Recueil des décisions des Cours fédérales

Federal Courts Reports

**NOTES 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*.

Cette décision a été infirmée en appel (A-129-23, 2024 CAF 140). Les motifs du jugement, qui ont été prononcés le 9 septembre 2024, seront publiés dans le volume de l'année 2024 du *Recueil des décisions des Cours fédérales* (RCF). Ils sont disponibles maintenant sur le site web du RCF.

T-190-20

2023 CF 533

**Commissaire à la protection de la vie privée du Canada** (*demandeur*)

*c.*

**Facebook, Inc.** (*défenderesse*)

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

Cour fédérale, juge Manson — Toronto, 6 mars; Ottawa, 13 avril 2023.

*Protection des renseignements personnels — Il s'agissait d'une demande présentée par le demandeur en vertu de l'alinéa 15a) de la Loi sur la protection des renseignements personnels et les documents électroniques — Le demandeur a allégué que la défenderesse (la défenderesse ou Facebook) a enfreint la Loi en partageant les renseignements personnels des utilisateurs de Facebook avec des applications tierces hébergées sur sa plateforme — Les allégations du demandeur ont fait suite à une plainte déposée après que des reportages aient révélé qu'une application tierce (l'application TYDL), avait obtenu des données de la plateforme Facebook et les avait communiquées à une firme de recherche britannique du nom de Cambridge Analytica Ltd. — En 2007, Facebook a lancé sa « plateforme » Facebook, un ensemble de technologies qui permet à des tiers de développer des applications intégrées à Facebook exploitables depuis celle-ci, que les utilisateurs de Facebook peuvent installer — Le scandale de Cambridge Analytica a éclaté après qu'un développeur d'une application tierce a obtenu les renseignements personnels des utilisateurs de Facebook à l'insu et sans le consentement de ces derniers, lesquels avaient installé son application grâce à l'accès à la plateforme Facebook et à l'API Graph — Les renseignements ont par la suite été communiqués, en contravention avec les politiques de Facebook, à des tiers — Au terme de son enquête, le demandeur a publié son rapport de conclusions et a jugé que Facebook avait enfreint la Loi; c'est alors que l'instance a été introduite — Il s'agissait de savoir si la demande était inappropriée du fait que le demandeur a omis d'obtenir le consentement de chacun des plaignants; si Facebook a omis d'obtenir le consentement valable des utilisateurs et des amis Facebook des utilisateurs lorsqu'elle a partagé leurs renseignements personnels avec des applications tierces; et si Facebook a omis de protéger suffisamment les renseignements concernant ses utilisateurs — La défenderesse a soulevé à titre préliminaire une question d'ordre procédural, et a soutenu que la demande était frappée de « nullité » du fait que le demandeur avait omis d'obtenir le consentement de tous les plaignants — La plainte a été déposée par trois*

*parlementaires; mais le demandeur a obtenu le consentement d'un seul de ces parlementaires avant d'introduire la présente demande — Selon la défenderesse, le demandeur devait obtenir le consentement des trois parlementaires — L'alinéa 15a) prévoit que le demandeur doive obtenir le consentement de chacun des plaignants — En l'espèce, il était loisible au demandeur de considérer le même texte signé par trois individus distincts comme trois plaintes distinctes — L'obtention du consentement d'un seul de ces individus répondait à cette condition de l'alinéa 15a) — Concernant le consentement des utilisateurs, bien qu'elles puissent se fier à des tiers pour obtenir le consentement, les organisations doivent prendre des mesures raisonnables pour s'assurer que ce consentement est valable — Selon le demandeur, le processus d'autorisations de partage de données granulaires de la défenderesse ne répondait pas aux critères du consentement valable — Étant donné la preuve limitée, la Cour a été réduite, à partir des photos de diverses politiques et ressources de Facebook, à faire des hypothèses et à tirer des inférences dénuées de fondement, notamment, sur ce que les utilisateurs liraient ou non — Le demandeur n'est donc pas parvenu à s'acquitter de la charge qui lui incombait de prouver que la défenderesse a enfreint la Loi pour avoir omis d'obtenir des consentements valables — En ce qui concerne les obligations en matière de sécurité des renseignements des utilisateurs, ces obligations de sécurité prennent fin une fois que les renseignements sont communiqués à des applications tierces — Même si les obligations en matière de sécurité s'appliquaient à la défenderesse après qu'elle ait communiqué des renseignements à des tiers, la preuve était trop mince pour pouvoir conclure que les accords contractuels de Facebook et les mesures prises pour encourager le respect de ses politiques constituaient des mesures de sécurité adéquates —Demande rejetée.*

