fccq | Fédération des chambres de commerce du Québec

PROJET DE LOI 64 - LOI MODERNISANT DES DISPOSITIONS LÉGISLATIVES EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

MÉMOIRE PRÉSENTÉ À LA COMMISSION DES COMMISSIONS DES INSTITUTIONS

LE 22 SEPTEMBRE 2020

PRÉAMBULE

Grâce à son vaste réseau de plus de 130 chambres de commerce et de 1 100 entreprises établies au Québec, la Fédération des chambres de commerce du Québec (FCCQ) représente plus de 50 000 entreprises exerçant leurs activités dans tous les secteurs de l'économie et sur l'ensemble du territoire québécois. Considérée comme le plus important réseau de gens d'affaires et d'entreprises au Québec, la FCCQ est à la fois une fédération de chambres de commerce et une chambre de commerce provinciale. Elle défend les intérêts de ses membres au chapitre des politiques publiques, favorisant ainsi un environnement d'affaires innovant et concurrentiel, respectueux des principes de développement durable. À ces fins, la FCCQ se fait un devoir de participer aux débats publics et de formuler des recommandations sur les enjeux politiques, économiques et sociaux qui font les manchettes de même que sur les enjeux qui préoccupent ses membres.

D'entrée de jeu, la FCCQ tient à souligner qu'elle reconnaît la nécessité de mettre à jour notre cadre législatif en matière de protection des données personnelles. L'évolution technologique des dernières décennies a soulevé des enjeux nouveaux et importants à l'égard de la protection des renseignements personnels des Québécois. L'avènement des entreprises dont le modèle d'affaires repose sur la commercialisation de renseignements personnels, le développement de nouvelles technologies utilisant les renseignements personnels tels que la biométrie et la reconnaissance faciale ainsi que les capacités d'analyse et de traitement d'une quantité toujours plus importante de renseignements personnels, notamment par l'utilisation de l'intelligence artificielle, amènent un lot de défis qui nécessitent une réflexion sur le cadre législatif applicable.

Par ailleurs, la transformation numérique soulève d'importantes questions sur la collecte et l'utilisation des données. De récentes fuites de données qui ont compromis la confidentialité des renseignements personnels de nombreux Québécois ont révélé la nécessité de responsabiliser les détenteurs de renseignements, dont les entreprises et divers les organismes publics et autres.

Les renseignements personnels méritent d'être protégés et les contrevenants d'être sanctionnés. Cependant, l'évolution de l'économie est généralement intimement liée à la capacité d'innover d'une province ou d'un pays. Dans un monde où le commerce est de plus en plus numérique et où l'information transite 24h par jour, 365 jours par année dans un environnement global, il est important de trouver un équilibre entre la protection des renseignements personnels, l'accès à ceux-ci et ce, sans pour autant compromettre la protection des renseignements personnels, mais tout en permettant aux entreprises d'innover et de compétitionner dans un marché ouvert.

SOMMAIRE EXÉCUTIF

La FCCQ salue le projet de loi 64. Il soulève beaucoup de réflexions importantes et nécessaires pour notre société. L'enjeu principal est de trouver le bon équilibre entre d'un côté la protection des données personnelles et de l'autre côté, l'innovation et le développement économique. Certes, trouver cet équilibre entre protection de données et innovation n'est pas facile. Avec ce projet, le Québec se présente comme un leader au Canada. Il est essentiel de s'assurer qu'il soit juste assez bien dosé par rapport aux autres juridictions au Canada et dans le monde.

Tout d'abord, il est important pour le Québec de ne pas s'isoler du reste du Canada ou de ses principaux partenaires internationaux. Bien que les changements proposés par le projet de loi 64 soient inspirés du

Règlement général sur la protection des données (« RGPD ») adopté par l'Union européenne, il est souhaitable que le Québec et le reste du Canada coordonnent leurs efforts en vue d'harmoniser le plus possible les attentes et obligations en matière de protection des renseignements personnels. Si le Québec devait décider de faire cavalier seul, il risquerait de pénaliser les entreprises québécoises et autres entreprises faisant affaire au Québec. Les partenaires économiques des entreprises québécoises sont principalement en Amérique et il serait imprudent d'isoler et de mettre à risque son économie.

Le Québec devrait adopter une position de leadership et entamer des discussions avec ses homologues tant provinciaux que fédéraux afin de favoriser l'élaboration d'un régime de protection des données pancanadiennes qui favorisera le développement économique des entreprises québécoises à l'intérieur de sa propre zone économique tout en protégeant adéquatement les données des Québécois.

Un autre enjeu très préoccupant est l'amendement concernant le flux de données transfrontalier. Ce dernier crée un processus d'évaluation obligatoire qui est complexe, ambigu, subjectif et incertain. Si le processus d'évaluation devait conclure que les informations bénéficieront d'une protection similaire à celle prévue par la législation du Québec, le résultat final sera un ensemble de dispositions contractuelles et d'engagements visant à établir les obligations réciproques en matière de protections des données, ce qui est, ou devrait, déjà être la réalité dans la majorité des ententes de transfert de données transfrontalier. Cette incertitude pourrait nuire au commerce et au développement économique du Québec. Ainsi, il est important d'harmoniser la législation dans notre principale zone économique, soit le Canada et les États-Unis autant que possible, et de simplifier les exigences de la loi.

Le projet de loi 64 crée des exigences en matière de notification des atteintes à la protection des données et en matière de notification et de consentement, y compris en ce qui concerne l'utilisation de la technologie. Celles-ci obligeront les entreprises à modifier leurs pratiques mondiales pour accommoder le marché québécois ou à cesser d'offrir l'accès à leurs produits ou services aux consommateurs et aux entreprises du Québec.

Les modifications proposées semblent suggérer un consentement spécifique pour chaque utilisation des renseignements personnels. Bien que la FCCQ comprenne l'objectif du législateur, cette approche est lourde et peu pratique. Il serait souhaitable de permette le consentement « en bloc » dans la mesure où ce consentement vise un objet clairement divulgué.

Les cas récents de fuites de données provenant de grandes entreprises ont occupé une place importante dans l'actualité. Cependant, toute grande entreprise qui ferait face à une telle situation aurait les moyens d'engager (si elle ne les possède pas déjà) toutes les ressources nécessaires afin de se conformer à de nouvelles exigences en matière de protection de renseignements personnels.

De leur côté, quel est le nombre de PME qui peut se vanter d'avoir un département des communications, un contentieux et un service de conformité prêt à gérer et à affronter une telle crise? Devant cette réalité, bon nombre d'entrepreneurs seront laissés à eux-mêmes dans des situations qui sont parfois très complexes. Nous croyons qu'il sera important d'accompagner nos entreprises à se conformer à cette législation, spécifiquement les PME qui n'auront pas toujours les ressources légales et financières. Elles devront être sensibilisées, formées et accompagnées.

La mise en application d'un tel projet de loi sera un chantier important pour notre société québécoise. La FCCQ sera aux premières loges pour assurer que cette transition se fasse dans le meilleur intérêt des citoyens et des entreprises du Québec.

