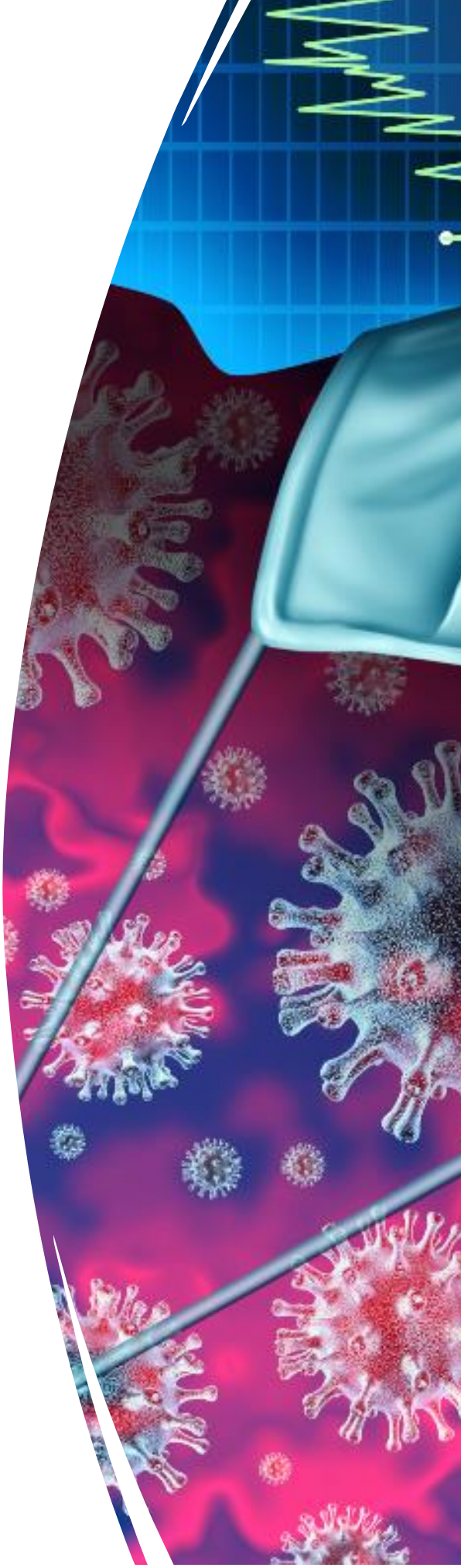
CHAIRE FINTECH
AMF-Finance Montréal
ESG UQÀM



CAHIER DE RECHERCHE DE LA CHAIRE FINTECH AMF – FINANCE MONTRÉAL

Open Banking et utilisation des données des consommateurs en contexte de Covid 19 : quel encadrement juridique ?

Par Arthur Oulaï
Patrick Mignault
Université de Sherbrooke
Serge Kablan
Université Laval

Mars 2022

Projet réalisé dans le cadre du 1er appel de projets de la Chaire « Les Fintechs et la COVID-19 »

CHAPITRE 8

L'exigence du consentement en matière de protection des données personnelles du consommateur québécois : regard sur les modifications récentes*

Arthur Oulaï
Université de Sherbrooke

Serge Kablan
Université Laval

Patrick Mignault
Université de Sherbrooke

INTRODUCTION

Les relations établies entre les consommateurs et les commerçants ouvrent des espaces de réalisation de nombreuses transactions portant sur des biens et services. Ces relations représentent également des occasions pour obtenir de précieuses informations sur ces consommateurs, informations dont l'importance et la valeur ne font plus de doute. L'association de défense des droits des consommateurs, Option consommateurs, a publié en avril 2013 un rapport de recherche consacré à la protection de la vie privée des consommateurs[1]. Ce rapport présenté au Commissariat à la protection de la vie privée du Canada établissait comme un enjeu majeur la convoitise suscitée par les renseignements personnels des consommateurs. La *Loi sur la protection des renseignements personnels*

* Cet article a bénéficié du soutien financier de la Chaire FinTech AMF – Finance Montréal

et les documents électroniques (ci-après, « loi fédérale »)[2] définit le renseignement personnel comme « tout renseignement concernant un individu identifiable » (article 2(1)). Au Québec, la *Loi sur la protection des renseignements personnels dans le secteur privé* (ci-après, « loi québécoise »)[3] présente celui-ci comme « tout renseignement qui concerne une personne physique et permet de l'identifier » (article 2). En Europe, où l'expression *données à caractère personnel* est privilégiée, celle-ci est décrite à l'article 4 1) du *Règlement général sur la protection des données* (ci-après, « RGPD »)[4] comme « toute information se rapportant à une personne physique identifiée ou identifiable ». Cette disposition fait la précision suivante : « est réputée être une "personne physique identifiable" une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ». Sous l'influence du RGPD, la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* intègre à la définition québécoise du renseignement personnel les termes *directement ou indirectement.* L'ensemble de ces définitions montre un spectre très large de la notion de renseignement ou de donnée à caractère personnel (dans la suite de notre texte, ces notions sont utilisées sans distinction)[5]. Non seulement ces définitions se rapportent à l'identité de la personne physique, mais elles concernent aussi tout ce qui permet de la singulariser, notamment dans son comportement[6].

