Recueil des décisions des Cours fédérales

Federal Courts Reports

NOTE DE L'ARRÊTISTE : Ce document fera l'objet de retouches de forme avant la parution de sa version définitive dans le *Recueil des décisions des Cours fédérales*.

A-129-23

2024 CAF 140

Le commissaire à la protection de la vie privée du Canada (*appelant*)

c.

Facebook, Inc. (*intimée*)

RÉPERTORIÉ : CANADA (COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE) C. FACEBOOK, INC.

Cour d'appel fédérale, juges Rennie, Gleason et Goyette, J.C.A—Ottawa, 21 février; 9 septembre 2024.

Protection des renseignements personnels — Loi sur la protection des renseignements personnels et les documents électroniques — Appel d'une décision de la Cour fédérale qui a rejeté une demande en vertu de l'alinéa 15(a) de la Loi sur la protection des renseignements personnels et les documents électroniques (la LPRPDE) alléguant que l'intimée Facebook, Inc. (Facebook) avait enfreint la LPRPDE en communiquant les données d'utilisateurs de Facebook à des applications tierces hébergées sur sa plateforme (les applications) — La "plateforme" Facebook, lancée en 2007, a permis à des tiers de développer des applications exploitables depuis Facebook, que les utilisateurs peuvent installer — Deux politiques de Facebook axées sur les utilisateurs étaient en vigueur pendant la période pertinente : la Politique de confidentialité et les Conditions de service — La Politique de confidentialité expliquait comment se faisait le partage de renseignements sur Facebook — En 2013, M. Aleksandr Kogan, alors professeur à l'Université de Cambridge, a lancé l'application "thisisyourdigitallife" (TYDL) sur la plateforme Facebook — Par l'intermédiaire de la plateforme Facebook, M. Kogan pouvait accéder aux renseignements contenus dans le profil Facebook de chaque utilisateur ayant installé l'application TYDL, ainsi qu'aux renseignements des amis Facebook de chacun de ces utilisateurs — Les données des utilisateurs obtenues par l'intermédiaire de l'application TYDL ont plus tard été vendues à une société appelée Cambridge Analytica Ltd. (Cambridge Analytica) — Des données de plus de 600 000 Canadiens ont été communiquées — Facebook a retiré l'application TYDL de sa plateforme et a demandé à Cambridge Analytica de supprimer les données qu'elle avait obtenues — Les parties ont convenu que M. Kogan a violé la Politique de la plateforme Facebook en demandant d'avoir accès à des données autres que celles qui étaient nécessaires à l'exploitation de son application, en utilisant les données des amis des utilisateurs à des fins autres que l'amélioration de l'expérience des utilisateurs-installateurs dans l'application, et en transférant et vendant les données des utilisateurs à un tiers — L'appelant a mené une enquête et a conclu que Facebook n'avait pas obtenu le consentement valable et éclairé des utilisateurs quant à la communication de renseignements aux applications, et n'avait pas protégé les données de ses utilisateurs — Le présent appel concernait la portée des obligations en matière de consentement valable et de mesures de sécurité énoncées à l'annexe 1 de la LPRPDE — Le consentement valable est décrit en tant que « troisième principe » à

l'article 4.3 de l'annexe 1 — Les questions centrales devant la Cour fédérale étaient de savoir si Facebook a omis d'obtenir le consentement valable des utilisateurs et de leurs amis Facebook avant de communiquer leurs données avec des applications tierces; et si Facebook a omis de protéger suffisamment les données des utilisateurs — La Cour fédérale n'a pas tenu compte de l'importance des éléments de preuve statistiques déposés par l'appelant — Elle a conclu que l'appelant n'avait pas démontré le caractère insuffisant de la protection des données des utilisateurs assurée par Facebook — Pour appuyer cette conclusion, la Cour fédérale a indiqué que l'occurrence d'une atteinte à la protection des données ne signifie pas nécessairement que les mesures de sécurité de l'organisation sont inadéquates; a conclu que les obligations de Facebook en matière de mesures de sécurité sont levées dès lors que les renseignements sont communiqués à des applications tierces; et a conclu qu'il n'y avait pas suffisamment d'éléments de preuve subjectifs et d'expert pour lui permettre de déterminer si les accords contractuels et les politiques relatives aux obligations contractuelles constituaient des mesures de sécurité adéquates — En l'espèce, la principale question en litige était de déterminer si la Cour fédérale a commis des erreurs dans l'interprétation et l'application de la LPRPDE, ainsi que dans l'appréciation des éléments de preuve — La Cour fédérale a commis une erreur en fondant sa conclusion exclusivement ou en grande partie sur l'absence d'éléments de preuve subjectifs et d'expert — Elle ne s'est pas penchée distinctement sur l'existence ou le caractère approprié du consentement des amis des utilisateurs-installateurs d'applications tierces — Elle ne s'est pas posé la question que la LPRPDE impose : est-ce que chaque utilisateur dont les données ont été communiquées a consenti à cette communication? — Elle ne s'est pas attardée aux éléments de preuve sur la question du consentement valable, tel qu'il est décrit à l'article 6.1 de la LPRPDE et à l'article 4.3 de l'annexe 1 — Elle a jugé que les éléments de preuve subjectifs provenant d'utilisateurs de Facebook au sujet de leurs attentes en matière de protection de la vie privée revêtaient une importance considérable dans son évaluation visant à déterminer si les utilisateurs avaient donné un consentement valable — L'analyse effectuée en tenant compte du point de vue de la personne raisonnable ne fait intervenir aucun élément de preuve subjectif — La loi exige la mise en équilibre non pas de droits concurrents, mais de renseignements dont l'organisation a besoin et non de renseignements que l'organisation a le droit de recueillir — Les circonstances entourant le consentement dans les présentes différaient pour les deux groupes d'utilisateurs de Facebook dont les données ont été communiquées : les utilisateurs ayant téléchargé des applications tierces et les amis Facebook de ces utilisateurs — Cette distinction entre les utilisateurs et leurs amis Facebook était fondamentale aux fins de l'analyse fondée sur la LPRPDE — Facebook n'a pas donné aux amis Facebook des utilisateurs la possibilité de donner un consentement valable quant à la communication de leurs données — Ceci contrevenait à l'article 4.3.2 de l'annexe 1 de la LPRPDE — La Politique de confidentialité donne des exemples banals de la façon dont les applications peuvent utiliser les données des utilisateurs — Le libellé de la Politique de confidentialité est trop général pour être efficace — Le consentement valable, au titre du troisième principe et de l'article 6.1 de la LPRPDE, repose sur la compréhension de la personne raisonnable quant à la nature, aux fins et aux conséquences de la communication — En l'espèce, il était impossible pour les amis Facebook des utilisateurs de s'informer, au moment de la communication, sur les fins auxquelles chaque application tierce utiliserait leurs données, ou même de savoir que leurs données étaient communiquées à ces applications — L'utilisateur qui accepte les Conditions de service est réputé avoir donné son consentement au sujet des Conditions de service et de la Politique de confidentialité — Il ne s'agit pas là du consentement actif, positif et ciblé que prévoient le troisième principe et l'article 6.1 — En se positionnant ainsi, Facebook a tenté de réduire, voire d'éliminer les responsabilités qui lui incombent en vertu de la LPRPDE — L'utilisateur de Facebook raisonnable s'attendrait à ce que Facebook eût mis en place de solides mesures préventives pour empêcher les acteurs malveillants de faire des déclarations trompeuses au sujet de leurs propres pratiques en matière de protection de la vie privée et d'accéder aux données des utilisateurs pour de fausses raisons — Facebook n'a pris aucune mesure à la suite de la demande que l'application TYDL a présentée en 2014 pour avoir accès à des données non essentielles sur les utilisateurs — Facebook n'a pas informé adéquatement les utilisateurs, lors de la création de leur compte Facebook, des risques entourant leurs données — La même vigilance accrue appliquée par la Cour suprême dans l'arrêt Douez c. Facebook, Inc. devrait être appliquée, en l'espèce, aux clauses de la Politique de confidentialité qui, selon Facebook, autorisent une large communication future de données, potentiellement à des acteurs malveillants — Aucun utilisateur n'a donné un consentement valable à toutes les communications de ses données par Facebook

pendant la période pertinente — En l'espèce, il existait un lien direct entre les communications non autorisées et les choix de Facebook quant à ses politiques et aux principes de conception axés sur l'utilisateur — Facebook a elle-même rendu possible l'atteinte à la protection des données; elle ne pouvait donc pas se soustraire à ses obligations légales — Pendant la période pertinente, Facebook a manqué à ses obligations en matière de mesures de sécurité puisqu'elle n'a pas assuré adéquatement le respect et la surveillance des pratiques en matière de protection de la vie privée des applications tierces qui utilisent sa plateforme — La distinction entre les droits conférés à l'individu et le besoin de l'organisation se veut un fondement conceptuel important de l'application de la LPRPDE — Il ne s'agit pas de se pencher sur l'existence d'une disposition, dissimulée dans les conditions de service, selon laquelle l'on peut conclure que l'utilisateur a donné son consentement — Cette question est certes importante, mais elle n'est pas déterminante du respect de la double obligation en vertu de la LPRPDE — Appel accueilli.

Fin de non-recevoir — La Cour fédérale a rejeté une demande en vertu de l'alinéa 15(a) de la Loi sur la protection des renseignements personnels et les documents électroniques (la LPRPDE) alléguant que l'intimée Facebook, Inc. (Facebook) avait enfreint la LPRPDE en communiquant les données d'utilisateurs de Facebook à des applications tierces hébergées sur sa plateforme (les applications) — L'appelant a mené une enquête et a conclu que Facebook n'avait pas obtenu le consentement valable et éclairé des utilisateurs quant à la communication de renseignements aux applications, et n'avait pas protégé les données de ses utilisateurs — La Cour fédérale a conclu que l'appelant n'avait pas démontré le caractère insuffisant de la protection des données des utilisateurs assurée par Facebook — En l'espèce, Facebook s'est appuyé sur les théories de la préclusion par assertion de fait et de l'erreur provoquée par une personne en autorité pour soutenir qu'il n'y a eu aucune violation de la LPRPDE — Cet argument tire son origine d'une enquête menée en 2008–2009 à la suite de laquelle l'appelant a formulé des recommandations, y compris que Facebook limite l'accès des applications tierces aux données des utilisateurs — L'appelant a par après envoyé une lettre à Facebook l'informant que Facebook avait honoré ses engagements — Le moyen de défense de Facebook fondé sur les théories de la préclusion par assertion de fait et de l'erreur provoquée par une personne en autorité a été rejeté pour trois motifs — Premièrement, les déclarations de l'appelant n'étaient elles-mêmes pas claires — Même en présumant que Facebook s'était conformée à ses obligations en 2010, la prise de mesures supplémentaires a été encouragée — Deuxièmement, les instances visées par la LPRPDE sont traitées comme des instances de novo — Enfin, la théorie de la préclusion a une application limitée en droit public — L'on ne saurait empêcher l'appelant de s'acquitter de ses obligations légales aujourd'hui en raison d'une déclaration obscure faite plus de 10 ans passés.

LOIS ET RÈGLEMENTS CITÉS

Charte canadienne des droits et libertés, qui constitue la partie I de la *Loi constitutionnelle de 1982*, annexe B, *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.) [L.R.C. (1985), appendice II, nº 44], art. 8

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5, art. 3, 5(1), 6.1, 7.2, 15(a), ann. 1, art. 4.1.2, 4.3, 4.3.2, 4.3.4, 4.3.5, 4.3.6, 4.7, 4.7.3, 6.1.

JURISPRUDENCE CITÉE

DÉCISIONS APPLIQUÉES :

Housen c. Nikolaisen, 2002 CSC 33, [2002] 2 R.C.S. 235; *Englander c. TELUS Communications Inc.*, 2004 CAF 387, [2005] 2 R.C.F. 572

DÉCISIONS DIFFÉRENCIÉES :

Ter Neuzen c. Korn, [1995] 3 R.C.S. 674, 1995 CanLII 72; *Kreutner v. Waterloo Oxford Co-Operative*, 50 O.R. (3d) 140, 2000 CanLII 16813 (C.A. Ont.); *Canada (Surintendant des faillites) c. MacLeod*, 2011 CAF 4, [2011] A.C.F. nº 48 (QL).

DÉCISIONS EXAMINÉES :

Bhasin c. Hrynew, 2014 CSC 71, [2014] 3 R.C.S. 494; *Taylor c. Canada (Procureur général)*, 2003 CAF 55, [2003] 3 C.F. 3 *Douez c. Facebook, Inc.*, 2017 CSC 33, [2017] 1 R.C.S. 751; *Malcolm c. Canada (Ministre des Pêches et des Océans)*, 2014 CAF 130, [2014] A.C.F. nº 499 (QL).

DÉCISIONS MENTIONNÉES :

Montalbo c. Banque Royale du Canada, 2018 CF 1155, [2018] A.C.F. nº 1172 (QL); *Toronto Real Estate Board c. Canada (Commissaire de la concurrence)*, 2017 CAF 236, [2018] 3 R.C.F. 563 *St-Arnaud c. Facebook inc.*, 2011 QCCS 1506; *R. c. Edwards*, [1996] 1 R.C.S. 128, 1996 CanLII 255; *R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432; *Jordan House Ltd. c. Menow*, [1974] R.C.S. 239, 1973 CanLII 16; *Lévis (Ville) c. Tétreault; Lévis (Ville) c. 2629-4470 Québec inc.*, 2006 CSC 12, [2006] 1 R.C.S. 420; *La Souveraine, Compagnie d'assurance générale c. Autorité des marchés financiers*, 2013 CSC 63, [2013] 3 R.C.S. 756; *USA v. Facebook*, 1 : 19-cv-02184 (D.D.C.).

DOCTRINE CITÉE

Crépeau, Laurent. « Responding to Deficiencies in the Architecture of Privacy : Co-Regulation as the Path Forward for Data Protection on Social Networking Sites » (2022), 19 : 2 *Can. J.L. & Tech.* 411.

