8 FÉVRIER 2023

La première décision rendue par le CPVP en 2023 aura des répercussions sur les contrats des tiers fournisseurs de services de traitement de données

Auteurs : Corey Omer, Sumeet Dang, Alexander Max Jarvie et Gillian R. Stacey

Le Commissariat à la protection de la vie privée du Canada (CPVP) a récemment publié ses conclusions en lien avec une plainte de client selon laquelle Home Depot du Canada (Home Depot) avait enfreint la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) en communiquant les renseignements personnels de clients à la société mère de Facebook, Meta Platforms Inc. (Meta), sans les en avoir informés et sans obtenir leur consentement.

Comme le CPVP l'explique dans ses conclusions, publiées le 26 janvier 2023, entre 2018 et octobre 2022, Home Depot a fait parvenir à Meta la version hachée de l'adresse électronique de clients et les détails de leurs achats en magasin à l'aide d'un outil connu sous l'appellation « Conversions hors ligne ». Meta a ensuite utilisé ces renseignements pour mesurer l'efficacité des publicités diffusées auprès de ces mêmes clients sur Facebook et en faire rapport à Home Depot. Le libellé des conditions générales d'utilisation de l'outil de Meta était suffisamment souple pour lui permettre d'utiliser les renseignements des clients à ses propres fins commerciales, sans lien avec Home Depot.

Le CPVP a conclu que l'échange de renseignements sur les clients entre Home Depot et Meta constituait une divulgation à un tiers en vertu du droit canadien sur la protection des renseignements personnels et que les clients ne pouvaient pas raisonnablement s'attendre à une telle divulgation. Le CPVP a conclu que Home Depot aurait dû obtenir, par conséquent, le consentement explicite actif des clients à l'égard de cette pratique au plus tard au moment de la collecte des renseignements.

Les conclusions – les premières publiées par le CPVP en 2023 – donnent un aperçu important du point de vue actuel du CPVP sur la forme de consentement à obtenir, l'étendue de la divulgation requise pour obtenir un consentement valable et l'autorisation à obtenir pour utiliser des renseignements personnels à des fins secondaires. Elles fournissent également une mise en garde contre les formulations vagues ou permissives dans les contrats des tiers fournisseurs de services.

Principaux points à retenir pour les entreprises

- Lorsqu'il s'agit de déterminer la forme de consentement à utiliser – en particulier lorsqu'il s'agit d'établir si un consentement implicite peut être invoqué –, il convient de tenir compte à la fois du caractère sensible des renseignements recueillis et des attentes raisonnables des personnes concernées.
- Pour obtenir un consentement valable et valide à la collecte, à l'utilisation ou à la divulgation de renseignements personnels, il faut à la fois faire des efforts raisonnables pour informer la personne des fins auxquelles les renseignements seront utilisés et s'assurer qu'il est raisonnable de s'attendre à ce que la personne comprenne la nature, les objectifs et les conséquences de la pratique.
- Lorsqu'elles concluent une convention avec un fournisseur de services qui traitera des renseignements personnels, les organisations devraient examiner attentivement la convention pour vérifier si elle renferme des dispositions autorisant le fournisseur de services à utiliser ces renseignements à des fins secondaires.
- Lorsqu'un fournisseur de services est autorisé à utiliser des renseignements personnels à des fins générales d'amélioration ou d'optimisation du produit qui profiteront à tous les utilisateurs du produit ou du service, ces utilisations secondaires ne peuvent pas

faire « partie du service prévu au contrat » et ne sont donc pas visées par l'exception relative au consentement pour les transferts à des fournisseurs de services.

- Lorsque de telles utilisations secondaires sont prévues, il faut s'assurer qu'elles soient expressément limitées à l'utilisation de données agrégées et anonymisées. Dans le cas contraire, le transfert de renseignements personnels sera probablement considéré comme une « divulgation » à un tiers, pour laquelle un consentement valable doit être obtenu.
- Les préoccupations relatives à la « lassitude du consentement » ne l'emportent pas sur l'utilisation d'avis « juste à temps » lorsque cela est possible et approprié.
- Bien que les conclusions du CPVP n'aient pas donné lieu à des sanctions pécuniaires ou à des amendes, si les modifications qu'il est prévu d'apporter à la législation canadienne sur la protection des renseignements personnels sont adoptées, les organisations qui ont des pratiques comparables pourraient encourir des sanctions pécuniaires et des amendes considérables.

