27 juin 2023

Présentation à la Commission d'accès à l'information sur les lignes directrices relatives aux critères d'un consentement valable

Introduction

L'Association canadienne du marketing (ACM) apprécie grandement l'occasion qui lui est donnée de faire part à la Commission d'accès à l'information (CAI) de ses commentaires sur son projet de lignes directrices relatives aux critères de validité du consentement. Compte tenu des changements importants apportés à la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec, il est essentiel que la CAI consulte l'industrie pour s'assurer que ses lignes directrices sont pratiques et efficaces.

Les économies modernes reposent sur l'échange de renseignements personnels. Lorsqu'une personne fournit des renseignements personnels à une organisation dans le cadre de l'achat de biens ou de services, elle s'attend raisonnablement à ce que l'organisation utilise ces renseignements pour mieux la servir. Les consommateurs exigent des renseignements beaucoup plus rapides et de meilleure qualité pour pouvoir identifier les services fournis par les entreprises, y accéder et prendre des décisions d'achat éclairées. L'utilisation responsable des données pour personnaliser leur expérience est essentielle pour offrir de la valeur aux consommateurs et répondre à leurs attentes de plus en plus complexes dans un monde en constante évolution. Une récente recherche révèle que 43 % des consommateurs canadiens conviennent que l'échange de données avec les entreprises est essentiel au fonctionnement de la société moderne – une hausse significative par rapport aux 35 % qui étaient d'accord avec cette affirmation en 2018[1].

La loyauté et la confiance des clients sont à la base de la réussite des entreprises. La plupart des organisations québécoises reconnaissent que de solides pratiques en matière de protection de la vie privée et des renseignements personnels leur confèrent un avantage concurrentiel. Elles s'efforcent de protéger et de respecter les intérêts des personnes qu'elles servent en matière de protection de la vie privée.

La loi sur la protection des renseignements personnels doit renforcer la protection de la vie privée des consommateurs tout en permettant aux organisations d'innover avec les données et de bien servir les consommateurs. Une approche de l'interprétation de la loi sur la protection des renseignements personnels fondée sur la gestion des risques et le contexte est essentielle pour garantir que la loi puisse résister à l'évolution rapide des technologies, des modèles d'entreprise et des attentes des consommateurs dans les années à venir.

Évaluation globale du projet de lignes directrices

Nous apprécions les efforts considérables déployés par la CAI pour élaborer ces lignes directrices détaillées et pour fournir des exemples concrets aux organisations. Cependant, comme indiqué ci-après, certaines interprétations de la CAI s'écartent considérablement du libellé du projet de loi C-25, entraînent des conséquences imprévues pour les consommateurs et les organisations, ou ne tiennent pas compte des difficultés pratiques liées à l'obtention du consentement dans un environnement de données complexe, exacerbant ainsi des problèmes tels que la lassitude de consentement.

Plusieurs exemples dans les lignes directrices considèrent explicitement les activités comme conformes ou non conformes. Cela amènera les organisations à éviter certaines activités sans analyse contextuelle suffisante. Il est essentiel que les exemples (et les lignes directrices) reflètent ce qui est exigé par la loi plutôt qu'une meilleure pratique facultative. Lorsque les directives suggèrent de telles mesures ambitieuses, elles doivent être clairement identifiées comme des meilleures pratiques, plutôt que comme des exigences légales.

Les lignes directrices sont longues (36 pages) et les entreprises, notamment les petites entreprises ayant un accès limité à des conseils juridiques, recherchent des conseils concis et simples sur la manière d'appliquer la Loi 25 à leurs activités. Les personnes qui n'ont pas de formation juridique devraient être en mesure de comprendre facilement comment les exigences légales de base s'appliquent dans la pratique. Nous félicitons

[1] Global Data Privacy: What the Consumer Really Thinks, GDMA, 2022.

la CAI d'avoir inclus le schéma de la page 13 en tant qu'outil visuel utile, et nous suggérons d'autres outils pratiques pour les organisations, tels qu'une liste de contrôle sommaire, un organigramme ou une vue d'ensemble des exigences juridiques de base « indispensables ».

L'ACM demande à la CAI de modifier les lignes directrices dans les sept domaines clés décrits ci-après. Dans tous les cas, nous exhortons la CAI de s'efforcer d'aligner ses lignes directrices sur celles des autres juridictions canadiennes afin de favoriser la compréhension des consommateurs, de veiller à ce que les entreprises puissent fonctionner de façon harmonieuse au-delà des frontières et de jeter les bases d'une large disponibilité des biens, des services et de l'investissement au Québec.

Demande d'un délai d'application raisonnable

Nous demandons à la CAI de confirmer publiquement que les lignes directrices ne seront pas appliquées avant 18 mois à compter de leur publication, compte tenu de l'incertitude qui entoure certaines dispositions et du fait que les organisations ont besoin du temps nécessaire pour mettre en œuvre les changements, y compris la préparation des systèmes et la formation du personnel.

