées en matière de **gouvernance des données de recherche**. Il est notamment important d'évaluer les risques que l'utilisation du SIA entraîne quant à l'**accès aux données**, à leur lieu d'**hébergement**, aux infrastructures utilisées ainsi qu'aux techniques de dépersonnalisation ou d'anonymisation employées.

Les techniques d'anonymisation employées dans le cadre de l'utilisation d'un SIA sont-elles suffisamment robustes pour éviter la réidentification des personnes participantes, notamment en cas de croisement avec d'autres bases de données ?

- Existe-t-il un risque que le SIA puisse involontairement générer des corrélations permettant d'identifier indirectement des personnes participantes ?

Les données des personnes participantes seront-elles utilisées pour entraîner un SIA ?

- Si oui, ont-elles été anonymisées ou pseudonymisées ?
- Comment s'assurer que les données des personnes participantes ne puissent pas être extraites ou reconstituées à partir du modèle entraîné ?
- Les données des personnes participantes utilisées pour l'entraînement du SIA peuvent-elles être supprimées du modèle après coup, et si oui, comment cela est-il garanti ?
- Existe-t-il un risque que le SIA conserve ou réutilise des informations personnelles même après la fin du projet de recherche, ou à d'autres fins ?

Où sont stockées les données traitées par le SIA (serveurs internes, nuage, infrastructures externes) ?

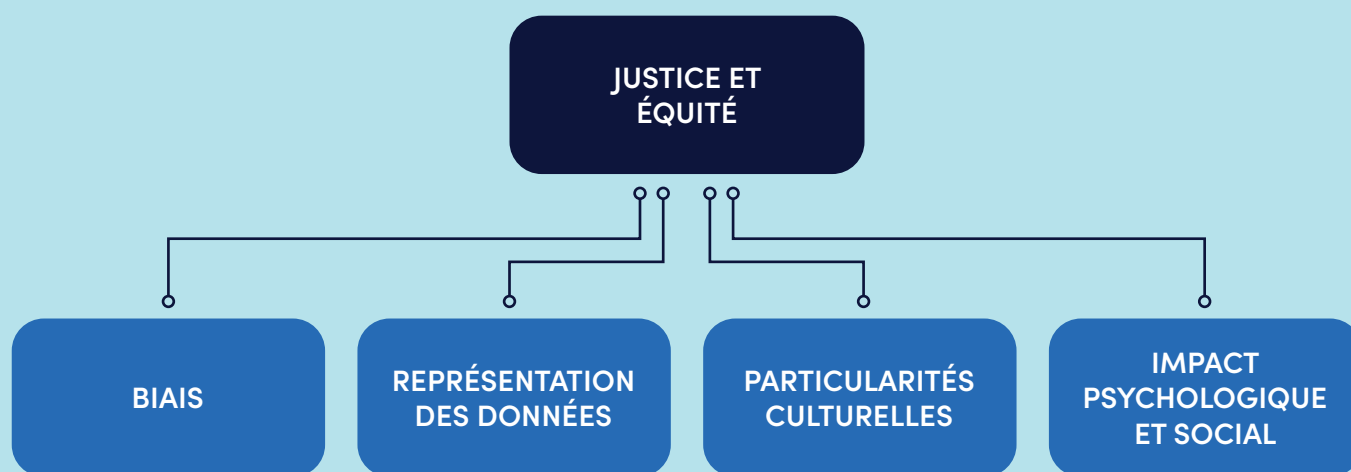
- Quels types de protocoles de sécurité sont mis en place pour protéger les données traitées par le SIA contre les accès non autorisés ?

Le SIA utilisé est-il développé par l'équipe de recherche ou son établissement d'attache ou s'agit-il d'un service ou d'un système externe ?

- S'il s'agit d'un service ou un système externe, quelles sont les modalités de contrôle, d'utilisation, de partage et de sécurisation des données par le tiers ?
- Si le SIA est développé par une entité externe, quelles sont les dispositions contractuelles quant à l'utilisation des données des personnes participantes ?



Thématique C : justice et équité



L'utilisation de SIA en recherche est susceptible de soulever certains risques spécifiques en ce qui a trait à la justice et l'équité. Un des enjeux principaux est associé au risque de **biais algorithmiques**, qui peuvent être issus des données ou de la conception des SIA. Les SIA sont entraînés à partir de données historiques qui peuvent présenter des biais socio-économiques, raciaux ou de genre. Il s'agit de s'assurer que les risques de préjudices associés à ces biais, qui peuvent être reproduits et amplifiés par les SIA, sont anticipés et mitigés. Il faut cependant noter que le phénomène de la boîte noire rend difficile, voire impossible, la correction de ces biais. Les biais algorithmiques pourraient notamment conduire **au traitement ou à la représentation inéquitables** des personnes participantes. C'est pourquoi il est nécessaire de s'assurer de la **représentativité des données** utilisées dans les SIA. De plus, l'automatisation des décisions et des processus par les SIA peut avoir des **répercussions psychologiques et sociales** importantes sur les personnes participantes. L'interaction avec ces systèmes peut notamment générer un sentiment de perte de contrôle, tout en augmentant les risques d'**exclusion, de stigmatisation ou de discrimination**. En effet, si les décisions sont perçues comme opaques, arbitraires ou inexplicables, le recours à un SIA peut susciter un sentiment d'injustice chez les personnes participantes. Un autre enjeu concerne le risque de résultats erronés ou fictifs produits par les SIA, communément appelées **hallucinations** ou **confabulations**, et qui peuvent induire en erreur les membres de l'équipe de recherche ou les personnes participantes, ce qui risque d'influencer indûment les décisions prises à l'égard de personnes participantes ou de générer des impacts psychologiques négatifs sur ces dernières.