Lie, David *et al*. "Automating Accountability? Privacy Policies, Data Transparency, and the Third-Party Problem" (2022), 72 : 2 *U. Toronto L.J.* 155.

APPEL d'une décision de la Cour fédérale (2023 CF 533) qui a rejeté une demande en vertu de l'alinéa 15(a) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (la LPRPDE) alléguant que l'intimée avait enfreint la LPRPDE en communiquant les données d'utilisateurs à des applications tierces hébergées sur sa plateforme. Appel accueilli.

ONT COMPARU :

Peter Engelmann, *Colleen Bauman*, et *Louisa Garib* pour l'appelant.

Michael A. Feder, c.r., *Gillian P. Kerr*, *Barry Sookman*, *Daniel G.C. Glover* et *Connor Bildfell* pour l'intimée.

AVOCATS INSCRITS AU DOSSIER

Goldblatt Partners LLP, Ottawa, et le *Commissariat à la protection de la vie privée du Canada*, Gatineau (Québec) pour l'appelant.

McCarthy Tétrault S.E.N.C.R.L., s.r.l., Vancouver, pour l'intimée.

Ce qui suit est la version française des motifs du jugement rendus par

LE JUGE RENNIE, J.C.A. :

Aperçu

[1] Le commissaire à la protection de la vie privée du Canada (le commissaire) a introduit une instance devant la Cour fédérale. Il alléguait que Facebook, Inc.

(Facebook) (maintenant Meta Platforms Inc.) avait enfreint la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5 (la LPRPDE), en communiquant les données d'utilisateurs de Facebook à des applications tierces hébergées sur sa plateforme (les applications). L'instance a été introduite à la suite de l'enquête du commissaire sur l'utilisation de données d'utilisateurs de Facebook par l'application « thisisyourdigitallife » (l'application TYDL) et la vente ultérieure de ces données par cette dernière, entre novembre 2013 et décembre 2015, à Cambridge Analytica Ltd. (Cambridge Analytica) qui a mis au point des modèles psychographiques à partir de ces données.

[2] La Cour fédérale, sous la plume du juge Manson (*Canada (Commissaire à la protection de la vie privée) c. Facebook, Inc.*, 2023 CF 533, [2023] A.C.F. nº 521 (QL)), a rejeté la demande du commissaire, concluant que ce dernier n'avait pas démontré que Facebook n'avait pas obtenu le consentement valable des utilisateurs avant de communiquer des données les concernant, ni démontré que Facebook n'avait pas protégé suffisamment les données des utilisateurs.

[3] J'accueillerais l'appel. La Cour fédérale a commis une erreur dans son analyse du consentement valable et des mesures de sécurité aux termes de la LPRPDE. Je conclus que Facebook ne s'est pas conformée à la LPRPDE, laquelle exige l'obtention du consentement valable des utilisateurs avant la communication de leurs données, et qu'elle a manqué à son obligation de protéger les données des utilisateurs.

Mesures prises par Facebook en matière de protection de la vie privée

[4] Facebook est une plateforme électronique de média social qui permet aux utilisateurs de transmettre de l'information. Le modèle d'affaires de Facebook repose notamment sur l'attraction d'utilisateurs sur sa plateforme, et sur la fidélité de ces derniers, dans le but de vendre de la publicité. Le nombre d'utilisateurs et la précision des données sur les utilisateurs qui sont mises à la disposition des annonceurs ont une incidence directe sur les revenus de Facebook. Comme il est mentionné ci-dessous, il s'agit d'un fait contextuel important qui encadre les obligations légales en cause dans le présent appel.

[5] En 2007, Facebook a lancé la « plateforme » Facebook, un ensemble de technologies permettant à des tiers de développer des applications, exploitables depuis Facebook, que les utilisateurs peuvent installer. Ces applications offrent aux utilisateurs une expérience personnalisée d'activités sociales et de divertissements telles que des jeux, le partage de photos et l'écoute de musique. En 2013, 41 millions d'applications étaient accessibles à partir de Facebook.

[6] Facebook a également déployé une interface de programmation d'applications appelée « API Graph », qui permet aux applications tierces de recevoir des données sur les utilisateurs. Entre 2013 et 2018, il y a eu deux versions de API Graph. Dans la première version (Graph v1), les applications pouvaient demander aux utilisateurs-installateurs l'autorisation d'accéder aux données les concernant ainsi qu'aux données concernant leurs amis Facebook. Dans la deuxième version (Graph v2), lancée en avril 2014, les applications ne pouvaient plus demander l'autorisation d'accéder aux données concernant les amis Facebook des utilisateurs-installateurs, à quelques exceptions près, lesquelles exceptions avaient toutes été éliminées en date de mars 2018. Parallèlement à Graph v2, Facebook a également lancé « App Review », un

programme dont l'objectif était d'obliger les développeurs d'applications souhaitant accéder à tout autre renseignement sur les utilisateurs, outre les renseignements de base, à expliquer en quoi les renseignements supplémentaires permettraient d'améliorer l'expérience des utilisateurs de l'application en question.

[7] Bien que Graph v2 ait été lancée en avril 2014, une période de grâce d'un an a été accordée pour les applications existantes utilisant Graph v1. Les violations présumées de la LPRPDE à l'origine de la présente instance concernent Graph v1 et se sont déroulées entre novembre 2013 (date de lancement de l'application TYDL) et décembre 2015 (date du retrait de laquelle l'application TYDL de la plateforme Facebook).

[8] Au cours de cette période, les pratiques et politiques de Facebook en matière de consentement comportent trois niveaux : les politiques applicables à l'ensemble de la plateforme, les contrôles utilisateur et les ressources de formation. Il convient de donner quelques explications au sujet de ces pratiques puisqu'elles fournissent un contexte quant aux questions relatives au consentement valable et aux mesures de sécurité.

Politiques applicables à l'ensemble de la plateforme Facebook

[9] Deux politiques de Facebook axées sur les utilisateurs étaient en vigueur pendant la période pertinente : la Politique de confidentialité et les Conditions de service. Bien que Facebook ait utilisé différentes versions de ces politiques au cours de la période pertinente, les politiques sont « restées pratiquement inchangées » (décision de la Cour fédérale, au paragraphe 16). Pour s'inscrire sur Facebook, les utilisateurs devaient accepter les Conditions de service, lesquelles incorporaient par renvoi la Politique de confidentialité. Ces deux politiques étaient accessibles depuis des hyperliens situés juste au-dessus du bouton « s'inscrire ».

[10] Les Conditions de service présentaient les droits et responsabilités des utilisateurs, y compris la façon dont ils pouvaient contrôler leurs renseignements. Les Conditions de service expliquaient que « [l]orsque vous utilisez une application, celle-ci est susceptible de solliciter votre autorisation afin de pouvoir accéder à vos contenus et informations ainsi qu'à ceux que d'autres personnes ont partagés avec vous », que « c'est l'accord que vous donnez à une application qui détermine dans quelle mesure celle-ci est libre d'utiliser, de conserver et de transférer ces contenus et informations », et que « vous pouvez également supprimer votre compte ou désactiver votre application à tout moment ».

[11] Les Conditions de service comptaient environ 4 500 mots, dans leur version originale anglaise.

[12] La Politique de confidentialité expliquait comment se faisait le partage de renseignements sur Facebook et comprenait la description des éléments suivants :

a) la définition du terme « informations publiques » (à savoir les informations que l'utilisateur « choisi[t] de rendre publiques, ainsi que les informations qui sont toujours publiques »), et ce que signifie le fait de rendre des informations publiques (notamment que les informations seront [TRADUCTION] « accessibles à quiconque utilise […] API Graph [de Facebook] »);

b) les autorisations et contrôles utilisateur de Facebook pour gérer le partage des données concernant les utilisateurs;

c) les données qui sont communiquées aux applications tierces au sujet des utilisateurs, y compris lorsque les amis Facebook de ces derniers utilisent des applications tierces, et les moyens dont disposent les utilisateurs pour déterminer quelles données ils souhaitent partager.

[13] La Politique de confidentialité, que l'utilisateur, en acceptant les Conditions de service, était réputé avoir lue, comptait environ 9 100 mots dans sa version originale anglaise.

Contrôles utilisateur de Facebook

[14] Les utilisateurs de Facebook pouvaient modifier certains paramètres et autorisations pour choisir dans quelle mesure les données étaient partagées avec les applications tierces.

[15] En 2010, Facebook a ajouté à sa plateforme le processus d'autorisations de partage de données granulaires (le processus GDP). Conformément au processus GDP, lors de l'installation d'une application, l'utilisateur recevait un avis l'informant du genre de données auxquelles l'application cherchait à accéder, recevait un hyperlien menant vers la politique de confidentialité visant l'application en question et avait la possibilité d'accorder ou de refuser les autorisations demandées. Dans sa version de 2014, le processus GDP de Facebook donnait aux utilisateurs la possibilité d'accorder ou de refuser aux applications l'autorisation d'accéder à des catégories précises de données.

[16] Les utilisateurs de Facebook avaient également accès à une page « paramètres Applications », qui leur permettait de voir toutes les applications utilisées, de supprimer les applications qu'ils ne souhaitaient plus utiliser ou de désactiver la plateforme pour empêcher les applications d'accéder à des renseignements non publics. Après le lancement du processus GDP, Facebook a mis à jour la page « paramètres Applications », permettant ainsi aux utilisateurs de voir les autorisations à jour associées à chaque application et de retirer certaines autorisations.

[17] La page « paramètres Applications » comprenait également un paramètre « Informations accessibles par l'intermédiaire de vos amis », qui permettait aux utilisateurs de restreindre les renseignements accessibles aux applications installées par leurs amis. À ce paramètre était associée la mention selon laquelle [TRADUCTION] « les utilisateurs de Facebook qui peuvent voir vos informations peuvent les partager s'ils utilisent des applications ».

[18] Enfin, les utilisateurs de Facebook avaient accès à une page « Paramètres de confidentialité », qui leur permettait de limiter l'accès à leurs publications à un groupe précis et leur rappelait que [TRADUCTION] « les personnes qui ont accès à vos informations peuvent les partager avec d'autres, notamment des applications ». Les utilisateurs de Facebook pouvaient également choisir de désactiver la plateforme, empêchant ainsi les applications d'accéder à leurs données, ou de supprimer leur compte et demander aux applications concernées de supprimer les données les concernant.

Ressources de formation de Facebook

[19] Les ressources offertes aux utilisateurs de Facebook entre 2013 et 2015 comprenaient des pages d'aide regroupant de la documentation sur des sujets liés à la confidentialité, notamment les données communiquées lorsque des amis utilisent des applications tierces ainsi que les paramètres de contrôle concernant ces données. D'autres outils étaient disponibles, notamment une visite virtuelle sur la confidentialité, une vérification de la confidentialité et les « Principes de base liés à la confidentialité », grâce auxquels les utilisateurs pouvaient se renseigner sur les politiques de confidentialité de Facebook et passer en revue certains paramètres de confidentialité, ainsi que les « Raccourcis de confidentialité », dont les boutons étaient situés à côté du bouton « Accueil » de Facebook, grâce auxquels les utilisateurs pouvaient trouver des renseignements sous les rubriques [TRADUCTION] « Qui peut voir mes publications? », [TRADUCTION] « Qui peut me contacter? », et [TRADUCTION] « Comment empêcher une personne de me déranger? ».

Contrats entre Facebook et les applications tierces

[20] Facebook exigeait des applications tierces qu'elles acceptent la Politique de la plateforme Facebook et les Conditions de service avant de leur donner accès à la plateforme. La Politique de la plateforme Facebook imposait aux applications des obligations contractuelles, notamment les suivantes :

a) ne demander que les données de l'utilisateur qui sont nécessaires à l'exploitation de l'application en question, et n'utiliser les données des amis de l'utilisateur que dans le contexte de l'expérience de l'utilisateur dans l'application;

b) mettre en place une politique de confidentialité indiquant à l'utilisateur quelles données l'application utilisera et comment elle les utilisera ou les communiquera;

c) obtenir le consentement explicite de l'utilisateur avant d'utiliser des données autres que les renseignements de base à toute autre fin que de les présenter à l'utilisateur dans l'application;

d) s'abstenir de vendre et d'acheter des données obtenues auprès de Facebook.

[21] Facebook admet ne pas avoir évalué ou vérifié le contenu réel des politiques de confidentialité des applications; Facebook ne vérifiait que l'hyperlien vers la politique de confidentialité de l'application pour s'assurer qu'il menait à une page Web active.

[22] Il était également précisé, dans la Politique de la plateforme, que Facebook se réservait le droit de prendre des mesures coercitives. Bien que Facebook ait pris environ 6 millions de mesures coercitives contre des applications entre août 2012 et juillet 2018, les motifs de chaque mesure coercitive ne sont pas connus.

Application TYDL et Cambridge Analytica

[23] En novembre 2013, M. Aleksandr Kogan, alors professeur à l'Université de Cambridge, a lancé l'application TYDL sur la plateforme Facebook (et a ainsi accepté la

Politique de la plateforme et les Conditions de service). L'application TYDL était présentée aux utilisateurs comme un test de personnalité. Par l'intermédiaire de la plateforme Facebook, M. Kogan pouvait accéder aux renseignements contenus dans le profil Facebook de chaque utilisateur ayant 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 mené à la communication des données de plus de 600 000 Canadiens. En décembre 2015, des reportages médiatiques ont révélé que les données des utilisateurs obtenues par l'intermédiaire de l'application TYDL avaient été vendues à une société appelée Cambridge Analytica et à une entité liée, et que les données avaient été utilisées pour mettre au point des modèles « psychographiques » dans le but de cibler des utilisateurs de Facebook et leur envoyer des messages politiques en vue de l'élection présidentielle de 2016 aux États-Unis.