Les organisations se sont préparées avec diligence à l'entrée en vigueur de la loi. Toutefois, certains aspects de la loi, en particulier l'article 8.1, ont donné lieu à une grande incertitude et à des désaccords fondamentaux en matière d'interprétation juridique. Les organisations ne seront pas suffisamment éclairées sur certains aspects de la loi tant que les lignes directrices officielles de la CAI n'auront pas été publiées. Cette publication devrait avoir lieu en octobre, soit un mois suivant l'entrée en vigueur des dispositions de la loi.

Les organisations auront besoin de suffisamment de temps pour mettre en œuvre les modifications requises aux plans de conformité, aux processus opérationnels, à la formation du personnel et aux systèmes TI. La mise en œuvre de l'article 8.1 nécessitera notamment que des modifications substantielles soient apportées aux politiques et procédures internes et externes, aux interfaces avec les consommateurs et aux ententes contractuelles avec les fournisseurs de services. À la lumière des difficultés opérationnelles insurmontables, certaines organisations et certains fournisseurs de services ont signalé leur intention de cesser leurs activités et leurs services au Québec s'il n'y a pas une période de mise en œuvre raisonnable.

Bon nombre de PME ne disposent pas des ressources nécessaires pour s'équiper rapidement afin de se conformer à cette disposition, tandis que les grandes entreprises disposant d'applications, de systèmes et de processus nombreux et complexes auront besoin de suffisamment de temps pour les reprogrammer et les reconcevoir, ainsi que pour former des centaines, voire des milliers d'employé(e)s.

Rétroaction détaillée

1. Consentement exprès obligatoire pour l'identification, le suivi et le profilage

Recommandation : Nous requérons que la section 13 des lignes directrices (afférente à l'article 8.1 de la loi) soit supprimée et fasse l'objet de lignes directrices distinctes – à élaborer en consultation avec l'ACM et d'autres intervenants du secteur – qui portent expressément sur la collecte de renseignements personnels par le biais de technologies d'identification, de localisation et de profilage. Cette recommandation se fonde sur le fait que l'article 8.1 de la loi n'est pas directement lié à l'objet de ces lignes directrices, que la nature et la portée des technologies de suivi et de profilage sont variées et nuancées et qu'il est absolument nécessaire que la CAI consulte le secteur de la publicité en ligne sur l'interprétation et la mise en œuvre de cet article afin d'éviter des conséquences imprévues pour les consommateurs et les organisations.

Si la CAI n'est pas disposée à créer des lignes directrices distinctes, il est essentiel que l'exigence de consentement exprès à l'article 8.1 soit appliquée de manière à se concentrer sur les situations qui dépassent les attentes raisonnables des individus et/ou qui comportent un risque de préjudice important. Dans ce cas, la demande d'un délai de 18 mois pour l'application active de cette ligne directrice devient critique.

La section 31b du projet de lignes directrices indique que les technologies qui permettent d'identifier des personnes, de les suivre ou d'effectuer un profilage doivent être désactivées par défaut, ce qui équivaut à une exigence de consentement exprès (adhésion) pour les organisations qui recueillent des renseignements personnels par le biais de l'une de ces technologies.

Cette approche va bien au-delà de l'interprétation de la loi, qui est rédigée comme une extension de l'obligation de transparence de l'article 8. La formulation de l'article 8.1 parle seulement d'une obligation d'informer les particuliers des moyens disponibles pour activer ces fonctions, sans indiquer explicitement que ces moyens doivent effectivement exister ou que les fonctions elles-mêmes doivent être désactivées par défaut. L'article 8.1 est totalement distinct de l'article 9.1, qui n'impose des paramètres de confidentialité par défaut qu'à l'offre au public d'un « produit ou service technologique doté de paramètres de confidentialité », et non à l'utilisation de technologies de profilage et de suivi de manière plus générale.

Nous soutenons pleinement une plus grande transparence. Cependant, l'interprétation extrême de cette disposition par la CAI exigerait un consentement exprès pour toute collecte de renseignements personnels par l'utilisation de la technologie, dans tous les cas et dans tous les contextes. En plus d'aller au-delà des exigences explicites de la loi, cette exigence catégorique de consentement exprès n'adopte pas une approche basée sur les risques et aura des conséquences inattendues pour les consommateurs, les organisations et l'économie numérique dont ils dépendent.

Il n'y a aucune raison de restreindre ce type d'activité, à moins qu'il n'y ait un risque clair de préjudice. L'époque où l'on recueillait des renseignements personnels au moyen d'un stylo et d'un papier est révolue depuis longtemps. C'est grâce à la technologie que les entreprises recueillent maintenant des données pour servir leurs clients. L'application de l'article 8.1 à **toutes** les technologies est extrêmement large et inapplicable. Par exemple, toutes les technologies qui « identifient » ou « localisent » des personnes couvriraient un large éventail d'activités courantes et non nuisibles.

Ainsi, il est courant que les sites Web déduisent la localisation afin de diriger les utilisateurs vers le site approprié pour leur pays, reflétant la tarification, la devise et la disponibilité des produits. Un site Web peut recueillir des adresses IP afin d'éviter de diffuser des contenus protégés par des droits d'auteur à des utilisateurs résidant dans une juridiction pour laquelle le fournisseur du site Web ne détient pas les droits de mise à disposition de ces contenus.

