30 SEPTEMBRE 2024

Donner un sens à la notion de « consentement valable » : décision phare de la Cour d'appel fédérale en matière de confidentialité des données

Auteurs : Corey Omer, Alexander Max Jarvie et Samuel St-Jean

Dans le cadre d'une décision récente, la Cour d'appel fédérale du Canada a établi que Facebook, Inc. (désormais Meta Platforms Inc.) avait manqué à ses obligations aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques* (la « LPRPDE ») du Canada en donnant accès aux renseignements personnels d'utilisateurs de Facebook à des applications de tiers hébergées sur la plateforme Facebook.

La poursuite découlait d'une enquête réalisée par le commissaire à la protection de la vie privée du Canada, laquelle portait sur la récupération de données d'utilisateurs de Facebook par l'application « thisisyourdigitallife » (« TYDL ») et la vente subséquente de ces données par TYDL à Cambridge Analytica, qui s'en était ensuite servie à des fins de profilage et de transmission de publicités politiques ciblées.

La Cour d'appel fédérale a déterminé que Facebook avait omis d'obtenir le consentement valable des utilisateurs avant de divulguer leurs données et avait omis de protéger adéquatement ces données. La décision de la Cour fournit aux entreprises qui exercent des activités au Canada des indications importantes quant aux exigences liées au consentement et aux mesures de sécurité qui sont prévues dans la LPRPDE. La décision soulève cependant d'importants enjeux de conformité pour les organisations qui transmettent les données de leurs utilisateurs à des fournisseurs de services tiers, y compris des plateformes et d'autres intermédiaires.

Principaux points à retenir

- Pour protéger adéquatement les renseignements personnels de leurs utilisateurs, les organisations qui communiquent de tels renseignements à des fournisseurs de services tiers devraient prendre des mesures pour faire le suivi des obligations de ces fournisseurs en matière de protection des renseignements personnels, veiller à les faire respecter et intervenir si une situation est préoccupante.
- La norme rattachée au consentement valable aux termes de la LPRPDE est de nature objective. Elle est établie en fonction de ce qu'une personne raisonnable pourrait comprendre compte tenu de tous les facteurs contextuels pertinents. Pour accorder son consentement de façon valable, une personne raisonnable doit comprendre la nature et les conséquences de la communication des renseignements personnels et l'utilisation qui en sera faite.
- Des politiques de confidentialité au contenu interminable dont le libellé est vague et truffé d'exemples anodins ne sont pas suffisantes pour obtenir un consentement valable. La personne accorde son consentement de façon valable après avoir pris connaissance des risques raisonnablement prévisibles, ce qui peut comprendre l'usage abusif de renseignements personnels par des personnes mal intentionnées.

Contexte

L'application TYDL, lancée sur la plateforme de l'application Facebook en 2013, était présentée aux utilisateurs sous forme de test de personnalité. Elle a permis à son développeur d'avoir accès aux renseignements figurant sur le profil Facebook de chaque utilisateur qui avait installé l'application TYDL ainsi qu'aux renseignements des amis Facebook de chacun de ces utilisateurs. Environ 272 utilisateurs

canadiens ont installé l'application TYDL, ce qui a entraîné la divulgation des données de plus de 600 000 Canadiens. Les données ont ensuite été vendues à Cambridge Analytica (en violation des politiques de l'application Facebook) et ont été utilisées par celle-ci pour élaborer des modèles « psychographiques » afin de transmettre des messages politiques ciblés aux utilisateurs de Facebook en vue de l'élection présidentielle américaine de 2016.

L'utilisation abusive qui avait été faite des données a été révélée publiquement en 2018. Le scandale qui s'en est suivi a retenu l'attention partout dans le monde et a entraîné de multiples enquêtes par des organismes de réglementation ainsi que de nombreuses amendes.

En 2020, le commissaire à la protection de la vie privée du Canada (le « Commissaire »), s'appuyant sur les conclusions de son enquête en lien avec la récupération de données par l'application TYDL et l'utilisation subséquente de celles-ci par Cambridge Analytica, a déposé un avis de requête auprès de la Cour fédérale afin d'obtenir une ordonnance exigeant de Facebook qu'elle modifie ses pratiques liées aux renseignements personnels pour les rendre conformes à la LPRPDE.

Plus particulièrement, l'avis était destiné à obtenir des ordonnances concernant les pratiques de Facebook quant à l'obtention d'un consentement valable et à la protection des données de ses utilisateurs, et prévoyait notamment l'obligation d'exercer un suivi continu des pratiques en matière de protection des renseignements personnels de tous les tiers qui ont accès aux données des utilisateurs de Facebook de quelque façon que ce soit et l'obligation de les faire respecter. Les tiers en question comprennent les développeurs et les exploitants d'applications de tiers qui utilisent la plateforme Facebook.

En 2023, la Cour fédérale a tranché en faveur de Facebook, a rejeté la demande du Commissaire et a établi que celui-ci n'avait pas démontré l'omission par Facebook d'obtenir le consentement valable de ses utilisateurs avant de communiquer leurs données ni celle de protéger adéquatement ces données. La Cour fédérale a conclu que le Commissaire n'avait pas présenté des éléments de preuve suffisants à l'appui des allégations qui soutenaient la demande d'ordonnance et que l'obligation de Facebook de protéger les données de ses utilisateurs prend fin lorsque ces derniers ont consenti à la communication de leurs renseignements personnels à des applications de tiers.