Des mesures sont-elles envisagées pour réduire l'incidence des biais algorithmiques dans le SIA et les risques qui y sont associés pour les personnes participantes ?

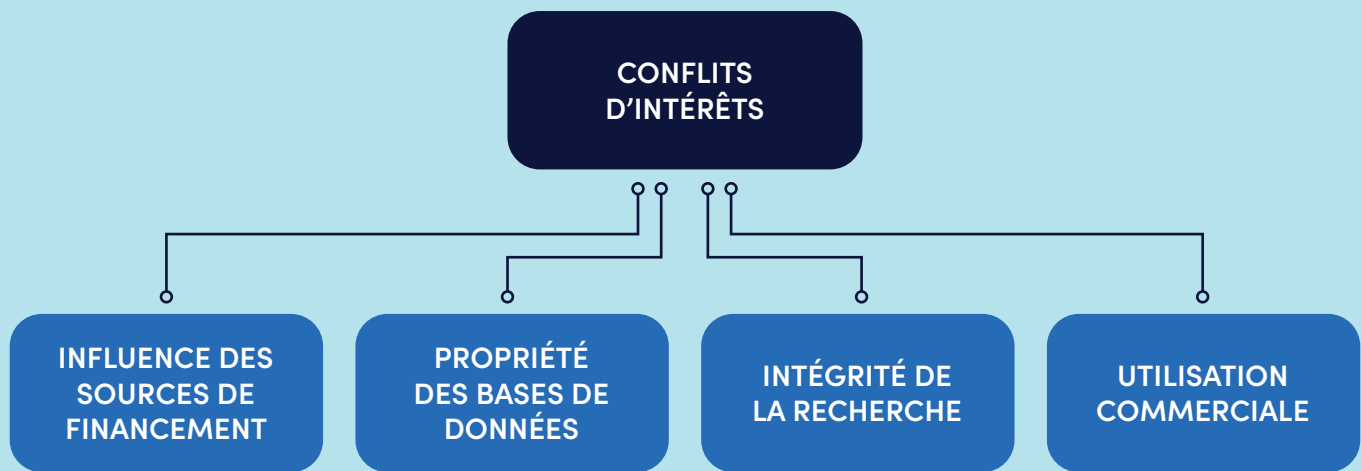
- Les données recueillies et utilisées par le SIA sont-elles représentatives, diversifiées et équilibrées, notamment au regard des objectifs de la recherche ?

Le recours à un SIA dans le cadre du projet pourrait-il avoir un impact psychologique ou social négatif sur les personnes participantes ?

- Le SIA est-il susceptible de renforcer des stéréotypes ou d'associer certains groupes de personnes participantes à des catégories qui pourraient les exclure ou les stigmatiser ?
- Comment le fonctionnement du SIA est expliqué aux personnes participantes afin d'éviter un sentiment d'impuissance ou d'injustice ?
- Le recours à un SIA implique-t-il une collecte de données potentiellement intrusive ou stigmatisante ?
- Les risques que des résultats erronés générés par un SIA aient un impact préjudiciable sur les personnes participantes ont-ils été évalués, et des moyens ont-ils été entrepris pour les mitiger ?



Thématique D : conflits d'intérêts



La recherche mobilisant des SIA tend à intégrer différents acteurs, notamment en raison de l'expertise de pointe et des infrastructures de calcul que ces systèmes nécessitent. Dans le cadre de projets de recherche mobilisant des SIA, les conflits d'intérêts peuvent être amplifiés par la **dépendance aux infrastructures technologiques** et aux financements d'entreprises privées. L'implication d'acteurs industriels privés (GAFAM – Google, Apple, Facebook, Amazon et Microsoft, startups spécialisées en IA, laboratoires privés, etc.) ou l'utilisation de leurs produits et services soulèvent des questions quant à l'influence des intérêts économiques sur les finalités de la recherche. La recherche peut alors notamment être soumise à une **influence liée aux sources de financement**, ou aux fournisseurs de services technologiques, ce qui pourrait en orienter la réalisation et les finalités. Dans cette perspective, il est essentiel de veiller à ce que la **propriété des bases de données et des algorithmes**, ainsi que les conditions d'accès à ces infrastructures n'influencent pas indûment le projet de recherche et ne génèrent pas de conflits d'intérêts. De plus, toute utilisation commerciale éventuelle des données ou des résultats de recherche doit être clairement définie, expliquée et communiquée aux personnes participant au projet de recherche. De façon générale, l'**intégrité de la recherche** doit être assurée en divulguant les relations d'intérêt pouvant exister entre les membres de l'équipe de recherche et les entreprises ou organismes externes dont les produits ou services sont impliqués dans le projet. Il s'agit de faire preuve de **transparence** quant aux **objectifs de la recherche** pour éviter les conflits d'intérêts ou l'apparence de conflits d'intérêts.