1. COORDINATION AVEC LES AUTRES LÉGISLATIONS DE NOTRE ZONE ÉCONOMIQUE

Au palier fédéral, c'est la *Loi sur la protection des renseignements personnels* qui encadre la protection des renseignements personnels détenus par le gouvernement fédéral et les institutions du secteur public fédéral. Celle-ci est entrée en vigueur en 1983. Nul besoin de mentionner que le monde dans lequel nous vivons s'est radicalement transformé, surtout d'un point de vue technologique, depuis cette date. Les attentes des Québécois quant à la façon dont nous traitons leurs données personnelles ont ainsi largement évoluées.

En 2016, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (Comité ETHI) de la Chambre des communes s'est penché sur la question. Les experts et les intervenants qui ont comparu devant le Comité avaient alors exprimé leurs inquiétudes du fait qu'une révision en profondeur du cadre de *la Loi sur la protection des renseignements personnels* aurait dû être effectuée depuis longtemps. Compte tenu des changements sociaux et technologiques, le gouvernement du Canada s'est engagé à revoir sa législation fédérale sur la protection des renseignements personnels dans le secteur public pour s'assurer qu'elle suit le rythme de ces changements. Pour donner suite à cette première consultation, le gouvernement fédéral a fait appel, l'année dernière, à des intervenants spécialisés pour obtenir leur opinion et leur rétroaction sur les aspects techniques et juridiques à prendre en considération dans la modernisation de la Loi sur la protection des renseignements personnels. De nouvelles consultations seront nécessaires, même si le processus a largement été ralenti en raison de la crise de la COVID-19. Le gouvernement du Canada affirme présentement être en train de travailler afin de développer des propositions plus concrètes de modifications éventuelles à la Loi.

Il est important pour le Québec de ne pas s'isoler du reste du Canada ou de ses principaux partenaires internationaux. Bien que les changements proposés par le projet de loi 64 soient inspirés en partie du Règlement général sur la protection des données (RGPD) adoptée par l'Union européenne (EU), il est souhaitable que le Québec et le reste du Canada conjuguent leurs efforts en vue de coordonner le plus possible les attentes et obligations en matière de protection des renseignements personnels. Également, l'Alberta et la Colombie-Britannique sont présentement en attente de la publication de la législation fédérale avant d'agir. Si le Québec devait décider de faire cavalier seul, il risquerait de pénaliser les entreprises québécoises et autres entreprises faisant affaire au Québec. Les partenaires économiques des entreprises québécoises étant principalement en Amérique, il serait imprudent de s'isoler et de mettre à risque notre économie.

Selon la FCCQ, le Québec aurait tout avantage à adopter une position de leadership et à entamer des discussions avec ses homologues tant provinciaux que fédéraux afin de favoriser l'élaboration d'un régime de protection des données pancanadiennes pour encourager le développement économique des entreprises québécoises à l'intérieur de sa propre zone économique tout en protégeant adéquatement les données des Québécois. En plus des modernisations législatives qui s'imposent, plusieurs projets l'implantation de moyens technologiques, telle l'identité numérique, nécessite des travaux effectués à l'échelle pancanadienne.

Compte tenu de l'importance de ne pas nuire à la compétitivité de nos entreprises sur le marché nord-américain, la FCCQ propose d'abord au législateur québécois de tenir compte des changements actuellement étudiés à la loi fédérale avant d'aller de l'avant avec sa propre loi. La FCCQ est convaincue qu'une plus grande harmonisation entre les différentes lois canadiennes permettrait de faciliter les échanges commerciaux et les liens économiques entre les différentes provinces canadiennes, de supprimer certaines barrières, notamment

en matière de transactions commerciales tout en offrant la protection nécessaire aux renseignements personnels.

Étant donné que chacune des juridictions au Canada peut légiférer en matière de protection des données personnelles, il est possible que certains problèmes puissent surgir notamment dans les cas suivants :

- Des conflits d'interprétation impliquant plusieurs provinces;
- Des interprétations différentes en fonction des juridictions;

Or, à l'instar de l'Union européenne qui a créé le comité européen de protection des données[1] (CEPD) de façon à assurer une certaine cohérence du Règlement général sur la protection des données (RGPD), la FCCQ croit qu'un comité similaire devrait être créé au Canada pour pallier différents problèmes pouvant survenir et assurer ainsi une meilleure cohésion et harmonisation des législations interprovinciales au Canada.

Recommandation #1 : coordonner avec les autres législations de notre zone économique afin de favoriser l'élaboration d'un régime de protection des données qui encouragera le développement économique des entreprises québécoises tout en protégeant adéquatement les données des Québécois.

2. PLUS GRAND RAPPROCHEMENT AVEC LA RGPD

Lors de la dernière consultation du gouvernement du Québec sur la thématique des données personnelles, « *Actualiser le cadre législatif du Québec en matière de renseignements personnels* », la FCCQ avait rappelé au gouvernement l'importance de tenir compte de l'entrée en vigueur des nouvelles règles européennes.

Plusieurs acteurs économiques souhaitaient que le cadre juridique québécois en matière de protection des renseignements personnels obtienne le statut de cadre juridique « adéquat » vis-à-vis du cadre juridique européen en la matière afin de préserver la réputation et la compétitivité de l'environnement d'affaires québécois sur la scène internationale.

Ruth Boardman grande spécialiste de la protection de la vie privée et des données au cabinet de Bird & Bird à Londres énonçait souhaiter dans une entrevue donnée à l'IAPP (International Association of Privacy Professionals) dans le cadre du 2e anniversaire de RGPD que : «… *maintenir l'équilibre entre la protection des données et l'innovation en cours de développement et être prêts à faire des ajustements***.** ». Elle ajoutait aussi « *Les autorités de protection des données et les législateurs disent souvent qu'il n'y a pas besoin de choisir entre une forte protection de la vie privée et les avantages que les nouvelles technologies peuvent apporter - que des lois solides de protection des données engendrent la confiance des consommateurs sur laquelle de nouveaux services dépendent*.»[2]. La FCCQ est du même avis que Mme Boardman qui souligne le fait qu'il est nécessaire d'instaurer un équilibre entre protection des données et innovation. Les technologies de l'information étant en constante évolution, il faut aussi que le législateur mette en place des dispositifs permettant de suivre ces évolutions et faire des ajustements rapidement. De plus, la version actuelle du projet de loi crée des règles de cessation de diffusion, de désindexation et de réindexation qui ne sont pas alignées au RGPD et pour lesquelles des normes reconnues à l'échelle internationale n'ont pas encore émergé. Au Canada, on ne sait pas si les

1 Comité Européen de la Protection des Données, https://edpb.europa.eu/edpb_fr

2 Traduction libre, texte intégral en Annexe - https://iapp.org/resources/article/gdpr-at-two-expert-perspectives/

règles de désindexation sont constitutionnelles ou introduites de façon appropriée par le biais de lois sur la protection des renseignements personnels. Ces deux questions font l'objet d'une référence à la Cour fédérale. En introduisant ces règles maintenant, le Québec forcerait les entreprises à mettre en place des solutions de conformité qui pourraient être incompatibles avec les nouvelles normes. Celles-ci seront à l'origine de dépenses pour les entreprises du Québec que les concurrents hors Québec n'engageront pas et peuvent entraîner la décision des entreprises de ne plus offrir de produits impactés aux clients québécois.