Les détaillants utilisent souvent des données de localisation déduites pour afficher le magasin le plus proche d'un utilisateur, ses heures d'ouverture et ses coordonnées, ainsi que les ventes ou les circulaires applicables à cet endroit. Les opérateurs des centres d'appels utilisent les codes de zone, à partir desquels la localisation peut être déduite, pour acheminer les appels vers un centre d'appels approprié.

Dans de nombreux cas, la fonction de suivi ou de profilage est l'objectif principal de l'application ou d'une autre technologie, rendant inutile l'exigence d'un consentement exprès et créant des charges inutiles pour les consommateurs. Par exemple, une application de covoiturage ne peut fonctionner sans accéder à la localisation; une application de suivi de la condition physique ne peut fonctionner sans suivre l'activité et les performances de l'utilisateur.

Bien entendu, dans d'autres cas, le consentement exprès serait raisonnablement requis, par exemple lorsqu'une fonction optimise la prestation du service global plutôt qu'elle ne lui est indispensable. Par exemple, le suivi de la localisation peut ne pas être nécessaire pour utiliser un site ou une application de rencontre, mais pourrait donner aux utilisateurs la possibilité d'activer la géolocalisation pour améliorer leur expérience en leur montrant les autres utilisateurs qui se trouvent à proximité.

Les entreprises nationales ou internationales devraient recueillir une certaine forme de renseignements personnels (comme une adresse IP) pour savoir si elles traitent avec un particulier au Québec, afin de se conformer non seulement à la Loi 25, mais aussi à d'autres réglementations, y compris les lois linguistiques du Québec. Si les entreprises ont besoin d'un consentement exprès pour déterminer la localisation des personnes, cette exigence semble absurde. Les utilisateurs qui visitent des sites Web devraient se voir présenter une page de renvoi leur permettant de consentir à la déduction de la localisation avant de

poursuivre. Dans quelle langue cette page serait-elle rédigée? Quelle formulation serait nécessaire pour répondre aux exigences de la juridiction locale si l'entreprise n'avait pas connaissance de cette juridiction?

La définition du profilage est également extrêmement large. Dans le secteur du marketing, le profilage sert à offrir aux consommateurs les types d'expériences significatives et intuitives qu'ils s'attendent aujourd'hui des organisations (contrairement à l'ancienne pratique du pollupostage générique de masse), notamment par l'utilisation d'outils et de logiciels d'analyse de tiers, tels que les témoins, les pixels et les balises. Par exemple, les organisations peuvent créer un profil afin de suggérer des produits et des services plus pertinents en fonction des préférences ou des intérêts d'une personne, ou de proposer des prix réduits pour des produits et des services en fonction des intérêts, de la fiabilité, du comportement ou de la localisation d'une personne.

Une enquête récente a révélé que 50 % des consommateurs souhaitent voir des publicités sur Internet qui leur soient pertinentes et ciblées[2]. D'autres recherches ont démontré que les gens veulent vivre des expériences qui ont de la valeur pour eux en tant qu'individus. Dans l'ensemble, les consommateurs se sentent plus à l'aise lorsqu'ils partagent leurs données et qu'ils comprennent ce qu'ils en retirent. En ce qui concerne la publicité en ligne, l'étude a démontré que l'attitude des gens à l'égard de la protection de la vie privée en ligne évolue en fonction de la valeur perçue de la publicité. Les gens apprécient les publicités lorsqu'elles sont adaptées à leurs centres d'intérêt, qu'elles leur permettent de gagner du temps ou de réaliser des économies, et qu'elles sont portées à leur attention au bon moment.

Les clients s'attendent de plus en plus des entreprises qu'elles prennent des mesures pour prévenir les problèmes avant qu'ils ne surviennent, qu'elles sachent quand, où et comment les contacter, et qu'elles interviennent de manière proactive si nécessaire. Ce type d'expérience consommateur nécessite une compréhension des clients grâce à des profils bien conçus. Au niveau le plus élémentaire, il pourrait s'agir d'un restaurant voulant utiliser un outil automatisé pour enregistrer le vin préféré d'un client afin de le lui proposer lors de sa prochaine visite.

Même dans le cadre du GDPR, le profilage n'est limité que par le droit d'une personne à se retirer des décisions uniquement automatisées qui produisent des effets juridiques ou des effets significatifs similaires. Comme le souligne Axel Voss (membre du Parlement européen et l'un des premiers rédacteurs du GDPR), l'absence de contexte reste une lacune du GRPR, car il observe « ...un manque de distinction entre le traitement automatisé, y compris le profilage, qui est attendu par les individus et qui contribue à des services plus efficaces pour les individus et à un contenu plus pertinent, et le profilage qui crée un préjudice, tel que la manipulation politique, ou un effet d'enfermement commercial pour lequel des garanties spécifiques devraient être mises en place... »[3].

Le consentement n'est qu'un des moyens pour garantir la protection de la vie privée. Il est important que le consentement ne soit pas surutilisé au point de devenir illusoire.