[24] L'application TYDL a été lancée avec Graph v1 et est demeurée sur la plateforme Facebook pendant la transition à Graph v2. Même si l'application ne respectait pas les exigences de Graph v2, son exploitation s'est poursuivie pendant la période de grâce d'un an suivant le lancement de Graph v2. À la suite de l'annonce concernant Graph v2, M. Kogan a demandé d'avoir accès à d'autres renseignements personnels. Facebook a rejeté la demande au motif que les renseignements n'auraient pas servi à « améliorer l'expérience des utilisateurs dans l'application » (décision de la Cour fédérale, au paragraphe 43). Il importe de mentionner que Facebook, même si elle était au courant des détails de cette demande, ne s'est pas davantage attardée à l'utilisation des données par l'application TYDL, qui était toujours exploitée avec Graph v1.

[25] En 2015, Facebook a retiré l'application TYDL de sa plateforme et a demandé à Cambridge Analytica de supprimer les données qu'elle avait obtenues. Facebook n'a ni informé les utilisateurs concernés ni exclu M. Kogan ou Cambridge Analytica de sa plateforme. Ce n'est qu'en 2018 que Facebook a suspendu M. Kogan et Cambridge Analytica de sa plateforme, à la suite de nouveaux reportages médiatiques selon lesquels les données n'avaient pas été supprimées, comme il leur avait été demandé de le faire en 2015.

[26] Les parties conviennent que M. Kogan a violé la Politique de la plateforme Facebook en demandant d'avoir accès à des données autres que celles qui étaient nécessaires à l'exploitation de son application, en utilisant les données des amis des utilisateurs à des fins autres que l'amélioration de l'expérience des utilisateurs-installateurs dans l'application, et en transférant et vendant les données des utilisateurs à un tiers. En outre, la prétendue politique de confidentialité de l'application TYDL contenait des modalités incompatibles avec la Politique de la plateforme Facebook.

[27] Le commissaire a par la suite reçu une plainte concernant la conformité de Facebook à la LPRPDE. Le commissaire a mené une enquête et a conclu que Facebook n'avait pas obtenu le consentement valable et éclairé des utilisateurs quant à la communication de renseignements aux applications, et n'avait pas protégé les données de ses utilisateurs. En février 2020, le commissaire a déposé l'avis de demande introduisant l'instance en cause devant la Cour fédérale (décision de la Cour fédérale, aux paragraphes 34 et 44). Je précise au passage que la demande a été déposée au début de la pandémie de COVID-19, ce qui explique le temps qui s'est

écoulé entre le dépôt de l'avis de demande et le moment où la Cour fédérale a rendu sa décision.

Dispositions légales

[28] Le présent appel concerne la portée des obligations en matière de consentement valable et de mesures de sécurité énoncées à l'annexe 1 de la LPRPDE. Aux termes du paragraphe 5(1) de la LPRPDE, toute organisation doit se conformer à l'annexe 1 de la LPRPDE.

[29] Le consentement valable et les mesures de sécurité figurent au nombre des conditions prescrites par la loi énoncées en tant que « principes » dans la LPRPDE. Le consentement valable est décrit en tant que « troisième principe » à l'article 4.3 de l'annexe 1 de la LPRPDE. Ajouté en 2015, l'article 6.1 de la LPRPDE incorpore en tant qu'article distinct (dans des termes un peu plus clairs) les obligations qui étaient déjà contenues dans le troisième principe de l'annexe :

> **Validité du consentement**
>
> **6.1** Pour l'application de l'article 4.3 de l'annexe 1, le consentement de l'intéressé n'est valable que s'il est raisonnable de s'attendre à ce qu'un individu visé par les activités de l'organisation comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles il a consenti.
>
> […]
>
> **4.3 Troisième principe — Consentement**
>
> Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu'il ne soit pas approprié de le faire.
>
> […]
>
> **4.3.1**
>
> Il faut obtenir le consentement de la personne concernée avant de recueillir des renseignements personnels à son sujet et d'utiliser ou de communiquer les renseignements recueillis. Généralement, une organisation obtient le consentement des personnes concernées relativement à l'utilisation et à la communication des renseignements personnels au moment de la collecte. Dans certains cas, une organisation peut obtenir le consentement concernant l'utilisation ou la communication des renseignements après avoir recueilli ces renseignements, mais avant de s'en servir, par exemple, quand elle veut les utiliser à des fins non précisées antérieurement.
>
> **4.3.2**
>
> Suivant ce principe, il faut informer la personne au sujet de laquelle on recueille des renseignements et obtenir son consentement. Les organisations doivent faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés. Pour que le consentement soit valable, les fins doivent être énoncées de façon que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués.
>
> **4.3.3**

Une organisation ne peut pas, pour le motif qu'elle fournit un bien ou un service, exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées.

4.3.4

La forme du consentement que l'organisation cherche à obtenir peut varier selon les circonstances et la nature des renseignements. Pour déterminer la forme que prendra le consentement, les organisations doivent tenir compte de la sensibilité des renseignements. Si certains renseignements sont presque toujours considérés comme sensibles, par exemple les dossiers médicaux et le revenu, tous les renseignements peuvent devenir sensibles suivant le contexte. Par exemple, les nom et adresse des abonnés d'une revue d'information ne seront généralement pas considérés comme des renseignements sensibles. Toutefois, les nom et adresse des abonnés de certains périodiques spécialisés pourront l'être.

4.3.5

Dans l'obtention du consentement, les attentes raisonnables de la personne sont aussi pertinentes. Par exemple, une personne qui s'abonne à un périodique devrait raisonnablement s'attendre à ce que l'entreprise, en plus de se servir de son nom et de son adresse à des fins de postage et de facturation, communique avec elle pour lui demander si elle désire que son abonnement soit renouvelé. Dans ce cas, l'organisation peut présumer que la demande de la personne constitue un consentement à ces fins précises. D'un autre côté, il n'est pas raisonnable qu'une personne s'attende à ce que les renseignements personnels qu'elle fournit à un professionnel de la santé soient donnés sans son consentement à une entreprise qui vend des produits de soins de santé. Le consentement ne doit pas être obtenu par un subterfuge.

4.3.6

La façon dont une organisation obtient le consentement peut varier selon les circonstances et la nature des renseignements recueillis. En général, l'organisation devrait chercher à obtenir un consentement explicite si les renseignements sont susceptibles d'être considérés comme sensibles. Lorsque les renseignements sont moins sensibles, un consentement implicite serait normalement jugé suffisant. Le consentement peut également être donné par un représentant autorisé (détenteur d'une procuration, tuteur).

4.3.7

Le consentement peut revêtir différentes formes, par exemple :

a) on peut se servir d'un formulaire de demande de renseignements pour obtenir le consentement, recueillir des renseignements et informer la personne de l'utilisation qui sera faite des renseignements. En remplissant le formulaire et en le signant, la personne donne son consentement à la collecte de renseignements et aux usages précisés;

b) on peut prévoir une case où la personne pourra indiquer en cochant qu'elle refuse que ses nom et adresse soient communiqués à d'autres organisations. Si la personne ne coche pas la case, il sera présumé qu'elle consent à ce que les renseignements soient communiqués à des tiers;

c) le consentement peut être donné de vive voix lorsque les renseignements sont recueillis par téléphone; ou

d) le consentement peut être donné au moment où le produit ou le service est utilisé.

[30] Les principes relatifs aux mesures de sécurité sont énoncés en tant que « septième principe » à l'article 4.7 de l'annexe 1 de la LPRPDE, dont les segments pertinents sont reproduits ci-dessous :

> **4.7 Septième principe — Mesures de sécurité**
>
> Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.
>
> **4.7.1**
>
> Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. Les organisations doivent protéger les renseignements personnels quelle que soit la forme sous laquelle ils sont conservés.
>
> **4.7.2**
>
> La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis, de la quantité, de la répartition et du format des renseignements personnels ainsi que des méthodes de conservation. Les renseignements plus sensibles devraient être mieux protégés. La notion de sensibilité est présentée à l'article 4.3.4.
>
> **4.7.3**
>
> Les méthodes de protection devraient comprendre :
>
> **a)** des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux;
>
> **b)** des mesures administratives, par exemple des autorisations sécuritaires et un accès sélectif; et
>
> **c)** des mesures techniques, par exemple l'usage de mots de passe et du chiffrement.
>
> **4.7.4**
>
> Les organisations doivent sensibiliser leur personnel à l'importance de protéger le caractère confidentiel des renseignements personnels.

[31] Enfin, l'objet de la LPRPDE est énoncé à l'article 3 de cette loi :

> **Objet**
>
> **3** La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

Décision de la Cour fédérale

[32] La Cour fédérale a commencé son analyse en faisant remarquer que les instances visées à l'alinéa 15a) de la LPRPDE sont des instances *de novo*, ajoutant que la question fondamentale consistait à déterminer si Facebook avait enfreint la

LPRPDE et, le cas échéant, quelle réparation devait être accordée. La Cour fédérale a fait remarquer que l'objet de la partie 1 de la LPRPDE (qui régit l'utilisation des renseignements personnels dans le secteur privé) est de mettre en équilibre le droit des utilisateurs à la protection des renseignements les concernant et « le droit des organisations de recueillir, d'utiliser et de communiquer des renseignements personnels » (décision de la Cour fédérale, au paragraphe 50). La Cour fédérale a reconnu que la LPRPDE est une loi quasi constitutionnelle, précisant toutefois que l'approche traditionnelle d'interprétation des lois s'appliquait toujours et qu'elle devait user de souplesse et de sens commun dans l'interprétation de cette loi.

[33] La Cour fédérale s'est ensuite penchée sur les deux questions centrales : Facebook a-t-elle omis d'obtenir le consentement valable des utilisateurs et de leurs amis Facebook avant de communiquer leurs données avec des applications tierces; et Facebook a-t-elle omis de protéger suffisamment les données des utilisateurs? La Cour fédérale a conclu que le commissaire ne s'était pas acquitté de son fardeau de preuve à l'égard des deux questions.

[34] Dans son analyse, la Cour fédérale a déclaré qu'elle « dispos[ait] de bien peu de preuve » (décision de la Cour fédérale, au paragraphe 71). Elle a précisé que le commissaire n'avait ni exercé ses pouvoirs pour contraindre Facebook à produire des éléments de preuve, ni fourni des éléments de preuve d'expert quant à ce que Facebook aurait pu faire différemment. La Cour fédérale a également mentionné l'absence d'éléments de preuve subjectifs de la part d'utilisateurs de Facebook quant à leurs attentes et à leur compréhension pour ce qui est de la confidentialité.

[35] La Cour fédérale a déclaré que de tels éléments de preuve (subjectifs et d'expert) n'étaient pas « nécessaires, à strictement parler », mais qu'ils auraient été utiles à son analyse « dans un domaine où la norme de raisonnabilité et les attentes des utilisateurs dépendent autant du contexte et sont en constante évolution ». En l'absence de tels éléments de preuve, la Cour fédérale a conclu que le commissaire ne pouvait s'acquitter de son fardeau à partir « d'hypothèses et de déductions [concernant le point de vue des utilisateurs] tirées de faits essentiels aussi clairsemés » (décision de la Cour fédérale, aux paragraphes 71, 72 et 78).

[36] Par ailleurs, la Cour fédérale n'a pas tenu compte de l'importance des éléments de preuve statistiques déposés par le commissaire. Ces éléments de preuve, tirés de Facebook, permettaient d'établir qu'en 2013, 46 p. 100 des développeurs d'applications Facebook n'avaient pas passé en revue la Politique de la plateforme ou les Conditions de service depuis le lancement de leur application. La Cour fédérale a conclu que cette statistique était sans importance (décision de la Cour fédérale, aux paragraphes 73 à 76).

[37] La Cour fédérale a ensuite conclu que le commissaire n'avait également pas démontré le caractère insuffisant de la protection des données des utilisateurs assurée par Facebook. La Cour fédérale s'est appuyée sur trois affirmations.

[38] Premièrement, la Cour fédérale a indiqué que l'occurrence d'une atteinte à la protection des données ne signifie pas nécessairement que les mesures de sécurité de l'organisation sont inadéquates (décision de la Cour fédérale, au paragraphe 82).

[39] Deuxièmement, la Cour fédérale a conclu que les obligations de Facebook en matière de mesures de sécurité sont levées dès lors que les renseignements sont communiqués à des applications tierces (décision de la Cour fédérale, aux paragraphes 86 à 88, renvoyant à l'arrêt *Englander c. TELUS Communications Inc.*, 2004 CAF 387, [2005] 2 R.C.F. 572 (*Englander*), ainsi que d'autres articles de la LPRPDE (4.1.2 et 4.7.3 de l'annexe 1, et 7.2) où il est fait mention de la nécessité de mettre en place des mesures de sécurité à l'égard des renseignements qui sont actuellement sous la responsabilité de l'organisation). La Cour fédérale a souligné que son interprétation de la LPRPDE, qui « s'applique également aux géants des réseaux sociaux, aux banques locales et aux concessionnaires automobiles », doit rester fondée sur des principes (décision de la Cour fédérale, au paragraphe 90).

[40] Enfin, la Cour fédérale a conclu que, même si les obligations en matière de mesures de sécurité s'appliquaient à Facebook après la communication de renseignements à des applications tierces, il n'y avait encore une fois pas suffisamment d'éléments de preuve subjectifs et d'expert pour lui permettre de déterminer si les accords contractuels et les politiques relatives aux obligations contractuelles constituent des mesures de sécurité adéquates. Renvoyant à l'arrêt *Bhasin c. Hrynew*, 2014 CSC 71, [2014] 3 R.C.S. 494, la Cour fédérale a affirmé que, dans leurs opérations contractuelles, les parties commerciales s'attendent raisonnablement à un niveau minimal d'honnêteté et de bonne foi, et donc que Facebook pouvait s'attendre à ce que les applications respectent les accords contractuels.