Recommandation #2 : Dans le cadre de la relance économique, s'assurer que le cadre législatif proposé n'introduise pas des dispositions plus contraignantes que celles prévues par Règlement général sur la protection des données de l'Union européenne (RGPD).

3. L'IMPACT POTENTIEL SUR LES PME

Les cas récents de fuites de données provenant de grandes entreprises ont occupé une place importante dans l'actualité. Cependant, toute grande entreprise qui ferait face à une telle situation aurait les moyens d'engager (si elle ne les possède pas déjà) toutes les ressources nécessaires afin de se conformer à de nouvelles exigences en matière de protection de renseignements personnels.

De leur côté, quel est le nombre de PME qui peut se vanter d'avoir un département des communications, un contentieux et un service de conformité prêt à gérer et à affronter une telle crise? Devant cette réalité, bon nombre d'entrepreneurs seront laissés à eux-mêmes dans des situations qui sont parfois très complexes. Pour certains, cela pourrait signifier la fin de leur entreprise. Pris au mur, ils devront informer leurs clients qu'ils ont été victimes d'une fuite de données. N'ayant pas les moyens juridiques et de communications nécessaires pour corriger la situation, plusieurs risquent de subir des dommages irréversibles.

De plus, la définition des données personnelles peut porter à confusion. Qui est réellement responsable? Si une entreprise collecte la donnée, est-ce elle qui est responsable, ou est-ce celle qui l'héberge, ou celui qui sécurise par contrat ? L'intelligence artificielle ouvre la porte à de nombreuses interprétations.

Par exemple, supposons qu'une compagnie souhaite se prévaloir des services d'une entreprise œuvrant en intelligence artificielle. Elle lui demande de lui faire un programme qui va lui permettre d'aller chercher de l'information et ainsi de mieux desservir ses clients. Afin de procéder, l'entreprise en intelligence artificielle aura besoin des vraies données, pas des données caviardées. Ainsi, la compagnie qui remet les données à l'entreprise en intelligence artificielle dans le but d'avoir un programme plus performant pour ses clients s'expose à une fuite potentielle de données personnelles. Elle risque donc fortement de ne pas prendre de risque et d'abandonner. Si le « bâton » est trop fort, plusieurs entreprises craindront de donner accès à leurs données.

La peur financière, celle de se faire poursuivre, pourrait donc avoir un effet pervers sur les échanges économiques. D'ailleurs, à l'origine, la législation européenne sur laquelle s'inspire grandement le projet de loi 64, avait été conçue pour encadrer les activités des GAFAM. Ces grandes entreprises donnent accès gratuitement à leur technologie en échange des données qu'elles collectent sur ses utilisateurs. Il ne faudrait

pas que les plus petits joueurs deviennent les victimes collatérales de modèles d'affaires des plus grosses entreprises qui font le "commerce" des données.

Recommandation #3: mettre en place un programme d'accompagnement qui permettrait aux PME de faire la transition et accorder une période de transition pour se conformer aux obligations prescrites par le projet de loi 64

4. L'IMPORTANCE DE PRÉSERVER LA COMPÉTITIVITÉ DU SECTEUR DE L'IA

Dans les dernières années, le gouvernement du Québec a choisi, avec raison, de miser gros sur le secteur de l'intelligence artificielle (IA). Plus de 2,3 milliards de dollars d'investissements gouvernementaux sont annoncés ou disponibles pour la recherche, le développement de technologies ou l'adoption de solutions d'intelligence artificielle. Une bonne partie de ces sommes a également été investie en capital-risque dans des entreprises québécoises en IA en forte croissance.

Le Québec constitue également un pôle d'excellence en recherche dans le domaine de l'IA, de la recherche opérationnelle et de la valorisation des données. Depuis 20 ans, le gouvernement du Québec soutient les activités de recherche fondamentale de groupes de chercheurs travaillant au développement de la science des données et de ses applications au sein de plusieurs établissements universitaires et centres de recherche du Québec.

Or, l'adoption rapide du projet de loi 64, sans harmonisation avec les autres provinces et avec le gouvernement fédéral, met à risque la compétitivité de ce secteur. En mai 2018, l'Union européenne a mis en œuvre un nouveau régime de protection des données personnelles pour tous les pays membres appelé le Règlement général sur la protection des données (RGPD). À la suite de l'adoption du RGDP en Europe, certaines entreprises américaines ont rendu leur site inaccessible aux Européens, car ils ne pouvaient se conformer aux règles en vigueur. Le Québec, ne possédant pas le poids commercial de l'Europe, serait donc mauvaise posture s'il choisissait d'agir de manière cavalière et d'être la seule juridiction en Amérique du Nord à adopter de nouvelles règles plus contraignantes.

Pour la FCCQ, le gouvernement doit prendre en considération que les entreprises québécoises en IA évoluent principalement dans la zone économique nord-américaine. Ainsi, pour la majeure partie de nos entreprises, l'axe économique demeure essentiellement Québec-États-Unis-Canada. En adoptant une législation similaire ou

même plus contraignante que le modèle européen (RGPD), le Québec risquerait de s'isoler dans la zone économique nord-américaine.

Recommandation #4 : favoriser une approche basée sur la protection des renseignements personnels adaptée à la réalité Nord-Américaine sans pour autant être un frein au développement économique et à l'innovation par le milieu des affaires.

5. RESTRICTIONS À LA CIRCULATION TRANSFRONTALIÈRE DE DONNÉES

Selon la FCCQ, l'amendement proposé à l'article 17 du projet de loi, concernant le flux de données transfrontalier, crée un processus d'évaluation obligatoire qui est complexe, ambigu, subjectif et incertain. Celui-ci restreint la circulation transfrontalière de données d'une manière qui peut empêcher l'utilisation de services infonuagiques, de plates-formes de commerce électronique, de systèmes de paiement, d'applications mobiles et d'autres technologies essentielles à l'économie moderne.

D'abord, parce que le projet de loi 64 prévoit que les entreprises qui opèrent au Québec ne peuvent transférer des renseignements personnels qu'aux États où les cadres juridiques garantissent des protections de la vie privée équivalentes à celles du Québec. Considérant la nature plus contraignante des changements prévue à la législation actuelle, cela pourrait être à l'origine de nombreuses problématiques pour les entreprises qui souhaitent faire affaire avec l'une des 52 juridictions américaines ou avec d'autres pays à l'international, qui eux aussi, peuvent être divisés en plusieurs juridictions.

De plus, étant donné que les produits et services disponibles sur le marché, y compris le *cloud*, le commerce électronique, les paiements, et autres, sont fournis à partir de centres de données dans les juridictions du monde entier, le projet de loi 64 dans sa forme actuelle et dans les faits, empêcherait effectivement les entreprises du Québec de les utiliser.