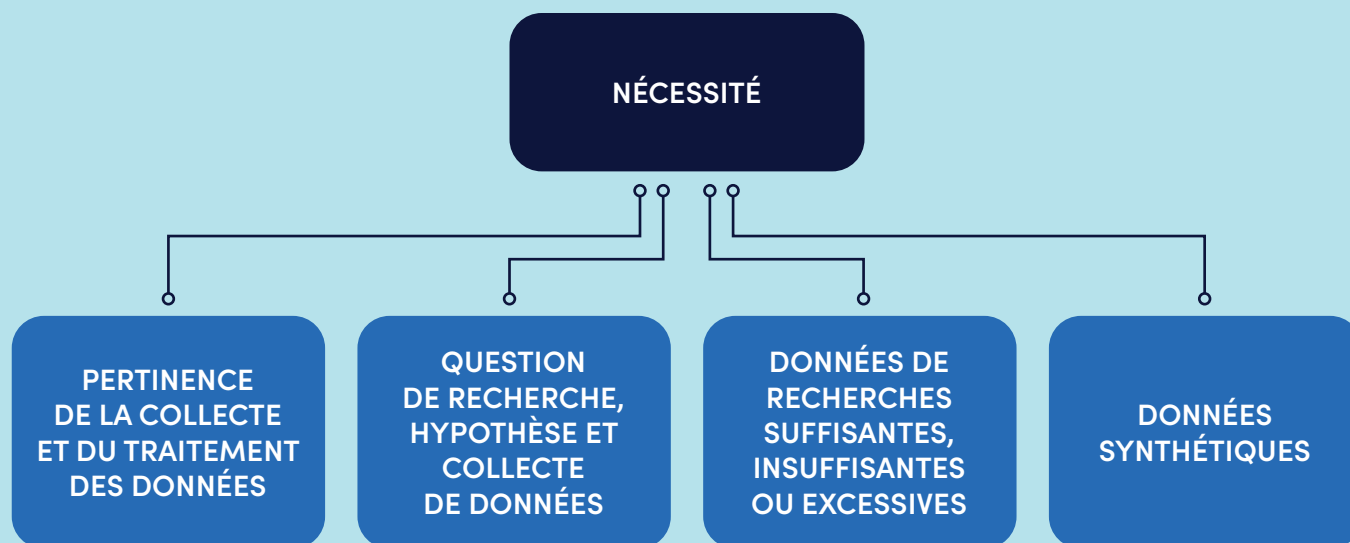
Les sources de financement du projet, en particulier liées à l'utilisation d'un SIA, ont-elles été déclarées de manière transparente ?

Le projet de recherche utilise-t-il un SIA impliquant des partenaires ou investisseurs privés ou encore utilise-t-il des produits ou services d'IA fournis par des entreprises externes ?

- Comment l'intégrité scientifique et l'indépendance du projet sont assurées afin que les attentes ou intérêts commerciaux de ces partenaires n'influencent ni la méthodologie, ni l'utilisation des données des personnes participantes et leur protection ?
- Les personnes participantes sont-elles informées de la présence de partenaires externes ayant un intérêt commercial dans l'utilisation d'un SIA ?
- Les personnes participantes sont-elles informées de la possibilité que les résultats obtenus à l'aide du SIA puissent être utilisés à des fins commerciales ou par des entreprises privées ainsi que de possibles risques associés à cette utilisation ?
- Comment le consentement libre et éclairé des personnes participantes est garanti face à d'éventuels conflits d'intérêts, notamment en ce qui concerne l'utilisation de leurs données au moyen d'un SIA lié à un tiers ?



Thématique E : nécessité



L'intégration d'un SIA dans un projet de recherche soulève des risques particuliers pour les personnes participantes, notamment en raison de la quantité de données requises, des possibilités accrues de réidentification et des limites au retrait du consentement. Ces systèmes, en raison de leur capacité à analyser de vastes ensembles de données et à identifier des corrélations, sont souvent perçus comme un outil privilégié pour la production de connaissances. Pourtant, leur mobilisation n'est pas toujours justifiée et peut entraîner des **risques inutiles** si elle n'est pas rigoureusement encadrée. Il est donc essentiel de s'assurer que **l'utilisation d'un SIA répond à un véritable besoin scientifique** et qu'elle ne résulte pas d'un simple engouement technologique. De même, la quantité de données collectées doit être évaluée avec attention afin de déterminer si elles **sont suffisantes** sans être **excessives** ou si leur collecte ou leur traitement expose les personnes participantes à des risques disproportionnés. Enfin, il peut être utile de se demander si l'utilisation de **données synthétiques** pourrait être envisagée afin de minimiser ces risques, tout en permettant d'atteindre les objectifs de recherche.