Les données, en général, se sont retrouvées au cœur de l'innovation technologique et des échanges socio-économiques, captant même l'attention d'acteurs aussi traditionnels que les institutions d'enseignement, dont on voit des curriculums proposer l'initiation au forage de données, c'est-à-dire au « [p]rocessus de recherche et d'analyse qui permet de trouver des corrélations cachées ou des informations nouvelles, ou encore, de dégager certaines tendances [par exemple, dans les ventes d'un magasin][7] ». Quand il s'étend aux données personnelles du consommateur, cet intérêt pour les données multiplie inévitablement les risques d'atteinte à la vie privée et peut rendre nécessaire le renforcement des protections initiales. Mais comment faire cohabiter l'objectif de protection de ces données avec celui de leur circulation et de leur mise en valeur ? En 1993, le Québec fut la première juridiction au Canada à légiférer pour protéger les renseignements personnels. La loi fédérale a été adoptée quelques années plus tard. Au fil des années, la protection prévue par ces deux textes a été mise à l'épreuve

par des phénomènes comme le ciblage publicitaire et l'intelligence artificielle. À travers le monde, l'appel à une mise à jour du cadre juridique portant sur le traitement des données personnelles se fait entendre. L'Europe y a répondu avec le RGPD qui, tant par les mesures qu'il prévoit que par sa portée extraterritoriale, est devenu emblématique des nouvelles tendances en matière de protection des données personnelles.

Ce RGPD, adopté en 2016 et entré en vigueur à partir du 25 mai 2018, marque un renforcement de la protection par la sévérité des sanctions qu'il prévoit et par les nombreuses mesures imposées aux organisations. En juin 2020, le gouvernement québécois a déposé le projet de *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (ci-après, « projet de loi 64 »). Après quelques amendements à l'automne 2021, ce projet de loi a été adopté pour modifier notamment la loi québécoise. Il a été sanctionné le 22 septembre 2021 (ci-après, « loi 64 ») et son entrée en vigueur sera complétée en 2024. Du côté fédéral, le gouvernement a déposé en novembre 2020 son projet de *Loi de 2020 sur la mise en œuvre de la Charte du numérique* (ci-après, « projet de loi C-11 »). Même si l'issue du projet de loi fédéral reste incertaine compte tenu du contexte politique, ses dispositions seront tout de même étudiées dans ce texte afin d'observer les grandes tendances en matière de protection des renseignements personnels.

Passer en revue l'ensemble des mesures de ces nouveaux textes nécessiterait une publication beaucoup plus ambitieuse que la présente contribution. Dans ce texte, nous avons donc choisi de limiter nos propos au consentement, une mesure devenue incontournable dans les lois sur la protection des renseignements personnels, en faisant ressortir les modifications adoptées au Québec et celles proposées au fédéral à la lumière du RGPD. En donnant à la personne concernée le contrôle de ses renseignements personnels, l'exigence du consentement est porteuse d'une certaine prétention consumériste. Si le consentement est soumis à des conditions de validité (1), les dispositions le concernant ouvrent la porte à une utilisation des données personnelles sans ce consentement (2). Ce sont ces conditions de validité du consentement et ces ouvertures que cette contribution entend examiner avec le RGPD européen comme toile de fond. Nous ciblons le consommateur sans prétendre que les textes étudiés lui sont exclusifs.

1. LE TRAITEMENT DES DONNÉES PERSONNELLES AVEC LE CONSENTEMENT DU CONSOMMATEUR

Dans le contexte du traitement des données à caractère personnel (entendu globalement de la collecte, la détention, l'utilisation ou la communication de ces données), les dispositions québécoises et canadiennes s'inscrivent dans la tendance générale des textes qui exigent le consentement du consommateur ou de la personne dont les données personnelles sont en jeu. À cet égard, le principe 4.3 de l'annexe 1 de la loi fédérale prévoit que « [t]oute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire ». L'article 6.1 de la même loi poursuit en précisant que « [p]our l'application de l'article 4.3 de l'annexe 1, le consentement de l'intéressé n'est valable que s'il est raisonnable de s'attendre à ce qu'un individu visé par les activités de l'organisation comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles il a consenti[8] ». L'article 14 de la loi québécoise prévoit pour sa part que « [l]e consentement à la collecte, à la communication ou à l'utilisation d'un renseignement personnel doit être manifeste, libre, éclairé et être donné à des fins spécifiques ». En se rapprochant de l'article 4, paragraphe 11 du RGPD qui définit le consentement comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque », la loi 64 reprend les termes de l'article 14 de la loi québécoise et ajoute que la demande de consentement pour chacune des fins spécifiques doit être formulée en des « termes simples et clairs. Lorsque la demande de consentement est faite par écrit, elle doit être présentée distinctement de toute autre information communiquée à la personne concernée[9] ». L'ensemble de ces dispositions évoque des conditions de validité du consentement qui traduisent deux préoccupations : l'une vise à éclairer ce consentement (section 1.1.) ; l'autre, en deux volets, permet de s'assurer que la manifestation de volonté est le fruit d'un véritable choix de son auteur, qu'elle est envisagée en toute transparence (section 1.2) et suivant les formes prescrites (section 1.3).

1.1 Un consentement éclairé

L'exigence est classique, comme en droit des contrats : le consentement doit être précédé de l'information qui permet d'éclairer la manifestation de volonté. La loi 64 reprend bel et bien cette exigence actuelle des lois

québécoise[10] et fédérale[11], mais il la renforce. Il s'agit ici de s'assurer que la personne dont les données personnelles sont sollicitées dispose, avant de donner son consentement, des informations qui lui permettent de saisir l'étendue de son acceptation. L'attention est portée sur deux éléments, soit la détermination des informations jugées importantes pour un consentement éclairé et la manière de les formuler ou de les faire connaître[12]. Les informations jugées importantes portent en général sur « la nature, les fins et les conséquences de ce à quoi [le consommateur] consent[13] ». Il est acquis que les politiques et les pratiques de gestion des renseignements personnels de l'organisation font partie des éléments dont la divulgation est requise[14].

