Commission
d'accès à l'information
du Québec

PANDÉMIE, VIE PRIVÉE ET PROTECTION DES RENSEIGNEMENTS PERSONNELS

ÉLÉMENTS DE RÉFLEXION CONCERNANT LE RECOURS À CERTAINES TECHNOLOGIES (EX. : TRAÇAGE DE CONTACTS, BRACELETS CONNECTÉS, UTILISATION DE DONNÉES DE GÉOLOCALISATION)

16 AVRIL 2020 (V.2)

CONTEXTE

Le Québec traverse présentement une crise sanitaire sans précédent, tout comme l'ensemble du Canada et des pays à travers le monde. Des choix difficiles sont faits et bouleversent nos vies. Les autorités gouvernementales ont mis en place un ensemble de mesures visant à protéger la santé de la population, comme le lui permet la *Loi sur la santé publique* lorsque l'état d'urgence sanitaire est déclaré.

Ces mesures ont un impact important sur notre quotidien, sur la santé publique et sur l'économie du Québec. Des réflexions sont en cours afin de planifier une reprise progressive de certaines activités, au moment opportun. Plusieurs initiatives technologiques voient le jour ou sont en développement à travers le monde avec pour objectif de favoriser cette reprise de l'activité économique tout en contribuant à limiter la pandémie : partage de données de géolocalisation, applications de traçage des contacts, outils électroniques pour alerter les autorités en cas de non-respect d'une consigne d'isolement, évaluation du niveau de risque qu'une personne soit infectée, etc. Certains pays ont déjà recours à ce genre d'outils, alors que d'autres l'envisagent.

Comme certains l'ont souligné, ces outils technologiques ne sont pas sans conséquence sur les droits fondamentaux : droit au respect de la vie privée, risque de discrimination, etc. Une réflexion sur les différents enjeux en cause s'impose avant d'envisager leur déploiement au Québec. Nos valeurs et notre encadrement juridique diffèrent de ceux de certains pays qui ont recours à ces solutions.

Malgré l'importance de la crise actuelle et le besoin pour le Québec de se positionner sur la question de manière diligente, on ne saurait faire l'économie de cette évaluation préalable, de cette pondération des différentes valeurs en présence afin de prendre une décision éclairée et de faire des choix judicieux et réfléchis. Le temps de « pause » actuel imposé au Québec est propice à cette réflexion.

Dans le cadre de son rôle de promotion de la protection des renseignements personnels, la Commission d'accès à l'information souhaite contribuer à cette réflexion, en soumettant certaines considérations relatives aux enjeux de vie privée et de protection des renseignements personnels susceptibles d'être soulevés par ces outils. L'objectif du présent document n'est pas d'analyser ces outils ni de conclure à leur conformité ou non à la législation en vigueur ni à leur opportunité, mais de résumer les éléments à considérer avant toute décision relative à leur déploiement ou à leur utilisation au Québec, le cas échéant, et de fournir, lorsque possible, certains outils visant à accompagner cette réflexion.

Compte tenu de l'évolution rapide de la situation, le présent document pourrait être mis à jour au besoin.

PROTECTION DES RENSEIGNEMENTS PERSONNELS ET VIE PRIVÉE

Dans un premier temps, il peut être utile de rappeler ce que constituent le droit à la vie privée et la protection des renseignements personnels.

Le **respect de la vie privée** est un droit fondamental consacré dans la *Charte des droits et libertés de la personne* au Québec (art. 5). Cette protection a aussi été incluse dès 1948 dans la *Déclaration universelle des droits de l'homme* des Nations unies (art. 12). Il s'agit d'un droit important tant sur le plan individuel (ex. : autonomie, liberté, intimité, dignité, protection d'une sphère privée nécessaire au bien-être psychologique, droit à l'image) que sur le plan collectif au sein d'une société démocratique (ex. : éviter la surveillance des individus, assurer la protection du domicile contre les fouilles et les perquisitions abusives). Le droit au respect de la vie privée peut aussi être intimement lié au respect d'autres droits, comme la protection contre la discrimination, le droit à l'autonomie, la liberté de circulation ou d'opinion, la sauvegarde de son honneur, de sa dignité et de sa réputation, etc.

Toutefois, le droit à la vie privée, comme tout droit fondamental, n'est pas absolu. Il s'exerce notamment dans le respect des valeurs démocratiques, de l'ordre public et du bien-être général des citoyens du Québec. Il est donc prévu qu'on puisse y porter atteinte, en certaines circonstances et à certaines conditions, afin d'assurer un équilibre et une pondération entre les besoins de la société et les droits des individus. Entre autres, cette atteinte sera justifiée s'il est démontré que la mesure poursuit un objectif légitime, sérieux et important et que l'atteinte au droit fondamental qu'elle constitue est proportionnelle à cet objectif. La Charte prévoit que la loi peut alors en fixer la portée et en aménager l'exercice.