L'exigence générale se traduira par une avalanche de fenêtres contextuelles, la plupart des consommateurs se retirant[4] au nom d'une réduction perçue du risque, même dans les cas où il n'y a pas de risque significatif pour eux et où ils peuvent même bénéficier d'un avantage substantiel. Cette exigence exacerbera également la lassitude généralisée à l'égard du consentement que les consommateurs ressentent déjà, ce qui les rendra encore moins enclins à examiner attentivement les notifications et à prendre des décisions éclairées en matière de protection de la vie privée.

En se désinscrivant sans examiner et prendre en compte l'avis de consentement, les consommateurs se priveront par inadvertance de renseignements qui pourraient leur être utiles.

[2] Canada's Digital Marketing Pulse, Ipsos, 2019.
[3] Axel Voss, Fixing the GDPR: Towards Version 2.0, Axel Voss, 2021.
[4] Nous pouvons estimer que ce sera le cas en nous basant sur la mise en œuvre de la transparence du suivi des applications par Apple au printemps 2021, qui a entraîné un plafonnement du taux de consentement au suivi et à la traçabilité à environ 25 %.

D'importantes recherches menées dans l'UE ont montré que les avis de confidentialité excessifs déchargent le consommateur d'une trop grande responsabilité sans qu'il soit possible de prouver qu'il comprend mieux la notion de confidentialité et qu'il y est sensibilisé. À titre d'exemple, 72 % des consommateurs indiquent qu'ils sont ennuyés par le nombre de fois où ils doivent accepter des témoins pour accéder à un contenu. Dans le but d'éviter des sanctions sévères, beaucoup d'organisations demandent le consentement de leurs clients à de multiples reprises, à travers de nombreux points de contact différents[5]. C'est pourquoi les réformes du gouvernement britannique sur la protection des données de 2023 comprennent une gamme élargie d'exemptions au consentement pour les témoins afin de réduire l'assaut des bannières de consentement pour les témoins. (La Loi 25 exclut expressément les témoins de navigateur de l'article 8.1, qui exige le plus haut niveau de confidentialité par défaut. Toutefois, les témoins de navigation ne sont pas exclus de cette disposition, ce qui est source de confusion pour les organisations.)

L'Alliance de la publicité numérique du Canada (APNC) collabore avec les gouvernements et les intervenants dans l'ensemble du pays pour mettre en place un programme d'autoréglementation qui offre transparence et choix aux consommateurs dans le contexte de la publicité ciblée par centres d'intérêt. Le programme a été conçu en tenant compte de la nature complexe des flux mondiaux de données dans le domaine de la publicité en ligne, et dans le but de donner aux consommateurs les moyens d'agir sans les accabler.

L'écosystème de la publicité numérique n'est qu'un des nombreux écosystèmes de données complexes qui offrent une valeur considérable aux individus et qui sont au cœur de la prospérité et de la compétitivité mondiale du Québec. Nous exhortons la CAI de collaborer avec l'ACM et d'autres associations industrielles clés afin d'approfondir sa compréhension des écosystèmes de données complexes dans différents secteurs et de s'appuyer sur les initiatives d'autoréglementation en cours. L'ACM serait heureuse d'organiser une réunion entre la CAI et d'autres acteurs de la publicité numérique pour discuter des aspects pratiques de l'opérationnalisation des exigences en matière de protection de la vie privée dans cet espace.

Sans tenir compte du contexte et du risque, l'exigence de consentement exprès est totalement inapplicable pour les organisations et inutilement contraignante pour les consommateurs, sans fournir de protection supplémentaire significative de la vie privée. Face à une exigence aussi large, nous nous attendons à ce que certaines entreprises cessent complètement de fournir des services aux individus situés au Québec plutôt que de faire face aux difficultés opérationnelles et aux taux de consentement probablement faibles. Cela s'est déjà produit dans l'UE, où certaines exigences peu pratiques de la loi ont entraîné une réduction de l'offre de biens et de services pour les consommateurs de l'Union européenne, sans qu'il y ait eu d'avantages avérés en matière de protection de la vie privée[6].

Nous sommes favorables à une plus grande transparence dans toutes les situations où une organisation recueille des renseignements personnels à l'aide d'une technologie permettant d'identifier, de localiser ou d'établir le profil d'une personne. Cela répond de manière adéquate à l'exigence du texte de loi, qui est d'informer une personne de l'utilisation d'une telle technologie et des moyens disponibles (le cas échéant) pour l'activer. Elle est également adaptée au risque d'atteinte à la vie privée que représentent les collectes régulières et non préjudiciables de renseignements personnels par le biais de ces technologies. Nous sommes également très favorables aux options qui permettent aux consommateurs de désactiver ou de refuser les technologies de suivi lorsqu'elles ne sont pas raisonnablement nécessaires à la prestation du service en question.