Contexte

Au moment de supprimer son compte Facebook, un client de Home Depot a appris que Meta avait un dossier faisant état de la plupart des achats en magasin qu'il avait effectués chez Home Depot. Après avoir échoué à résoudre le problème directement avec Home Depot, il a déposé une plainte auprès du CPVP.

Enquête et conclusions

La relation entre Home Depot et Meta n'était pas une relation de pur « fournisseur de services »

Au cours de l'enquête du CPVP, Home Depot a confirmé qu'elle faisait parvenir à Meta les données relatives aux achats en magasin de certains clients à l'aide d'un outil commercial connu sous l'appellation « Conversions hors ligne ».

Grâce à cet outil, Home Depot pouvait évaluer l'efficacité de ses publicités sur Facebook. Plus précisément, lorsqu'un client en magasin choisissait de recevoir un reçu électronique, il était invité à fournir son adresse électronique. Home Depot faisait ensuite parvenir la version hachée de l'adresse électronique du client et les détails de l'achat à Meta, qui associait l'adresse électronique à un compte Facebook existant et comparait ensuite les achats en magasin aux publicités Facebook diffusées sur ce compte Facebook. Meta fournissait ensuite à Home Depot les résultats de son analyse sous la forme d'un rapport agrégé.

Home Depot a plaidé que Meta agissait en tant que fournisseur de services en « effectuant à l'externe ce que Home Depot aurait pu faire à l'interne ». Home Depot a fait valoir que cette pratique constituait donc une activité de traitement pour laquelle aucun consentement supplémentaire n'était requis.

Le CPVP n'était pas d'accord. Il a noté que les conditions applicables aux outils de Facebook Business (les conditions) – le contrat type entre Home Depot et Meta qui régissait l'utilisation de l'outil Conversions hors ligne – permettaient à Meta d'utiliser les renseignements obtenus à de multiples fins secondaires. Plus précisément, les conditions stipulaient que Meta pouvait utiliser les renseignements personnels pour « améliorer l'efficacité des modèles de diffusion des publicités et déterminer la pertinence des publicités pour les personnes » et « personnaliser les fonctionnalités et le contenu (y compris les publicités et les recommandations) que nous présentons aux personnes sur nos produits des entités Facebook et en dehors ».

Le CPVP a également rejeté l'argument de Home Depot selon lequel ces utilisations potentielles étaient directement à l'avantage de Home Depot, par exemple en améliorant l'efficacité des publicités de Home Depot sur Facebook. Le CPVP a estimé que les fins énoncées dans les conditions allaient au-delà des fins commerciales de Home Depot et permettaient à Meta d'utiliser les données des clients de Home Depot afin d'améliorer les services de Meta pour les tiers, notamment en créant des « auditoires semblables » que d'autres entreprises pouvaient cibler au moyen de publicités. Meta a confirmé au CPVP qu'elle considérait ces fins comme ses propres fins commerciales.

Le CPVP a déterminé, sur la base de ce qui précède, que Home Depot était tenu d'obtenir le consentement de ses clients pour divulguer les renseignements en question à Meta.

Consentement implicite insuffisant

Home Depot a fait valoir qu'elle avait obtenu un consentement implicite par le biais à la fois de la Déclaration de Home Depot sur la sécurité et la confidentialité et de la Politique de confidentialité de Meta, du matériel connexe et des paramètres de confidentialité. Home Depot n'a aucunement mentionné ces politiques ou la façon dont les renseignements recueillis au moment de l'achat seraient utilisés ou divulgués aux clients qui fournissaient leur adresse électronique afin de recevoir un reçu électronique. Home Depot a expliqué qu'elle n'avait pas fourni d'avis « juste à temps » (c'est-à-dire au moment où les clients fournissaient leur adresse électronique afin de recevoir un reçu électronique) parce qu'elle craignait la « lassitude du consentement » qui pouvait survenir « si chaque activité unique de traitement est communiquée à chaque phase ».