Pour sa part, la **protection des renseignements personnels** constitue l'une des dimensions du droit au respect de la vie privée, soit sa dimension informationnelle. Au Québec, cette protection est consacrée dans deux lois, l'une s'appliquant au secteur public et l'autre au secteur privé. Celles-ci ont un caractère prépondérant sur l'ensemble des autres lois au Québec, témoignant de l'importance de ces droits au sein de notre société.

Leur objectif est de préciser les règles permettant d'assurer à chacun le contrôle sur leurs renseignements personnels et de définir les limites de ce que peuvent faire les organismes publics et les entreprises qui doivent nécessairement recueillir et utiliser certains renseignements dans le cours de leurs activités respectives. La protection des renseignements personnels ne se résume pas à assurer la confidentialité de ces renseignements : elle se traduit par un ensemble de règles qui visent à limiter l'intrusion dans la vie privée que constitue la collecte, l'utilisation, la communication ou la conservation de renseignements personnels. Deux principes essentiels de ces législations sont la minimisation de la collecte et de l'utilisation des renseignements personnels à ce qui est strictement nécessaire et le consentement de la personne concernée.

Bien qu'une modernisation de ces législations soit requise, les principes mis de l'avant par ces législations peuvent tout de même servir de phare dans le cadre de la réflexion visée par le présent document.

Toute réflexion portant sur l'impact des solutions technologiques envisagées implique une évaluation à deux niveaux. L'une vise à pondérer l'objectif poursuivi (est-ce nécessaire?) et son

impact sur la vie privée (l'atteinte est-elle proportionnelle?). Si, et seulement si, ce premier test permet de conclure que l'objectif poursuivi justifie de mettre en place une telle solution et que l'atteinte à la vie privée qu'elle implique est proportionnelle à cet objectif, il convient alors de procéder à la seconde partie de l'évaluation qui vise à s'assurer que les modalités de la solution envisagée respectent les principes et les meilleures pratiques de protection des renseignements personnels.

I - L'ATTEINTE AU DROIT À LA VIE PRIVÉE QU'ELLE CONSTITUE EST-ELLE JUSTIFIÉE ET PROPORTIONNELLE?

OBJECTIF POURSUIVI LÉGITIME (EST-CE NÉCESSAIRE?)

Cette réflexion doit d'abord poser un regard sur l'objectif poursuivi par la solution technologique envisagée. En effet, cet objectif est déterminant pour évaluer ensuite la proportionnalité de la mesure proposée.

L'objectif poursuivi doit être suffisamment important pour justifier que l'on restreigne un droit protégé par la Charte. Cet objectif doit être légitime et se rapporter à des préoccupations sociales urgentes et réelles.

Concrètement, il s'agit donc de s'interroger sur l'objectif de la technologie proposée. Bien entendu toutes celles envisagées visent à contribuer à enrayer la COVID-19, à limiter la propagation du virus. Mais il importe d'être plus précis et de répondre à la question : Comment cette application ou cet outil technologique est-il susceptible de le faire? Que vise-t-il spécifiquement à faire dans le contexte de cette lutte? Par exemple, est-ce qu'on vise à : aider les autorités de santé publique à effectuer les enquêtes épidémiologiques et à retracer les contacts ou à avoir un portrait plus global de la prévalence au sein de la population? Assurer le respect de mesures d'isolement par les personnes porteuses du virus? Identifier les personnes susceptibles d'avoir été en contact avec des personnes infectées et si oui, dans quel but (dépistage, recommandations de consignes sanitaires, portrait d'une situation, etc.)? Prodiguer des conseils aux personnes selon leur « niveau de risque » d'avoir été en contact avec une personne infectée ou leurs symptômes? Etc.

On peut également se demander comment cet objectif s'inscrit dans la stratégie actuelle des autorités de santé publique. En effet, dans le contexte d'urgence sanitaire déclaré par les autorités gouvernementales, la légitimité d'une mesure ou d'une solution portant atteinte aux droits fondamentaux susceptible de nuire aux actions des autorités de santé publique serait questionnable. Ceci implique aussi de s'interroger sur qui propose et développe cette solution et qui en détermine l'objectif : un organisme public? les autorités de santé publique? une entreprise privée? un autre groupe? Est-ce qu'ils poursuivent un ou plusieurs autre(s) objectif(s) secondaires? Quelle est la légitimité de tous ces objectifs, le cas échéant?