L'information peut se faire par différents moyens et les organisations peuvent adopter une approche à plusieurs niveaux, selon ce qui est approprié et raisonnable (p. ex. des renseignements généraux dans une politique de confidentialité, des conditions générales, un site Web, des FAQ et des renseignements plus précis sur des formulaires ou dans d'autres communications directes telles qu'un avis « juste à temps » ou une fenêtre contextuelle). La notification doit toujours être raisonnablement visible, et les organisations doivent indiquer clairement à leurs clients quelles fonctions sont activées par défaut (c.-à-d. « En téléchargeant cette application, vous serez profilé, ce qui signifie… »). En plus d'indiquer clairement à leurs clients quelles

[5] Consent Fatigue,The Data Privacy Group, 2022.
[6] Les écueils des lois sur la protection de la vie privée : Enseignements tirés de l'Union européenne, Association canadienne du marketing, 2022.

fonctions sont activées par défaut, les organisations devraient préciser les choix dont disposent les personnes pour accepter expressément les fonctions correspondant à leurs préférences.

Si l'exigence de consentement exprès est maintenue dans cette version des lignes directrices (c.-à-d. celles sur le consentement valable et non dans des lignes directrices distinctes à venir), les lignes directrices devraient exiger des organisations qu'elles prennent des mesures plus importantes pour les activités potentiellement préjudiciables en procédant à une évaluation contextuelle pour déterminer si le consentement exprès est approprié dans les circonstances.

Les organisations devraient tenir compte des facteurs suivants dans leur évaluation.

- **Les attentes raisonnables des particuliers**. Voici quelques exemples :
  - Une personne télécharge l'application d'un café. Le café suit la localisation du client pour déterminer quand un visiteur entre dans le magasin d'un concurrent afin de lui envoyer une offre ou un coupon personnalisé. Le suivi de la localisation lorsqu'une application n'est pas utilisée activement dépasserait les attentes raisonnables d'une personne, et un consentement exprès serait raisonnable.
- **La sensibilité des renseignements concernés**. L'identification, la localisation et le profilage devraient nécessiter un consentement exprès pour toute activité susceptible d'être associée à des renseignements médicaux, biométriques ou autrement intimes, ou de les révéler, ou dont le contexte d'utilisation ou de divulgation donne lieu à une attente raisonnable élevée en matière de respect de la vie privée (conformément à la section 31a des lignes directrices). Voici quelques exemples :
  - Une personne membre d'un groupe communautaire sur une plateforme de médias sociaux se voit proposer une publicité pour un produit lié à la santé ou à l'intimité en fonction des messages postés au sein du groupe ou des amis de l'utilisateur. Étant donné que ce profilage est associé à des renseignements pour lesquels il existe une attente raisonnable élevée en matière de respect de la vie privée, un consentement exprès serait raisonnable.
  - Le consentement exprès serait requis en cas d'utilisation d'une empreinte digitale ou d'une image faciale, de suivi du rythme cardiaque d'une personne ou de collecte de renseignements relatifs à l'origine ethnique, aux opinions politiques, aux croyances religieuses ou philosophiques, à l'état de santé ou à la vie sexuelle, ou à l'orientation sexuelle.
- **Le risque de préjudice pour la personne**. Voici quelques exemples :
  - Étant donné le risque de problèmes de sécurité réels, un consentement exprès serait raisonnablement requis pour la localisation précise dans le contexte de certaines applications de médias sociaux, telles que les applications de rencontres.

Il est essentiel que les lignes directrices définissent mieux ce que l'on entend par « profilage », « identification » et « localisation » et, en collaboration avec les intervenants du secteur, qu'elles réduisent le champ d'application de la technologie à laquelle l'exigence s'appliquerait. Par exemple, le terme « localisation » devrait être défini comme une tentative de déterminer l'emplacement géographique d'une personne physique avec une exactitude et une précision raisonnables, comme l'identification des coordonnées de longitude/latitude, ou avec une précision de quelques mètres. La « localisation » ne doit pas permettre de déduire qu'un utilisateur se trouve dans un pays ou une ville en particulier, ce qui peut être déduit de l'adresse IP ou du fournisseur d'accès à Internet. La portée des technologies de profilage auxquelles s'applique cette exigence devrait également être clarifiée, car l'interprétation actuelle couvre bien plus que les risques perçus liés à certaines applications et à certains réseaux sociaux, qui semblaient être l'objectif initial de l'article 8.1.

2. Consentement exprès et lassitude de consentement

Recommandation : Pour garantir un consentement valable, nous demandons à la CAI d'indiquer que le consentement exprès peut être la forme préférée de consentement dans de nombreux cas; de ne pas encourager les organisations à demander un consentement exprès dans la mesure du possible (section 30). La Loi 25 n'exige pas de consentement exprès « dans la mesure du possible » et le fait d'encourager les organisations à recueillir un consentement explicite de cette manière aurait pour effet d'exacerber considérablement t la lassitude de consentement. De plus, les exemples visant à réduire la lassitude de consentement à la section 33 devraient être remplacés par des meilleures pratiques plus efficaces.