Au demeurant, la loi 64 prévoit de bonifier le droit à l'information du consommateur de l'article 8 de la loi québécoise en prévoyant que toute personne qui recueille des renseignements personnels doit donner à la personne concernée l'information relative aux fins de la collecte, de même que les moyens utilisés pour ce faire. Elle doit aussi l'informer de l'existence des droits d'accès, de rectification, de retrait du consentement à la communication ou à l'utilisation des renseignements collectés et de la possibilité, si celle-ci existe, d'une communication de ces renseignements à l'extérieur du Québec. Lorsque la collecte est effectuée pour le compte d'un tiers, le nom de ce dernier doit également être divulgué[15]. À la différence du projet de loi C-11, qui impose d'emblée la divulgation du type de renseignement personnel collecté[16], la loi 64 précise que cette information est communiquée sur demande de la personne dont les renseignements personnels sont recueillis. Cette dernière pourra aussi réclamer la divulgation des catégories de personnes qui ont accès à ces renseignements au sein de l'entreprise, la durée de conservation de ces renseignements et les coordonnées de la personne responsable de la protection des renseignements personnels[17]. D'autres informations s'ajoutent à cette énumération lorsque l'entreprise qui collecte les renseignements fait appel à une technologie qui utilise des fonctions d'identification, de localisation ou de profilage[18]. Il faudrait alors préalablement informer le consommateur « du recours à une telle technologie [et] des moyens offerts pour activer les fonctions permettant d'identifier, de localiser ou d'effectuer un profilage[19] ». L'on retrouve en grande partie ces éléments, dont la divulgation est exigée, dans le projet fédéral, lequel prend toutefois le soin d'ajouter l'obligation de fournir des informations sur « les conséquences raisonnablement prévisibles de la collecte, de l'utilisation ou de la communication des renseignements personnels[20] ».

Même renforcé, le contenu de cette obligation d'information n'est pas inédit. Les textes européens le mentionnaient déjà[21]. Dans une perspective de protection du consommateur, il faut résister à la tentation d'épaissir ce contenu en voulant prévenir des risques putatifs ou avérés d'atteinte à la vie privée. La protection du consommateur commande par préférence de s'en tenir à des éléments jugés essentiels, car la surcharge informationnelle peut produire l'effet contraire, c'est-à-dire décourager la prise de connaissance de ce qui est communiqué[22]. Les textes québécois et fédéral semblent soucieux de cet enjeu et évitent les formules qui peuvent suggérer une énumération indicative ou non exhaustive.

Concernant la manière de faire connaître l'information nécessaire au consentement, le projet de loi C-11 exige une divulgation dans « un langage clair[23] ». La loi 64, comme les textes européens, prévoit quant à elle que la demande de consentement doit être formulée « en termes simples et clairs[24] ». De telles formulations visent à apporter une solution au problème connu de la divulgation des informations dans de longs textes et dans un langage complexe, truffé de termes technico-juridiques souvent indéchiffrables pour le consommateur moyen. Mais il faut décoder, surtout à la lumière de la formulation du projet de loi fédéral, une intention qui pourrait dépasser le simple bannissement du jargon technique. D'une part, le langage clair s'apparente à une méthode de rédaction intégrale[25] ; d'autre part, il est un des outils de promotion de la protection du consommateur, en particulier dans le contexte des transactions électroniques[26]. Le langage clair en matière consumériste invite ainsi à concevoir et à rédiger tout texte en fonction de son destinataire, le consommateur notamment[27], ce qui rejaillit sur l'ensemble du texte, soit sa structure, son apparence, le contexte de son utilisation, la clarté de l'information qu'il véhicule, etc. Il en va de son intelligibilité, de sa lisibilité et de son utilité pour le destinataire[28].

Par ailleurs, si l'objectif de clarté de l'information suppose la compréhension de celle-ci, son accessibilité doit aussi être assurée[29]. C'est ainsi qu'il faut comprendre l'exigence formulée dans la loi 64, lorsque la demande de consentement est faite par écrit, de présenter cette demande distinctement de toute autre information communiquée au consommateur[30]. Le législateur n'impose pas cette exigence dans les autres cas. En pratique, cela peut impliquer une désignation spécifique de la demande écrite de consentement[31]. Les *Lignes directrices 5/2020 sur le consentement au sens du règlement (UE) 2016/679* précisent : « [l]e consentement doit être clair et se distinguer des autres questions, et doit être présenté sous une forme compréhensible et aisément accessible. Cette exigence signifie

essentiellement que les informations nécessaires à une prise de décision éclairée concernant le consentement ne peuvent être cachées dans des conditions générales[32] ». Une garantie supplémentaire est prévue pour confirmer que les informations sont bien comprises par le destinataire : ce dernier pourra, s'il le souhaite, demander l'assistance de l'entité qui sollicite son consentement afin de l'éclairer[33]. Au fédéral aussi, le destinataire doit pouvoir saisir la portée de son consentement. C'est une condition de validité du consentement qui est prévue à l'article 6.1 de la loi fédérale. Selon cette disposition, « le consentement de l'intéressé n'est valable que s'il est raisonnable de s'attendre à ce qu'un individu visé par les activités de l'organisation comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles il a consenti ». Cette exigence n'est toutefois pas reprise dans la formulation retenue par l'article 15(3) du projet de loi C-11. Le Commissaire à la protection de la vie privée du Canada y voit un recul en matière de protection du consommateur, estimant que l'obligation d'information à elle seule est insuffisante pour assurer une telle protection[34].