Il s'agissait d'une demande présentée par le demandeur en vertu de l'alinéa 15a) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (la Loi). Le demandeur a allégué que la défenderesse (la défenderesse ou Facebook) a enfreint la Loi en partageant les renseignements personnels des utilisateurs de Facebook avec des applications tierces hébergées sur sa plateforme. Les allégations du demandeur ont fait suite à une plainte déposée en vertu de la Loi, après que des reportages ont révélé qu'une application tierce, « thisisyourdigitallife » (l'application TYDL), avait obtenu des données de la plateforme Facebook et les avait communiquées à une firme de recherche britannique du nom de Cambridge Analytica Ltd.

En 2007, Facebook a lancé sa « plateforme » Facebook — un ensemble de technologies qui permet à des tiers de développer des applications intégrées à Facebook exploitables depuis celle-ci que les utilisateurs de Facebook peuvent installer. Facebook fournit une interface de programmation d'applications, connue sous le nom d'« API Graph ». Cette dernière est un protocole de communication qui permet aux applications tierces de recevoir de l'information sur les utilisateurs et d'inscrire des informations au nom de ces derniers. Pendant la période visée — soit de novembre 2013 à décembre 2015 — il existait deux versions de l'API Graph, Graph v1 et Graph v2. Le processus de notification et de consentement de Facebook, qui s'appliquait durant la période visée, comportait trois niveaux : 1) les politiques applicables à l'ensemble de la plateforme; 2) les autorisations, les paramètres et les contrôles utilisateur; et 3) les ressources de formation. Facebook appliquait deux autres mesures de confidentialité : les contrôles contractuels et l'observation.

Le 19 mars 2018, le demandeur a reçu une plainte (la plainte) en vertu du paragraphe 11(1) de la Loi. Cette plainte soulevait des préoccupations au sujet de la conformité de Facebook à la Loi à la suite de reportages sur Cambridge Analytica qui aurait eu accès aux renseignements personnels des utilisateurs de Facebook à l'insu et sans le consentement de ces derniers. Le scandale de Cambridge Analytica a éclaté après qu'un développeur d'une application tierce a obtenu les renseignements personnels des utilisateurs de Facebook qui avaient installé son application grâce à l'accès à la plateforme Facebook et à l'API Graph. Les renseignements ont par la suite été communiqués, en contravention avec les politiques de Facebook, à des tiers. En novembre 2013, M. Aleksandr Kogan, professeur à l'Université de Cambridge, a lancé sur la plateforme Facebook l'application TYDL. Quelque 272 Canadiens utilisateurs de Facebook ont installé l'application TYDL et accordé les autorisations sollicitées. Ainsi, M. Kogan a pu avoir accès aux renseignements personnels des utilisateurs-installateurs et à ceux de leurs amis Facebook. En décembre 2015, des reportages médiatiques ont révélé que M. Kogan (et son entreprise, Global Science Research Ltd.) avait vendu des données sur des utilisateurs de Facebook à Cambridge Analytica et à une filiale,

SCL Elections Ltd. Après la parution de ces reportages, Facebook a retiré l'application TYDL de sa plateforme et a demandé à Cambridge Analytica de supprimer toutes les données qu'elle avait obtenues. Les parties ont convenu que M. Kogan et Global Science Research ont enfreint plusieurs dispositions de la Politique de la plateforme Facebook. En décembre 2015, M. Kogan a envoyé à Facebook un document censé être la politique de confidentialité de l'application TYDL. Cette politique renfermait des conditions qui enfreignaient la Politique de la plateforme Facebook et les Conditions de service. Au terme de son enquête, le 25 avril 2019, le demandeur a publié son rapport de conclusions et a jugé que Facebook avait enfreint la Loi. Le 6 février 2020, le demandeur a déposé un avis de demande pour introduire l'instance.