Le volume de données traité par le SIA est-il justifié par les objectifs de la recherche, et comment évite-t-on le risque de collecte excessive ?

- L'utilisation d'un SIA est-elle nécessaire et pertinente dans le cadre du projet de recherche ?

Comment l'utilisation d'un SIA soutient les objectifs spécifiques de la recherche ?

Serait-il possible d'utiliser des données synthétiques afin d'éviter des risques inutiles pour les personnes participantes ?



Banque d'outils

Documents officiels – Éthique de la recherche

- Énoncé de politique des trois conseils : Éthique de la recherche avec des êtres humains – EPTC 2
https://ethics.gc.ca/fra/policy-politique_tcps2-eptc2_2022.html.
- Déclaration de principes des trois organismes sur la gestion des données numériques
<https://science.gc.ca/site/science/fr/financement-interorganismes-recherche/politiques-lignes-directrices/gestion-donnees-recherche/declaration-principes-trois-organismes-gestion-donnees-numeriques>.
- La recherche à l'aide des plateformes de médias sociaux exige-t-elle une évaluation éthique de la recherche? – Lignes directrices à l'appui de la mise œuvre de l'Énoncé politique des trois conseils : Éthique de la recherche avec des êtres humains (2022).
https://ethics.gc.ca/fra/reb-cer_social-sociaux.html.
- Politique des trois organismes sur la gestion des données de recherche. (2021).
<https://science.gc.ca/site/science/fr/financement-interorganismes-recherche/politiques-lignes-directrices/gestion-donnees-recherche/politique-trois-organismes-gestion-donnees-recherche>
- Mise en garde sur l'éthique humaine de la recherche fondée sur l'intelligence artificielle et les mégadonnées. (2017).
<https://nrc.canada.ca/fr/organisation/valeurs-ethique/recherche-participants-humains/mise-garde-lethique-humaine-recherche-fondee-lintelligence-artificielle-megadonnees-2017>

Cadres en éthique de l'IA

- Déclaration de Montréal pour un développement responsable de l'IA. (2018).
<https://declarationmontreal-iaresponsable.com/la-declaration/>,
<https://op.europa.eu/fr/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>.
- Convention-cadre sur l'IA. (2022). Conseil de l'Europe,
<https://rm.coe.int/1680afae3d>.
- Lignes directrices en matière d'éthique pour une IA digne de confiance. (2022). Commission européenne
<https://op.europa.eu/fr/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1>.
- Recommandations sur l'éthique de l'intelligence artificielle. (2022). UNESCO,
https://unesdoc.unesco.org/ark:/48223/pf0000381137_fre

Documents de référence sur l'utilisation responsable de l'IA en recherche

- Living guidelines on the responsible use of generative AI in research, Commission Européenne
https://research-and-innovation.ec.europa.eu/document/download/2b6cf7e5-36ac-41cb-aab5-0d32050143dc_en?filename=ec_rtd_ai-guidelines.pdf
- Orientations pour l'intelligence artificielle générative dans l'éducation et la recherche, UNESCO
<https://unesdoc.unesco.org/ark:/48223/pf0000389901>.

Documents de référence en matière de protection des données personnelles et de la vie privée

- Réduire l'identifiabilité dans la perspective internationale : définitions législatives et politiques relatives à l'anonymisation, la pseudonymisation et la dépersonnalisation dans les pays du G7. (2024). Commissariat à la protection de la vie privée du Canada, https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2024/de-id_20241011/.
- L'anonymisation de données personnelles. (2020). Commission nationale de l'informatique et des libertés, France. <https://www.cnil.fr/fr/technologies/lanonymisation-de-donnees-personnelles>.
- Réaliser une évaluation des facteurs relatifs à la vie privée : Guide d'accompagnement à la démarche et à sa documentation, Commission d'accès à l'information du Québec https://www.cai.gouv.qc.ca/uploads/pdfs/CAI_GU_EFVP.pdf?gt=%C3%89valuer
- Devane, H. (2022). What are the top data anonymization techniques, IMMUTA, <https://www.immuta.com/blog/data-anonymization-techniques/>.
- Guide to basic data anonymization techniques. (2018). Personal Data Protection Commission, Singapore [https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-\(250118\).pdf](https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Other-Guides/Guide-to-Anonymisation_v1-(250118).pdf)

Guides et outils d'évaluation en éthique de l'IA

- AI Blindspot <https://aibindspot.media.mit.edu/index.html#about>
- AI Ethics guidelines global inventory - AlgorithmWatch. <https://inventory.algorithmwatch.org/>
- Aequitas – Bias and fairness audit toolkit <http://www.datasciencepublicpolicy.org/our-work/tools-guides/aequitas/>
- Ethical Operating System (OS) – A guide to anticipating the future impact of today's technology. <https://ethicalos.org/>
- Ethics & Algorithms Toolkit – A risk management framework for governments (and everyone) <http://ethicstoolkit.ai/>
- Assembling Accountability. Algorithmic Impact Assessment for the Public Interests. Data & Society Institute <https://datasociety.net/library/assembling-accountability-algorithmic-impact-assessment-for-the-public-interest/>.
- Observatoire international sur les impacts sociétaux de l'IA et du numérique – *Grille de réflexivité sur les enjeux éthiques des systèmes d'intelligence artificielle (SIA)* (2021). <https://www.obvia.ca/actualites/grille-de-reflexivite-portant-sur-les-enjeux-ethiques-des-systemes-dintelligence-artificielle-sia>.
- RRI Tool for self-reflection <https://rri-tools.eu/self-reflection-tool>

Cadres juridiques

Québec

Loi modernisant des dispositions législatives en matière de protection des données personnelles, LQ, c. 25.
<https://www.canlii.org/fr/qc/legis/loisa/lq-2021-c-25/derniere/lq-2021-c-25.html>.