En somme, si la « méthode » du langage clair parvient à guider la rédaction des textes relatifs à la protection des renseignements personnels, il devrait en résulter un assainissement des pratiques rédactionnelles dans ce domaine. Malgré les efforts des autorités, la lecture à l'écran reste un défi pour le consommateur. La Commission d'accès à l'information du Québec avait fait ce constat dans son rapport quinquennal publié en 2011. Elle y recommandait la rédaction de politiques de confidentialité simplifiées et le recours à des pictogrammes comme moyen de divulgation de l'information nécessaire au consentement. Elle faisait écho à l'adage voulant qu'une image vaut mille mots[35]. Le Commissariat à la protection de la vie privée du Canada souscrit à l'idée et présente les icônes comme une des solutions visant à améliorer le consentement[36]. Cette solution figure dans le RGPD et ouvre la voie à la cohabitation entre une formulation de l'information en des termes clairs et simples et le recours à des éléments visuels[37]. Le texte européen précise que les « […] informations peuvent être fournies accompagnées d'icônes normalisées afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible du traitement prévu[38] ». La doctrine avait vu également dans ce procédé une avenue pour satisfaire le critère de la divulgation adéquate, suffisante et raisonnable dégagé de la jurisprudence en matière de contrat électronique[39]. Or, ce passage du RGPD précité met en évidence deux éléments. Le premier indique que les pictogrammes ne se substituent pas au format

textuel des politiques applicables, mais en sont un complément ; en pratique, le consommateur doit pouvoir accéder aux textes correspondant aux pictogrammes[40]. Le second élément met en évidence l'enjeu de la standardisation dont est tributaire le succès du recours aux pictogrammes comme outil de divulgation de l'information. Par souci de cohérence, les mêmes pictogrammes devraient mener aux mêmes informations. En cela, l'apport de la Commission d'accès à l'information du Québec et du Commissariat à la protection de la vie privée du Canada, dans l'effort de standardisation, pourrait être déterminant. Au même degré que le consentement éclairé, l'attention du législateur est portée sur la manifestation du consentement.

1.2 Un consentement libre et donné à des fins spécifiques

Tant sous la loi québécoise que sous la loi fédérale, le consentement au traitement des données personnelles doit être libre, c'est-à-dire que sa manifestation doit être le fruit d'un véritable choix de son auteur[41]. Dans le cadre particulier des activités en ligne, le consommateur doit pouvoir refuser de donner son consentement sans subir de préjudices[42]. L'article 7(4) du RGPD mentionne qu'« [a]u moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement des données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat ». Autrement dit, si le traitement des données personnelles du consommateur est nécessaire à l'exécution du contrat ou à la prestation de service, le consentement que ce dernier doit donner ne peut être considéré comme contraint, puisque sans un tel consentement, le contrat ou le service devient impossible. De même, l'article 15(5) du projet fédéral précise que « [l]'organisation ne peut, pour le motif qu'elle fournit un bien ou un service, exiger d'un individu qu'il consente à la collecte, à l'utilisation ou à la communication de renseignements personnels qui ne sont pas nécessaires à la fourniture du bien ou du service ». Le lien entre l'opération relative aux données personnelles et la prestation de services ou l'exécution du contrat doit être direct et objectif[43]. Par ailleurs, pour être libre, le consentement ne doit pas avoir été obtenu par des pratiques trompeuses ou mensongères[44].

L'exigence du consentement dit spécifique, déjà prévue par les lois québécoise[45] et canadienne[46] et reconduite dans les nouveaux textes des deux paliers de gouvernements, est clairement posée dans le nouvel article

14 québécois qui prévoit que le consentement doit être donné à des fins spécifiques[47]. L'utilisation des données du consommateur doit être restreinte à ces seules fins. Une utilisation pour d'autres fins est soumise à l'obtention d'un consentement distinct[48]. Une pluralité de finalités doit faire l'objet d'un consentement séparé pour chacune d'elles. Il en va de même pour l'ajout de nouvelles finalités ou pour toute modification apportée à ces finalités[49]. Pour le consommateur, l'exigence du consentement spécifique est une assurance contre l'utilisation inattendue de ses données personnelles[50]. L'objectif de protection du consommateur conduit également à une « séparation claire des informations liées à l'obtention du consentement au traitement des données et des informations concernant d'autres sujets[51] ». À cet égard, la nouvelle mouture de l'article 14 de la loi québécoise, en plus de prévoir une demande de consentement pour chaque finalité identifiée, exige qu'une telle demande de consentement, lorsqu'elle est faite par écrit, soit formulée séparément de toute autre information communiquée au consommateur. La combinaison de ces deux exigences semble donc mener à l'interdiction des pratiques privilégiant un consentement en bloc pour des finalités distinctes[52]. Qu'en est-il, toutefois, de la possibilité d'obtenir un consentement en bloc pour plusieurs finalités proches ou liées ? En d'autres termes, faut-il voir dans la formulation de l'article 14 le triptyque suivant : une finalité ; une demande de consentement ; un consentement ? Au contraire, est-il possible de regrouper plusieurs finalités proches (similaires) dans une même demande pouvant déboucher sur un seul consentement ? La formulation actuelle de l'article 14 n'écarte pas la possibilité d'un consentement pour plusieurs finalités. Il semble que seule la demande de consentement par écrit est astreinte à une communication distincte de toute autre information adressée au consommateur[53]. Si cette dernière interprétation devait prévaloir, on pourrait y déceler la prépondérance donnée à l'information du consommateur, mais avec la crainte d'une surcharge informationnelle que la « méthode » du langage clair ne saurait à elle seule dissiper. Il faut alors craindre une diminution de la protection du consommateur. Cela dit, la préoccupation pour la protection du consommateur concerne aussi la forme du consentement.