Il s'agissait de savoir si la demande était inappropriée du fait que le demandeur a omis d'obtenir le consentement de chacun des plaignants; si Facebook a omis d'obtenir le consentement valable des utilisateurs et des amis Facebook des utilisateurs lorsqu'elle a partagé leurs renseignements personnels avec des applications tierces; et si Facebook a omis de protéger suffisamment les renseignements concernant ses utilisateurs.

*Jugement* : la demande doit être rejetée.

En ce qui concerne la question de savoir si la demande du demandeur était inappropriée, la défenderesse a soulevé à titre préliminaire une question d'ordre procédural, et a soutenu que la demande était frappée de « nullité » du fait que le demandeur a omis d'obtenir le consentement de tous les plaignants. La plainte a été déposée par trois parlementaires, mais le demandeur a obtenu le consentement d'un seul de ces parlementaires avant d'introduire la présente demande. Selon la défenderesse, le demandeur devait obtenir le consentement des trois parlementaires. L'alinéa 15a) de la Loi prévoit que le demandeur peut intenter un recours devant la Cour avec le consentement du plaignant. En l'espèce, il était loisible au demandeur de considérer le même texte signé par trois individus distincts comme trois plaintes distinctes. Ainsi, l'obtention du consentement d'un seul de ces individus répondait à cette condition de l'alinéa 15a).

En ce qui concerne la question de savoir si la défenderesse a omis d'obtenir le consentement valable des utilisateurs et des amis Facebook des utilisateurs lorsqu'elle a partagé leurs renseignements personnels avec des applications tierces, les principes du consentement valable, énoncés à titre de troisième principe prévu à l'article 4.3 de l'annexe 1 de la Loi, ont été examinés. Selon l'article 4.3.2 de l'annexe 1, il faut informer la personne au sujet de laquelle on recueille des renseignements et obtenir son consentement. Cet article prévoit en outre que la norme applicable au consentement valable est l'« effort raisonnable » déployé par l'organisation pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés et que cette information doit être énoncée de façon que la personne puisse la « comprendre raisonnablement ». Le litige tirait son origine de la qualification de ces faits en l'espèce. La question qui devait être résolue consistait à déterminer si la défenderesse a déployé des efforts raisonnables pour s'assurer que les utilisateurs de Facebook et les amis Facebook de ces utilisateurs avaient été informés des fins pour lesquelles les renseignements les concernant seraient utilisés par les applications tierces. Le demandeur a avancé que la défenderesse n'a pas obtenu le consentement valable de ses utilisateurs avant de communiquer les renseignements les concernant à l'application TYDL; il a soutenu que la défenderesse s'est fiée aux développeurs de l'application pour obtenir le consentement de tiers et que le consentement en soi n'était pas valable au sens de la Loi. Bien qu'elles puissent se fier à des tiers pour obtenir le consentement, les organisations doivent prendre des mesures raisonnables pour s'assurer que ce consentement est valable. Selon le demandeur, le processus d'autorisations de partage de données granulaires (GDP)[1] de la défenderesse ne répondait pas aux critères du consentement valable. Pour ce qui est précisément de l'application TYDL, le demandeur a soutenu que la défenderesse n'a présenté aucune preuve de l'information que recevaient ses utilisateurs lors de l'installation de l'application TYDL. En gros, les mesures de protection de la vie privée de la défenderesse étaient, selon le demandeur, obscures, truffées d'ambiguïtés intentionnelles. La Cour disposait de bien peu de preuve, à part les photos des pages

[1] Ce processus obligeait les développeurs à 1) présenter un écran d'installation dressant la liste des catégories de renseignements que leur application recevrait; et 2) fournir un lien vers leur politique de confidentialité.