Également, la FCCQ constate que le projet de loi 64 exige des entreprises qu'elles évaluent l'équivalence des lois sur la protection des données dans chaque État où l'information peut être communiquée, ce qui oblige essentiellement les entreprises du Québec à assumer les dépenses et les retards associés, à devenir experts en matière de lois sur la protection des renseignements personnels à l'échelle internationale, ce qui est évidemment irréaliste, principalement pour les PME. Or, si le processus d'évaluation devait conclure que les informations bénéficieront d'une protection similaire à celle prévue par la législation du Québec, le résultat final serait un ensemble de dispositions contractuelles et d'engagements visant à établir les obligations réciproques en matière de protections des données, ce qui est, ou devrait, déjà être la réalité dans la majorité des ententes

de transfert de données transfrontalier. L'exigence d'une évaluation aussi complexe et onéreuse ne devrait pas être une obligation, mais une recommandation sous la forme de « meilleure pratique ».

De plus, le Québec devrait être prudent et s'assurer que les modifications à la législation sur la protection des renseignements personnels n'aboutissent pas en une abdication de sa juridiction la matière.

En effet, une récente décision (*Schrems II*) de la Cour de justice de l'Union européenne (CJUE) vient démontrer :

• Qu'une décision d'un tribunal étranger pourrait avoir un impact direct sur la transmission de données à l'étranger;
• Que les clauses contractuelles types (CCT) proposées par le RGDP ne peuvent à elles seules pallier le défaut de reconnaissance d'équivalence du régime de protection des données d'un état étranger;

• Qu'à défaut d'une reconnaissance d'équivalence d'un régime de protection des données d'un état étranger une analyse rigoureuse de l'étendue de la protection offerte aux renseignements personnels d'un état étranger par une entreprise n'aura aucun effet de garantir le flux de données à l'étranger, celui-ci étant toujours susceptible d'être interrompu suite à une interprétation restrictive de la loi par un état.

En conséquence, les restrictions proposées du flux transfrontalier d'informations risquent de créer de l'incertitude, nuisant ainsi au commerce et au développement économique du Québec. Ainsi, il est important d'harmoniser la législation dans notre principale zone économique, soit le Canada et les États-Unis autant que possible, et de simplifier les exigences de la loi. Considérant l'environnement économique concurrentiel dans lequel nous nous trouvons et les défis que pose une relance économique suite à la pandémie de la COVID-19, il devient essentiel de trouver un équilibre entre la protection des données entre les frontières et la protection de ces mêmes données.

Recommandation #5 : réévaluer et coordonner avec les autres juridictions provinciales et fédérales le mécanisme d'évaluation et d'autorisation relativement à la circulation transfrontalière de données afin de trouver une réglementation harmonisée qui n'affectera pas la compétitivité des entreprises québécoises.

6. LA NOTION DE CONSENTEMENT

Le projet de loi 64 crée des exigences en matière de notification des atteintes à la protection des données et en matière de notification et de consentement, y compris en ce qui concerne l'utilisation de la technologie. Celles-ci obligeront les entreprises à modifier leurs pratiques mondiales pour accommoder le marché québécois ou à cesser d'offrir l'accès à leurs produits ou services aux consommateurs et aux entreprises du Québec.

Les modifications proposées semblent suggérer un consentement spécifique pour chaque utilisation des renseignements personnels. Bien que la FCCQ comprenne l'objectif du législateur, cette approche est lourde et peu pratique. Même le RGPD, duquel le projet de loi 64 s'inspire, permet le consentement « en bloc » dans la mesure où ce consentement vise un objet clairement divulgué. La réalité est que pour la grande majorité des renseignements personnels obtenue dans le cadre d'un consentement « en bloc », le refus de consentir à un

élément du consentement risque d'entrainer le refus de fournir le service, car le consentement vise généralement à accéder aux informations nécessaires à l'exécution des obligations légales des contrats.

Recommandation #6 : permettre le consentement « en bloc » dans la mesure où ce consentement vise un objet clairement divulgué, comme c'est le cas dans le RGPD européen.

7. AMENDES ET SANCTIONS

Bien que conforme aux tendances actuelles, il est à craindre que les entreprises agissant dans de nombreuses juridictions se voient infliger des amendes dans plusieurs juridictions pour une seule et même infraction, auquel cas la sanction pourrait être disproportionnée par rapport à la faute. Or, la réglementation européenne en vigueur fait en sorte qu'une entreprise ne peut avoir qu'une seule amende à payer dans la juridiction où la faute commise a été identifiée.

De plus, considérant le montant et l'impact des sanctions proposées, la loi devrait permettre à une partie qui pourrait être visée par une sanction de transmettre des observations et de contester la conclusion d'une enquête administrative avant l'émission de telles sanctions, le tout conformément aux règles élémentaires de justice naturelle.

Recommandation #7a : permettre à une partie qui pourrait être visée par une sanction de transmettre des observations et de contester la conclusion d'une enquête administrative avant l'émission de telles sanctions.
Recommandation #7b: imposer une seule amende dans la juridiction où la faute a été commise.

8. EXIGENCE DE PORTABILITÉ DES DONNÉES

La portabilité des données est un concept qui donne le droit à une personne d'accéder à ses données personnelles détenues par une entreprise ou une organisation. Il permet aussi à une organisation de transférer ses données à un tiers en son nom.

Le droit à la portabilité des données s'inscrit dans un mouvement international qui a pour objectif de donner un plus grand contrôle aux citoyens sur leurs renseignements personnels. L'objectif en général est de favoriser la concurrence en facilitant la comparaison et le changement de fournisseurs grâce à la portabilité des données. Par exemple, dans le contexte bancaire, depuis janvier 2018 toutes les banques du Royaume-Uni ont pour obligation de se conformer aux règles « d'Open Banking » qui ont pour objectif de simplifier la portabilité des

données dans le secteur financier. En procédant ainsi, les citoyens peuvent passer plus facilement d'une banque à une autre.

Certains de nos membres nous ont mentionné leurs préoccupations relatives à la mise en œuvre d'une pleine portabilité. Leurs préoccupations sont en lien avec le respect de la vie privée, de la cybersécurité ainsi qu'avec le coût que cette mise en œuvre pourrait entraîner.

En principe, le concept est louable. Cependant, nous pensons qu'il devrait être adapté secteur par secteur. Pour y arriver, il serait probablement plus judicieux de traiter ces spécificités de secteur par règlementation en travaillant avec les entreprises des différents écosystèmes.

Recommandation #8 : Définir un cadre de règlementation adapté, secteur par secteur, qui facilitera sa compréhension, son adoption et sa mise en œuvre.