PROPORTIONNALITÉ DE LA MESURE PROPOSÉE

En second lieu, les concepteurs de ces solutions ou les autorités gouvernementales qui les adoptent ou en font la promotion doivent démontrer qu'il s'agit d'un moyen raisonnable et que sa justification peut se démontrer, i.e. que l'intrusion dans la vie privée qu'implique la solution proposée est proportionnelle à l'objectif poursuivi ou à la situation que l'on souhaite contrer. Il

s'agit de trouver un équilibre entre le moyen choisi pour répondre à la problématique identifiée et le respect des droits des individus.

La proportionnalité de la mesure proposée s'évalue en trois temps.

1) D'abord, il doit exister un **lien rationnel** ente l'objectif poursuivi (incluant les objectifs secondaires) et la solution proposée, i.e. qu'il doit s'agir d'un moyen efficace pour atteindre cet ou ces objectif(s).

Concrètement, il s'agit de se demander : Est-il est raisonnable de conclure que la solution proposée permettra d'atteindre l'objectif poursuivi? Comment concrètement l'application ou la technologie proposée pourrait-elle permettre d'atteindre l'objectif poursuivi? En quoi la collecte, l'utilisation ou la communication des renseignements personnels envisagée permettrait-elle d'atteindre cet objectif? Quel est le degré d'efficacité du dispositif (ou à tout le moins le degré prévisible, basé sur des données concrètes)? Est-ce que cet outil a été efficace pour lutter contre la COVID-19 ailleurs? Si oui, selon les mêmes paramètres? Était-il jumelé avec une autre mesure comme une politique de dépistage (tests) ou autre?

2) S'agissant d'un droit fondamental, **l'intrusion à la vie privée des individus doit être minimale** et s'imposer en l'**absence d'autre solution** efficace moins intrusive pour la vie privée.

Il s'agit de s'interroger sur la portée de la solution envisagée et de se demander si d'autres moyens, moins intrusifs, ne pourraient pas apporter une solution efficace ou permettre d'atteindre l'objectif poursuivi. Se demander par exemple : est-ce que l'objectif peut être atteint autrement, sans porter atteinte à la vie privée des individus, sans recueillir ou utiliser des renseignements personnels? Quels moyens permettent de limiter l'atteinte à ce droit au strict minimum? Est-ce que ce genre d'outil devrait être encadré de manière spécifique dans le contexte actuel et compte tenu des enjeux importants de vie privée qu'il soulève? Si oui, comment?

La nature des renseignements que l'on envisage de recueillir et d'utiliser aura un impact sur cette évaluation. Le recours à des renseignements sensibles, comme les renseignements de santé (ex. : un résultat positif à un test de dépistage du coronavirus ou des symptômes) ou les déplacements d'une personne sont plus intrusifs que des renseignements d'une autre nature ou agrégés.

Le lieu de conservation (centralisé ou décentralisé) est aussi pertinent à cette évaluation, de même que la circulation et l'accès à ces renseignements. Combien de temps seront-ils conservés?

Une importance doit aussi être portée aux objectifs ou aux utilisations secondaires envisagées dans le cadre de la solution proposée : sont-elles essentielles? Est-ce qu'elles constituent une atteinte supplémentaire à la vie privée? Si oui, peut-on retirer cet ou ces autre(s) objectif(s) ou utilisation(s) des renseignements personnels?

Quelles mesures sont prévues pour mettre fin à cette intrusion dans la vie privée au terme de cette situation exceptionnelle? L'application sera-t-elle retirée du marché? Les données seront-elles détruites?

3) Enfin, les **avantages concrets** de la solution proposée **doivent surpasser les conséquences préjudiciables** pour les individus.

Il s'agit essentiellement d'une balance des avantages et des inconvénients concrets d'avoir recours à la solution technologique envisagée. Quels sont-ils? Est-ce que le ou les avantage(s) pour le bien collectif surpasse(nt) l'atteinte aux droits individuels?

Il est pertinent de considérer toutes les conséquences concrètes susceptibles de se réaliser. Par exemple, est-ce que la mesure envisagée est susceptible d'entraîner une atteinte à d'autres droits, comme la dignité ou la sauvegarde de sa réputation, d'entraîner de la discrimination, de stigmatiser certains individus? Est-elle susceptible d'avoir un impact, positif ou négatif, sur les mesures adoptées par les autorités pour lutter contre la pandémie (ex. : créer un faux sentiment de sécurité dans la population ou au contraire, inquiéter inutilement certains individus, risquer de nuire à certaines consignes de santé publique, miner la confiance des individus envers les autorités et nuire à certaines mesures volontaires, etc. La solution est-elle en phase avec la stratégie de dépistage en place? Vise-t-elle à faciliter les enquêtes épidémiologiques?). Quels sont les enjeux selon que les renseignements sont recueillis et utilisés par les autorités publiques ou une entreprise privée? Si cette application est disponible sur une base volontaire, quels sont les avantages et les inconvénients de cette approche?