Web pertinentes tirées de l'affidavit déposé en faveur de la défenderesse. En l'absence de preuve, le demandeur, dans ses observations, a invité à de multiples reprises la Cour à tirer des « inférences », dont la plupart étaient dénuées de fondement en droit ou au vu du dossier. La Cour a été ainsi réduite, à partir des photos de diverses politiques et ressources de Facebook, à faire des hypothèses et à tirer des inférences dénuées de fondement, notamment, sur ce que les utilisateurs liraient ou non. Le demandeur n'est donc pas parvenu à s'acquitter de la charge qui lui incombait de prouver que la défenderesse a enfreint la Loi pour avoir omis d'obtenir des consentements valables.

En ce qui concerne la question de savoir si la défenderesse a omis de protéger suffisamment les renseignements concernant ses utilisateurs, la défenderesse a soutenu que, une fois que l'utilisateur a autorisé la défenderesse à communiquer des renseignements à une application, l'obligation de la défenderesse concernant les mesures de sécurité selon la Loi prend fin. L'article 4.7 de l'annexe 1 de la Loi définit le septième principe, applicable aux mesures de sécurité. Il prévoit que « [l]es renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité ». De l'avis de la défenderesse, la Loi ne l'oblige pas à s'assurer que l'utilisation ultérieure des renseignements en question par l'application est légale. La défenderesse avait raison de soutenir que ses obligations de sécurité prennent fin une fois que les renseignements sont communiqués aux applications tierces. Cela ressortait également clairement du contexte donné par d'autres dispositions de la Loi, notamment par l'article 4.1 qui expose le principe de la responsabilité. Même si les obligations en matière de sécurité s'appliquaient à la défenderesse après qu'elle ait communiqué des renseignements à des tiers, la preuve était trop mince pour pouvoir conclure que les accords contractuels et les mesures prises pour encourager le respect de ses politiques constituaient des mesures de sécurité adéquates.

LOIS ET RÈGLEMENTS CITÉS

*Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5, art. 3, 5(1), 6.1, 7.2, 11, 12, 12.1, 13, 15(a), 16, ann. 1, art. 4.1, 4.1.3, 4.3, 4.3.2, 4.3.4, 4.7, 4.7.1, 4.7.3.

*Loi d'interprétation*, L.R.C. (1985), ch. I-21, art. 33(2).

JURISPRUDENCE CITÉE

DÉCISIONS APPLIQUÉES :

*Englander c. Telus Communications Inc.* , 2004 CAF 387, [2005] 2 R.C.F. 572.

DÉCISIONS MENTIONNÉES :

*Kniss c. Canada (Commissaire à la protection de la vie privée)*, 2013 CF 31; *Alberta (Information and Privacy Commissioner) c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401*, 2013 CSC 62, [2013] 3 R.C.S. 733; *Nammo c. TransUnion of Canada Inc.*, 2010 CF 1284, [2012] 3 R.C.F. 600; *Bertucci c. Banque royale du Canada*, 2016 CF 332; *Renvoi relatif au paragraphe 18.3(1) de la Loi sur les Cours fédérales*, 2021 CF 723, [2021] 3 R.C.F. 503; *Lavigne c. Canada (Commissariat aux langues officielles)*, 2002 CSC 53, [2002] 2 R.C.S. 773; *Bhasin c. Hrynew*, 2014 CSC 71, [2014] 3 R.C.S. 494; *Canadian Superior Oil c. Hambly*, [1970] R.C.S. 932; *Lévis (Ville) c. Tétreault; Lévis (Ville) c. 2629-4470 Québec inc*, 2006 CSC 12, [2006] 1 R.C.S. 420.

DEMANDE en vertu de l'alinéa 15a) de la *Loi sur la protection des renseignements personnels et les documents électroniques* (la Loi) alléguant que la défenderesse a enfreint la Loi en partageant les renseignements personnels des utilisateurs de Facebook avec des applications tierces hébergées sur sa plateforme. Demande rejetée.