1.3 La forme du consentement

La manière d'exprimer le consentement soulève la question de la forme que devrait prendre ce consentement pour qu'il soit considéré comme juridiquement valide. Sous la loi québécoise, il est bien établi à

l'article 14 que le consentement du consommateur doit être manifeste[54]. De façon générale, le consommateur manifeste explicitement son consentement en posant un acte clair qui exprime son acquiescement ou en faisant une déclaration ayant le même effet[55]. Il s'agit, par exemple, de cocher une case sur un site Web ou de soumettre une déclaration écrite grâce à un formulaire électronique ou à un courriel[56]. Quant à la loi fédérale, elle se montre plus souple sur la forme du consentement, en ajoutant la possibilité d'un consentement implicite et en précisant que la forme, explicite ou implicite, dépend des circonstances et de la nature des renseignements en cause[57]. Il demeure toutefois, selon certains auteurs, que le consentement implicite tient de l'exception, la règle étant celle de la forme explicite du consentement[58]. En fait, sous la loi fédérale, deux éléments doivent être pris en compte afin de déterminer la forme appropriée du consentement, soit la sensibilité des renseignements et les attentes raisonnables de la personne[59] dont les renseignements vont être collectés. Lorsque des renseignements sensibles sont concernés, l'organisation qui les collecte doit privilégier l'obtention d'un consentement explicite[60]. Dans la loi canadienne, « tous les renseignements peuvent devenir sensibles suivant le contexte », tandis que des renseignements tels que les dossiers médicaux et les documents de nature financière sont presque toujours considérés comme sensibles. Le projet de loi fédéral confirme son ouverture aux deux formes du consentement, mais en posant clairement le principe selon lequel le consentement doit être obtenu expressément ; le consentement implicite reste l'exception[61]. L'article 15(4) ajoute ceci : « compte tenu de la nature délicate des renseignements personnels qu'elle a l'intention de recueillir, d'utiliser ou de communiquer et des attentes raisonnables de l'individu concerné, une organisation peut conclure que le consentement implicite de l'individu est approprié ». Le consentement implicite est toutefois interdit, d'une part, dans les cas de collecte et d'utilisation de l'adresse électronique d'une personne « à l'aide d'un programme d'ordinateur conçu ou mis en marché principalement pour produire ou rechercher des adresses électroniques et les recueillir […] » et, d'autre part, lorsque les renseignements personnels sont collectés au moyen d'un ordinateur en violation d'une loi fédérale[62].

La loi 64 semble désormais ouvrir la porte au consentement implicite, puisque les nouveaux articles 12 et 13 imposent la manifestation expresse du consentement dans le cas d'un renseignement personnel sensible, de sorte qu'une expression implicite de ce consentement pourrait suffire pour les autres types de renseignements. Ce faisant, le gouvernement répond aux appels à une reconnaissance formelle de la forme implicite

du consentement en droit québécois[63]. Il rejoint ainsi la tendance générale à la reconnaissance des deux formes de consentement dans la protection des données personnelles telle qu'elle est observée au fédéral et sous le RGPD. Ce dernier retient également la forme explicite du consentement pour le traitement des données sensibles[64], pour toute décision individuelle fondée exclusivement sur un traitement automatisé, y compris le profilage[65] et pour le transfert des données vers des pays tiers qui n'offrent pas de protection équivalente à celle du RGPD[66]. Il importe par ailleurs de souligner que le RGPD a le mérite d'identifier précisément les données sensibles. Son article 9 définit le traitement de ces données comme celui qui « révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique ». La Commission d'accès à l'information a repris en grande partie cette définition dans son rapport quinquennal de 2016[67]. La version finale de la loi 64 se rapproche davantage du texte fédéral que du RGPD en définissant le renseignement personnel sensible en considération de sa nature et de son contexte. En effet, selon l'article 102 (nouvel article 12, al. 4, paragraphe 2 de la loi québécoise), un renseignement personnel est « sensible lorsque, de par sa nature notamment médicale, biométrique ou autrement intime, ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée ».

De ce qui précède, retenons que les conditions de validité du consentement relatif au traitement des données personnelles s'inscrivent dans une perspective de protection du consommateur, dont l'utilité n'est plus à démontrer. Mais l'exigence du consentement doit également tenir compte de l'importance grandissante de ces données pour le développement économique, social, technologique, scientifique, etc. On n'ose pas insinuer que l'exigence du consentement peut saper ce développement, mais l'idée de l'atténuer pour optimiser le flux des données est envisagée et elle doit être discutée.

2. LE TRAITEMENT DES DONNÉES PERSONNELLES SANS LE CONSENTEMENT DU CONSOMMATEUR

La possibilité d'un traitement des données personnelles à l'insu du consommateur ou sans son consentement découle des exceptions prévues par les différents textes. Elle fonde aussi les critiques contre les modalités du consentement, voire contre la place prépondérante qui lui est reconnue.

2.1 Les exceptions au consentement

Le projet de loi fédéral propose de redéfinir les exceptions au consentement à la collecte ou l'utilisation des renseignements personnels aux articles 7 et suivants de la loi fédérale. Il prévoit, à son article 18(1), la possibilité pour une organisation de collecter ou d'utiliser les renseignements personnels d'un individu sans son consentement ou à son insu. Cette possibilité est toutefois encadrée. L'organisation est dispensée de l'obligation d'obtenir le consentement de l'individu si la collecte des renseignements ou leur utilisation « est faite en vue d'une activité d'affaires ». Le projet de loi fait une énumération des activités d'affaires visées. Il s'agit :

> [des] activités nécessaires à la fourniture ou à la livraison d'un produit ou à la prestation d'un service demandé par l'individu à l'organisation ; [des] activités menées à des fins de diligence raisonnable pour réduire ou prévenir les risques commerciaux de l'organisation ; [des] activités nécessaires à la sécurité de l'information, des systèmes ou des réseaux de l'organisation ; [des] activités nécessaires pour assurer la sécurité d'un produit ou d'un service que l'organisation fournit ou livre ; [et des] activités dans le cadre desquelles il est pratiquement impossible pour l'organisation d'obtenir le consentement de l'individu, en raison de l'absence de lien direct avec celle-ci[68].