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, RLRQ, c. A-2.1.
<https://www.legisquebec.gouv.qc.ca/fr/document/lc/A-2.1>

Règlement sur les incidents de confidentialité, RLRQ, c. A-2.1, r. 3.1.
<https://www.legisquebec.gouv.qc.ca/fr/document/rc/A-2.1,%20r.%203.1%20/>

Règlement sur l'anonymisation des renseignements personnels, RLRQ, c. A-2.1, r. 0.1.
<https://www.legisquebec.gouv.qc.ca/fr/document/rc/A-2.1,%20r.%200.1%20/>

Loi sur la protection des renseignements personnels dans le secteur privé, RLRQ, c. P-39.1.
<https://www.legisquebec.gouv.qc.ca/fr/document/lc/p-39.1>

Loi sur les renseignements de santé et de services sociaux, RLRQ, c. R-22.1.
<https://www.legisquebec.gouv.qc.ca/fr/document/lc/R-22.1>

Canada

Projet de loi C-27, *Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois*
<https://www.parl.ca/DocumentViewer/fr/44-1/projet-loi/C-27/premiere-lecture>.

N.B. Compte tenu de la prorogation du parlement du Canada annoncée en janvier 2025, le projet de loi C-27 est tombé et devra être réintroduit lors de la prochaine session si le gouvernement souhaite poursuivre les travaux législatifs amorcés.

Glossaire

Algorithme

Un algorithme est une suite finie d'opérations ou d'instructions permettant de résoudre un problème ou d'obtenir un résultat. Une recette de cuisine est un bon exemple d'algorithme puisqu'il s'agit d'une séquence d'instructions permettant d'obtenir un résultat, soit un plat cuisiné. Dans le cas de l'intelligence artificielle, il s'agit de la suite d'opérations appliquées aux données d'entrées pour arriver au résultat désiré.

Algorithmique

Ce qui réfère à la logique opérationnelle des algorithmes.

Biais algorithmique

Un biais algorithmique se produit lorsque les données utilisées pour entraîner un système d'apprentissage automatique reflètent les valeurs implicites des humains impliqués dans la collecte, la sélection, ou l'utilisation de ces données. Les biais peuvent provenir des données elles-mêmes, du choix des données ou de l'algorithme qui permet de traiter ces données. Les biais algorithmiques ont été identifiés et critiqués pour leur impact sur les résultats des moteurs de recherche, les services de réseautage social, le respect de la vie privée, et le profilage racial. Dans les résultats de recherche, ce biais peut créer des résultats reflétant des biais racistes, sexistes ou d'autres biais sociaux.

Boîte noire

Le phénomène de la boîte noire réfère à l'opacité des SIA, qui fait que l'on ne peut retracer précisément les mécanismes internes de décision du système. On peut savoir quelles données entrent (ou intrants) dans le SIA et quels résultats en sortent (les extrants), mais il est souvent impossible de savoir comment ces données ont été traitées pour arriver au résultat obtenu.

Centre de données

Lieu où sont regroupées des ressources informatiques et de télécommunication afin d'offrir des services de gestion, de stockage et de traitement des données informatiques.

Cycle de vie des données

Le cycle de vie des données renvoie aux différentes étapes suivantes : la création ou collecte, le traitement, l'analyse, la conservation, l'accès et la réutilisation des données.

Discrimination algorithmique

Type de discrimination indirecte qui peut résulter de biais présents dans un SIA et qui a pour effet de désavantager systématiquement un groupe de personnes.

Données massives (*big data*)

En français, « *big data* » se traduit par deux termes acceptables : mégadonnées et données massives. Les données massives ou mégadonnées désignent des ensembles de données devenus si volumineux qu'ils dépassent les capacités humaines d'analyse et même celles des outils informatiques classiques.

Donnée anonymisée

Une donnée numérique personnelle est anonymisée lorsqu'il est raisonnable de prévoir dans les circonstances qu'elle ne permet plus, et ce, de façon irréversible, d'identifier directement ou indirectement une personne. Une telle donnée ne contient pas d'identifiants directs (ex : nom, prénom) ni de code qui pourrait permettre une réidentification ultérieure de la personne. De plus, le risque de réidentification à partir des identifiants indirects (ex : âge, sexe) sont faibles ou très faibles. L'anonymisation de données est un processus complexe qui doit être réalisé sous la supervision d'une personne compétente en la matière.