ONT COMPARU :

*Brendan Van Niejenhuis, Andrea Gonsalves, Justin Safayeni, Arb.B, Louisa Garib* et *Lucia Shatat* pour le demandeur.

*Michael A. Feder, C.R., Gillian P. Kerr, Daniel G.C. Glover, Connor Bildfell et Barry B. Sookman* pour la défenderesse.

AVOCATS INSCRITS AU DOSSIER

*Stockwoods LLP*, Toronto, et *Commissariat à la protection de la vie privée du Canada*, Gatineau, pour le demandeur.

*McCarthy Tétrault S.E.N.C.R.L., s.r.l.*, Vancouver, pour la défenderesse.

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

LE JUGE MANSON :

## I. Introduction

[1] La Cour est saisie d'une demande présentée par le commissaire à la protection de la vie privée (le commissaire) en vertu de l'alinéa 15a) de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5 (la LPRPDE). Le commissaire allègue que Facebook a enfreint la LPRPDE en partageant les renseignements personnels des utilisateurs de Facebook avec des applications tierces hébergées sur sa plateforme.

[2] Les allégations du commissaire font suite à une plainte déposée en vertu de la LPRPDE, après que des reportages ont révélé qu'une application tierce, « thisisyourdigitallife » (l'application TYDL), avait obtenu des données de la plateforme Facebook et les avait communiquées à une firme de recherche britannique du nom de Cambridge Analytica Ltd. (Cambridge Analytica).

## II. Contexte

### A. *Parties*

[3] Le commissaire dirige le Commissariat à la protection de la vie privée (le Commissariat). Le mandat du commissaire est de protéger les droits des Canadiens à la vie privée. La LPRPDE confère au commissaire compétence sur les organisations du secteur privé et établit les règles régissant la collecte, l'utilisation et la communication de renseignements personnels concernant les Canadiens. Le commissaire est en outre chargé de faire enquête sur les plaintes déposées par toute personne qui estime qu'une organisation contrevient à des dispositions précises de la LPRPDE (voir l'article 11 de la LPRPDE). Au dépôt de la plainte, le commissaire doit, sauf exception, faire enquête sur la plainte et dresser un rapport exposant ses conclusions (aux articles 12 et 13 de la LPRPDE).

[4] Facebook est une plateforme électronique de média social qui permet aux utilisateurs de partager de l'information. Les gens se joignent à Facebook et l'utilisent

pour demeurer en contact notamment avec des amis et des membres de leur famille, pour apprendre ce qui se passe dans le monde ainsi que pour partager et exprimer leurs opinions sur les sujets qui les intéressent.

[5] Toute personne âgée de 13 ans et plus peut s'ouvrir un compte sur Facebook et devenir utilisateur : 1) en se rendant sur le site Web de Facebook ou en téléchargeant son application mobile; 2) en inscrivant son nom, son adresse électronique ou son numéro de téléphone portable; 3) en cliquant sur le bouton « s'inscrire » et en acceptant les politiques de Facebook. Les utilisateurs peuvent avoir accès à Facebook au moyen d'un ordinateur, d'un téléphone intelligent ou autre appareil.

[6] Après s'être inscrit, l'utilisateur peut créer des liens avec d'autres utilisateurs en les ajoutant comme « amis ». Pour ce faire, il envoie une « invitation » à ces derniers et ceux-ci acceptent l'invitation. Une fois rendus amis Facebook, les utilisateurs peuvent plus facilement voir leurs activités Facebook, y participer et partager entre eux de l'information. Les utilisateurs de Facebook peuvent partager de l'information de divers moyens, notamment en affichant des photos et des messages, en communiquant leur approbation ou leur intérêt dans une publication d'un autre utilisateur de Facebook, en y affichant leurs commentaires ou en cliquant sur l'icône « J'aime ».

[7] Facebook est le plus grand média social au monde : il comptait plus de 500 millions d'utilisateurs actifs en 2010, plus de 1,4 milliard en 2014, et plus de 2,8 milliards en 2021.