La décision

La Cour d'appel a infirmé la décision de la Cour fédérale, ayant établi que cette dernière avait mal évalué la question du consentement des utilisateurs de Facebook et celle de l'obligation de Facebook de protéger les renseignements personnels de ses utilisateurs.

Consentement valable

La Cour d'appel a déterminé que Facebook n'avait pas obtenu le consentement valable des utilisateurs dont les renseignements personnels avaient été divulgués à TYDL et à Cambridge Analytica, à savoir les utilisateurs qui avaient installé l'application TYDL et leurs amis Facebook.

En ce qui a trait aux utilisateurs qui avaient installé l'application TYDL, la Cour d'appel a expliqué que la Cour fédérale avait fait erreur en fondant sa conclusion relative au consentement valable en grande partie sur l'absence d'éléments de preuve subjectifs fournis par les utilisateurs et de témoignages d'experts. La Cour d'appel a expliqué que des éléments de preuve subjectifs faisant état de la compréhension par les utilisateurs de Facebook des pratiques de celle-ci en matière de protection des renseignements personnels n'étaient pas pertinents, puisque la norme rattachée au consentement valable aux termes de la LPRPDE est de nature objective et établie en fonction de ce qu'une personne raisonnable pourrait comprendre.

La Cour d'appel a ajouté que les témoignages d'experts au sujet des mesures que Facebook pourrait avoir prises pour obtenir un consentement valable étaient des éléments de preuve tout aussi non pertinents, étant donné que l'ampleur des efforts déployés par Facebook ne pouvait être évoquée en réduction de son obligation d'obtenir réellement le consentement valable de ses utilisateurs.

La Cour d'appel était d'avis que, dans le contexte, une personne raisonnable n'aurait pas nécessairement compris qu'elle consentait, en installant l'application TYDL, au risque que l'application puisse s'approprier ses données et les données de ses amis pour ensuite les divulguer d'une façon qui contrevient aux politiques établies pour l'application Facebook.

Pour rendre sa conclusion, la Cour a examiné la politique portant sur les conditions de service et l'utilisation des données de Facebook et a indiqué que la présentation de modalités qui semblent à première vue claires ne peut suffire à l'obtention d'un consentement valable. Un texte qui est clair en apparence peut cesser de l'être si la longueur du document et la complexité de ses modalités viennent en obscurcir ou en masquer le sens. La Cour a également tenu compte de différents autres facteurs, notamment le fait que la Politique d'utilisation des données était intégrée par renvoi dans les Conditions de service, que les paramètres de confidentialité de Facebook sont configurés par défaut de façon à permettre la communication des renseignements personnels, et que le contrat qui lie Facebook et ses utilisateurs est un contrat d'adhésion de l'utilisateur.

La Cour d'appel a précisé, à l'égard de la Politique d'utilisation des données, que même si Facebook avait mis en garde ses utilisateurs contre le fait que les applications de tiers ne faisaient pas partie de Facebook et n'étaient pas sous sa maîtrise, et les avait invités à toujours prendre connaissance des conditions de service et des politiques de confidentialité de ces applications afin de comprendre le traitement réservé par celles-ci aux données des utilisateurs, « on ne peut conclure que les utilisateurs qui ont lu la Politique d'utilisation des données savaient que de telles applications pouvaient être mal intentionnées et feraient fi des politiques de Facebook ou de la législation locale en matière de protection des renseignements personnels, et encore moins qu'elles vendraient leurs renseignements personnels à une tierce partie » [*traduction*]. La Cour a ajouté qu'« un utilisateur de Facebook raisonnable peut s'attendre à ce que Facebook ait mis en place des mesures préventives solides afin d'empêcher des personnes mal intentionnées de faire de fausses déclarations quant à leurs pratiques en matière de protection des renseignements personnels et d'obtenir un accès aux données des utilisateurs de manière fallacieuse » [*traduction*].

En bref, la Cour d'appel en est venue à la conclusion qu'« il n'est pas en accord avec l'objet de la LPRPDE d'établir que des utilisateurs de Facebook qui ont téléchargé l'application TYDL (ou d'autres applications) ont consenti à un risque de divulgation massive de leurs données à tout moment à des parties dont ils ne connaissent pas l'existence parce qu'on leur a présenté une politique générique, en format numérique, aux termes de laquelle ils sont réputés avoir lu une deuxième politique renfermant une clause les informant de la divulgation potentielle de leurs renseignements personnels, le tout pour permettre à Facebook de faire croître son chiffre d'affaires » [*traduction*].