La section 30 des lignes directrices indique qu'une organisation doit rechercher le consentement exprès chaque fois que cela est possible. Cette priorité au consentement exprès n'existe pas dans la loi, et il ne s'agit pas d'une interprétation raisonnable de la loi. La loi exige une autorisation légale, qui peut être obtenue de différentes manières, par exemple en remplissant les conditions du consentement présumé, implicite ou exprès. Une fois les conditions remplies, la collecte, l'utilisation ou la divulgation de renseignements personnels est légale.

Cette disposition est conforme à d'autres cadres de protection de la vie privée au Canada. Compte tenu des préoccupations sérieuses concernant la lassitude de consentement, il est essentiel que les organisations aient la possibilité de choisir le type de consentement approprié en fonction des circonstances. Encourager les organisations à opter par défaut pour le consentement exprès n'est pas seulement peu pratique, mais cela compromet également l'utilité du consentement exprès, qui pourrait être vidé de son sens s'il est utilisé trop souvent et s'il n'est pas réservé aux renseignements sensibles ou aux utilisations inattendues. En outre, le fait de demander systématiquement un consentement exprès aurait une incidence négative sur l'expérience du client et pourrait également créer une confusion pour les personnes en donnant à penser qu'elles n'ont pas besoin de consentir au traitement des renseignements personnels qui est nécessaire pour fournir le produit ou le service.

Dans la section 33 des lignes directrices, la CAI a explicitement reconnu que la lassitude de consentement était un problème. Toutefois, les exemples présentés comme des solutions pour y remédier, notamment la rupture du rythme par une question mathématique ou une période d'attente, ne feront qu'accroître la frustration et la lassitude des consommateurs, les amenant à se désengager du processus. Il est important de traiter la cause sous-jacente, à savoir la surcharge de renseignements attribuable à la fréquence et au volume élevés des demandes, et non le symptôme. Il ne s'agit pas d'être attentif, mais d'avoir la capacité générale d'accepter les renseignements et les actions demandés. En outre, la suggestion d'une période d'attente ou d'un compte à rebours pourrait être perçue comme une pression exercée sur le consommateur pour qu'il donne son consentement, ce qui va à l'encontre du concept de consentement « libre ». En fin de compte, la meilleure défense contre la lassitude de consentement consiste à s'assurer que le consentement exprès n'est requis qu'à des fins qui dépassent les attentes raisonnables des individus ou qui pourraient donner lieu à un préjudice important.

Les exemples devraient plutôt refléter les meilleures pratiques ayant fait l'objet de recherches approfondies, telles que celles figurant dans le guide du Commissariat à la protection de la vie privée du Canada sur le consentement valable.

3. Caractère granulaire : un consentement distinct pour chaque finalité

Recommandation : L'exigence de caractère granulaire de la section 59 des lignes directrices devrait permettre de regrouper des finalités similaires et logiquement liées, pour autant que chaque finalité soit clairement précisée et que les regroupements ne soient pas flous ou trompeurs.

La section 59 du projet de lignes directrices indique que le consentement doit être granulaire et demandé séparément pour chaque finalité. Cette disposition est inapplicable pour les organisations et se traduira par une expérience très médiocre pour les individus. De nombreuses entreprises, y compris celles qui offrent des biens et des services essentiels aux Québécois, ont de multiples secteurs d'activité et interactions avec leurs clients. Par exemple, si l'entreprise de télécommunications moyenne devait demander le consentement séparément pour chaque finalité, les consommateurs seraient confrontés à des douzaines de demandes.

Nous convenons que chaque finalité doit être clairement précisée et que les entreprises doivent identifier de manière transparente les finalités dans un format granulaire. Cependant, il n'est pas réaliste d'attendre des organisations, des clients et des employés qu'ils suivent un processus de consentement aussi lourd et répétitif.

Les entreprises devraient être autorisées à recueillir un seul consentement pour des finalités multiples si ces finalités sont liées et si cela n'induit pas en erreur. Par exemple, une entreprise peut choisir de regrouper les finalités par thème (p. ex. celles qui sont essentielles à la fourniture du produit/service demandé, à des fins de

fraude, d'analyse, de communication avec le client (marketing personnalisé), de consultation (enquêtes, etc.)).Les organisations devraient déterminer la meilleure approche à adopter en fonction des circonstances pour améliorer la compréhension des consommateurs, en concentrant l'exigence de granularité sur les finalités secondaires ou sur les situations où les personnes ont un choix significatif.

La création d'une mosaïque de consentements, avec des personnes consentant à certains éléments mais pas à d'autres, créerait un environnement excessivement complexe tant pour les organisations que pour les consommateurs, et ne tiendrait pas compte du fait que les finalités sont souvent interconnectées. Les exemples 60.1 et 60.2 sont trop simples pour montrer la véritable nature nuancée du fonctionnement des organisations; le fait que vous consentiez à l'un n'a pas d'incidence sur le fait que vous consentiez à l'autre.