Cette énumération n'est pas exhaustive, puisque le projet de loi prévoit des ajouts par règlement. L'inscription dans la liste des activités d'affaires visées s'accompagne de deux autres conditions : d'une part, une personne raisonnable doit s'attendre à une telle collecte ou utilisation de ses renseignements personnels ; d'autre part, ces renseignements ne doivent pas être recueillis ou utilisés en vue d'influencer le comportement ou les décisions de l'individu[69].

De nombreuses autres exceptions sont prévues par le projet de loi. Par exemple, le transfert des renseignements personnels à des fournisseurs de services[70] et l'opération de dépersonnalisation des renseignements d'un individu peuvent être entrepris sans le consentement de ce dernier[71]. L'utilisation de renseignements personnels à des fins de recherche et de

développement interne d'une organisation peut être également réalisée sans le consentement de la personne concernée, à condition que de tels renseignements soient dépersonnalisés avant leur utilisation[72].

Du côté québécois, l'article 6 de la loi actuelle (qui n'est pas affecté par la loi 64), prévoit que la *collecte* des renseignements personnels doit être effectuée auprès de la personne concernée. Cette dernière peut donner son consentement à la collecte auprès d'un tiers. Il est aussi possible de collecter les renseignements auprès d'un tiers sans le consentement de la personne concernée dans les cas permis par la loi ou lorsque la personne qui collecte ces renseignements a un intérêt sérieux et légitime[73]. Le projet de loi 64 a ajouté de nouvelles exceptions, cette fois en ce qui regarde l'*utilisation* de renseignements personnels déjà collectés. Il permet l'utilisation des renseignements personnels d'un individu pour des fins différentes de celles pour lesquelles ils ont été collectés sans être tenus d'obtenir le consentement de cet individu. Dans le premier cas, l'utilisation doit être faite à des fins compatibles avec celles pour lesquelles les renseignements ont été collectés. L'exigence de compatibilité suppose un lien pertinent et direct avec les fins de la collecte initiale. Le texte québécois écarte la prospection commerciale ou philanthropique des fins considérées comme compatibles. Dans le deuxième cas, l'utilisation des renseignements personnels sans le consentement d'un individu est autorisée si une telle utilisation est manifestement au bénéfice de ce dernier. L'utilisation des renseignements personnels à des fins d'étude, de recherche ou de production de statistiques n'est pas non plus soumise à l'exigence du consentement. Les renseignements doivent, dans ce dernier cas, être dépersonnalisés, c'est-à-dire qu'ils ne doivent plus permettre d'identifier directement la personne concernée[74].

Lors des débats parlementaires, un premier amendement à ce dispositif ajoutait que l'utilisation des renseignements personnels sans le consentement de la personne concernée était permise « 2.1° lorsque [cette] utilisation est nécessaire aux fins des pratiques administratives courantes de l'entreprise ». Ces pratiques administratives courantes de l'entreprise étaient ainsi définies :

> 1° la fourniture ou la livraison d'un produit ou la prestation d'un service demandé par la personne concernée ;
>
> 2° la prévention et la détection de la fraude ;
>
> 3° l'évaluation et l'amélioration des mesures de protection et de sécurité ;

> 4° la planification, la gestion, l'évaluation ou le contrôle des ressources ou des services de l'entreprise ;
>
> 5° d'établir, de gérer ou de mettre fin à une relation d'emploi entre la personne concernée et l'entreprise ;
>
> 6° toute autre pratique administrative courante prescrite par règlement. »

La version finale de la loi 64 restreint la portée de cet amendement en ne retenant que les paragraphes 1 à 3 du premier amendement à l'intérieur des paragraphes 2.1 et 2.2 de l'al. 2 du nouvel article 12 de la loi 64 :

> « 2.1° lorsque son utilisation est nécessaire à des fins de prévention et de détection de la fraude ou d'évaluation et d'amélioration des mesures de protection et de sécurité ;
>
> 2.2° lorsque son utilisation est nécessaire à des fins de fourniture ou de livraison d'un produit ou de prestation d'un service demandé par la personne concernée ; ».

On peut donc retenir que la possibilité d'ajouter par règlement d'autres pratiques administratives courantes a été définitivement écartée par le législateur.

Par ailleurs, la loi 64 vient revoir les situations où des renseignements personnels peuvent être *communiqués* à des tiers sans le consentement de la personne concernée en vertu des articles 18 et suivants. Parmi ceux-ci, l'exception concernant le consentement donné dans le cadre d'une transaction commerciale mérite d'être soulignée, puisqu'elle permet au Québec de rejoindre les textes fédéraux en la matière. Il sera désormais permis à une entreprise, en vertu de l'article 18.4 de la loi 64, de communiquer à l'autre partie, dans le cadre d'une transaction commerciale[75], tout renseignement personnel utile à la conclusion de ladite transaction, sans être tenu d'obtenir le consentement de la personne concernée. La disposition impose, pour ce faire, la conclusion d'une entente visant à garantir la protection des données personnelles en cause. Le projet québécois, tout comme le projet fédéral, permet également à une entreprise de communiquer des données personnelles à un mandataire ou à un prestataire de services sans consentement[76].