Si cette première partie de l'évaluation permet de conclure que la solution envisagée est une mesure justifiée et nécessaire dans le contexte actuel et que l'intrusion dans la vie privée qu'elle constitue est proportionnelle et permet d'assurer un équilibre et une pondération entre les besoins de la société et les droits des individus, il convient d'évaluer les modalités d'application afin de s'assurer qu'elles respectent les principes et les meilleures pratiques en matière de protection des renseignements personnels.

II - RESPECT DES PRINCIPES ET MEILLEURES PRATIQUES DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

Tel que mentionné précédemment, la protection des renseignements personnels ne se résume pas à assurer la confidentialité et la sécurité de l'information concernant les individus. Il s'agit d'un ensemble de principes et de bonnes pratiques visant à encadrer et à minimiser la collecte, l'utilisation, la communication et la conservation des renseignements personnels.

Selon que la collecte de renseignements personnels envisagée par le biais d'une solution technologique sera faite par un organisme public ou une entreprise privée, voire les deux, il importe de se référer à la législation pertinente : les organismes publics doivent respecter les dispositions de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* alors que les entreprises doivent se référer aux obligations prévues par la *Loi sur la protection des renseignements personnels dans le secteur privé*.

Bien que cette liste ne soit pas exhaustive, la Commission souhaite attirer l'attention sur les principes et bonnes pratiques suivants :

1- Prévention

Avant de déployer un outil technologique ou une mesure qui implique la collecte, l'utilisation ou la communication de renseignements personnels, il convient d'identifier sa conformité avec la législation et les principes de protection des renseignements personnels et de vie privée généralement reconnus. Cette évaluation des facteurs relatifs à la vie privée est obligatoire dans plusieurs pays et dans certaines provinces canadiennes. Elle permet d'identifier dès le début d'un projet les enjeux en ces matières et d'ajuster la solution de manière à respecter la loi et à minimiser les impacts sur la vie privée.

L'EFVP consiste à réaliser une analyse ayant pour objet :

• de présenter le projet (objectif, procédures internes concernées, etc.);

• d'identifier les renseignements personnels visés par le projet, ainsi que leur circulation au sein du système d'information (cycle de vie du renseignement);

• de décrire quelles sont les répercussions du projet à l'égard des renseignements personnels visés;

• de faire un lien entre le projet et les principes légaux de protection des renseignements personnels (objet du fichier, nécessité, collecte, information, utilisation, consentement, communication, destruction, sécurité, accès, etc.);

• d'identifier les risques et les conséquences en matière de protection des renseignements personnels;

• de déterminer et de mettre en place des moyens pour minimiser l'intrusion dans la vie privée et assurer la protection des renseignements personnels.

Pour plus de détails : https://www.cai.gouv.qc.ca/documents/CAI_FI_efvp.pdf. La Commission rendra aussi disponible sous peu une version préliminaire d'un guide d'accompagnement qui sera accessible sur son site Internet : https://www.cai.gouv.qc.ca/.

Une autre bonne pratique préventive consiste à élaborer la solution ou l'application envisagée en appliquant le principe de vie privée et protection des renseignements personnels dès la conception *(Privacy by design*) et par défaut (*Privacy by default*). Comme leur nom respectif l'indique, la première consiste à concevoir une solution maximisant le respect de la vie privée à toutes les étapes de son développement, incluant l'analyse, le design, la mise en œuvre, la vérification, la sortie, la maintenance et la mise hors service. Ces mesures doivent viser toutes les étapes du cycle de vie d'un renseignement (de sa collecte à sa destruction) et être transparentes (diffusées aux utilisateurs). La seconde consiste à définir de manière automatique tous les paramètres de l'application, par défaut (sans que l'utilisateur ait à définir de paramètres spécifiques), de manière à ce qu'elles assurent un niveau de protection maximal des données.

Enfin, certains développements technologiques peuvent aussi être utilisés pour améliorer la protection des renseignements personnels. Il existe des technologies favorisant la vie privée (*Privacy enhancing technologies - PET*). Par exemple, elles peuvent aider à limiter la collecte de renseignements personnels (ex. : anonymisation), à augmenter leur confidentialité ou la sécurité

de certaines communications, à limiter l'accès aux seules personnes concernées ou encore à améliorer le contrôle d'une personne sur ses renseignements personnels (ex. : pseudonymisation, confidentialité différentielle, cryptographie, chiffrement homomorphe, hachage cryptographique, techniques de divulgation sélective, marquage des données, etc.). Pour plus d'exemples sur ces différentes techniques : https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/recherche/consulter-les-travaux-de-recherche-sur-la-protection-de-la-vie-privee/2017/pet_201711/.