4. Authentification de la personne concernée – consentement parental

Recommandation : La section 25 des lignes directrices devrait indiquer que les organisations doivent faire tout leur possible pour vérifier le consentement parental avec un degré de certitude raisonnable compte tenu des circonstances. En outre, l'exigence d'un tel degré de certitude devrait être axée sur les organisations qui savent, ou sont réputées savoir, qu'elles traitent des renseignements personnels de mineurs. Cette approche est conforme à celle adoptée par la Children's Online Privacy Protection Act (loi sur la protection de la vie privée des enfants en ligne) aux États-Unis, ainsi qu'aux lois sur la protection de la vie privée en Californie et dans l'UE, et éviterait de cibler les organisations qui ne traitent les données des mineurs qu'incidemment et sans le savoir.

L'ACM soutient la protection des données des mineurs et, depuis de nombreuses années, joue un rôle de premier plan dans l'établissement de normes en matière de marketing auprès des enfants par le biais de son Code de déontologie et des normes de pratique du Canada.

La section 25 des lignes directrices indique que lorsque le consentement parental est requis pour un mineur de moins de 14 ans, l'organisation doit vérifier le statut de la personne qui donne son consentement « toujours avec un degré de certitude raisonnable ». L'exigence d'un degré de certitude raisonnable pourrait s'avérer être un standard incroyablement strict pour de nombreuses organisations. Dans la plupart des contextes en ligne, il est impossible de vérifier si le consentement parental est authentique ou si un mineur de moins de 14 ans atteste et accède lui-même à un service sans la collecte intrusive de pièces d'identité délivrées par le gouvernement, de données biométriques et d'autres renseignements sensibles.

Par conséquent, les lignes directrices proposées peuvent conduire inutilement à la collecte et à la conservation systématiques de renseignements personnels sensibles dans le seul but de satisfaire à l'exigence de certitude que l'organisation ne traite pas avec des mineurs. En outre, les organisations seront incitées à conserver ces informations d'authentification afin de prouver qu'elles respectent la loi en cas de contestation.

Les renseignements personnels requis pour vérifier l'âge peuvent être parmi les plus sensibles (p. ex. une pièce d'identité délivrée par le gouvernement avec la date de naissance). Ils présentent le plus grand risque en cas de violation et sont les plus recherchés par les criminels. Dans de nombreux cas, les risques associés à la collecte et à la conservation de ces renseignements dépasseraient de loin le risque potentiel pour la vie privée d'un mineur qui accèderait à un service destiné aux adultes ou à une population plus générale. En l'absence de la modification proposée par l'ACM, les organisations qui ne ciblent pas les mineurs, ou dont les activités ne sont pas connues pour attirer un grand nombre de mineurs, collecteront et conserveront des renseignements personnels supplémentaires sur tous les clients, sans autre raison que de confirmer qu'ils ne sont pas mineurs. Compte tenu des risques sérieux de préjudice associés à l'accès non autorisé à ces renseignements personnels, il s'agit peut-être d'un cas où le remède est pire que le mal.

5. Absence de consentement valable en tant qu'incident de confidentialité

Recommandation : La section 16 des lignes directrices devrait être supprimée et traitée dans le cadre des lignes directrices sur les incidents de confidentialité, qui traitent de manière plus appropriée des situations de perte et d'utilisation ou de divulgation non autorisée.

La section 16 des lignes directrices indique que le défaut d'obtention d'un consentement valable est un incident de confidentialité, ce qui signifie que si une organisation détecte un problème lié au défaut d'obtention d'un consentement valable, elle doit se conformer aux obligations liées à l'incident (tenue de registres, évaluation du risque ou du préjudice, notification, etc.).

Nous sommes tout à fait d'accord sur le fait que le défaut d'obtention d'un consentement valable constitue une violation de la loi et peut faire l'objet d'une mise en application. Toutefois, cette extension des obligations liées aux incidents de confidentialité typiques est très inhabituelle et contraste avec la façon dont ces incidents sont actuellement considérés au Québec et dans l'ensemble du pays. La grande majorité des incidents de confidentialité ne constituent pas une violation du consentement. De plus, la grande majorité des circonstances dans lesquelles le consentement n'a pas été respecté ne donneraient pas lieu à un déclenchement de la notification (préjudice important).

La raison pour laquelle cette question, qui est liée à la gouvernance des données, est abordée ici (dans les lignes directrices relatives aux critères de consentement valable) plutôt que dans les lignes directrices relatives aux incidents de confidentialité n'est pas claire.

6. Demandes répétées de consentement en tant que violation du consentement libre

Recommandation : La section 41b des lignes directrices devrait être adaptée pour permettre aux organisations de demander à nouveau le consentement à des intervalles appropriés.

La section 41b des lignes directrices indique que le consentement ne peut généralement être demandé qu'une seule fois pour la même finalité (à moins qu'un changement substantiel du contexte ne le justifie). Il ne s'agit pas d'une exigence de la loi et, dans certains cas, cette exigence n'est absolument pas pratique.

Dans de nombreux cas, les entreprises ne peuvent pas savoir si une personne a déjà été invitée à donner son consentement, par exemple si une personne utilisant un ordinateur public pour consulter un site Web en libre accès (où elle ne s'identifie pas) choisit de ne pas se soumettre au suivi des témoins. Cette exigence est du même coup en contradiction avec l'obligation imposée aux organisations de réduire au minimum la quantité de données recueillies, étant donné que l'un des meilleurs moyens d'éviter de demander un consentement répété est d'obtenir suffisamment de données.