[8] Facebook recueille des renseignements personnels sur ses utilisateurs, dont des millions de Canadiens. Grâce au grand nombre d'utilisateurs et à l'accès à l'information que ceux-ci partagent sur sa plateforme, Facebook peut offrir à des tiers des « publics personnalisés » pour leur publicité.

B. *Plateforme Facebook et applications tierces*

[9] En 2007, Facebook a lancé sa « plateforme » Facebook — un ensemble de technologies qui permet à des tiers de développer des applications intégrées à Facebook exploitables depuis celle-ci que les utilisateurs de Facebook peuvent installer. De telles applications offrent aux utilisateurs une expérience personnalisée d'activités sociales et de divertissements. Elles permettent, par exemple, aux utilisateurs de jouer à des jeux, de partager des photos et d'écouter de la musique.

[10] Facebook fournit une interface de programmation d'applications, connue sous le nom d'« API Graph ». Cette dernière est un protocole de communication qui permet aux applications tierces de recevoir de l'information sur les utilisateurs et d'inscrire des informations au nom de ces derniers.

[11] Pendant la période visée — soit de novembre 2013 à décembre 2015 — il existait deux versions de l'API Graph. Avec Graph v1, les développeurs d'applications pouvaient demander aux utilisateurs-installateurs l'autorisation d'accéder 1) aux renseignements sur les utilisateurs-installateurs eux-mêmes et 2) aux renseignements sur les amis des utilisateurs-installateurs. Graph v2, lancée en avril 2014, donnait aux applications existantes un délai d'un an, jusqu'en mai 2015, pour migrer à Graph v1. Pour ce qui est des applications qui utilisaient Graph v2, les développeurs ne pouvaient plus, sauf exception, demander l'accès aux renseignements concernant les amis des

utilisateurs-installateurs. Facebook a aussi lancé un nouveau programme appelé « App Review » pour obliger les développeurs d'applications qui souhaitent accéder à toute autre information concernant les utilisateurs, outre les renseignements de base, à expliquer de quelle façon l'information additionnelle serait utilisée pour améliorer l'expérience qu'ont les utilisateurs des applications en question.

C. *Processus de notification et de consentement de Facebook*

[12] Le processus de notification et de consentement de Facebook, qui s'appliquait durant la période visée, comportait trois niveaux : 1) les politiques applicables à l'ensemble de la plateforme; 2) les autorisations, les paramètres et les contrôles utilisateur; et 3) les ressources de formation.

1) Politiques

[13] Facebook a maintenu deux politiques axées sur les utilisateurs : la Politique de confidentialité (autrefois connue sous le nom de Politique d'utilisation des données) et les Conditions de service (autrefois connues sous le nom de Déclaration des droits et responsabilités). Pour s'inscrire, les nouveaux utilisateurs devaient accepter les Conditions de service, lesquelles incorporaient par renvoi la Politique de confidentialité. Par ailleurs, les utilisateurs ont été informés qu'en cliquant sur le bouton « s'inscrire », ils seraient réputés avoir lu la Politique d'utilisation des données. Ces deux politiques étaient accessibles depuis des hyperliens situés juste au-dessus du bouton « s'inscrire ».

[14] Au moment du lancement de l'application TYDL, sur Facebook, c'était la Politique d'utilisation des données de Facebook du 11 décembre 2012 qui s'appliquait. Cette politique expliquait de quelle façon les données étaient partagées sur Facebook et, notamment :

1. Contenait la définition du terme « informations publiques » et exposait les conséquences pour les utilisateurs qui décident de rendre des informations publiques. Les informations publiques sont les informations que [TRADUCTION] « vous avez choisi de rendre publiques, ainsi que les informations qui sont toujours accessibles au public »;

2. Prévoyait que la décision de rendre des informations publiques signifie que ces informations [TRADUCTION] « seront accessibles à quiconque utilise les API de Facebook, notamment l'API Graph »;

3. Prévoyait que les informations qui sont toujours publiques incluent le nom des utilisateurs, leur profil, leur photo de couverture, leurs amis, leurs réseaux, leur sexe, leur nom d'utilisateur et leur identifiant;

4. Présentait les autorisations et contrôles utilisateur de Facebook pour gérer le partage des données concernant les utilisateurs;

5. Exposait les informations qui sont partagées avec les applications tierces et les moyens dont disposent les utilisateurs pour déterminer les informations qu'ils souhaitent partager;

6. Exposait les informations concernant les utilisateurs qui sont partagées lorsque leurs amis Facebook utilisent des applications tierces et la mesure dans laquelle les utilisateurs pouvaient gérer le partage des informations les concernant avec les applications tierces que leurs amis utilisent.