9. L'UTILISATION DES DONNÉES DANS LE SECTEUR DE LA SANTÉ

Les données sont de plus en plus utilisées dans le secteur de la santé et permettent notamment : « de développer des technologies pour faciliter et améliorer la détection et les diagnostics de maladies comme le cancer, d'optimiser les ressources dans l'ensemble du système de santé et d'accélérer la découverte de nouveaux traitements[1]. » Sans contredit, ces activités contribuent à l'amélioration des soins de santé et à la prévention, mais permettent aussi de limiter la croissance des coûts de santé. À cet égard, rappelons que dans le budget 2020-2021 du gouvernement du Québec, les dépenses en santé et services sociaux totalisaient plus de 42 milliards de dollars, soit près de 50 % des dépenses totales de programme[2]. Ceci est sans mentionner les 3,7 milliards de dollars qui ont été déployés par le gouvernement du Québec pour renforcer le système de santé afin de faire face à la pandémie de COVID-19[3]. Ainsi, dans un souci d'optimisation, il est de notre intérêt d'intégrer la science des données au sein du réseau de la santé afin d'en assurer sa pérennité.

Par ailleurs, le succès et le développement de certains secteurs clés de l'économie québécoise tels que l'intelligence artificielle, les technologies médicales et l'industrie biotechnologique et pharmaceutique dépendent grandement de l'accès aux recherches effectuées grâce au traitement de données en santé. Ces dernières permettent notamment de démontrer la valeur d'un produit ou d'une innovation, favorisant ainsi leur intégration dans le réseau tant au Québec qu'à l'international.

Il est également à noter que la Stratégie québécoise des sciences de la vie 2017-2027[4] visait à favoriser l'exploitation des mégadonnées en santé et à améliorer l'accès aux bases de données afin d'attirer des investissements étrangers au Québec et d'assurer le développement de ce secteur. La quantité de données dont le Québec bénéficie par l'entremise de son système de santé universel ainsi que son expertise reconnue

en matière de traitement de données et en intelligence artificielle représentent des avantages concurrentiels majeurs qui doivent être exploités.

Pour ces raisons, nous sommes d'avis que le Québec a avantage à valoriser davantage les données de santé tout protégeant de façon adéquate les renseignements personnels des citoyens.

L'accès aux données par l'industrie : l'importance de corriger le tir

Le récent débat portant sur l'accès aux données de la Régie de l'assurance maladie du Québec (RAMQ), par l'industrie pharmaceutique notamment, démontre l'importance de rassurer la population quant à leur utilisation.

À cet égard, il importe de rappeler que l'industrie biotechnologique et pharmaceutique ne désire pas « acheter » des données ni accéder directement aux renseignements de santé des Québécois. Cette industrie souhaite plutôt être en mesure d'obtenir des réponses à certaines questions soumises aux gestionnaires de renseignements personnels de diverses banques de données. En clair, ce sont les résultats de recherche qui favorisent l'avancement de la science et non les données brutes.

Selon l'article 27 du projet de loi, des organismes publics, tels qu'un CIUSSS, pourraient se voir attribuer un rôle de gestionnaire de renseignements personnels et par conséquent, mettre en place des bases de données. Les entreprises biotechnologiques et pharmaceutiques pourraient alors soumettre leurs problématiques au gestionnaire de renseignements personnels qui lui, pourrait valider ou non les hypothèses soumises par l'industrie. Ce gestionnaire de renseignements personnels agirait en quelque sorte en tant que fiduciaire des données.

Afin d'assurer une protection adéquate, la mise en place d'un système de certification ou d'accréditation imposant aux gestionnaires de renseignements personnels les plus hauts standards en matière de protection et d'accès aux données devrait être envisagée.

Ainsi, la mise en valeur des données de santé conjuguée à un encadrement rigoureux est primordiale. C'est pourquoi nous sommes d'avis que les entreprises devraient pouvoir obtenir les résultats de recherche anonymisés ou dépersonnalisés, et ce, en temps opportun.

L'utilisation des données pour des fins de recherches

Au Québec, le processus d'approbation pour avoir obtenir des données de recherche est complexe et peut engendrer de longs délais. En fait, il appert que les délais d'attente peuvent atteindre 2 ans[5] dans certains cas. Or, un accès en temps opportun permet un développement plus rapide des innovations, améliorant ainsi la compétitivité des entreprises québécoises et ultimement, le système de santé québécois.

Actuellement, les personnes ou organismes qui désirent obtenir des renseignements personnels à des fins de recherche doivent, en vertu de l'article 125 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Loi sur l'accès), obtenir une autorisation de la Commission d'accès à l'information avant d'avoir accès à des données détenues par un organisme public. Le Québec est la seule province au Canada qui nécessite deux niveaux approbations au lieu d'une seule.

Le projet de loi nº 64 prévoit abroger l'article 125 de la Loi sur l'accès. Par ailleurs, l'article 23 du projet de loi indique que les personnes ou les organismes qui désireront utiliser des données à des fins d'étude, de recherche ou de production de statistiques devront effectuer leur demande directement auprès de l'organisme détenteur des renseignements en soumettant une demande par écrit.

Nous avons bon espoir que ces dispositions permettront d'accélérer le développement et l'innovation et de l'intelligence artificielle en santé. À cet égard, rappelons que certaines entités canadiennes assurent un accès

rapide à certaines données. C'est notamment le cas de l'Institut de recherche en services de santé (IRSS) de l'Ontario qui permet d'avoir accès à des données en moins de 2 mois[6].

Tel que prévu à l'article 23 du Projet de loi nº 64 :

« La personne ou l'organisme qui souhaite utiliser des renseignements personnels à des fins d'étude, de recherche ou de production de statistique doit :

1. Faire sa demande par écrit ;
2. Joindre à sa demande son protocole de recherche ;
3. Exposer les motifs pouvant soutenir que les critères mentionnés aux paragraphes 1° à 5° du deuxième alinéa de l'article 67.2.1 sont remplis ;
4. Mentionner toutes les personnes et tous les organismes à qui il fait une demande similaire aux fins de la même étude, recherche ou production de statistiques ;
5. Le cas échéant, décrire les différentes technologies qui seront utilisées pour effectuer le traitement des renseignements ;
6. Le cas échéant, transmettre la décision documentée d'un comité d'éthique de la recherche relative à cette étude, recherche ou production de statistiques[7]. »

Il est également prévu qu'une entente devra être conclue entre l'organisme qui détient les renseignements personnels et la personne ou l'organisme qui désire les utiliser à des fins de recherche ou d'étude. Soulignons qu'actuellement, un des obstacles majeurs à l'attrait d'investissements en recherche clinique au Québec réside dans la multiplicité et le manque d'uniformité des contrats entre les différents établissements qui participent à des essais cliniques multicentriques. Il importe de ne pas dupliquer le même genre de situation avec le type d'ententes prévues au projet de loi. Il serait donc important que l'élaboration d'un contrat type soit faite par une instance plus centrale.

En somme, bien que nous sommes favorables à ces dispositions, nous croyons qu'elles ne doivent pas entraîner de délais supplémentaires.