Home Depot a également fait valoir que le consentement implicite était une forme appropriée de consentement dans ces circonstances parce que i) les renseignements fournis à Meta n'étaient pas sensibles et que ii) les clients « s'attendraient raisonnablement à ce que ces renseignements soient transmis à la plateforme des médias sociaux dont Home Depot se sert pour faire des publicités en ligne en vue de réaliser une analyse globale de l'efficacité ».

Le CPVP n'était pas d'accord. Tout d'abord, il a estimé qu'en réalité, Home Depot n'avait pas obtenu de consentement implicite valable, car i) « la plupart des clients ne seraient absolument pas au courant de la pratique » et « ne s'y attendraient raisonnablement pas » et ii) le fait que les clients fournissent leur adresse électronique pour obtenir des reçus électroniques ne peut être considéré comme un consentement implicite à l'utilisation des renseignements pour mesurer l'impact des campagnes publicitaires en ligne de Home Depot, et encore moins pour les propres fins commerciales de Meta.

En outre, le CPVP a conclu qu'un consentement explicite et actif était nécessaire dans ces circonstances. Tout en reconnaissant qu'en réalité, les renseignements en question n'étaient pas sensibles, le CPVP a souligné qu'ils pouvaient le devenir lorsqu'ils étaient combinés à d'autres renseignements détenus par Meta sur la personne concernée. Plus important encore, le CPVP a estimé que les clients de Home Depot ne pouvaient pas raisonnablement s'attendre à ce que leur adresse électronique et les détails de leurs achats hors ligne soient partagés avec Meta afin que Home Depot s'en serve à des fins secondaires ou que Meta s'en serve à ses propres fins.

La politique de confidentialité de Home Depot n'est pas suffisamment claire aux fins de l'obtention d'un consentement valable

En tout état de cause, le CPVP a estimé que la Déclaration de Home Depot sur la sécurité et la confidentialité ne constituait pas le fondement d'un consentement valable, étant donné que i) lorsqu'ils demandaient un reçu électronique, les clients n'étaient ni avisés de la communication de leurs renseignements personnels à Meta, ni dirigés vers les politiques de confidentialité de Home Depot ou de Meta, et ii) la Déclaration de Home Depot sur la sécurité et la confidentialité n'était pas suffisamment précise, n'expliquant pas suffisamment les diverses fins auxquelles les renseignements des clients pouvaient être communiqués à Meta.

Home Depot a accepté de cesser d'utiliser l'outil Conversions hors ligne et, par conséquent, le CPVP a estimé que l'affaire était close.

Analyse

Tenir compte des attentes raisonnables des personnes lors de la détermination de la forme du consentement et de la rédaction des politiques relatives à la protection des renseignements personnels

Les organisations qui ont l'intention d'utiliser des renseignements personnels à des fins qui peuvent aller au-delà des attentes raisonnables des personnes auprès desquelles elles recueillent des renseignements devraient se demander si un consentement explicite et actif (par exemple, par le biais d'avis « juste à temps ») est nécessaire dans ces circonstances. Le risque de « lassitude du consentement » ne l'emportera pas sur l'utilisation de ces avis « juste à temps » lorsque cela est possible et approprié.

Dans la mesure où le consentement implicite est invoqué, les organisations devraient veiller à ce que leurs politiques relatives à la protection des renseignements personnels soient claires, précises, complètes et compréhensibles, en particulier lorsqu'elles décrivent des pratiques qui peuvent ne pas être anticipées par les personnes.

Examiner la manière dont les fournisseurs de services utilisent les renseignements personnels à leurs propres fins

Il n'est pas rare que les fournisseurs de services qui traitent des données pour le compte d'une organisation se réservent le droit, dans leurs contrats, d'utiliser ces données pour effectuer des analyses internes, généralement dans le but d'améliorer ou d'optimiser leurs propres produits ou services.

Ces droits sont souvent, mais pas toujours, assortis d'une réserve limitant une telle utilisation à des données agrégées, statistiques ou anonymisées. Cela n'était pas clairement indiqué dans les conditions de Meta, qui prévoyaient seulement que Meta utiliserait les renseignements recueillis pour « l'optimisation de la diffusion uniquement après leur agrégation avec d'autres données recueillies auprès d'autres annonceurs ou autrement sur les produits Facebook ».