2. Limiter la collecte aux seuls renseignements personnels nécessaires

Un des principes importants de la législation en matière de protection des renseignements personnels est que seuls les renseignements personnels nécessaires peuvent être recueillis. Cette règle ne peut être contournée par l'obtention du consentement de la personne concernée : une entreprise ou un organisme public ne peut recueillir un renseignement non nécessaire même si un individu y consent.

Ainsi, la nécessité de recueillir chacun des renseignements personnels envisagés doit pouvoir être expliquée et démontrée. Pour ce faire, il convient de se demander en quoi chaque renseignement permet de contribuer à atteindre l'objectif poursuivi par la solution proposée. Ici encore, la proportionnalité de cette collecte pour atteindre l'objectif poursuivi est pertinente pour en déterminer la nécessité. Il importe donc de déterminer la nature des renseignements dont la collecte est envisagée et de prendre toutes les mesures pour minimiser l'impact sur la vie privée que constitue celle-ci.

Par exemple, s'il s'agit de renseignements sensibles, les mesures mises en place pour minimiser l'intrusion dans la vie privée devront être plus importantes et tout autre moyen pour atteindre l'objectif poursuivi devrait être privilégié. Par contre, s'il est possible de réaliser l'objectif poursuivi en ne recueillant que des renseignements anonymisés, dépersonnalisés, pseudonymisés ou agrégés, ces autres moyens devront être mis en œuvre. Cela peut aussi impliquer de recueillir un renseignement moins sensible ou de devoir justifier pourquoi ce dernier n'est pas aussi efficace. À titre d'exemple, certaines applications de traçage des contacts utilisent la géolocalisation alors que d'autres utilisent plutôt uniquement les informations de proximité (ex. : Bluetooth) évitant une surveillance ou un suivi des déplacements.

Pour vous aider à déterminer la nature des renseignements recueillis, voici quelques précisions :

Renseignements personnels : Un renseignement est personnel s'il concerne une personne physique et permet de l'identifier. L'évaluation du critère « permet de l'identifier » réfère à la capacité de distinguer cette personne d'une autre, de maintenir un lien entre cette personne et des renseignements qui la concernent.

Renseignements personnels sensibles : le caractère « sensible » ou non d'un renseignement s'apprécie soit par sa nature particulièrement intime ou par les conséquences préjudiciables susceptibles de résulter de sa divulgation. Il peut s'agir, par exemple, de renseignements de santé, fiscaux, financiers, génétiques ou en lien avec la sexualité d'une personne. On inclut aussi généralement dans cette catégorie des renseignements en lien avec des risques de discrimination (par exemple, race, origine ethnique, religion, handicap) ou de vols d'identité (coordonnées,

identifiants uniques comme le numéro d'assurance maladie, le permis de conduire ou le numéro d'assurance sociale). Les renseignements biométriques, de par leur caractère unique, permanent et intime, font aussi partie de cette catégorie. Pour en savoir davantage sur la nature des renseignements biométriques et les règles particulières à respecter, voir la section 6.1 du présent document.

Renseignements anonymes : Un renseignement peut être qualifié d'anonyme s'il n'est plus possible d'identifier un individu, de manière irréversible, même en ayant recours à d'autres informations ou techniques de réidentification. Ainsi, le retrait d'identifiants directs (ex. : nom, adresse, numéro d'assurance maladie ou de permis de conduire, adresse IP, etc.) ne suffit pas à rendre un renseignement anonyme. Le caractère irréversible est essentiel pour conclure à l'anonymisation de renseignements. Avant de conclure qu'un renseignement est anonymisé, les risques de réidentification d'un renseignement doivent donc être soigneusement analysés et démontrés.

Par exemple, l'anonymisation de certaines données pose des défis particuliers compte tenu de leur nature. Par exemple, il peut être assez facile de déduire l'adresse du domicile ou de travail d'une personne à partir de ces données de géolocalisation et, par conséquent, son identité.

Renseignements dépersonnalisés : Il s'agit de renseignements personnels dont on a retiré les identifiants directs ou dont il n'est pas possible d'identifier une personne sans avoir recours à d'autres renseignements, à une clé de correspondance ou à d'autres techniques de réidentification. Il existe différentes techniques comme la pseudonomisation (on remplace les identifiants directs par des pseudonymes, numériques ou autre), le chiffrement, etc. Il importe toutefois de retenir que ces renseignements conservent leur caractère personnel; ils sont donc assujettis à l'ensemble des règles de protection des renseignements personnels de la législation applicable.