Le consentement

Par ailleurs, bien que le projet de loi prévoie l'introduction d'un consentement donné à des fins spécifiques, une exception est prévue pour des fins de recherches, d'études et de production de statistique afin de faciliter l'utilisation secondaire des données. Plus précisément, le projet de loi indique que :

Article 23 : « un organisme public peut communiquer des renseignements personnels sans le consentement des personnes concernées à une personne ou à un organisme qui souhaite utiliser ces renseignements à des fins d'étude, de recherche ou de production de statistiques[8]. »

Toutefois, l'article 9 du projet de loi spécifie que le consentement doit être « demandé à chacune de ces fins, en termes simples et clairs, distinctement de toute autre information communiquée à la personne concernée. » Il

serait important de préciser qu'un individu peut consentir de façon explicite à une utilisation multiple de ses renseignements comme le prévoit l'article 9 du règlement de l'Union européenne :

« La personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques[9]. »

En fait, dans le domaine de la santé, il est fréquent qu'une donnée ou qu'un échantillon de tissu biologique puisse servir à plusieurs recherches ou études.

La conservation des données

Le projet de loi prévoit également la destruction ou l'anonymisation des renseignements personnels lorsque les fins pour lesquels ils ont été recueillis sont accomplies. Or, en recherche, certaines données méritent d'être conservées au-delà des délais initialement prévus afin de ne pas restreindre son développement.

À cet égard, l'article 5 du Règlement général sur la protection des données de l'Union européenne prévoit que:

« *Les données à caractère personnel doivent être conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire au regard des finalités pour lesquelles elles sont traitées ; les données à caractère personnel peuvent être conservées pour des durées plus longues dans la mesure où elles seront traitées exclusivement à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques* »[10].

Recommandation #9 : Nous recommandons la modification de l'article 111 du projet de loi no 29 modifiant l'article 23 de la *Loi sur la protection des renseignements personnels dans le secteur privé* comme suit :

« Lorsque les fins auxquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, la personne qui exploite une entreprise doit le détruire ou l'anonymiser, sous réserve d'un délai de

conservation prévu par une loi, à moins que ce renseignement serve à des fins de recherche, d'étude ou de production de statistiques.

Les données sensibles

Les données utilisées pour la recherche en santé sont souvent des renseignements physiques et médicaux qui peuvent être considérés comme sensibles. À cet égard, le projet de loi prévoit qu'un « consentement doit être manifesté de façon expresse dès qu'il s'agit d'un renseignement personnel sensible. »

Recommandation #10 : clarifier la définition d'un renseignement personnel sensible par le biais de lignes directrices, par exemple.

[1] Gouvernement du Québec, *Stratégie québécoise des sciences de la vie 2017-2027* (2017) : https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/economie/publications-adm/politique/PO_strategie_sciences_vie_2017-2027_MEI.pdf?1569264678

[2] Ministère des Finances, *Budget des dépenses 2020-2021 – crédits des ministères et organismes* (mars 2020) : https://www.tresor.gouv.qc.ca/fileadmin/PDF/budget_depenses/20-21/3-Credits_des_ministeres_et_organismes.pdf

[3] Cabinet du ministre des Finances, Portrait de la situation économique et financière 2020-2021 - Donner l'heure juste aux Québécois et Québécoises, communiqué de presse diffusé le 19 juin 2020 : http://www.budget.finances.gouv.qc.ca/budget/portrait_juin2020/fr/documents/Communique.pdf

[4] Ministère de l'Économie et de l'Innovation, Stratégie québécoise des sciences de la vie 2017-2027 : l'innovation prend vie (2017) : https://cdn-contenu.quebec.ca/cdn-contenu/adm/min/economie/publications-adm/politique/PO_strategie_sciences_vie_2017-2027_MEI.pdf?1569264678

[5] Mémoire du Scientifique en chef du Québec présenté à la Commission des institutions démocratiques du Québec (septembre 2015) : http://www.scientifique-en-chef.gouv.qc.ca/wp-content/uploads/2015-09-24-Memoire_gouv_transparent_FRQ.pdf

[6] Conseil des académies canadiennes, *l'accès aux données sur la santé et aux données connexes au Canada* (2016) : https://rapports-cac.ca/wp-content/uploads/2018/10/healthdata_fullreport_fr.pdf

[7] Projet de loi nº 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* : http://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-64-42-1.html

[8] Ibid.

[9] Article 9 du *Règlement général sur la protection des données* : https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[10] Parlement européen et le conseil de l'Union européenne, *Règlement général sur la protection des données* (avril 2016) : https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=fr

10. CONCLUSION

Le projet de loi 64 s'inspire clairement du Règlement général sur la protection des données (RGPD). On y retrouve les concepts de « droit à l'effacement des informations » que nous appelons aussi « le droit à l'oubli », « le droit de la portabilité des données personnelles » qui permet aux clients de transférer facilement des informations personnelles entre organisations et le droit lié à l'utilisation des technologies qui permet d'être informée de l'utilisation d'une technologie particulière si elle a pour fonction l'identification, la localisation ou le profilage.

Ce projet de loi promet clairement de protéger les Québécois. Néanmoins, il soulève certaines **inquiétudes au niveau de son application**. Il posera certains problèmes de conformité pour nos entreprises, mais aussi aux autorités de règlementation. L'exigence « **d'équivalence** que l'on retrouve au 4e paragraphe du 1er alinéa de l'article 15 » viendra très certainement causer des maux de tête à nos entreprises. En vertu de cette disposition, les entreprises opérant au Québec ne peuvent transférer des renseignements personnels qu'aux « États » dont le cadre juridique offre une protection de la vie privée équivalente à celle du Québec. En fait, il sera probablement plus facile de transmettre des données personnelles vers l'Europe que vers une autre province canadienne. Il est de même pour notre voisin les États-Unis, grand partenaire économique où l'équivalence est très incertaine.

Nous sommes tout à fait en accord avec un tel projet de loi. Nous sommes convaincus qu'il est important de protéger les informations personnelles des citoyens et citoyennes du Québec. Néanmoins, nous croyons qu'il est **important d'accompagner nos entreprises à se conformer à cette législation**, spécifiquement les PME qui n'auront pas toujours les ressources légales et financières. Elles devront être sensibilisées, formées et accompagnées.

Comme nous l'avons mentionné dans ce mémoire, nous souhaitons une harmonisation pancanadienne le plus rapidement possible de façon à ne pas provoquer d'effet négatif qui pourrait **provoquer un ralentissement économique au Québec**. Lors de la mise en vigueur de ce projet de loi, nous anticipons un moment de transition qui pourrait provoquer un ralentissement de projets B2B entre entreprises travaillant avec des données personnelles. Un phénomène qui risque d'être important, et même peut-être catastrophique pour les PME faisant des affaires avec les grandes entreprises (GE).

Cette loi modernisant des dispositions législatives en matière de protection des renseignements personnels est saluée par la FCCQ. Elle soulève beaucoup de réflexions importantes et nécessaires pour notre société. L'enjeu principal pour les parlementaires est de **trouver le bon équilibre entre d'un côté la protection des données personnelles et de l'autre côté l'innovation et le développement économique**.