[41] Compte tenu de ces conclusions, la Cour fédérale ne s'est pas penchée sur deux des moyens de défense avancés par Facebook, à savoir la théorie de la préclusion par assertion de fait et celle de l'erreur provoquée par une personne en autorité, et qui, selon Facebook, devaient entraîner le rejet de la plainte.

Questions en litige et positions des parties

[42] Le commissaire soutient que la Cour fédérale a commis des erreurs dans l'interprétation et l'application de la LPRPDE, ainsi que dans l'appréciation des éléments de preuve.

[43] Premièrement, le commissaire soutient que la Cour fédérale a [TRADUCTION] « placé la barre trop bas » dans son interprétation du consentement valable aux termes de la LPRPDE. Facebook ayant admis ne pas avoir pris connaissance des politiques de confidentialité des applications tierces avant de communiquer des renseignements à ces dernières, la Cour fédérale n'a pas examiné en quoi le modèle de Facebook en matière de notification et de consentement constituait un consentement valable. La Cour fédérale n'a également pas analysé les éléments de preuve relatifs à la longueur des Conditions de service et de la Politique de confidentialité de Facebook et au fait que la plupart des gens ne les lisaient ou ne les comprenaient pas, ni les éléments de preuve selon lesquels la politique de confidentialité de l'application TYDL ne mentionnait pas le ciblage de messages politiques au nombre des fins pour lesquelles les renseignements des utilisateurs étaient communiqués.

[44] Deuxièmement, le commissaire soutient que la Cour fédérale a également commis une erreur en ne faisant aucune distinction entre le consentement valable des utilisateurs-installateurs et le consentement valable de leurs amis Facebook, malgré les différents processus de consentement et mesures de sécurité applicables à ces

groupes. Selon le commissaire, si la Cour fédérale avait fait cette distinction, elle aurait conclu, sans avoir besoin d'éléments de preuve subjectifs ou d'expert, qu'aucun des deux groupes n'avait donné un consentement valable.

[45] Troisièmement, le commissaire soutient que, s'agissant de l'établissement de l'existence d'un consentement valable, la Cour fédérale a commis une erreur en exigeant des éléments de preuve subjectifs quant à l'expérience des utilisateurs, des éléments de preuve d'expert ou des éléments de preuve concernant ce que Facebook aurait pu faire différemment, et qu'elle aurait plutôt dû appliquer la norme objective de la décision raisonnable, axée sur l'utilisateur. Le commissaire attire l'attention sur l'utilisation du terme « raisonnable » à l'article 6.1 de la LPRPDE et à l'article 4.3 de l'annexe 1 de cette même loi, ainsi que dans la jurisprudence sur les attentes raisonnables en matière de protection de la vie privée, qui fait intervenir l'application d'un critère normatif défini de manière objective.

[46] En ce qui concerne l'obligation en matière de mesures de sécurité, le commissaire soutient que le défaut de protéger les renseignements est lié au défaut d'obtenir le consentement. La conclusion de la Cour fédérale quant à l'obligation de Facebook en matière de mesures de sécurité repose sur le fait que Facebook n'avait aucune obligation après la communication des renseignements, mais la Cour fédérale a commis une erreur puisqu'elle n'a pas tenu compte de la conduite de Facebook avant la communication des renseignements personnels (notamment l'omission, par Facebook, de prendre connaissance des politiques de confidentialité des applications tierces, malgré des [TRADUCTION] « signaux d'alarme » liés à la protection de la vie privée). Renvoyant à la décision *Montalbo c. Banque Royale du Canada*, 2018 CF 1155, [2018] A.C.F. nº 1172 (QL), le commissaire allègue que la Cour fédérale aurait dû traiter cette conduite comme une preuve *prima facie* du défaut de Facebook quant à la prise de mesures appropriées pour protéger les renseignements, et tirer des conclusions supplémentaires à partir des éléments de preuve à sa disposition, plus particulièrement en raison des difficultés associées au fait d'établir qu'une organisation n'a pas protégé à l'interne les renseignements personnels d'une personne.

[47] Enfin, selon le commissaire, la Cour fédérale a commis une erreur en concluant qu'elle disposait de « bien peu de preuve » concernant à la fois la question du consentement valable et la question des mesures de sécurité, puisque le dossier contenait de [TRADUCTION] « nombreux éléments de preuve détaillés » quant au manquement de Facebook à l'égard de ces obligations, notamment les suivants :

a) les moyens par lesquels Facebook prétendait obtenir un consentement valable : la longueur et la portée des Conditions de service et de la Politique de confidentialité, l'obligation pour les utilisateurs de prendre des mesures proactives pour passer ces politiques en revue après avoir créé un compte, et le témoignage, devant le Sénat américain, du chef de la direction de Facebook, Mark Zuckerberg, selon lequel les utilisateurs ne lisent pas ou ne comprennent pas les Conditions de service ou la Politique de confidentialité;

b) le fait que les amis des utilisateurs-installateurs n'étaient pas informés de la communication, par Facebook, de leurs renseignements personnels à des applications tierces, et le fait que Facebook savait que les utilisateurs étaient [TRADUCTION] « souvent surpris » d'apprendre qu'un de leurs amis avait transmis leurs renseignements personnels à une application tierce;

c) l'aveu de Facebook, en mars 2018, selon lequel il restait beaucoup de travail à faire [TRADUCTION] « pour faire respecter [ses] politiques et aider les utilisateurs à comprendre […] les choix qui s'offrent à eux au sujet de leurs données » et [TRADUCTION] « que les paramètres de confidentialité et d'autres outils importants sont trop difficiles à trouver »;

d) l'inaction de Facebook quant aux [TRADUCTION] « signaux d'alarme » au sujet des applications tierces, le fait qu'elle savait qu'il y avait des « acteurs malveillants » parmi les applications tierces sur la plateforme et le fait qu'elle savait que certains développeurs d'applications ne prenaient pas connaissance de la Politique de la plateforme.

[48] En réponse, Facebook soutient que la Cour fédérale n'a commis aucune erreur dans son appréciation des éléments de preuve, faisant valoir que la Cour fédérale a examiné tous les éléments de preuve pertinents et a conclu que le commissaire ne s'était pas acquitté de son fardeau. Ainsi, selon Facebook, notre Cour ne devrait pas intervenir au simple motif qu'elle est en désaccord avec la Cour fédérale.

[49] Facebook affirme que la Cour fédérale a correctement interprété la LPRPDE. La Cour fédérale a reconnu le statut quasi constitutionnel de cette loi, mais Facebook soutient qu'elle avait en fin de compte — et à juste titre — conclu que ce statut n'a pas pour effet de modifier l'approche traditionnelle d'interprétation des lois, que la LPRPDE devait être interprétée en usant de souplesse et de sens commun, et que la LPRPDE a notamment pour objet la mise en équilibre de la protection des renseignements personnels et des intérêts commerciaux.

[50] Facebook propose quatre réponses à l'argument du commissaire selon lequel la Cour fédérale n'a pas mis ces éléments en équilibre parce qu'elle n'avait pas exigé de Facebook qu'elle fournisse des éléments de preuve de son incapacité, d'un point de vue commercial, de passer en revue les politiques de confidentialité des applications qu'elle hébergeait : le fardeau de la preuve incombant au commissaire; les éléments de preuve non contestés de Facebook selon lesquels il serait pratiquement impossible d'assurer une telle surveillance; le caractère non pertinent des politiques des applications tierces pour ce qui est des obligations de Facebook en matière de consentement et de mesures de sécurité; et le droit de Facebook de s'attendre à un minimum d'honnêteté quant à l'exécution de ses contrats.

[51] Facebook soutient que la Cour fédérale n'a commis aucune erreur dans son analyse du consentement valable. Facebook affirme que la Cour fédérale a compris l'argument du commissaire selon lequel ni les utilisateurs ni leurs amis Facebook n'avaient donné un consentement valable, mais qu'elle avait en fin de compte jugé que les éléments de preuve ne lui permettaient pas de conclure à une violation de la LPRPDE. Quoi qu'il en soit, Facebook a respecté les normes applicables en matière de consentement valable : il n'était possible d'utiliser Facebook qu'après avoir accepté sa Politique de confidentialité et ses Conditions de service, et Facebook, par l'entremise de ces politiques ainsi que de divers paramètres, outils et autorisations, avait expliqué à tous ses utilisateurs comment leurs renseignements seraient communiqués et comment ils pouvaient assurer un contrôle à l'égard de leurs renseignements (renvoyant à *Toronto Real Estate Board c. Canada (Commissaire de la concurrence)*, 2017 CAF 236, [2018] 3 R.C.F. 563 et à *St-Arnaud c. Facebook inc.*, 2011 QCCS 1506).

[52] Facebook conteste également le fondement probatoire de la demande, soutenant qu'il ne justifie pas la conclusion d'absence de consentement valable. Le commissaire n'a produit aucun témoignage d'utilisateurs de Facebook, a produit très peu d'éléments de preuve au sujet des utilisateurs de Facebook et n'a produit aucun témoignage d'expert ni aucun élément de preuve quant à ce que Facebook aurait pu faire différemment. Les éléments de preuve selon lesquels Facebook n'a pas passé en revue les politiques de confidentialité des applications tierces, et l'argument selon lequel les utilisateurs de Facebook ne comprenaient pas la nature, les fins et les conséquences de la communication aux applications tierces, ne sont d'aucune utilité pour déterminer si Facebook avait obtenu le consentement aux fins de la communication des renseignements à ces applications. Enfin, Facebook soutient que, quoi qu'il en soit, ses pratiques cadraient avec les lignes directrices et les observations du commissaire qui prévalaient pendant la période pertinente.

[53] S'agissant de l'analyse des mesures de sécurité, Facebook soutient, dans un premier temps, que l'article 4.7 de l'annexe 1 de la LPRPDE n'exige pas que les intermédiaires comme Facebook s'assurent de la conformité de tiers à la LPRPDE. Facebook ajoute, dans un deuxièmement temps, que, selon les lignes directrices du commissaire en vigueur en 2014, les plateformes devaient fournir des liens vers les politiques de confidentialité externes. Facebook s'est pliée à ces lignes directrices, a utilisé des outils automatisés pour vérifier la validité de chaque lien et a exhorté les utilisateurs, par l'entremise de sa Politique de confidentialité, à [TRADUCTION] « [s']assur[er] de lire les conditions de service et les politiques de confidentialité » des applications tierces.

Analyse

[54] Les parties conviennent que les normes de contrôle établies dans l'arrêt *Housen c. Nikolaisen*, 2002 CSC 33, [2002] 2 R.C.S. 235, s'appliquent en l'espèce : la norme de la décision correcte pour les questions de droit, et la norme de l'erreur manifeste et déterminante pour les questions de fait ou les questions mixtes de fait et de droit.

[55] J'estime que les motifs de la Cour fédérale sont entachés d'erreurs. J'accueillerais l'appel et j'accueillerais la demande du commissaire, en partie.

[56] Compte tenu de la nature objective de l'analyse qu'elle devait mener, la Cour fédérale a commis une erreur en fondant sa conclusion exclusivement ou en grande partie sur l'absence d'éléments de preuve subjectifs et d'expert. De plus, la Cour fédérale ne s'est pas penchée distinctement sur l'existence ou le caractère approprié du consentement des amis des utilisateurs-installateurs d'applications tierces et sur l'existence ou le caractère approprié du consentement des utilisateurs-installeurs de ces applications. Par conséquent, la Cour fédérale ne s'est pas posé la question que la LPRPDE impose : est-ce que chaque utilisateur dont les données ont été communiquées a consenti à cette communication? Ces erreurs de premier ordre ont imprégné l'analyse. L'appel devrait donc être accueilli.

[57] J'ajouterais que la Cour fédérale ne s'est pas attardée aux éléments de preuve sur la question du consentement valable, tel qu'il est décrit à l'article 6.1 de la LPRPDE et à l'article 4.3 de l'annexe 1 de la même loi. En toute honnêteté, il s'agit d'une conséquence logique de la décision préliminaire de ne pas exiger la production d'éléments de preuve subjectifs et d'expert. En ayant ainsi décidé, le juge de la Cour

fédérale ne s'est pas penché sur les répercussions des éléments de preuve dont la Cour fédérale était saisie concernant l'application de l'article 6.1 de la LPRPDE et de l'article 4.3 de l'annexe 1 de la même loi, précisant que les faits essentiels étaient « clairsemés » (au paragraphe 72).

[58] Il y avait, à mon sens, d'importants éléments de preuve sur les questions dont était saisie la Cour fédérale, y compris les suivants : les Conditions de service et la Politique de confidentialité; la transcription du témoignage du chef de la direction de Facebook, Mark Zuckerberg, selon qui [TRADUCTION] « la plupart des utilisateurs ne lisent [ou ne comprennent] probablement pas » les Conditions de service ou la Politique de confidentialité dans leur intégralité; le fait que 46 p. 100 des développeurs d'applications n'avaient pas lu la Politique de la plateforme ou les Conditions de service depuis le lancement de leurs applications; le fait que la demande de renseignements de l'application TYDL ne se limitait pas aux renseignements nécessaires au fonctionnement de l'application; et le fait que la décision de permettre à l'application TYDL de continuer, pendant un an, d'accéder aux données des amis des utilisateurs malgré des [TRADUCTION] « signaux d'alarme » quant au non-respect des politiques de Facebook.

Exigence de la Cour fédérale quant à la production d'éléments de preuve subjectifs ou d'expert

[59] Dans son évaluation visant à déterminer si les utilisateurs de Facebook avaient donné un consentement valable pour la communication de leurs données, la Cour fédérale a déploré le manque d'éléments de preuve à la fois d'expert, quant à ce que Facebook aurait pu faire différemment, et subjectifs, provenant d'utilisateurs de Facebook au sujet de leurs attentes en matière de protection de la vie privée. Reconnaissant que de « telles preuves ne sont pas nécessaires, à strictement parler », la Cour fédérale a tout de même fondé sa décision sur « l'absence de preuve » qui l'a contrainte « à faire des hypothèses et à tirer des inférences dénuées de fondement sur ce que les utilisateurs liraient ou non, ce qu'ils considéreraient comme décourageant et ce qu'ils comprendraient ou non » (décision de la Cour fédérale, aux paragraphes 71, 77 et 78). Ainsi, après avoir affirmé que la production d'éléments de preuve subjectifs n'était pas nécessaire, la Cour fédérale a jugé que de tels éléments de preuve revêtaient une importance considérable dans son évaluation visant à déterminer si les utilisateurs avaient donné un consentement valable.