Donnée dépersonnalisée

Une donnée numérique personnelle est dépersonnalisée lorsqu'elle ne permet plus d'identifier directement une personne. Par exemple, tous les identifiants directs sont retirés et remplacés par un code. Si ce code est accessible, il peut être possible de réidentifier des personnes.

Donnée numérique personnelle

Une donnée numérique personnelle est une information portée par un support numérique, qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier. Par exemple, des informations numériques telles que l'adresse IP, la date de naissance, le code postal ou une photo sont des données numériques personnelles.

Donnée numérique sensible

Une donnée numérique personnelle est dite sensible lorsque, de par sa nature (notamment médicale, biométrique, intime, politique, culturelle, religieuse, etc.) ou en raison du contexte de son utilisation ou de sa communication, elle suscite un haut degré d'attente raisonnable en matière de vie privée.

Donnée synthétique

Une donnée synthétique est une donnée créée artificiellement à partir de données réelles de référence et qui présente les mêmes propriétés statistiques que l'ensemble de données de référence. L'avantage de cette méthode est qu'elle permet de travailler avec des données ayant des propriétés spécifiques, mais qui ne contiennent pas de données personnelles ou sensibles. Ainsi, les risques de réidentification et les enjeux de vie privée reliés peuvent être contournés.

Grand modèle de langue

Modèle de langue statistique constitué par apprentissage profond à partir de mégadonnées. Les grands modèles de langue permettent à des agents conversationnels de répondre à des requêtes en langage naturel de façon syntaxiquement et sémantiquement correcte, en s'appuyant sur des modèles de plusieurs milliards de paramètres.

Hallucinations ou confabulation

Même s'ils sont très efficaces pour réaliser certaines tâches, les modèles d'IA générative peuvent générer du contenu erroné ou fictif. Cela est dû au fait que ces systèmes sont conçus pour produire du contenu qui obéit à une logique statistique probabiliste de prédiction de pertinence qui n'est pas assujettie à une vérification factuelle des résultats produits.

Intelligence artificielle

L'intelligence est l'ensemble des processus retrouvés dans des systèmes plus ou moins complexes, vivants ou non, qui mettent en jeu la mémoire, le langage, le raisonnement, l'apprentissage, la résolution de problèmes, la compréhension du réel, l'adaptation à l'environnement, la prise de décision, la perception et l'attention. L'intelligence artificielle désigne donc l'ensemble des techniques et processus qui permettent à une machine de simuler l'intelligence à partir de ces différentes composantes.

Intelligence artificielle générative

Sous-ensemble de l'apprentissage profond où l'on entraîne des modèles à base de réseaux de neurones qui peuvent ensuite produire de nouveaux contenus, notamment des textes (grand modèle de langues), des images (Synthèse texte-à-image), de l'audio et des données synthétiques. En d'autres mots, un système d'IA générative apprend de données existantes, puis crée un nouveau contenu similaire aux données sur lesquelles il a été entraîné.

Langage naturel

Terme qui désigne le langage tel que parlé par un humain, par opposition au langage informatique.

Plan de gestion des données

Le plan de gestion des données est un document évolutif permettant de décrire comment seront gérées les données numériques personnelles recueillies pour une recherche, et ce, tout au long du cycle de vie de ces données (de leur collecte jusqu'à leur destruction). Ce plan comprend généralement des informations sur la manière dont les données seront recueillies, documentées, formatées, protégées, conservées, et communiquées (le cas échéant). Il comprend aussi des informations à propos de la personne responsable de gérer les données du projet et, advenant son départ de l'équipe ou son décès, la personne qui pourrait la remplacer.

Système d'intelligence artificielle

Un système d'intelligence artificielle désigne un système automatisé utilisant des algorithmes d'intelligence artificielle, c'est-à-dire l'ensemble des techniques permettant de simuler certains traits de l'intelligence humaine, tels que le raisonnement, l'apprentissage, la prédiction, la prise de décision, la perception du monde environnant et la génération de contenu. Par exemple, les systèmes à base de connaissances (systèmes experts) et ceux fondés sur l'apprentissage automatique qui permettent notamment la reconnaissance de la parole, le traitement du langage naturel, la vision artificielle et les agents conversationnels sont des systèmes d'IA.

« Shadow AI »

Le terme anglais *Shadow AI*, parfois traduit par « utilisation occulte ou souterraine » de l'IA réfère à l'utilisation non autorisée et non supervisée de l'IA en contexte professionnel. Compte tenu de l'accessibilité des outils d'IA générative, et également que ces outils peuvent faciliter différentes tâches, notamment dans le cadre de la conduite de projets de recherche (transcription, traduction, résumé, rédaction, etc.), l'attrait pour l'utilisation de ces produits est fort, tant pour les membres de l'équipe de recherche que pour les auxiliaires de recherche. Cependant, une telle utilisation peut comporter des risques accrus pour les personnes participantes, et soulève des enjeux relatifs au consentement et à la protection des données.