Les organisations qui retiennent les services de fournisseurs de services pour stocker, traiter ou gérer d'une autre manière des renseignements personnels en leur nom devraient examiner attentivement les dispositions de leurs conventions pour déterminer si des droits relatifs aux utilisations secondaires sont accordés. Dans la mesure du possible, les organisations devraient s'assurer que les fournisseurs de services acceptent expressément de prendre des mesures pour supprimer tout renseignement personnel pouvant faire partie des données utilisées (par exemple, par l'anonymisation) avant tout traitement ultérieur. Les organisations devraient également demander à leurs fournisseurs de services des précisions sur ces utilisations secondaires et sur les mesures qu'ils prendront pour retirer les renseignements personnels. Lorsque ces utilisations secondaires ne peuvent être évitées, par exemple lorsqu'elles font partie des conditions générales (c'est-à-dire non négociables) et qu'elles ne se limitent pas à des données anonymisées, les organisations devraient déterminer ce qui peut devoir être fait pour obtenir des personnes concernées les consentements pertinents, y compris la forme de consentement appropriée.

S'assurer que le fournisseur de services utilise les renseignements personnels dans l'intérêt exprès de l'organisation

Lorsqu'elles examinent les dispositions relatives aux utilisations secondaires, les organisations se contentent parfois d'une formulation laissant entendre que l'utilisation des renseignements personnels par le fournisseur de services présente des avantages directs ou indirects pour l'organisation elle-même (par exemple, l'amélioration du produit ou du service faisant l'objet du contrat) et fait donc « partie du service », sans tenir compte des utilisations externes qui peuvent profiter à d'autres utilisateurs du même service. Les conclusions du CPVP indiquent qu'il est peu probable que cet argument ait beaucoup de poids à l'avenir.

En cas d'ambiguïté ou d'incertitude quant à la ou aux façons dont un fournisseur de services utilisera les renseignements personnels, ou si les clients du fournisseur de services en général profiteront de cette ou ces utilisations, il existe un risque que le transfert de renseignements personnels au fournisseur de services soit considéré comme une divulgation à un tiers qui n'est pas visée par l'exception relative au consentement pour les transferts à des fournisseurs de services.

En pareil cas, les organisations devraient se demander si elles doivent obtenir un consentement valable pour cette divulgation et, le cas échéant, quelle serait la forme appropriée de ce consentement.

Les utilisations secondaires peuvent faire d'un fournisseur de services un « contrôleur » de données

Les organisations doivent également savoir que, lorsque des utilisations secondaires sont prévues, le fournisseur de services devient la principale organisation responsable en vertu de la LPRPDE (c'est-à-dire le « contrôleur ») en ce qui concerne ces utilisations secondaires. Ainsi, lorsqu'une demande d'accès est adressée à un tel fournisseur de services, les restrictions contractuelles que ce dernier peut avoir concernant les demandes d'accès qu'il reçoit en tant que fournisseur de services ne s'appliquent pas. Le fournisseur de services sera tenu de communiquer les renseignements personnels pertinents en réponse à une telle demande et, en fonction de la nature des renseignements en question, la manière dont les renseignements personnels ont été obtenus.

Conclusion

Les conclusions du CPVP pourraient avoir des répercussions sur un large éventail d'accords d'externalisation ou de fourniture de services.

En vertu des modifications qui seront probablement bientôt apportées à la législation canadienne sur la protection des renseignements personnels, les organisations reconnues coupables d'avoir enfreint la loi pourraient non seulement se voir infliger des sanctions pécuniaires et des amendes considérables, mais aussi entacher leur réputation. Les entreprises devraient prendre le temps de réexaminer la façon dont elles utilisent le consentement implicite et d'examiner les conventions qu'elles ont conclues avec des fournisseurs de services – surtout celles qui sont basées sur les conditions générales des fournisseurs de services –, en particulier les dispositions relatives aux utilisations secondaires telles que celles qui sont discutées dans les présentes.

Personnes-ressources : Sumeet Dang, Corey Omer et Alexander Max Jarvie