En ce qui a trait aux amis Facebook des utilisateurs qui avaient installé l'application TYDL, la Cour d'appel a noté que ces derniers n'avaient jamais eu la possibilité de passer en revue la politique de confidentialité de TYDL avant la divulgation de leurs renseignements personnels. La Cour a plutôt établi que les « amis des utilisateurs n'avaient été informés que de manière générale, par l'intermédiaire de la Politique d'utilisation des données de Facebook, que leurs renseignements personnels pouvaient être transmis à des applications de tiers lorsque leurs amis utilisaient de telles applications » [*traduction*]. La Cour a également caractérisé les exemples fournis par Facebook à des fins d'illustration dans la Politique d'utilisation des données comme étant « anodins » [*traduction*]. Elle a indiqué qu'aucun des exemples fournis ne portait sur la collecte massive de données n'ayant aucun lien avec les fins auxquelles l'application en elle-même est destinée, comme dans le cas de TYDL. La Cour a ajouté que, aux termes de la Politique d'utilisation des données, « en créant un compte Facebook, les amis des utilisateurs directs des applications consentaient effectivement à la communication ultérieure de renseignements pouvant être utilisés à des fins non précisées, à tout moment, à une application dont ils ne connaissent pas l'existence, sans qu'ils en soient informés et sans connaître la nature de cette divulgation » [*traduction*], ce qui ne constitue pas un « consentement valable » [*traduction*].

Obligation de protection des données

La Cour d'appel a également établi que Facebook avait manqué à son obligation de protéger les données de ses utilisateurs en invitant des dizaines de millions d'applications sur sa plateforme et en omettant de superviser adéquatement le respect par celles-ci des modalités et des conditions de Facebook qui régissaient l'intégration d'applications à la plateforme. La Cour a souligné que Facebook n'avait pas examiné le contenu des politiques de confidentialité de ces applications et qu'elle n'avait pris aucune mesure en réaction aux signaux d'alarme indiquant un usage abusif potentiel des données des utilisateurs. La Cour a par ailleurs établi que Facebook aurait dû prendre des mesures supplémentaires afin de surveiller le respect des modalités contractuelles par les tiers.

Dans son analyse de la réponse de Facebook selon laquelle il lui aurait été impossible en pratique de lire toutes les politiques de confidentialité des applications de tiers afin d'en assurer la conformité à ses propres politiques, la Cour d'appel a indiqué que ce problème

émanait de Facebook en elle-même. Facebook, selon les conclusions de la Cour, ne peut restreindre la portée de ses responsabilités aux termes de la LPRPDE en évoquant le caractère impossible d'une mesure à prendre.

Analyse et commentaires

La décision de la Cour d'appel fédérale renferme d'importants points à retenir au sujet des exigences liées au consentement valable et aux mesures de sécurité qui sont prévues dans la LPRPDE, en particulier pour les organisations qui mettent des services de tiers à la disposition de leurs utilisateurs et qui transmettent les données de leurs utilisateurs aux tiers en question.

La décision établit sans équivoque que le consentement valable doit être évalué de façon objective, compte tenu de tous les facteurs contextuels pertinents, dont la longueur et le libellé des politiques de confidentialité, les paramètres configurés par défaut et la nature du contrat. Des politiques de confidentialité au contenu interminable dont le libellé est vague et truffé d'exemples anodins ne sont pas suffisantes pour obtenir un consentement valable des utilisateurs à la divulgation de leurs renseignements personnels et aux risques auxquels ceux-ci ne peuvent raisonnablement s'attendre. Les organisations gagnent à passer en revue leurs politiques de confidentialité et à s'assurer que celles-ci font état, dans un langage clair et concis, des risques raisonnablement prévisibles, y compris les risques découlant de la violation des modalités contractuelles ou de la législation locale par des personnes mal intentionnées.

La décision de la Cour d'appel remet également en question la pratique consistant à transmettre les renseignements personnels d'utilisateurs ou de clients à des fournisseurs de services tiers tout en se dégageant de toute responsabilité pour la conduite de ceux-ci en matière de protection des renseignements personnels.

Le libellé de la Politique d'utilisation des données de Facebook, qui met en garde les utilisateurs contre les applications de tiers et les invite à consulter les politiques de confidentialité de ces applications, est courant dans le marché. Un vaste éventail d'organisations, y compris celles qui ont recours à un modèle de plateforme et qui se considèrent comme des intermédiaires ou des teneurs de marché, ont, comme Facebook, déterminé que leur obligation de protéger les renseignements personnels de leurs utilisateurs prend fin hors du cadre des services qu'elles leur offrent directement et ne comprend pas la surveillance des services de fournisseurs tiers rendus accessibles par l'intermédiaire de leur plateforme.

Dans sa décision, la Cour d'appel fédérale met l'accent sur le modèle d'affaires particulier qui est propre à Facebook et indique que « l'application [de la LPRPDE] varie selon le contexte » [*traduction*], mais les conclusions auxquelles elle parvient devraient néanmoins inciter d'autres organisations ayant un profil semblable à réévaluer leur approche. Les organisations qui permettent la transmission des renseignements personnels de leurs clients à des fournisseurs de services tiers auraient avantage à procéder de manière proactive à l'examen des pratiques de protection des renseignements personnels adoptées par ces derniers, notamment les politiques en matière de protection des données. Elles devraient également intervenir avec diligence lorsque certaines de ces pratiques de protection des renseignements personnels soulèvent des préoccupations.

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