Malgré ces exceptions au consentement, les nouveaux textes, en particulier le projet de loi québécois, restent soumis aux critiques, dont certaines proposent l'admission franche d'autres bases juridiques de traitement des renseignements personnels.

2.2 La protection des renseignements personnels au-delà du consentement

Comme il a déjà été précisé, en exigeant le consentement pour le traitement des renseignements personnels, on entend généralement assurer au consommateur ou à la personne concernée un contrôle sur ces renseignements. Mais la réalité de ce contrôle est douteuse, surtout relativement à la multiplication des outils numériques et à la démocratisation de l'intelligence artificielle (ci-après, « IA »). L'Observatoire international sur les impacts sociétaux de l'IA et du numérique a déjà fait remarquer que « [l]e consentement semble plus ou moins bien adapté à la quantité et à la variété de traitements de renseignements personnels qui sont traités par des systèmes d'intelligence artificielle. De plus, l'opacité derrière les traitements de données, ainsi que l'utilisation de données pour des fins autres que celles pour lesquelles la personne a consenti (un traitement de renseignements personnels peut en cacher un autre), ou encore l'utilisation de données personnelles générées par des personnes qui ne connaissent même pas l'existence de ces données, rendent l'application efficace du consentement problématique[77] ». Lors de l'examen du projet de loi 64, les dispositions sur le consentement se sont retrouvées parmi celles qui ont suscité de nombreux commentaires et à l'égard desquelles des réticences ont été exprimées. L'un des reproches tient à la rigidité du texte par rapport au projet de loi fédéral, même s'il semble ouvrir désormais la porte au consentement implicite. En général, l'obligation d'obtenir un consentement distinct préalable au traitement des données personnelles[78] est perçue comme inadaptée au contexte actuel des technologies de l'information[79], lequel est marqué par la profusion des données, dont le flux incessant est alimenté autant par notre empreinte numérique routinière que par celle de nos innombrables objets connectés. La collecte enfarinée de ces données en vue de leur valorisation est une tentation à laquelle il peut être difficile de résister. Dans ce contexte, exiger un consentement pour chaque fin spécifique peut devenir fastidieux pour un consommateur trop souvent sollicité, avec le risque de l'exposer à ce que plusieurs appellent la « fatigue du consentement » (ou *consent fatigue*)[80]. La multiplication des demandes de consentement pourrait ainsi nuire à l'objectif de protection du consommateur. Les exigences québécoises sur le consentement semblent même plus contraignantes que celles du RGPD dont elles s'inspirent[81]. Il faut craindre ici une multiplication des demandes de consentement qui pourrait nuire à l'objectif de protection du consommateur. En outre, l'exigence d'un consentement distinct pour chaque finalité spécifique pourrait être

difficilement conciliable avec l'hypothèse du consentement implicite à laquelle la loi 64 semble ouvrir désormais la porte au Québec[82].

Pour revenir sur la rigueur reprochée aux exigences québécoises par rapport au RGPD, il faut remarquer que la critique peut sembler surprenante à première vue, dans la mesure où la loi 64 reprend dans sa définition du consentement (article 14) les termes de l'article 4 du RGPD. Il importe cependant de préciser que, si le texte européen impose des conditions de validité du consentement particulièrement sévères[83], cette exigence n'occupe pas la place centrale observée dans le texte québécois : « […] il est faux de croire que le RGPD impose de systématiser le consentement. Au contraire, en tant que base de licéité, le consentement est plutôt rare[84] ». Dans son mémoire concernant le projet de loi 64, le Barreau du Québec, après avoir fait le constat que « […] le consentement manifeste, libre, éclairé et donné à des fins spécifiques constitue la pierre angulaire permettant l'utilisation de renseignements personnels[85] », rappelle sa position en cette matière ; à l'image du RGPD, cette position recommande de prévoir d'autres bases juridiques sur lesquelles la collecte et l'utilisation des renseignements personnels pourraient se fonder[86]. À cet égard, l'article 6 du RGPD dispose :

> Le traitement n'est licite que si, et dans la mesure où, au moins une des conditions suivantes est remplie :
>
> a. le personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
>
> b. le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
>
> c. le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
>
> d. le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
>
> e. le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
>
> f. le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

La sixième base de licéité du traitement prévue par le RGPD (point f) a retenu l'attention au Québec, certains souhaitant son introduction en droit québécois. La Commission d'accès à l'information émet toutefois des réserves relativement à une telle proposition. Elle précise tout d'abord que « […] le consentement n'est pas la principale ou seule base juridique permettant actuellement à une entreprise de recueillir, d'utiliser ou de communiquer des renseignements personnels[87] » au Québec. La Commission rappelle les exigences traditionnelles : concernant la collecte, la loi fait obligation à l'entreprise d'avoir un intérêt sérieux et légitime ; elle doit déterminer également les fins de la collecte et divulguer l'information sur ses finalités ; la collecte elle-même doit se limiter aux seules données nécessaires aux finalités qui ont été préalablement déterminées ; par ailleurs, les dispositions législatives présentement en vigueur permettent une utilisation des données pour « toute autre fin pertinente à l'objet du dossier[88] » sans nécessiter le consentement du consommateur. Quant à la communication des données, la loi envisage déjà de nombreuses hypothèses où celle-ci est permise sans le consentement du consommateur[89]. En ce qui concerne spécifiquement la proposition de permettre le traitement sans le consentement quand ce traitement est nécessaire aux fins des intérêts légitimes poursuivis par l'entreprise[90], la Commission indique que le projet de loi 64 introduit une exception qui permet l'utilisation d'un renseignement personnel à une fin autre sans le consentement de la personne concernée lorsque cette utilisation est à des fins compatibles avec celles pour lesquelles le renseignement a été recueilli. La Commission estime que cette exception donne déjà une marge de manœuvre aux entreprises sans qu'il soit nécessaire d'exempter les autres utilisations des données personnelles de l'obligation d'obtenir le consentement de la personne concernée[91]. L'analyse de la Commission sur ce point semble être partagée par le Commissaire à la protection de la vie privée du Canada. Celui-ci note « […] qu'au Québec, une entreprise doit avoir un intérêt sérieux et légitime pour recueillir des renseignements personnels. C'est une notion proche des "intérêts légitimes" du droit européen[92] ». En outre, il met en garde contre une interprétation large de l'exception pour fins compatibles qui pourrait ouvrir la porte à d'autres utilisations que celles envisagées par le projet québécois[93].