Bien que nous soyons d'accord pour dire qu'il est inacceptable de harceler un consommateur avec des demandes fréquentes, il est raisonnable et bénéfique pour les organisations de fournir aux gens des options supplémentaires pour ajuster leurs préférences à des intervalles appropriés. Les préférences des consommateurs évoluent avec le temps, et les consommateurs sont souvent invités à donner leur consentement après un laps de temps approprié. À titre d'exemple, si vous êtes un utilisateur non connecté qui achète un livre sur un site web, on peut vous demander votre consentement pour vous inscrire sur la liste de diffusion de l'entreprise lors de vos prochaines visites d'achat de livres. Cela ne violerait pas la nature libre du consentement, à condition qu'il y ait un avis visible et la possibilité d'exercer votre choix. Même la Cour suprême du Canada a indiqué que le fait de poser la même question des dizaines de fois à un accusé qui a fait valoir son droit au silence ne s'oppose pas à la Charte canadienne des droits et libertés[7].

La section 41b des lignes directrices devrait reprendre l'expression « intervalles appropriés » de la section 69 des lignes directrices (qui indique que lorsqu'une organisation demande un consentement pour une très longue période, elle devrait accorder une attention particulière à la transparence sur une base continue, en effectuant un appel aux individus à intervalles appropriés). En ce qui concerne la section 69 des lignes directrices, nous notons que le fait d'informer les personnes de la durée de validité du consentement n'est pas une exigence de la loi et que, dans certains cas, cela peut ne pas être nécessaire ou approprié. Il s'agit d'un exemple où les lignes directrices vont au-delà de ce qui est exigé par la loi. Cela devrait donc être identifié comme une meilleure pratique, plutôt qu'une exigence.

[7] R. c. Singh, [2007] 3 RCS 405.

Nous notons également que les exemples donnés dans les lignes directrices suggèrent souvent des fenêtres contextuelles comme moyen d'obtenir le consentement. Il est important d'illustrer les nombreuses autres façons par lesquelles les organisations peuvent obtenir le consentement, d'autant plus que de nombreux consommateurs les trouvent ennuyeux et que de nombreux navigateurs de gestion de la vie privée bloquent les fenêtres contextuelles.

7. Renseignements requis pour le consentement présumé

Recommandation : Afin d'éviter toute confusion pour les organisations, les lignes directrices devraient mieux articuler les renseignements expressément requis d'emblée pour que le consentement présumé soit valable.

Les lignes directrices semblent exiger davantage de renseignements pour justifier le consentement présumé que ce que prévoit la loi, y compris certains renseignements qui ne doivent être disponibles que sur demande. D'un point de vue pratique, il serait utile que les lignes directrices suggèrent lesquels de ces renseignements doivent être mentionnés dans une politique de protection de la vie privée ou incluses dans une approche stratifiée. Il est important que les organisations adoptent une approche pragmatique de la superposition des renseignements. Par exemple, il est raisonnable que les organisations s'appuient sur une politique de protection de la vie privée fournie au consommateur lorsque le consentement est demandé pour des activités courantes et qu'une notification plus ciblée, juste à temps, puisse être déclenchée pour des pratiques qui dépassent les attentes raisonnables d'une personne.

Il serait également utile que les lignes directrices clarifient la manière dont les organisations doivent assurer le suivi du consentement présumé, qui est vraisemblablement assuré par la tenue d'un registre de la divulgation des finalités et de la fourniture ultérieure de renseignements personnels par la personne concernée.

Pour toute question ou tout commentaire concernant cette soumission, veuillez communiquer avec :

Sara Clodman
VP, Affaires publiques et leadership éclairé

sclodman@theCMA.ca

Fiona Wilson
Directrice, Politiques publiques et cheffe de la protection des renseignements personnels
fwilson@theCMA.ca

À propos de l'Association canadienne du marketing

L'ACM est la voix du marketing au Canada et notre objectif est de défendre l'impact puissant du marketing. Nous sommes le catalyseur qui aide les spécialistes du marketing du Canada à prospérer aujourd'hui, tout en construisant l'état d'esprit et l'environnement marketing de demain.

Nous offrons à nos membres, d'un océan à l'autre, la possibilité de se développer professionnellement, de contribuer au leadership éclairé en matière de marketing, de créer des réseaux solides et de renforcer le climat réglementaire propice à la réussite des entreprises. Notre titre de Chartered Marketer (CM) signifie que les récipiendaires sont hautement qualifiés et qu'ils sont au fait des meilleures pratiques, comme en témoigne le Code de déontologie et des normes du marketing du Canada. Nous représentons pratiquement tous les grands secteurs d'activité du Canada, ainsi que toutes les disciplines, tous les canaux et toutes les technologies du marketing. Notre Centre des consommateurs aide les Canadiens à mieux comprendre leurs droits et obligations. Pour de plus amples renseignements, visitez le site thecma.ca.