À titre d'illustration, il est maintenant reconnu que le Québec est un pôle important dans le monde relativement à l'intelligence artificielle. Nous avons ici l'un de ceux qui ont découvert l'apprentissage profond, Pr Yoshua Bengio. Le gouvernement actuel et le précédent ont investi des sommes importantes pour développer ce secteur. Or, comme vous le savez probablement, les données sont au centre de ces innovations. Dans un contexte éthique et bienveillant, **il serait malheureux que les dispositions (volontairement ou involontairement) viennent ralentir la recherche et le développement de ces technologies d'intelligence artificielle dans nos institutions et entreprises**.

Un autre sujet que nous traitons dans ce mémoire est celui de l'utilisation des données dans le milieu de la santé. Il est facile de comprendre que lorsqu'on conjugue ces données provenant du milieu de la santé avec les

avancés en intelligence artificielle, il devient alors possible de faire des choses auparavant inimaginables. Prenons l'exemple de la compagnie Imagia de Montréal qui a développé une technologie basée sur l'intelligence artificielle capable d'identifier un cancer colorectal lors d'une coloscopie[3]. Fini les temps d'attente interminable pour le patient. **En utilisant une telle technologie, combiné à l'expertise du médecin, ce dernier est en mesure de rassurer presque immédiatement le patient sur son état de santé**. Il peut également dans le cas contraire procéder plus rapidement à une intervention. Ce type d'innovation n'aurait jamais pu voir le jour sans avoir eu accès à des renseignements personnels.

Certes, **trouver cet équilibre entre protection de données et innovation n'est pas facile à doser**. Avec ce projet, le Québec se présente comme un leader au Canada, il est essentiel de s'assurer qu'il soit juste assez bien dosé par rapport aux autres juridictions au Canada et dans le monde. Par ailleurs, le numérique évoluant très rapidement, nous croyons qu'il serait important que ce projet de loi **permette de s'ajuster rapidement selon les expériences et usages relativement aux dispositions de celui-ci.**

La COVID-19 a bouleversé notre économie et nos entreprises. La FCCQ se présente à la commission en tentant d'amener un éclairage du point de vue des entreprises. **Nous sommes en mode solution et cherchons à contribuer à la réflexion générale**. Nous comprenons les enjeux des citoyens et ceux entrepreneurs. Nous sommes d'avis qu'il est important de légiférer pour une meilleure protection et un meilleur encadrement de l'utilisation des données personnelles.

Pour conclure, la mise en application d'un tel projet de loi sera **un chantier important pour notre société québécoise**. La FCCQ tient à vous informer que nous serons aux premières loges pour vous aider et pour aider les entreprises du Québec à faire cette transition dans le meilleur intérêt des citoyens et des entreprises du Québec.

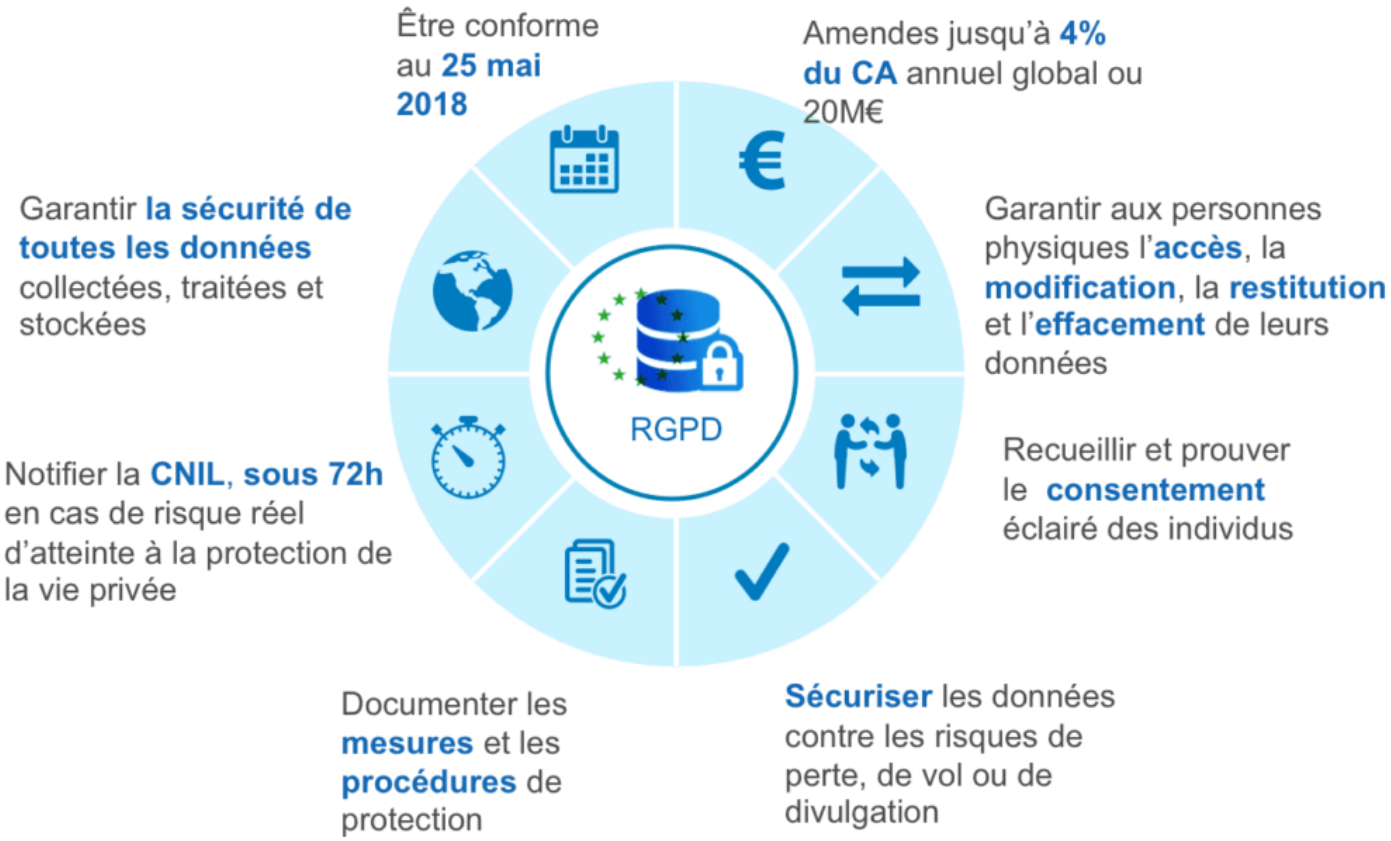
[3] Une coloscopie est un examen où un médecin observe l'intérieur du côlon et du rectum à l'aide d'un tube flexible muni d'une lumière et d'une lentille à une extrémité, soit un coloscope la présence de polypes suspectes.

ANNEXE

Les éléments qui suivent sont présentés à titre de complément pour offrir des pistes de réflexion à la commission et aux parlementaires. Bien entendu, une vigie rigoureuse et en continu des différentes juridictions s'impose puisque la situation évolue rapidement.