Renseignements personnels inférés : certains projets sont susceptibles d'avoir recours à des systèmes d'intelligence artificielle. Les algorithmes peuvent inférer de nouveaux renseignements à partir des renseignements recueillis, par exemple votre degré de risque d'être infecté par le virus ou d'avoir été en contact avec une personne atteinte du virus. Lorsque ces renseignements concernent une personne physique et permettent de l'identifier, ils sont aussi des renseignements personnels soumis aux obligations de la législation en matière de renseignements personnels. Cela signifie qu'une entreprise ou un organisme public qui détient un renseignement inféré doit s'assurer du respect des obligations visant à assurer la protection des renseignements personnels, incluant la nécessité de ce renseignement, limiter son utilisation et sa communication à ce qui est autorisé par la loi, assurer sa confidentialité et le détruire. L'individu concerné a, pour sa part, le droit d'avoir accès à ce renseignement et de le faire rectifier.

3. Faire preuve de transparence

La législation en matière de protection des renseignements personnels prévoit que l'individu doit être informé de plusieurs éléments lors de la collecte des renseignements personnels. Il en est de même lorsque son consentement doit être obtenu pour utiliser ou pour communiquer à un tiers un renseignement personnel qui le concerne. Enfin, la transparence quant à l'ensemble des

mesures prises par l'organisme public ou l'entreprise privée pour assurer la protection des renseignements personnels est essentielle pour démontrer la responsabilité de l'organisation.

Pour faire preuve de transparence, il s'agit d'indiquer avant toute utilisation de l'application, en termes simples et compréhensibles, mais complets :

- quels renseignements sont recueillis : énumérer tous les renseignements, incluant ceux qui seront inférés par un algorithme, le cas échéant. Une attention particulière doit être apportée à la qualification des renseignements : tel qu'indiqué précédemment, un renseignement dépersonnalisé n'est pas anonymisé.

- à quelles fins les renseignements seront utilisés : décrire tous les usages projetés et préciser quels renseignements seront utilisés pour chacun d'entre eux;

- si le recours à un traitement automatisé incluant l'utilisation d'un algorithme est prévu, expliquer les facteurs et les paramètres les plus importants qui mèneront à la prise d'une décision, à une prédiction ou à un profilage. Quelle est la logique du mécanisme de traitement automatisé utilisé pour cette analyse. Quels sont les renseignements personnels qui seront ainsi utilisés;

- qui aura accès à quels renseignements : être précis et indiquer en quoi est-ce nécessaire pour ces catégories de personne ou ces autres organismes ou entreprises d'avoir accès aux renseignements;

- à quel endroit seront conservés les renseignements;

- quelles sont les mesures mises en place pour assurer la confidentialité et la sécurité des renseignements personnels tout au long de leur cycle de vie;

- comment l'individu pourra-t-il exercer ses droits d'accès et de rectification aux renseignements personnels le concernant : désigner un responsable et indiquer ses coordonnées. Cette personne pourrait aussi répondre aux questions et aux préoccupations des individus quant à la protection accordée à leurs renseignements personnels par votre organisation.

4. Limiter l'utilisation et la communication des renseignements personnels

La législation applicable aux secteurs public et privé prévoit que les renseignements recueillis ne peuvent être utilisés qu'aux fins pour lesquels ils ont été recueillis ou à des fins compatibles. Compte tenu de la sensibilité des renseignements en cause dans plusieurs des applications utilisées dans le monde ou dont le développement est rapporté dans les médias actuellement et de leur niveau élevé d'intrusion dans la vie privée des citoyens ou d'atteinte à d'autres droits fondamentaux, l'utilisation des renseignements personnels devrait être limitée aux finalités déclarées lors de la collecte.

Ce principe invite aussi à dépersonnaliser ou à anonymiser les renseignements personnels chaque fois que cela est possible.

La législation prévoit aussi que les renseignements ne peuvent être communiqués à des tiers, sans le consentement de la personne concernée ou l'autorisation de la loi. Une communication à l'extérieur du Québec doit aussi respecter des obligations supplémentaires, notamment s'assurer

que les renseignements bénéficieront d'une protection équivalente à celle prévue selon la législation québécoise.