Bibliographie

- Annany, M. & Crawford, K. (2017). Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability, *New media & Society*, 20(3), p.1-17. DOI: 10.1177/1461444816676645.
- Arnold, T. & Scheutz, M. (2018). The “big red button” is too late: an alternative for the ethical evaluation of AI systems, *Ethics and information technology*, 20(1), p.59-69. <https://doi.org/10.1007/s10676-018-9447-7>.
- Bouhouita-Guermech, S., Gogonon, P. & Bélisle-Pipon, J.-C. (2023). Specific challenges posed by artificial intelligence in research ethics, *Frontiers in artificial intelligence*, 6. <https://doi.org/10.3389/frai.2023.1149082>.
- Carvallo, S. (2019). L'éthique de la recherche entre réglementation et réflexivité, *Revue d'anthropologie des connaissances*, 13 (2), p. 299-326.
- CERNA Collectif. (2018). Research Ethics in Machine Learning. CERNA. ALLISTENE.
- Coeckelbergh, M. (2020). *AI ethics*, Cambridge, Massachusetts: MIT Press.
- Convery, I. & Cox, d. (2012). A review of research ethics in internet-based research, *Practitioner research in higher education*, 6 (1), p.50-57.
- Coutellec, L. (2019). Penser l'indissociabilité de l'éthique de la recherche, de l'intégrité scientifique et de la responsabilité sociale de la science. Clarification conceptuelle, proposition épistémologiques, *Revue d'anthropologie des connaissances*, 13(2), p.381-398.
- Coutellec, L., Coulée, F. & Hirsch, E. (2021). De nouveaux territoires pour l'éthique de la recherche Repères, responsabilités et enjeux. <https://doi.org.ezproxy.usherbrooke.ca/10.3917/eres.coute.2021.01>.
- Doucet, H. (2010). De l'éthique de la recherche à l'éthique en recherche, *Revue internationale d'éthique sociétale et gouvernementale*, 12(1), p.13-30.
- Ferretti, A., Ienca, M., Sheehan M., Blasimme, A., Dove, E. S., Farsides, B., Friesen, P., Kahn, J., Karlen, W., Kleist, P. et al. (2021). Ethics review of big data research: What should stay and what should be reformed? *BMC Medical Ethics* 22 (1), p.1-13. <https://doi.org/10.1186/s12910-021-00616-4>.
- Ferretti, A., Ienca, M., Velardes, M. R., Hurst, S. & Vayena, E. (2022). The challenges of big data for research ethics committees. A qualitative Swiss study, *Journal of Empirical Research on Human Research Ethics*, 17 (1-2), p.129-143. <https://doi.org/10.1177/15562646211053538>.
- Gagnon, E. (2010). Le comité d'éthique de la recherche, et au-delà, *Revue internationale d'éthique sociétale et gouvernementale*, 12(1), p.299-308.
- Gagnon, E. (2020). Sur la régulation institutionnelle de l'éthique de la recherche, *SociologieS*, Dossiers 2020. <https://doi-org.ezproxy.usherbrooke.ca/10.4000/sociologies.13161>.
- Gebru, T., Morgenstern, J., Vecchione, B., Vaughan, J. W., Walach, H., Daumé, H. & Crawford, K. (2021). Datasheets for datasets, *ArXiv*, <https://arxiv.org/abs/1803.09010>.

- Gosselin, T. (2022). Conjuguer principes et pratiques éthiques au temps des données socionumériques : le nécessaire dialogue, *Politiques et société*, 41(3), 241-246. <https://doi.org/10.7202/1092346ar>.
- Gouvernement du Canada (2022). *Énoncé politique des trois conseils. Éthique de la recherche avec êtres humaines (EPTC-2)*, https://ethics.gc.ca/fra/policy-politique_tcps2-eptc2_2022.html.
- Gouvernement du Canada. (2021). *Cadre de référence des trois organismes sur la Conduite responsable de la recherche*, <https://rcr.ethics.gc.ca/fra/framework-cadre-2021.html>.
- Gouvernement du Canada (2021). *Déclaration de principe des trois organismes sur la gestion des données numériques*, <https://science.gc.ca/site/science/fr/financement-interorganismes-recherche/politiques-lignes-directrices/gestion-donnees-recherche/declaration-principes-trois-organismes-gestion-donnees-numeriques>.
- Gouvernement du Canada (2023). *La recherche à l'aide des plateformes de médias sociaux exige-t-elle une évaluation éthique de la recherche? – Lignes directrices à l'appui de la mise œuvre de l'Énoncé politique des trois conseils : Éthique de la recherche avec des êtres humains*, https://ethics.gc.ca/fra/reb-cer_social-sociaux.html.
- Greene, K. K., Theofanos, M. F., Watson, C., Andrews A. & Barron, E. (2024). Avoiding past mistakes in unethical human subjects research: Moving from artificial intelligence principles to practice. *Computer*, 57(02), p, 53-63, <https://doi.org/10.1109/MC.2023.3327653>.
- Groupe en éthique de la recherche (2023). *La recherche à l'aide des plateformes de médias sociaux exige-t-elle une évaluation par un comité d'éthique de la recherche ? Lignes directrices à l'appui de la mise en œuvre de l'Énoncé de politique des trois conseils : Éthique de la recherche avec des êtres humains – EPTC 2 (2022)*, https://ethics.gc.ca/fra/reb-cer_social-sociaux.html.
- Hagendorff, T. (2020). The ethics of AI ethics: And evaluation of guidelines, *Minds and machines*, 30, p.99-120, <https://doi.org/10.1007/s11023-020-09517-8>.
- Hine, C. (2021). Evaluating the prospects for university-based ethical governance in artificial intelligence and data-driven innovation. *Research Ethics*, 17, p. 464 – 479. <https://doi.org/10.1177/17470161211022790>.
- Hossain, S. Q. & Ahmed, S. I. (2021). Towards a new participatory approach for designing artificial intelligence and data-driven technologies, *ArXiv*, <https://arxiv.org/abs/2104.04072>.
- Jobin, A., Ienca, M. & Vayena, E. (2019). The global landscape of AI ethics guidelines, *Nature Machine intelligence*, p.389-399. <https://doi.org/10.1038/s42256-019-0088-2>.
- Larouche, J.-M. (2019). Les sciences sociales et l'éthique en recherche en contexte canadien, *Revue d'anthropologie des connaissances*, 13(2), p. 479-501.
- Latzko-Thot, G. & Pastinelli, M. (2022). L'éthique de la recherche dans les espaces en ligne : clarifications de quelques notions, *Politiques et société*, 41(3), p. 241-246. <https://doi.org/10.7202/1092344ar>.
- Limongi, R. (2024). The use of artificial intelligence in scientific research with integrity and ethics. *Future Studies Research Journal: Trends and Strategies*. <https://doi.org/10.24023/futurejournal/2175-5825/2024.v16i1.845>.