[60] L'analyse effectuée en tenant compte du point de vue de la personne raisonnable ne fait intervenir aucun élément de preuve subjectif.

[61] Les articles de l'annexe 1 de la LPRPDE portant sur le consentement valable, ainsi que l'objet de cette loi, reposent sur le point de vue de la personne raisonnable. S'agissant de la collecte, de l'utilisation et de la communication de renseignements par l'organisation, l'article 6.1 de la LPRPDE ne protège ces activités que dans la mesure où la personne raisonnable considérerait qu'elles sont appropriées dans les circonstances. Selon l'article 4.3.2 de l'annexe 1 de la LPRPDE, il faut se demander si la personne visée aurait pu « raisonnablement comprendre » comment ses renseignements seraient utilisés ou communiqués (voir également l'article 3 de la LPRPDE et l'article 4.3.5 de l'annexe 1 de la même loi).

[62] Fait important, la notion de point de vue de la personne raisonnable est encadrée par la loi, laquelle fait mention de renseignements dont l'organisation a besoin et non de renseignements que l'organisation a le droit de recueillir, d'utiliser ou de communiquer. Cette différence est primordiale. La loi exige la mise en équilibre non pas de droits concurrents, mais d'un besoin et d'un droit.

[63] La personne raisonnable est une personne fictive et non une personne réelle. Imaginée par l'esprit judiciaire, la personne raisonnable se veut une norme objective, et non une norme subjective. En conséquence, une cour ne saurait attribuer arbitrairement le statut de « personne raisonnable » à une ou deux personnes qui témoignent en fonction de leur point de vue particulier et subjectif sur la question. Comme l'a écrit le juge Evans pour notre Cour, « [d]éfinir les caractéristiques de la "personne raisonnable" présente des difficultés dans la mesure où des gens raisonnables peuvent considérer une affaire différemment, selon la perspective adoptée […] Cependant, l'opinion de la personne raisonnable dans les critères juridiques constitue une norme indicative interprétée par les tribunaux, non une hypothèse qui puisse se vérifier empiriquement » (*Taylor c. Canada (Procureur général)*, 2003 CAF 55, [2003] 3 C.F. 3, au paragraphe 95).

[64] C'est d'autant plus vrai dans le contexte de Facebook, qui compte des millions d'utilisateurs canadiens représentant le plus large éventail possible de données démographiques liées à l'âge, au genre, au statut social et à la situation économique.

[65] Facebook soutient que les cours [TRADUCTION] « évaluent les normes objectives en renvoyant aux éléments de preuve », y compris les « éléments de preuve d'expert sur les connaissances et les pratiques courantes dans le domaine », ainsi que « la disponibilité de solutions de rechange », dans leur évaluation de la sécurité des produits, ou « les circonstances pertinentes », dans leur évaluation de la diligence raisonnable d'une partie. À l'appui de cet argument, Facebook renvoie aux arrêts suivants : *Ter Neuzen c. Korn*, [1995] 3 R.C.S. 674, 1995 CanLII 72 (*Ter Neuzen*); *Kreutner v. Waterloo Oxford Co-Operative*, 50 O.R. (3d) 140, 2000 CanLII 16813 (C.A. Ont.) (*Kreutner*); et *Canada (Surintendant des faillites) c. MacLeod*, 2011 CAF 4, [2011] A.C.F. nº 48 (QL) (*MacLeod*). Toutefois, la jurisprudence sur laquelle Facebook s'appuie n'est manifestement pas utile ou porte sur des faits qui se distinguent de ceux en l'espèce.

[66] Les affaires *Ter Neuzen* et *Kreutner* portent sur des vocations professionnelles et des industries spécialisées. Le juge n'étant ni un médecin praticien ni un ingénieur agréé, la cour saisie d'une telle affaire aurait bien sûr besoin d'éléments de preuve d'expert pour déterminer les normes applicables au médecin raisonnable (comme dans l'affaire *Ter Neuzen*) ou aux produits conçus de manière sécuritaire (comme dans l'affaire *Kreutner*). Cette même affirmation ne saurait s'appliquer lorsque le juge doit tenir compte du point de vue de la personne raisonnable, qui est fictive, mais sur qui l'expérience de la vie quotidienne influe.

[67] Il est vrai, bien sûr, que les circonstances pertinentes peuvent être utiles à une cour dans l'analyse qu'elle effectue en tenant compte du point de vue de la personne raisonnable, notamment pour déterminer le point de vue qu'aurait la personne raisonnable dans une situation donnée. En l'espèce, il y avait des éléments de preuve quant aux circonstances pertinentes, notamment les faits relatifs à la communication par Cambridge Analytica elle-même ainsi que les politiques et pratiques de Facebook.

La Cour fédérale disposait d'éléments de preuve qui lui auraient été utiles dans son analyse du respect des obligations énoncées au troisième principe et à l'article 6.1 de la LPRPDE.

[68] Facebook soutient également que les cours tiennent compte des attentes subjectives en matière de protection de la vie privée dans leur évaluation de l'existence d'attentes raisonnables en matière de protection de la vie privée suivant l'article 8 de la *Charte canadienne des droits et libertés*, partie I de la *Loi constitutionnelle de 1982*, annexe B, *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.) [L.R.C. (1985), appendice II, nº 44] (la Charte) (renvoyant à *R. c. Edwards*, [1996] 1 R.C.S. 128, 1996 CanLII 255 (*Edwards*)).

[69] Dans le contexte du droit pénal et de la protection qu'offre l'article 8 de la Charte contre les fouilles, les perquisitions et les saisies abusives, il est possible d'admettre les éléments de preuve de l'accusé, s'il témoigne, quant à ses attentes en matière de protection de la vie privée. Il en est ainsi parce que les attentes subjectives peuvent avoir une incidence sur l'évaluation du caractère raisonnable d'une fouille. Néanmoins, l'analyse fondée sur l'article 8 est en fin de compte normative, les attentes subjectives de la personne en matière de protection de la vie privée n'étant qu'un des facteurs dont les cours tiennent compte (*R. c. Tessling*, 2004 CSC 67, [2004] 3 R.C.S. 432 (*Tessling*), au paragraphe 42; *Edwards*, au paragraphe 45). En effet, la Cour suprême fait une mise en garde quant à l'importance à accorder aux attentes subjectives en matière de protection de la vie privée dans l'évaluation des attentes raisonnables en matière de protection de la vie privée (*Tessling*, au paragraphe 42), ce qui ne cadre pas avec l'argument de Facebook.

[70] Il incombait à la Cour fédérale de préciser en quoi consiste l'attente objective et raisonnable au sujet du consentement valable. Elle a commis une erreur en refusant de le faire au motif qu'elle ne disposait d'aucun élément de preuve subjectif ou d'expert.

[71] Reste la question de l'étonnant double critère de raisonnabilité énoncé à l'article 4.3.2 de l'annexe 1 de la LPRPDE. Selon cet article, l'organisation doit « faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés », et, pour que le consentement soit valable, « les fins doivent être énoncées de façon que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués ». Autrement dit, il semblerait que tant l'effort déployé par l'organisation que la façon dont l'organisation s'y prend pour obtenir le consentement doivent être raisonnables.

[72] Ce double critère de raisonnabilité n'a aucune incidence sur l'analyse qu'effectue notre Cour. S'il est établi que la personne raisonnable n'aurait pas été en mesure de comprendre comment ses renseignements seraient utilisés ou communiqués, comme en l'espèce, l'analyse prend fin. En effet, l'on ne saurait conclure que l'organisation déploie des efforts raisonnables alors qu'elle cherche à obtenir le consentement d'une manière qui est déraisonnable en soi. Si les efforts raisonnables que l'organisation déploie pouvaient éclipser la capacité de la personne raisonnable de comprendre l'objet du consentement, il serait inutile d'exiger que la personne soit informée de la collecte, de l'utilisation ou de la communication des renseignements personnels et qu'elle y consente. Pour dire les choses plus simplement, s'il est conclu que la personne raisonnable n'aurait pas compris l'objet du consentement, cette conclusion resterait la même, peu importe l'ampleur des efforts raisonnables que déploie l'organisation. Au vu

de l'objet de la LPRPDE, le consentement de la personne, déterminé de manière objective, l'emporte.

[73] Des facteurs de nature juridique et pratique renforcent cette conclusion. Sur le plan juridique, il est clair, selon l'exigence relative au consentement valable énoncée à l'article 6.1 de la LPRPDE, que la validité du consentement de la personne concernée dépend de la compréhension qu'elle a de ce à quoi elle consent. Sur le plan pratique, le fait d'exiger d'une partie qu'elle produise des éléments de preuve suffisants pour établir ce qu'une organisation aurait pu ou aurait dû faire pourrait, selon la complexité des questions en litige, représenter un fardeau de preuve dont il est impossible de s'acquitter.

Consentement valable : amis Facebook des utilisateurs

[74] Selon les articles 4.3.4 et 4.3.6 de l'annexe 1 de la LPRPDE, la forme du consentement qu'une organisation cherche à obtenir et la façon dont une organisation obtient le consentement peuvent varier en fonction des circonstances. En l'espèce, les circonstances entourant le consentement différaient pour les deux groupes d'utilisateurs de Facebook dont les données ont été communiquées : les utilisateurs ayant téléchargé des applications tierces et les amis Facebook de ces utilisateurs.

[75] Seuls les utilisateurs ayant installé des applications tierces ont eu la possibilité, après avoir pris connaissance de la politique de confidentialité des applications en question, de consentir directement à l'utilisation de leurs données par l'application TYDL (ou par d'autres applications). Il en a été autrement pour les amis Facebook de ces utilisateurs. En outre, les utilisateurs directs d'applications tierces étaient en mesure de recourir au processus GDP, grâce auquel ils étaient informés des catégories de renseignements auxquels les applications souhaitaient accéder, recevaient un lien vers la politique de confidentialité des applications et avaient la possibilité d'accorder ou de refuser les autorisations de communication des données.

[76] Cette distinction entre les utilisateurs et leurs amis Facebook est fondamentale aux fins de l'analyse fondée sur la LPRPDE. Les amis Facebook des utilisateurs ne pouvaient pas recourir au processus GDP de chaque application et n'étaient pas en mesure de connaître ou de comprendre les fins auxquelles leurs données seraient utilisées, comme l'exige la LPRPDE.

[77] La seule conclusion que pouvait tirer la Cour fédérale à la lumière des éléments de preuve était que Facebook n'a pas obtenu un consentement valable de la part des amis Facebook des utilisateurs quant à la communication de leurs données, et a ainsi enfreint la LPRPDE. Cette conclusion repose principalement sur le fait que les pratiques de Facebook en matière de consentement différaient selon qu'il s'agissait des utilisateurs d'applications ou des amis Facebook de ces utilisateurs, ainsi que sur les politiques et pratiques de Facebook en matière de confidentialité en lien avec les applications tierces de manière plus générale. Ces éléments de preuve ayant été admis par la Cour fédérale, cette dernière a commis une erreur manifeste et déterminante en concluant qu'il n'y avait pas eu violation de la LPRPDE.

[78] Les amis Facebook des utilisateurs ayant téléchargé des applications tierces n'ont pas eu la possibilité de donner un consentement valable quant à la communication de leurs données puisqu'ils n'étaient tout simplement pas en mesure de

consulter les politiques de confidentialité de ces applications avant la communication de leurs données. Facebook ne leur a pas donné cette possibilité, ce qui contrevient à la LPRPDE : l'article 4.3.2 de l'annexe 1 de la LPRPDE exige que les organisations fassent « un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés ».

[79] La Politique de la plateforme Facebook exigeait que les applications tierces, grâce à leurs politiques de confidentialité, informent les utilisateurs quant aux données qui seraient utilisées par les applications et quant à la façon dont ces données seraient utilisées ou communiquées. Même si cette pratique avait été suffisante quant à l'obtention d'un consentement valable de la part des utilisateurs ayant installé une application, elle ne l'aurait été que pour les utilisateurs en mesure d'accéder à la politique pertinente au moment de la communication; les amis Facebook des utilisateurs-installateurs étant donc exclus.

[80] Les amis des utilisateurs n'ont été informés que de manière générale, par le truchement de la Politique de confidentialité de Facebook, que leurs renseignements pourraient être communiqués à des applications tierces lors de l'utilisation de ces applications par leurs amis : la Politique de confidentialité indiquait que, « si vous publiez quelque chose sur Facebook, toute personne qui peut y accéder peut permettre à d'autres (comme des jeux, des applications ou des sites Web qu'ils utilisent) d'y accéder » et que « [s]i vous avez rendu [certaines] information[s] publique[s], l'application peut alors y accéder comme n'importe qui d'autre. Mais si vous n'avez ouvert vos intérêts qu'avec vos amis, l'application doit demander à votre ami de l'autoriser à y accéder » (non souligné dans l'original).