Le règlement général sur la protection des données (RGPD)

Voici un schéma qui résume simplement le Règlement général sur la protection des données européennes (RGPD) vue par les Français.



Source : https://www.ipe.fr/rgpd/

Comité Européen de la Protection des Données (CEPD)

« Le Comité Européen de la Protection des Données (EDPB) est un organe européen indépendant qui contribue à l'application cohérente des règles en matière de protection des données au sein de l'Union européenne et encourage la coopération entre autorités de l'UE chargées de la protection des données. »[4]

[4] https://edpb.europa.eu/about-edpb/about-edpb_fr

La publicité comportementale en ligne (PCL)

La PCL se définit comme le suivi et le ciblage des activités sur le Web des personnes, dans plusieurs sites et au fil du temps, afin de leur présenter des publicités adaptées à leurs intérêts présumés[5].

Il s'agit d'une technique qui permet, suite à l'analyse de votre comportement sur les sites Web, de vous proposer une publicité qui pourrait vous intéresser.

Le site www.youronlinechoices.com permet de vérifier et d'identifier les sociétés qui font partie des fournisseurs qui travaillent avec des sites Web en vue de collecter et d'utiliser des informations visant à proposer des publicités ciblées par centres d'intérêt. Voici une liste de fournisseurs obtenus suite à une analyse d'un poste de travail d'un utilisateur au hasard.

1plusX	eyeota	Neodata Group	ShareThis
33Across	Facebook	NEORY	Signals (Next14 Group)
4W MARKETPLACE SRL	Flashtalking	Neustar	Sizmek Inc.
Accordant Media	Fonecta Oy	News IQ	Skimlinks
ADARA	Gamned	Nextperf	Smartclip
ADEX	Google	NextRoll	Sojern
Adform	GroundTruth	Nielsen	Spot.IM Ltd.
AdGear	Gumgum	Numberly	Taboola Europe Limited
ADITION	Illuma	OpenX	Tapad
Adobe	Intent Media, Inc.	Oracle	Teads
advanced store	iPromote	Orange	Temelio
Affectv	Knorex	Outbrain	The Trade Desk
Amazon Ad System	KUPONA media	Platform161	TripleLift
Amobee	Lotame	Plista	Unicredit
Captify	MediaForge	Programattik	Ve Global
Conversant	MediaMath	Publicis Media	Verizon Media
Criteo	Microsoft Advertising	Quantcast	Vibrant Native
DataXu, Inc.	MiQ	Rakuten Marketing	Weborama
Delta Projects	mobile.de GmbH	Rubicon Project	Xaxis
Emerse	mPlatform	Salesforce DMP	Yieldlab AG
emetriq GmbH	Myntelligence	Scoota	Zemanta
Exponential Interactive	Nano Interactive	Semasio GmbH	Ziff Davis

** généré à partir du site https://www.youronlinechoices.com/

Il va sans dire que beaucoup de sociétés collectent des données. Les liens suivants montrent comment configurer son navigateur pour supprimer, autoriser et gérer les témoins (cookies)

- Comment supprimer, autoriser et gérer les cookies dans **Chrome** https://support.google.com/chrome/answer/95647?hl=fr
- Comment supprimer, autoriser et gérer les cookies dans **FireFox**

[5] https://www.priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/technologie/protection-de-la-vie-privee-en-ligne-surveillance-et-temoins/pistage-et-publicite/bg_ba_1206/

https://support.mozilla.org/fr/kb/parametres-vie-privee-historique-pas-pister

- Comment supprimer, autoriser et gérer les cookies dans **Safari** https://support.apple.com/fr-fr/guide/safari/sfri35610/mac
- Comment supprimer, autoriser et gérer les cookies dans **Edge** https://support.microsoft.com/fr-ca/help/17442/windows-internet-explorer-delete-manage-cookies

Concept d'anonymisation

L'article 23 du PL-64 précise le concept anonymisation :

> «23. Lorsque les fins auxquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, la personne qui exploite une entreprise doit le détruire ou l'anonymiser, sous réserve d'un délai de conservation prévu par une loi.
>
> **Pour l'application de la présente loi, un renseignement concernant une personne physique est anonymisé lorsqu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne.**
>
> Les renseignements anonymisés en vertu de la présente loi doivent l'être selon les **meilleures pratiques généralement reconnues**. ».

Texte de l'entrevue de Ruth Boardman[6]

Ruth Boardman, *Bird & Bird, Partner and International Data Protection Practice Co-Head*

Personal data protection and focus going forward
The EU General Data Protection Regulation has been responsible for a significantly increased focus on and protection of personal data.

We see the evidence of this all around us on a daily basis. Publicly, we see the more detailed data protection notices required by Articles 13 and 14, as well as the increased media coverage of stories in which privacy and data protection issues are key. Professionally, we have all worked (very!) hard to review personal data processing activities against the exacting GDPR standards and strengthen privacy programs to ensure compliance going forward. We have also welcomed many new people as data protection and privacy professionals and as new friends and colleagues.

The GDPR has achieved this not just in the European Economic Area, but also on a worldwide basis, with countries from Brazil to Thailand updating their laws and looking to the GDPR as a major point of reference.

With all these (and other) achievements, the GDPR must be regarded as a success. But because there is always room for improvement, I'd like to suggest two birthday wishes for the

[6] https://iapp.org/resources/article/gdpr-at-two-expert-perspectives/

European Commission to make, when it blows out the candles on the GDPR's second birthday cake.

First, enforcement. The EDPB's contribution to the commission's report on the GDPR shows that data protection authorities are taking enforcement measures. However, there are still relatively few decisions imposing significant sanctions. When data protection professionals advise their commercial colleagues on what is needed to comply with the GDPR, increasingly, businesses push back and point to competitors who are not fully complying and where no sanctions have been imposed. The fact that others are behaving in a particular way does not, of course, mean that the approach is correct. We are seeing increasing volumes of data protection litigation, from small claims by individuals, through to representative actions and group litigation. However, private enforcement by individuals cannot take the place of action by supervisory authorities, and the more time goes by without substantial sanctions being imposed, the more this undermines the credibility of GDPR and the ability of data protection officers and privacy counsel to promote compliance in their organizations.

Second, **keep the balance between data protection and innovation** under review and **be willing to make adjustments**. **Data protection authorities and legislators often say that there is no need to choose between strong privacy protection and the benefits that new technology can bring — that strong data protection laws engender consumer trust on which new services depend**. While this is a rhetorical commonplace — and can sometimes be true — it is not always the case. Often, there are trade-offs; data protection laws can inhibit new services and this is not always to the benefit of individuals. To take one example of this, consumers suffer when they are the victims of identity theft and when payments are fraudulently allocated to them. However, in some member states, it is not possible to provide such services and comply with data protection law. It is important that the commission and member states are alert to areas where data protection is proving overly restrictive so that appropriate adjustments can be made.

[1] Because (in some member states) this would be regarded as an automated individual decision, would not be regarded as contractually necessary and would not be authorised by an EU or member state law. The services would not be effective if purchasers have a free choice as to whether or not to consent to the fraud prevention technology being used.