- Markham, A. N. (2016) From using to sharing: A story of shifting fault lines in privacy and data protection narratives, in Vanacker, B. & Heider, D. (dir.), *Ethics in the Digital Age*, London: Peter Lang, p. 189–205.
- Mittelstadt, B. R., Allo, P., Taddeo, M., Wachter, S. & Floridi, L. (2016). The ethics of algorithms: Mapping the debate, *Big Data & Society*, 3(2), p.1–21. <https://doi.org/10.1177/2053951716679679>.
- Mollina et al. (2023). Research ethics in the age of digital platforms, *Science and Engineering ethics*, 29 (3), p.1–17.
- Morley, J., Floridi, L., Kinsy, L., & Elhalal, A. (2019). From what to how: An initial review of publicly available AI ethics tools, methods and research to translate principles into practices, *Science and engineering ethics*, 26, p.2141–2168. <https://doi.org/10.1007/s11948-019-00165-5>.
- Rességuier, A. & Ufert, F. (2023). AI research ethics is in its infancy: the EU's AI Act can make it a grown-up. *Research Ethics*, 20, p. 143–155. <https://doi.org/10.1177/17470161231220946>.
- Resnik D. B. & Hosseini, M. (2024). The ethics of using artificial intelligence in scientific research: new guidance needed for a new tool, AI and ethics, <https://doi.org/10.1007/s43681-024-00493-8>.
- Simonnot, B. (2019). Conduire des recherches en régime numérique : vers un cadre conceptuel de réflexion éthique, dans Balicco, L. (dir.), *L'éthique en contexte info-communicationnel numérique. Déontologie, régulation, algorithme, espace public*, p. 11–21.
- Shaw, J. (2022). Emerging paradigms for ethical review of research using artificial intelligence. *The American Journal of Bioethics*, 22, p. 42–44. <https://doi.org/10.1080/15265161.2022.2055206>.
- Srikumar, M., Finlay, R., Abuhamad, G. et al. (2022). Advancing ethics review practices in AI research. *Nat Mach Intell.* 4, p. 1061–1064 <https://doi.org/10.1038/s42256-022-00585-2>.
- Stahl, B. C. & Wright, D. (2018). Ethics and privacy in AI and Big Data: Implementing responsible research and innovation, *EEE Security & Privacy*, 16(3), p.26–33.
- Tiidenberg, K. (2017). Ethics in digital research, dans Flick, U. (ed.), *The SAGE Handbook of qualitative data collection*, p.466–481. <https://doi.org/10.1109/MSP.2018.2701164>.
- Torous, J. & Nebeker, C. (2017). Navigating ethics in the digital age: Introducing connected and open research ethics (CORE), a tool for researchers and institutional review boards, *J Med Internet Res*, 19(2). <https://doi.org/10.2196/jmir.6793>.
- Unesco (2021). *Recommandation sur l'éthique de l'intelligence artificielle*, <https://www.unesco.org/en/artificial-intelligence/recommendation-ethics>.
- Van den Hoonard, W. C. (2011). *The seduction of ethics. Transforming the social sciences*, Toronto, Buffalo, London, Toronto University Press.
- Van den Hoonaard, W. C. & Tolich, M. (2014). The New Brunswick declaration of research ethics: A simple and radical perspective, *Canadian journal of sociology/Cahiers canadiens de sociologie*, 39(1), p.87–98.