5. Le consentement

Plusieurs principes, essentiellement en lien avec nos valeurs démocratiques et les libertés et droits fondamentaux, militent en faveur de l'utilisation uniquement sur une base volontaire de ces différentes solutions technologiques lorsqu'il s'agit d'applications. Pour d'autres projets, par exemple s'il s'agit de communiquer des renseignements personnels, le consentement est généralement requis, à moins que la loi autorise cette communication.

Pour être valide, un consentement doit être :

- Libre : exprimé sans conditions, contraintes, menaces ou promesses. Une personne peut donc retirer son consentement en tout temps;
- Éclairé : donné en ayant conscience de sa portée, en toute connaissance de cause, d'où l'importance de la transparence;
- Spécifique : autorisant l'utilisation ou la communication d'un renseignement personnel donné, à des personnes données, à des fins données et à un moment donné. Si plusieurs utilisations ou communications sont prévues, chacune d'entre elles devrait faire l'objet d'un consentement distinct;
- Limité dans le temps : valide pour la durée requise à la réalisation des objectifs pour lesquels le consentement est demandé :
- Manifeste : exprimé de manière claire et non équivoque. S'il concerne des renseignements sensibles, il devrait être exprès, donc consigné par écrit.

Pour certaines applications dont ont fait état les médias, il est mentionné que leur efficacité est tributaire du degré d'utilisation des citoyens et que certaines mesures d'encouragement, voire une forme de pression sociale, seraient souhaitables. Ceci pourrait remettre en cause le caractère libre et éclairé du consentement et avoir un impact sur l'évaluation de la proportionnalité de la mesure par rapport à l'atteinte aux droits qu'elle constitue.

La possibilité que l'utilisation d'une application devienne, de facto, une condition d'entrée dans un immeuble, un commerce ou au travail doit être prise en considération. Cela inclut aussi les risques que certains exigent d'une personne utilisant l'application de consulter les renseignements personnels : degré de risque d'être infecté, symptômes déclarés, résultats de tests de dépistage du virus, recommandations de l'application, etc. En plus de remettre en cause la validité du consentement qui serait donné, le risque de déni de service ou de porter atteinte à d'autres droits est une considération importante de toute décision concernant le recours à ces applications.

6. Évaluer les impacts du recours à un système d'intelligence artificielle

Si le recours à un système d'intelligence artificielle (ou d'information automatisée) impliquant des renseignements personnels est envisagé, la Commission considère que certains principes doivent être mis en œuvre bien qu'ils ne soient pas présentement inclus dans la législation en cette matière au Québec, compte tenu de son caractère désuet.

Certains de ces principes ont été intégrés aux sections précédentes du présent document. Toutefois, d'autres mesures, notamment en matière de gouvernance et de responsabilité, devraient aussi être considérées. Par exemple, il pourrait être pertinent de réaliser une évaluation d'impact algorithmique d'un système automatisé que l'on envisage d'utiliser. Pour un exemple d'une telle évaluation, voir : https://www.canada.ca/fr/gouvernement/systeme/gouvernement-numerique/technologiques-modernes-nouveaux/utilisation-responsable-ai/evaluation-incidence-algorithmique.html.

Pour plus de détails au sujet de particularités et de principes de protection des renseignements personnels pertinents au recours à l'intelligence artificielle, le document de consultation de la Commission peut être consulté ici.

Bien que ces deux derniers documents n'en soient pas à leur version finale, ils peuvent contribuer à la réflexion.

6.1. Respecter les règles spécifiques applicables aux renseignements biométriques et aux données de géolocalisation

Géolocalisation :

L'article 43 de la *Loi concernant le cadre juridique des technologies de l'information* (RLRQ, c. C-1.1; ci-après la LCCJTI) limite l'utilisation d'un dispositif permettant de savoir où se trouve une personne, comme les données de géolocalisation : [...] « *À moins que la loi le prévoie expressément en vue de protéger la santé des personnes ou la sécurité publique, nul ne peut exiger qu'une personne soit liée à un dispositif qui permet de savoir où elle se trouve*. »

Un organisme public, une entreprise ou toute autre organisation qui envisage le recours à des mesures ou des caractéristiques biométriques pour atteindre l'objectif de prévenir la COVID-19 doit tenir compte du caractère particulier des renseignements biométriques.

Renseignements biométriques :

La biométrie désigne la technique qui permet d'associer à une identité une personne voulant procéder à une action grâce à la reconnaissance automatique d'une ou de plusieurs caractéristiques physiques et comportementales de cette personne qui ont été préalablement enregistrées.

Il existe deux grandes catégories de biométrie :

- la biométrie morphologique basée sur l'identification de traits physiques particuliers. Cette catégorie regroupe notamment la reconnaissance des empreintes digitales, la forme de la main, du visage, de la rétine et de l'iris de l'œil;
- la biométrie comportementale basée sur l'analyse de certains comportements d'une personne comme le tracé de sa signature, l'empreinte de sa voix, sa démarche, sa façon de taper sur un clavier, etc.