[81] Toutefois, la Politique de confidentialité donne des exemples banals de la façon dont ces applications peuvent utiliser les données des utilisateurs. La Politique de confidentialité ne prévoit pas l'utilisation des données à grande échelle, sans lien avec la raison d'être de l'application elle-même, comme ce fût le cas en l'espèce :

> Vos amis et les autres personnes avec qui vous communiquez fréquemment souhaitent partager vos informations avec des applications afin d'obtenir une expérience plus personnalisée et sociale. Par exemple, un de vos amis pourrait souhaiter utiliser une application de musique qui lui permet de voir ce que ses amis écoutent. Pour profiter pleinement de cette application, votre ami doit permettre à l'application d'accéder à sa liste d'amis (ce qui comprend votre identifiant d'utilisateur) pour qu'elle puisse savoir lesquels de vos amis l'utilisent également. Votre ami souhaite également indiquer à l'application la musique que vous avez indiqué aimer sur Facebook.
>
> […]
>
> Lorsqu'une application demande la permission à quelqu'un d'autre de pouvoir accéder à vos informations, cette application sera autorisée à utiliser cette information uniquement en rapport avec la personne qui a donné cette permission et personne d'autre.
>
> Par exemple, certaines applications utilisent des informations telles que votre liste d'amis pour personnaliser votre expérience et vous indiquer quels sont ceux de vos amis qui utilisent cette application particulière.
>
> (Non souligné dans l'original.)

[82] Ce libellé est trop général pour être efficace. La lecture de ce libellé ne permettrait pas à l'utilisateur d'obtenir une information suffisante sur la multitude de moyens par lesquels une application peut utiliser ses données. L'utilisateur ne pourrait donc pas donner un consentement valable à la communication future de ses données à des applications tierces inconnues téléchargées par leurs amis. De plus, selon le libellé de la Politique de confidentialité, il y aurait des limites quant à l'utilisation qu'une application pourrait faire des données des amis de l'utilisateur. En l'espèce, même si le consentement peut être déduit des circonstances, les données ont été utilisées à des fins au-delà de celles qui auraient pu raisonnablement être envisagées.

[83] Il faut garder à l'esprit que le consentement valable, au titre du troisième principe et de l'article 6.1 de la LPRPDE, repose sur la compréhension de la personne raisonnable quant à la nature, aux fins et aux conséquences de la communication. En l'espèce, il était impossible pour les amis Facebook des utilisateurs de s'informer, au moment de la communication, sur les fins auxquelles chaque application tierce utiliserait leurs données, ou même de savoir que leurs données étaient communiquées à ces applications. Ce privilège était réservé aux utilisateurs directs de chaque application. Au mieux, la lecture de la Politique de confidentialité donnait aux amis Facebook des utilisateurs directs de ces applications une image vague et optimiste de la façon dont les applications tierces pouvaient utiliser leurs données. En se créant un compte Facebook, les amis des utilisateurs directs des applications donnaient effectivement leur accord au sujet d'une communication inconnue, à une application inconnue et à un moment inconnu dans le futur, de données pouvant être utilisées à des fins inconnues. On ne saurait affirmer qu'il s'agit d'un consentement valable.

Consentement valable : installateurs de l'application TYDL

[84] J'arrive à la même conclusion en ce qui concerne les utilisateurs ou installateurs des applications : ils n'ont pas donné un consentement valable. L'analyse comporte certaines différences compte tenu des éléments contextuels et factuels propres à chacun des deux groupes. La différence fondamentale réside dans le fait que les utilisateurs-installateurs pouvaient recourir au processus GDP, tandis qu'il en était autrement pour leurs amis Facebook. Toutefois, l'analyse des politiques de Facebook et des attentes des utilisateurs-installateurs à la lumière de ces politiques permet d'en arriver à la même conclusion au sujet du consentement valable.

[85] Les Conditions de service et la Politique de confidentialité constituent le point de départ. À elles deux, elles décrivent les types de renseignements des utilisateurs que recueille Facebook, les renseignements des utilisateurs qui sont publics et la façon dont ces renseignements sont utilisés. À la lecture littérale de ces documents, l'on pourrait comprendre que l'utilisateur a été averti des risques et qu'il a donné son consentement. La question est tout autre, cependant, lorsqu'il s'agit de qualifier de valable un tel consentement.

[86] Les termes qui sont en apparence clairs ne donnent pas nécessairement lieu à un consentement valable. La clarté apparente peut s'évaporer ou s'embrouiller en raison de la longueur du document et du brouillard qui s'y installe ainsi que de la complexité des termes utilisés. De la longueur qu'une nouvelle d'Alice Munro, les Conditions de service et la Politique de confidentialité — que probablement peu de personnes lisent, de l'aveu de Mark Zuckerberg lui-même lors de son témoignage

devant un comité sénatorial américain — ne constituent pas un consentement valable aux communications en cause en l'espèce.

[87] Le mot « consentement » n'est pas vide de contenu, et en l'espèce, le contenu est prescrit par la loi. Il comprend une compréhension de la nature, des fins et des conséquences de la communication. En l'espèce, la Cour fédérale devait donc se demander si la personne raisonnable aurait compris que, en téléchargeant un test de personnalité (ou toute autre application), elle consentait au risque que l'application s'empare de ses données et de celles de ses amis pour les utiliser d'une manière contraire aux règles internes de Facebook (c.-à-d. les vendre à une entreprise à des fins de ciblage publicitaire en prévision des élections américaines de 2016). Si la question avait été posée à la personne raisonnable, elle aurait pu prendre une décision éclairée.

[88] D'autres éléments de preuve contextuels étayent ce point de vue de la personne raisonnable.

[89] D'abord, les principales dispositions sur lesquelles Facebook s'appuie pour établir le consentement se trouvent dans la Politique de confidentialité, et non dans les Conditions de service. Devant le Sénat américain, Mark Zuckerberg a laissé entendre que même Facebook ne pouvait pas s'attendre à ce que tous ses utilisateurs lisent, et encore moins comprennent, les Conditions de service ou la Politique de confidentialité; il a déclaré que [TRADUCTION] « la plupart des utilisateurs ne lisent probablement pas [les politiques] dans leur intégralité ». Pire encore, les Conditions de service embrouillent le consentement relatif à la Politique de confidentialité elle-même puisqu'elles incorporent cette dernière par renvoi. Ainsi, l'utilisateur qui accepte les Conditions de service est réputé avoir donné son consentement au sujet des deux documents. Il ne s'agit pas là du consentement actif, positif et ciblé que prévoient le troisième principe et l'article 6.1 de la LPRPDE.

[90] Facebook n'a pas averti les utilisateurs que des acteurs malveillants pourraient accéder à la plateforme Facebook, et y accéderaient probablement, et pourraient donc avoir accès à leurs données. Comme il est précisé ci-dessous, Mark Zuckerberg a admis en 2018 qu'il serait [TRADUCTION] « difficile de […] garantir » qu'aucun acteur malveillant ne pourra jamais utiliser la plateforme Facebook. Par conséquent, Facebook se positionne en tant qu'intermédiaire neutre et passif, comme un interlocuteur entre les membres de la communauté Facebook, sans engager sa responsabilité à l'égard de ce qui se passe sur sa plateforme.

[91] En se positionnant ainsi, Facebook tente de réduire, voire d'éliminer les responsabilités qui lui incombent en vertu de la LPRPDE. Facebook a certes averti les utilisateurs, par le truchement de sa Politique de confidentialité, que les applications tierces ne faisaient [TRADUCTION] « pas partie de Facebook ou [n'étaient] pas contrôlées par Facebook », et leur a recommandé de [TRADUCTION] « toujours lire les conditions de service et les politiques de confidentialité [des applications] pour comprendre comment elles traitent [leurs] données ». L'on ne peut cependant pas en déduire que les utilisateurs qui ont lu la Politique de confidentialité savaient que ces applications tierces pouvaient être des acteurs malveillants ayant l'intention de ne pas respecter les politiques de Facebook ou les lois locales en matière de protection de la vie privée, encore moins que ces acteurs malveillants pourraient avoir l'intention de vendre les données des utilisateurs à une tierce partie.

[92] Fait important, l'utilisateur de Facebook raisonnable s'attendrait à ce que Facebook eût mis en place de solides mesures préventives pour empêcher les acteurs malveillants de faire des déclarations trompeuses au sujet de leurs propres pratiques en matière de protection de la vie privée et d'accéder aux données des utilisateurs pour de fausses raisons. Les organisations peuvent se fier à des tiers pour obtenir le consentement quant à la communication de données, mais elles doivent tout de même prendre des mesures raisonnables pour s'assurer que ce consentement est valable (décision de la Cour fédérale, au paragraphe 65). L'on peut difficilement concevoir comment Facebook peut faire valoir ce moyen de défense au vu de ses propres éléments de preuve selon lesquels 46 p. 100 des développeurs d'applications n'ont pas lu les politiques applicables depuis le lancement de leurs applications.

[93] La Cour fédérale avait en main des éléments de preuve relatifs aux obligations en matière de consentement et de mesures de sécurité. Selon ces éléments de preuve, Facebook avait adopté, pendant la période pertinente, une approche passive quant à la surveillance de la conduite des applications tierces utilisant la plateforme Facebook en matière de protection de la vie privée. Facebook n'a pas passé en revue le contenu des politiques de confidentialité des applications tierces, telles qu'elles étaient présentées aux utilisateurs; Facebook s'est contentée de s'assurer que l'hyperlien menait à un site Web fonctionnel.

[94] En réponse, Facebook décrit différents types de mécanismes de conformité, exécutés à la fois par des humains et de manière automatisée, qu'elle a mis en place pour protéger le droit à la vie privée des utilisateurs. Facebook ajoute qu'elle a pris 6 millions de mesures coercitives pendant la période pertinente, sans toutefois donner de précisions quant aux cibles et aux raisons d'être de ces 6 millions de mesures coercitives, ni à leurs conséquences ou à leur efficacité. À lui seul, ce chiffre est peu révélateur; l'on ne sait pas combien de mesures coercitives Facebook a prises contre des applications tierces pour non-respect de ses politiques de confidentialité.

[95] Enfin, Facebook n'a pris aucune mesure à la suite de la demande que l'application TYDL a présentée en 2014 pour avoir accès à des données non essentielles sur les utilisateurs. En fait, Facebook a permis à l'application de continuer à recueillir les données des amis Facebook des utilisateurs pendant une année supplémentaire (décision de la Cour fédérale, au paragraphe 43). Cette inaction est révélatrice. Les demandes de données non essentielles sur les utilisateurs, comme celles présentées par l'application TYDL, ont été qualifiées, par le souscripteur de l'affidavit de Facebook, de [TRADUCTION] « signaux d'alarme » quant au potentiel non-respect des politiques par une application.

[96] Je suis d'accord, et j'ajoute que cette inaction suscite des interrogations quant aux raisons pour lesquelles Facebook n'a pas enquêté davantage sur l'application TYDL et ses pratiques en matière de protection de la vie privée, malgré ce signal d'alarme.

[97] Au vu de l'ensemble de ces pratiques, la seule conclusion possible est que Facebook n'a pas informé adéquatement les utilisateurs, lors de la création de leur compte Facebook, des risques entourant leurs données (risques qui se sont concrétisés avec l'application TYDL et Cambridge Analytica). Aucun consentement valable n'a par conséquent été obtenu. Comme il en est question ci-dessous, ces mêmes pratiques et

mesures — ou l'absence de telles pratiques et mesures — ont mené au manquement, par Facebook, à ses obligations en matière de mesures de sécurité.

[98] Je conclus en précisant que l'argument de Facebook repose principalement sur l'hypothèse selon laquelle les utilisateurs lisent les politiques de confidentialité qui leur sont présentées lors de leur inscription sur des sites de réseaux sociaux. Ainsi que je le mentionne plus haut, la longueur des politiques s'apparentant à celle d'une nouvelle, cette hypothèse soulève des doutes; voir, par exemple, les critiques de Laurent Crépeau quant à l'efficacité des politiques de confidentialité des sites de réseaux sociaux, dans son article intitulé « Responding to Deficiencies in the Architecture of Privacy : Co-Regulation as the Path Forward for Data Protection on Social Networking Sites » (2022), 19:2 *Can. J.L. & Tech.* 411, à la page 446 :

> [TRADUCTION]
>
> […] les consommateurs entretiennent une relation des plus déséquilibrée avec [les sites de réseaux sociaux]. Ils savent rarement comment leurs données sont recueillies et utilisées, et encore moins quelle quantité de données le sont. En outre, l'information relative aux pratiques de l'entreprise en matière de protection de la vie privée est généralement épurée dans la documentation fournie dans les sections d'aide et les politiques de confidentialité, ou est rédigée avec si peu de précision qu'il est impossible de saisir concrètement ce qui y est réellement décrit.

[99] Je suis d'accord. J'ajoute que ces critiques concordent avec les propres aveux de Facebook quant à la portée et à l'efficacité de ses politiques de consentement, qui, dans le contexte de la présente affaire, sont des aveux préjudiciables à leur auteur. En outre, plusieurs paramètres de confidentialité de Facebook autorisent la communication par défaut, ce qui nécessite à la fois une compréhension de la part de l'utilisateur quant aux risques associés à ces paramètres par défaut et une démarche proactive de la part de l'utilisateur quant à la modification de ses paramètres. Le consentement nécessite un choix actif et affirmatif, et non un choix par défaut.

[100] Un autre élément contextuel important réside dans le fait qu'il est question de contrats d'adhésion en matière de consommation. Les clauses de Facebook en matière de confidentialité et de communication sont ainsi situées dans leur contexte contractuel. Le contrat d'adhésion en matière de consommation ne donne au consommateur aucune possibilité de négociation. Pour se créer un compte Facebook, il faut accepter toutes les conditions énoncées dans les Conditions de service et dans la Politique de confidentialité. Comme l'a fait observer la juge Abella dans ses motifs concordants dans l'arrêt *Douez c. Facebook, Inc.*, 2017 CSC 33, [2017] 1 R.C.S. 751 (*Douez*), « [i]l n'y a ni négociation, ni choix, ni modulation » (au paragraphe 98).

[101] Cette absence de négociation n'est pas sans conséquence : elle accroît la probabilité d'une divergence des attentes quant à ce que le contrat implique. Encore une fois, comme l'a écrit la juge Abella, au paragraphe 99 de l'arrêt *Douez* :

> Un contrat conclu en ligne comme celui considéré en l'espèce met à l'épreuve les principes traditionnels du droit contractuel. Qu'en est-il du « consentement » lorsqu'il y a accord sur simple pression d'une touche de clavier? Est-il réaliste de penser que le consommateur a pris connaissance de toutes les conditions et donné un consentement véritable? Autrement dit, j'estime que les tribunaux doivent tenir compte du caractère automatique des engagements qui résultent de ce genre de contrat, non pas pour invalider le contrat comme tel, mais pour

> resserrer à tout le moins l'examen d'une clause qui a l'effet de compromettre l'accès du consommateur à d'éventuels recours.