Faisant écho à ce débat, le législateur québécois a ajouté à l'article 12 de la loi 64 deux autres cas dans lesquels le renseignement personnel peut être utilisé sans le consentement de la personne concernée : « 2.1° lorsque son utilisation est nécessaire à des fins de prévention et de détection de la fraude ou d'évaluation et d'amélioration des mesures de protection et de

sécurité ; 2.2° lorsque son utilisation est nécessaire à des fins de fourniture ou de livraison d'un produit ou de prestation d'un service demandé par la personne concernée ; ». Certains ont vu dans cette ouverture l'introduction des « fins d'affaires légitimes » en droit québécois[94]. Comme nous l'avons indiqué dans la section précédente de notre texte, il s'agit certes d'une ouverture du législateur québécois à l'utilisation du renseignement personnel sans le consentement du consommateur, mais cette ouverture demeure prudente et s'inscrit à l'intérieur d'une liste limitative de cas bien identifiés. Cette liste limitative ne pourra par ailleurs être modifiée par procédure règlementaire conformément à la version finale de la loi 64.

En terminant, le Commissaire à la protection de la vie privée du Canada souligne les éléments suivants, qui sont favorables à la protection des consommateurs : « [c]e qui compte, c'est que la loi autorise les utilisations de données personnelles dans l'intérêt public, les fins légitimes ou le bien commun, à l'intérieur d'un régime fondé sur le respect des droits. Ce régime devrait *imposer aux entreprises* […] *la transparence et l'obligation d'une responsabilité démontrable à l'organisme de réglementation* [nos italiques][95] ». Ces notions de transparence et de responsabilisation des entreprises apparaissent dans le mémoire déposé par Option consommateurs lors de l'étude du projet de loi 64[96]. Il semble que le renforcement de ces éléments, avec l'exigence du consentement, permettraient une protection idoine du consommateur en ce qui concerne ses renseignements personnels. La nouvelle obligation, pour les entreprises qui collectent des données personnelles, d'assurer la protection de ces données par défaut[97], de même que l'obligation de procéder à une évaluation des facteurs relatifs à la vie privée de tout projet de système d'information ou de prestation électronique de services[98], s'inscrivent dans cette démarche proactive de responsabilisation des entreprises[99] et, par voie de conséquence, de protection des données des consommateurs.

CONCLUSION

L'engouement des entreprises pour les données n'a pas tendance à s'essouffler. Comment (ou pourquoi) une entreprise voudrait renoncer à tous ces octets d'informations qu'un objet connecté qu'elle a conçu et commercialisé amasse de façon permanente sur les habitudes de vie les plus intimes des utilisateurs ? Traitées, ces informations dévoilent des profils, des tendances, des besoins, des projections plus précis et plus fiables que ce que l'on peut tirer d'un sondage classique, parce qu'elles sont captées sur le vif, dans les conditions du réel[100]. Le mouvement qu'on a appelé

l'*automesure connectée*, c'est-à-dire la « [p]ratique consistant, pour une personne, à mesurer elle-même à l'aide d'objets connectés [montre, podomètre, téléphone mobile, etc.] des variables physiologiques la concernant, relatives notamment à sa nutrition, à ses activités physiques ou à son sommeil [calories absorbées ou brûlées, nombre de pas effectués, fréquence cardiaque, etc.][101] », peut laisser croire que la personne concernée contrôle ses informations en tout temps. Évidemment, en elle-même, cette présomption est sans vertu pour la protection des données personnelles. De plus, non seulement elle confirme jusqu'où l'Internet des objets a envahi l'intimité du consommateur, mais surtout, cette présomption voile parfaitement l'instrumentalisation du consommateur, c'est-à-dire le fait que l'on soit parvenu à le faire participer activement à la collecte de ses propres données. Peut-être y a-t-il consenti. Mais à quel point a-t-il été informé ou a-t-il saisi la portée de son engagement ? Le législateur est bien avisé d'insister sur ce consentement dès que des données personnelles sont en jeu (dans le cadre de l'automesure connectée et ailleurs), et de faire de l'information préalable du consommateur une condition de validité de ce consentement. Cela dit, la protection des données personnelles du consommateur basée sur le consentement requiert du réalisme. En mettant en œuvre cette exigence, la flexibilité est certainement un atout, parfois imposé par la variété des contextes électroniques. Qui plus est, les mesures qui accentuent la responsabilité des entreprises doivent être sous le contrôle d'autorités régulatrices bénéficiant de pouvoirs accrus, de moyens et d'outils pratiques pour veiller à leur observation. La protection efficiente des données personnelles des consommateurs est à ce prix.