Qu'ils soient au format brut (image ou empreinte) ou numérique (code dérivé à partir d'un algorithme), il s'agit de renseignements personnels sensibles auxquels s'appliquent des règles

supplémentaires. Celles-ci sont prévues aux articles 43 à 45 de la *Loi concernant le cadre juridique des technologies de l'information*.

La Commission a publié des documents utiles pour toute initiative fondée sur la biométrie, parmi lesquels la fiche d'information *La biométrie au Québec* et le document *La biométrie au Québec : les principes d'application pour un choix éclairé*. D'autres outils d'information sont en préparation.

7. Détruire les renseignements personnels

Un renseignement personnel doit être détruit lorsque les fins pour lesquelles il a été recueilli sont accomplies. La sensibilité des renseignements de santé et de géolocalisation, renseignements généralement en cause dans les projets ayant fait l'objet d'articles dans les médias ou utilisés dans d'autres pays, et l'intrusion dans les droits et libertés fondamentales qu'ils représentent commandent une destruction de tout renseignement personnel recueilli et utilisé par celles-ci.

8. Permettre l'exercice de ces droits par la personne concernée

La loi prévoit qu'une personne a le droit d'avoir accès aux renseignements personnels qui la concernent et qu'elle peut les faire rectifier. Comment ce droit pourra être exercé au sujet des renseignements recueillis par les solutions envisagées, mais aussi ceux qui sont inférés notamment par un algorithme?

9. Encadrement, reddition de compte, contrôle externe indépendant et réévaluation

Toute mise en service d'une solution impliquant la collecte, l'utilisation ou la communication de renseignements personnels devrait aussi être assujettie à des mesures de gouvernance et soumise à une autorité de contrôle indépendante.

Les responsables de ces outils devraient rendre compte publiquement et régulièrement de l'efficacité :

- De cette mesure pour atteindre l'objectif sanitaire visé et de la pertinence de la maintenir en vigueur;
- Des mesures mises en place pour assurer la protection des renseignements personnels et pour minimiser l'intrusion dans la vie privée des personnes concernées.

CONCLUSION

Le présent document ne vise pas à énoncer l'ensemble des enjeux et des éléments à considérer dans l'évaluation de l'opportunité, de la légalité ou de l'efficacité de ces outils. Toutefois, la Commission souhaite soumettre ces principaux éléments pour considération. Elle réitère l'importance de ne pas faire l'économie de cette réflexion avant de décider d'aller de l'avant avec de tels outils. Ceux-ci ne peuvent être envisagés ni déployés sans l'assurance que la vie privée des citoyens sera respectée et que toutes les mesures sont en place pour assurer le respect de la législation applicable au Québec.

POUR POURSUIVRE LA RÉFLEXION…

Sans vouloir recenser ici toute l'information rendue disponible sur le sujet, les ressources suivantes sont également susceptibles de contribuer à la présente réflexion :

- Cadre de réflexion sur les enjeux éthiques liés à la pandémie de la COVID-19 : https://www.inspq.qc.ca/publications/2958
- Traçage des données mobiles dans la lutte contre le Covid-19 : Analyse des potentiels et des limites, par Mounir MAHJOUBI : http://d.mounirmahjoubi.fr/TracageDonneesMobilesCovidV1.pdf. Pour un résumé : https://medium.com/@mounir/tra%C3%A7age-des-donn%C3%A9es-mobiles-dans-la-lutte-contre-le-covid-19-e718b1e15dfb
- Recommandation de la Commission européenne sur l'utilisation d'une boîte à outils commune concernant notamment l'utilisation de données de géolocalisation et d'applications mobiles : https://ec.europa.eu/info/sites/info/files/recommendation_on_apps_for_contact_tracing_4.pdf
- Lettre du 14 avril 2020 du Comité européen de la Protection des Données concernant une ébauche de guide au sujet du recours à des applications dans le contexte de la COVID-19: https://edpb.europa.eu/sites/edpb/files/files/file1/edpbletterecadvisecodiv-appguidance_final.pdf
- Site de la CDPDJ : http://www.cdpdj.qc.ca/fr/COVID-19/Pages/FAQ-Charte.aspx.
- Lettre de scientifiques et spécialistes allemands provenant de disciplines diverses : http://allai.nl/wp-content/uploads/2020/04/Online-version-Letter-to-President-Rutte-Ministers-De-Jonge-Van-Rijn-Grapperhaus-re.-COVID-19-apps.pdf