[102] Cette même vigilance accrue devrait être appliquée, en l'espèce, aux clauses de la Politique de confidentialité qui, selon Facebook, autorisent une large communication future de données, potentiellement à des acteurs malveillants.

[103] Certes, l'arrêt *Douez* s'attaque à une autre bête : une clause d'élection de for. Après s'être créé un compte Facebook, l'utilisateur n'avait aucun moyen de modifier individuellement ses droits en matière d'élection de for, ce qui ne cadre pas avec la flexibilité caractérisant les paramètres de confidentialité de l'utilisateur sur Facebook. Toutefois, comme je l'explique plus haut, l'on ne peut avoir la certitude que la personne qui s'est créé un compte Facebook comprenait les subtilités de la Politique de confidentialité et l'éventuelle communication de données à laquelle elle consentait en premier lieu. De plus, je ne suggère pas que les clauses en question en l'espèce deviendraient inapplicables du fait qu'elles sont incluses dans un contrat d'adhésion en matière de consommation, comme dans l'affaire *Douez* (voir les motifs majoritaires, aux paragraphes 52 à 57, et les motifs concordants de la juge Abella, au paragraphe 104). En l'espèce, la nature du contrat agit plutôt comme un prisme interprétatif qui limite l'effet des dispositions applicables.

[104] Dans leur article intitulé « Automating Accountability? Privacy Policies, Data Transparency, and the Third-Party Problem » (2022), 72:2 *U. Toronto L.J.* 155, David Lie et ses co-auteurs reconnaissent l'importance que revêtent les politiques de confidentialité lorsqu'il est question de la transparence des données. Ils font cependant remarquer que les politiques de confidentialité [TRADUCTION] « sont largement considérées comme ne parvenant pas à améliorer la compréhension qu'ont les consommateurs des flux de données », puisque [TRADUCTION] « la plupart des gens ne les lisent pas, bon nombre les trouvent difficiles à comprendre et, même s'ils lisaient et comprenaient les politiques visant directement les services qu'ils utilisent, l'exercice leur prendrait un temps déraisonnable » (aux pages 157 et 158).

[105] Ces auteurs critiquent également l'incapacité des politiques de confidentialité à [TRADUCTION] « fournir une image claire des paramètres de confidentialité "par défaut" », notant qu'il est déclaré, dans la Politique de confidentialité de Facebook elle-même, que, [TRADUCTION] « [l]orsque vous partagez et communiquez du contenu en utilisant nos [produits], vous choisissez le public [à qui sera partagé ou communiqué le contenu] ». Cette formulation [TRADUCTION] « [n']aide [pas] l'utilisateur […] à analyser les paramètres par défaut initiaux » (à la page 165; le libellé de la Politique de confidentialité mis à jour en tenant compte de la plus récente Politique de confidentialité de Facebook au dossier devant notre Cour). Les paramètres par défaut peuvent également [TRADUCTION] « inciter la personne à faire un choix en matière de confidentialité qui ne correspond pas à ses préférences en matière de confidentialité ou qui soulève des préoccupations sociales de plus grande portée » (à la page 165). L'auteur Laurent Crépeau précise également que les sites de réseaux sociaux sont généralement conçus de manière à inciter à la communication des données des utilisateurs grâce à des paramètres par défaut [TRADUCTION] « qui donnent lieu à l'autorisation de la communication des données puisque les utilisateurs prennent rarement le temps de les modifier, quand ils savent qu'une telle modification est possible » (à la page 420).

[106] En 2018, Mark Zuckerberg a reconnu devant le Sénat américain que Facebook ne s'était pas acquittée de [TRADUCTION] « sa responsabilité fondamentale en matière de protection des renseignements des utilisateurs » et qu'elle n'en avait pas fait suffisamment pour [TRADUCTION] « empêcher que les outils [de Facebook] soient utilisés à des fins malveillantes ». Il a ajouté, de son propre aveu, que [TRADUCTION] « la plupart des utilisateurs ne lisent probablement pas [la Politique de confidentialité et les Conditions de service] dans leur intégralité ». De plus, la vice-présidente et directrice de la confidentialité de Facebook a annoncé, dans un communiqué de 2018, que la violation commise par Cambridge Analytica [TRADUCTION] « a montré combien [de travail il reste à Facebook] à faire pour faire respecter [ses] politiques et pour aider les utilisateurs à comprendre comment fonctionne Facebook ainsi que les choix qui s'offrent à eux au sujet de leurs données ».

[107] Dans ces aveux, aucune distinction n'est faite entre les utilisateurs de l'application TYDL et les amis Facebook de ces utilisateurs.

[108] Si la Cour fédérale avait tenu compte de tous les facteurs dont il est fait mention plus haut, elle aurait conclu qu'aucun utilisateur n'a donné un consentement valable à toutes les communications de ses données par Facebook pendant la période pertinente.

Obligation en matière de mesures de sécurité

[109] L'organisation qui se conforme en tout point à la LPRPDE n'est pas à l'abri d'une atteinte à la protection des données. Toutefois, en l'espèce, il existe un lien direct entre les communications non autorisées et les choix de Facebook quant à ses politiques et aux principes de conception axés sur l'utilisateur. Facebook a invité des millions d'applications à joindre sa plateforme et a omis d'assurer une surveillance adéquate à leur égard. La Cour fédérale n'a pas tenu compte des éléments de preuve pertinents sur ce point, commettant ainsi une erreur de droit.

[110] Facebook n'a pas pris connaissance du contenu des politiques de confidentialité des applications tierces, même si ces applications ont accès aux données des utilisateurs qui les téléchargent, ainsi qu'aux données des amis Facebook de ces utilisateurs. Facebook n'ayant jamais passé en revue ces politiques de confidentialité, et les amis des utilisateurs qui téléchargent les applications n'ayant également pas pu en prendre connaissance, les mesures de contrôle quant à l'utilisation et à la communication des données par les applications étaient laissées entre les mains d'un petit nombre d'utilisateurs qui téléchargeaient les applications et qui n'avaient eux-mêmes peut-être jamais lu les politiques.

[111] Par ailleurs, Facebook n'a également pris aucune mesure à la suite de la demande que l'application TYDL a présentée en 2014 pour avoir accès à des données non essentielles sur les utilisateurs, bien que cette demande ait été qualifiée de [TRADUCTION] « signal d'alarme » par le souscripteur de l'affidavit de Facebook. En ne vérifiant pas les politiques de confidentialité des applications tierces, Facebook a certes manqué à son obligation de prendre des mesures préventives suffisantes contre la communication non autorisée des données des utilisateurs. Toutefois, en ne prenant aucune mesure après avoir constaté l'existence de signaux d'alarme, Facebook a fait fi de son obligation de protéger adéquatement les données des utilisateurs.

[112] J'ajouterais que l'inaction de Facebook en l'espèce s'inscrivait dans une tendance plus large : en décembre 2015, lorsque Facebook a découvert que l'application TYDL s'était emparée des données d'utilisateurs et d'amis Facebook de ces utilisateurs et les avait vendues, en violation des politiques de Facebook, elle n'a pas informé les utilisateurs concernés et n'a pas chassé Cambridge Analytica ou M. Kogan de la plateforme. Ce n'est qu'après avoir découvert que M. Kogan et Cambridge Analytica n'avaient peut-être pas supprimé les données d'utilisateurs qu'ils avaient obtenues de manière inappropriée que Facebook les a expulsés de sa plateforme, en mars 2018, soit deux ans et demi après que les médias ont révélé que l'application TYDL s'était emparée des données d'utilisateurs et les avait vendues (décision de la Cour fédérale, au paragraphe 39; voir également la réponse partielle de Facebook au commissaire en 2018).

[113] Précisons que la conduite de Facebook après la communication des données à l'application TYDL n'est pas utile sur le plan juridique. Comme l'a établi la Cour fédérale, le principe relatif aux mesures de sécurité est lié à la façon dont l'organisation gère les données, et non à la surveillance des données après leur communication. Toutefois, les mesures prises par Facebook après la communication des données étayent, sur le plan contextuel, la conclusion selon laquelle l'entreprise n'a pas pris des précautions suffisantes pour garantir la protection des données qui étaient en sa possession avant la communication.

[114] Facebook soutient qu'il lui aurait été pratiquement impossible de lire toutes les politiques de confidentialité des applications tierces pour s'assurer de leur conformité, et qu'elle était en droit de s'en remettre à l'exécution de bonne foi des contrats conclus avec les applications tierces.

[115] Il aurait peut-être été pratiquement impossible pour Facebook de lire chacune des politiques de confidentialité des applications tierces, mais Facebook est elle-même à l'origine de cette difficulté. Elle a invité les applications sur sa plateforme et ne peut pas invoquer l'impossibilité pour que soit limitée la portée des responsabilités qui lui incombent en vertu de l'article 6.1 et du troisième principe de la LPRPDE.

[116] L'on peut faire en l'espèce une analogie flottante, malgré ses limites évidentes, avec la jurisprudence relative à la responsabilité des hôtes commerciaux (en commençant par l'arrêt *Jordan House Ltd. c. Menow*, [1974] R.C.S. 239, 1973 CanLII 16, à la page 248) : ayant invité des clients avec pour motif clair de réaliser des profits, l'hôte ne peut pas ensuite prétendre que trop de personnes ont répondu à l'appel et que certaines se sont mal comportées, l'empêchant ainsi de respecter ses obligations. Certes, la question dont est saisie notre Cour n'en est pas une de négligence — il s'agit plutôt de déterminer si Facebook a pris des mesures raisonnables pour protéger les données des utilisateurs qu'elle avait invités sur sa plateforme. La portée de cette observation est encore plus grande lorsque l'on tient compte du modèle d'affaires de Facebook : plus il y a d'applications, plus il y a d'utilisateurs, et plus l'achalandage est grand, plus Facebook génère des revenus. Facebook a elle-même rendu possible l'atteinte à la protection des données; elle ne peut donc pas se soustraire à ses obligations légales.

[117] Facebook peut s'en remettre à l'exécution de bonne foi des contrats qu'elle a conclus avec les applications tierces, mais seulement jusqu'à un certain point. Je rappelle que Mark Zuckerberg a admis qu'il serait difficile de garantir qu'aucun « acteur

malveillant » n'utiliserait sa plateforme. L'on ne saurait s'attendre à ce qu'un acteur malveillant exécute un contrat de bonne foi. Facebook aurait donc dû prendre des mesures supplémentaires pour s'assurer du respect des contrats par les applications tierces.

[118] Je conclus que, pendant la période pertinente, Facebook a manqué à ses obligations en matière de mesures de sécurité puisqu'elle n'a pas assuré adéquatement le respect et la surveillance des pratiques en matière de protection de la vie privée des applications tierces qui utilisent sa plateforme.

Équilibre téléologique au titre de la LPRPDE

[119] Dans ses motifs du rejet de la demande du commissaire, la Cour fédérale a précisé que les observations des parties se contentaient de « milite[r] en faveur d'une législation fédérale mûrement réfléchie et équilibrée qui relève les défis que posent les médias sociaux et le partage numérique de renseignements personnels », et qu'une conclusion selon laquelle il y a eu violation de la LPRPDE constituerait « une interprétation dénuée de tout principe que la Cour [fédérale] pourrait faire de la loi actuelle qui s'applique également aux géants des réseaux sociaux, aux banques locales et aux concessionnaires automobiles » (décision de la Cour fédérale, au paragraphe 90).

[120] Une telle affirmation ne tient pas compte de l'importance du contexte. Bien qu'une loi normative s'applique effectivement à tous et de manière égale, son application varie en fonction du contexte. Le modèle d'affaires de Facebook repose notamment sur le regroupement de données et sur la fidélité des utilisateurs envers sa plateforme dans le but de vendre de la publicité. La raison d'être de Facebook façonne le contenu et les limites de ses obligations quant à la protection des renseignements et à l'obtention d'un consentement valable. Il n'y a aucun frein ou limite interne au « besoin » de Facebook en matière de données, compte tenu de l'utilisation qu'elle en fait, des caractéristiques démographiques de sa clientèle et du lien direct entre cette utilisation et les profits de l'organisation. Le « besoin » du concessionnaire automobile en matière de données diffère en tout point; la nature des données et leurs utilisations sont raisonnablement compréhensibles, prévisibles et limitées. L'analogie avec le concessionnaire automobile est inappropriée.

[121] Je précise au passage que la Cour fédérale a renvoyé au « droit des organisations de recueillir, d'utiliser et de communiquer des renseignements personnels » (au paragraphe 50, non souligné dans l'original). Toutefois, l'objet de la LPRPDE, tel qu'il est énoncé à l'article 3, renvoie au droit de l'individu à la vie privée et au besoin de l'organisation de recueillir, d'utiliser ou de communiquer des renseignements personnels. L'organisation n'a aucun droit inhérent aux données, et son besoin doit être mesuré en fonction de la nature de l'organisation elle-même. S'agissant de l'application de la LPRPDE, cette distinction entre les « droits » conférés à l'individu et le « besoin » de l'organisation se veut un fondement conceptuel important.

[122] Le dispositif de la présente affaire concorde avec l'objet de la LPRPDE, énoncé à l'article 3 de cette même loi. Il en est autrement de la conclusion selon laquelle les utilisateurs de Facebook ayant téléchargé l'application TYDL (ou d'autres applications) ont accepté le risque que leurs données soient, à un moment inconnu, communiquées

à des tiers inconnus, et ce, après qu'on leur a présenté, sous forme numérique, une politique générique en présumant qu'ils avaient lu une autre politique les avertissant de la possibilité que leurs données soient communiquées, le tout pour permettre à Facebook d'augmenter ses profits.

[123] Le législateur a inséré le mot « valable » à l'article 4.3.2 de l'annexe 1 de la LPRPDE, et il est entendu que chaque mot utilisé dans le libellé d'une loi doit avoir un sens. Si le consentement pur et contractuel constituait l'unique critère, l'issue de la présente affaire pourrait être différente. Toutefois, telle n'était pas l'intention du législateur. En d'autres termes, il ne s'agit pas de nous pencher sur l'existence d'une disposition, dissimulée dans les conditions de service, selon laquelle l'on peut conclure que l'utilisateur a donné son consentement. Une telle disposition, sur laquelle une partie peut s'appuyer, existe presque toujours. Cette question est certes importante, mais elle n'est pas déterminante du respect de la double obligation en vertu de la LPRPDE; l'analyse se veut plutôt contextuelle et d'une plus grande portée.

[124] Pour déterminer si le consentement est valable, il convient de tenir compte de tous les éléments contextuels applicables, notamment les caractéristiques démographiques des utilisateurs, la nature des données, la manière dont l'utilisateur et la personne en possession des données interagissent, le fait que le contrat en cause en est un d'adhésion ou non, la clarté et la longueur du contrat et des conditions connexes ainsi que la nature des paramètres de confidentialité par défaut. L'on peut également faire intervenir les principes de l'iniquité et de l'inégalité du pouvoir de négociation. Tous ces éléments caractérisent le point de vue de la personne raisonnable et permettent de déterminer si cette dernière a consenti ou non à la communication.

Non-application des théories de la préclusion par assertion de fait et de l'erreur provoquée par une personne en autorité

[125] Facebook s'appuie sur les théories de la préclusion par assertion de fait et de l'erreur provoquée par une personne en autorité pour soutenir qu'il n'y a eu aucune violation de la LPRPDE.

[126] La théorie de l'erreur provoquée par une personne en autorité est un moyen de défense pouvant être invoqué contre des accusations criminelles ou à l'égard d'infractions réglementaires. Voir, par exemple : *Lévis (Ville) c. Tétreault; Lévis (Ville) c. 2629-4470 Québec inc.*, 2006 CSC 12, [2006] 1 R.C.S. 420, aux paragraphes 20 à 26; et *La Souveraine, Compagnie d'assurance générale c. Autorité des marchés financiers*, 2013 CSC 63, [2013] 3 R.C.S. 756, au paragraphe 57. Dans le même ordre d'idées, la théorie de la préclusion promissoire peut être invoquée contre une autorité publique (*Malcolm c. Canada (Ministre des Pêches et des Océans)*, 2014 CAF 130, [2014] A.C.F. nº 499 (QL) (*Malcolm*), au paragraphe 38).

[127] Je comprends le fondement de ces arguments. Les formulations que le commissaire a utilisées dans ses échanges avec Facebook étaient générales. L'argument ne saurait être retenu pour les motifs ci-dessous. Il convient toutefois de souligner que les fonctionnaires doivent éviter les déclarations potentiellement catégoriques lorsque les faits sont flous et que la relation entre la technologie et le droit à la vie privée évolue rapidement.

[128] Cet argument tire son origine d'une enquête menée en 2008–2009 par le commissaire au sujet des pratiques de Facebook en matière de protection de la vie privée, y compris la communication, par Facebook, de données d'utilisateurs à des applications tierces. À la suite de cette enquête, le commissaire a notamment formulé les recommandations suivantes à l'intention de Facebook : limiter l'accès des applications tierces aux données des utilisateurs afin qu'elles ne puissent accéder qu'aux données nécessaires à leur fonctionnement; informer les utilisateurs quant aux données précises auxquelles les applications peuvent accéder ainsi qu'aux fins pour lesquelles elles y accèdent; et exiger que les utilisateurs consentent à la communication des données auxquelles les applications souhaitent accéder.

[129] En outre, le commissaire a initialement recommandé à Facebook d'interdire la communication des données des utilisateurs qui n'installaient pas eux-mêmes une application (c.-à-d. les amis Facebook des utilisateurs-installateurs), mais est revenu sur sa décision compte tenu de la mise en œuvre proposée du processus GDP ainsi que de la nature sociale et interactive de nombreuses applications (décision de la Cour fédérale, aux paragraphes 45 et 46).

[130] Dans une lettre de septembre 2010, le commissaire a informé Facebook qu'elle avait honoré ses engagements envers le Commissariat, tout en encourageant Facebook « à continuer d'améliorer ses moyens de surveillance et à informer les développeurs de leurs responsabilités en matière de protection de la vie privée » (décision de la Cour fédérale, au paragraphe 47).

[131] Le moyen de défense de Facebook fondé sur les théories de la préclusion par assertion de fait et de l'erreur provoquée par une personne en autorité est rejeté pour trois motifs.

[132] Premièrement, pour ce qui est des faits, les déclarations du commissaire n'étaient elles-mêmes pas claires : le commissaire a constaté « avec plaisir » que Facebook avait « mi[s] en place [le] modèle [GDP] », mais a également encouragé Facebook à « continuer d'améliorer ses moyens de surveillance et à informer les développeurs » (décision de la Cour fédérale, au paragraphe 47). L'enquête et les échanges connexes ont eu lieu entre 2008 et 2010. La protection de la vie privée et la norme de l'attente raisonnable en matière de protection de la vie privée sont grandement tributaires du contexte, et il va sans dire que le paysage technologique a évolué et continue d'évoluer à une vitesse fulgurante. Même en présumant que Facebook s'était conformée à ses obligations en 2010, la prise de mesures supplémentaires a été encouragée. Facebook peut adapter ses mesures de protection de la vie privée au fil du temps — et l'on devrait s'attendre à ce qu'elle le fasse —, alors que notre compréhension des risques relatifs à la vie privée que représentent les médias sociaux se perfectionne.

[133] Deuxièmement, les instances visées par la LPRPDE sont traitées comme des instances *de novo*. Comme l'a établi notre Cour dans l'arrêt *Englander*, il n'y a pas lieu de faire preuve de retenue à l'égard du rapport que le commissaire présente à l'issue de son enquête, puisque ce qui est en litige dans la demande, « ce n'est pas le rapport du commissaire, mais la conduite de la partie contre laquelle la plainte est déposée » (au paragraphe 47). La préoccupation ultime de Facebook à l'égard de la période pertinente aurait donc dû concerner son respect de la LPRPDE, et non la position du commissaire quant à ses pratiques en 2010.

[134] Enfin, la théorie de la préclusion a une application limitée en droit public et « exige […] que l'on détermine l'intention que le législateur avait en conférant le pouvoir dont on cherche à empêcher l'exercice » (*Malcolm*, au paragraphe 38). L'on ne saurait empêcher le commissaire de s'acquitter de ses obligations légales aujourd'hui en raison d'une déclaration obscure faite il y a plus d'une décennie.

Dispositif

[135] Les pratiques de Facebook entre 2013 et 2015 étaient contraires au troisième principe, au septième principe et à l'article 6.1 de la LPRPDE. Un jugement déclaratoire devrait donc être rendu en ce sens.

[136] De plus, le commissaire demande notamment une ordonnance enjoignant à Facebook de se conformer à la LPRPDE en mettant en place des « mesures efficaces, précises et facilement accessibles en vue d'obtenir le consentement valable de tous les utilisateurs […] et de s'assurer de le conserver » pour la communication des renseignements personnels des utilisateurs à des tiers. Le commissaire énumère des mesures précises que Facebook devrait prendre pour se conformer à cette ordonnance, notamment « indiqu[er] clairement aux utilisateurs la nature, les fins et les conséquences de la communication de leurs renseignements personnels à des tierces parties », « obten[ir] le consentement explicite des utilisateurs lorsque Facebook utilise et communique des renseignements personnels sensibles », « s'assur[er] que les utilisateurs peuvent déterminer, à tout moment, quelle tierce partie a accès à leurs renseignements personnels », « s'assur[er] que les utilisateurs peuvent modifier leurs préférences de manière à mettre un terme en partie ou en totalité aux accès par de telles tierces parties », et « veill[er] constamment à la surveillance de l'ensemble des communications des tierces parties relatives à la protection de la vie privée et à l'application de l'ensemble des pratiques des tierces parties en matière de confidentialité ».

[137] Le commissaire demande également une ordonnance obligeant Facebook « à détailler les révisions, modifications et amendements techniques à apporter à ses pratiques ainsi qu'aux activités et aux fonctions du service Facebook afin de se conformer à la réparation demandée », à la satisfaction du commissaire, sous réserve de l'approbation ultérieure de notre Cour.

[138] Le commissaire demande à notre Cour de rester saisie de la question du contrôle et de l'exécution des ordonnances demandées, et de se prononcer sur toute question qui pourrait être soulevée entre les parties relativement à l'exécution des ordonnances.

[139] La demande de réparation du commissaire s'inscrit dans le contexte de mesures de nature juridique et réglementaire prises ailleurs dans le monde à la suite de la communication de données à Cambridge Analytica.

[140] Aux États-Unis, la Federal Trade Commission (FTC) a notamment imposé une amende de 5 milliards de dollars à Facebook; interdit à Facebook de faire des déclarations trompeuses quant à l'étendue de ses pratiques en matière de sécurité et de protection de la vie privée; exigé que Facebook adopte des pratiques plus explicites et plus claires en matière de consentement; exigé que Facebook rende des comptes à la FTC en matière de conformité; et exigé que Facebook mette en place un programme

de protection de la vie privée dans le cadre duquel elle doit fournir de la documentation quant au contenu du programme, à sa mise en œuvre et à son maintien, évaluer les risques relatifs à la vie privée ainsi que les mesures de sécurité connexes, mettre sur pied un comité indépendant de protection de la vie privée et faire évaluer son programme de protection de la vie privée de façon continue et indépendante (décision et ordonnance de règlement, *USA v. Facebook*, 1:19-cv-02184 (D.D.C.)).

[141] Au Royaume-Uni, en 2018, l'Information Commissioner's Office (ICO) a imposé une amende de 500 000 livres sterling à Facebook concernant des violations aux lois sur la protection des données (notamment pour manque de transparence et non-protection des données des utilisateurs en raison d'un contrôle insuffisant des applications utilisant sa plateforme) (communiqué de l'ICO du 25 octobre 2018).

[142] Je précise que Facebook a négocié un règlement avec les organismes de réglementation des États-Unis et du Royaume-Uni, sans toutefois admettre l'un quelconque des actes répréhensibles allégués (décision et ordonnance de règlement, *USA v. Facebook*; communiqué de l'ICO du 30 octobre 2019).

[143] Soulignant le caractère extraordinaire des mesures demandées ainsi que l'insuffisance du fondement probatoire à l'appui, Facebook soutient que rien ne justifie la prise des [TRADUCTION] « mesures radicales » que demande le commissaire.

[144] Facebook allègue en outre que la demande du commissaire est en fait théorique, puisque ses [TRADUCTION] « pratiques en matière de protection de la vie privée ont évolué de manière significative depuis les événements en cause »; par exemple, Facebook ne permet plus aux applications de demander l'accès aux données sur les amis Facebook des utilisateurs-installateurs, en plus d'avoir renforcé son processus d'examen des applications, amélioré davantage API Graph et clarifié ses Conditions de service ainsi que sa Politique de confidentialité. Je note au passage que cet argument ne concorde pas avec son argument selon lequel l'enquête et les échanges connexes ayant eu lieu entre 2008 et 2010 sont déterminants quant à la demande en l'espèce. Facebook ne peut pas l'emporter sur tous les plans.

[145] Je ne souscris pas à l'argument selon lequel la nature des réparations demandées constitue un motif convaincant aux fins du refus de la réparation. S'il y a un fondement juridique et probatoire à la réparation, son caractère [TRADUCTION] « extraordinaire » ou [TRADUCTION] « radica[l] » est sans importance. Il en va toutefois autrement de la possibilité, pour notre Cour, de rendre une ordonnance de réparation, compte tenu de l'affirmation relative à l'évolution du dossier de preuve depuis le dépôt de la demande. En effet, le potentiel caractère théorique de cette question doit être pris en compte du fait que notre Cour ne rendra aucune ordonnance qui serait inopérante.

[146] Les événements à l'origine de la présente demande se sont produits il y a une décennie. Facebook allègue avoir depuis apporté de nombreux changements à ses pratiques en matière de protection de la vie privée, de sorte qu'aucun lien ne peut donc être établi entre les violations au principal et la question des réparations demandées. En outre, dans les plaidoiries devant notre Cour, il n'a pas été fait mention du caractère suffisant du dossier de preuve dont était saisie la Cour fédérale pour que notre Cour puisse trancher cette question équitablement. À défaut d'avoir à sa disposition d'autres observations ou, potentiellement, de nouveaux éléments de preuve, notre Cour n'est pas à même de décider si l'une ou l'autre des réparations que demande le commissaire

à l'égard de la conduite actuelle de Facebook est raisonnable, utile et justifiée sur le plan juridique.

Conclusion

[147] J'accueillerais l'appel, avec dépens; je déclarerais que les pratiques de Facebook entre 2013 et 2015 étaient contraires au troisième principe, énoncé à l'article 4.3 de l'annexe 1 de la LPRPDE, au septième principe, énoncé à l'article 4.7 de la même annexe, ainsi qu'à l'article 6.1 de la LPRPDE, après son entrée en vigueur. Je recommanderais que notre Cour demeure saisie de l'affaire et exige des parties qu'elles l'informent, dans les 90 jours suivant la date des présents motifs, si elles parviennent ou non à s'entendre sur les modalités d'une ordonnance de réparation sur consentement. Si les parties ne s'entendent pas, des observations supplémentaires sur la question des réparations seront demandées.

LA JUGE GLEASON, J.C.A. : Je suis d'accord.

LA JUGE GOYETTE, J.C.A. : Je suis d'accord.