[15] Ce sont les Conditions de service de Facebook du 11 décembre 2012 qui s'appliquaient au moment du lancement de l'application TYDL, en novembre 2013. Les Conditions de service présentent les droits et responsabilités des utilisateurs, notamment pour ce qui est du partage des informations les concernant. Elles incorporaient par renvoi la Politique de confidentialité et informaient les utilisateurs que [TRADUCTION] : « [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 »; [TRADUCTION] « 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 »; [TRADUCTION] « vous pouvez supprimer votre compte et désactiver les applications en tout temps ».

[16] Les Conditions de service et la Politique de confidentialité appliquées durant la période visée sont restées pratiquement inchangées.

2) Contrôles utilisateur

[17] Facebook offrait aux utilisateurs la possibilité de gérer les paramètres et les contrôles pour déterminer les informations partagées avec les applications tierces.

[18] En 2010, Facebook a introduit le processus d'autorisations de partage de données granulaires sur sa plateforme (le processus GDP). Ce processus comporte trois particularités : 1) l'utilisateur-installateur reçoit un avis l'informant du genre d'informations auxquelles une application souhaite avoir accès; 2) l'utilisateur reçoit un lien pour accéder à la politique de confidentialité qui régit l'application; et 3) l'utilisateur a la possibilité d'accorder ou de refuser les autorisations demandées. L'utilisateur doit accorder l'autorisation avant que l'application puisse avoir accès aux informations. Ces étapes se reproduisent à chaque installation d'application par l'utilisateur.

[19] Pour évaluer la politique de confidentialité des applications, Facebook reconnaît avoir vérifié seulement que l'hyperlien fourni par le développeur donne effectivement accès à une page Web fonctionnelle. Facebook ne vérifiait pas le contenu réel des politiques de confidentialité.

[20] En 2014, Facebook a lancé une quatrième version du processus GDP : « GDP v4 ». Cette version offrait aux utilisateurs la possibilité d'accorder aux applications l'autorisation d'accéder à des catégories précises de données, une catégorie à la fois. Dans cette version, les applications n'avaient accès qu'aux renseignements publics de base concernant les utilisateurs-installateurs à moins de recevoir de la part de ces derniers l'autorisation d'avoir accès à plus d'informations.

[21] Facebook a aussi fourni aux utilisateurs une page de « paramètres Applications » qui leur permettaient de visualiser toutes les applications qu'ils utilisent, de supprimer les applications qu'ils ne souhaitent plus utiliser ou de désactiver toutes

les applications basées sur la plateforme pour empêcher complètement les applications d'accéder à des informations non publiques.

[22] Après le lancement initial du processus GDP, en 2010, Facebook a mis à jour sa page paramètres Applications. Grâce à cette mise à jour, les utilisateurs pouvaient voir les autorisations actuelles de chaque application et permettaient aux utilisateurs de supprimer certaines autorisations. Certaines autorisations « devaient » être accordées à des applications précises. Pour éviter le partage des informations visées, les utilisateurs pouvaient soit refuser d'installer l'application soit retirer leur consentement en supprimant l'application installée antérieurement.

[23] La page à jour des paramètres Applications incluait un paramètre de réglage « Informations accessibles par l'intermédiaire de vos amis » (plus tard appelée « Applications utilisées par d'autres ») qui permettait aux utilisateurs de restreindre les catégories d'informations accessibles aux applications installées par leurs amis. Sous ce paramètre, les utilisateurs pouvaient lire [TRADUCTION] « les utilisateurs de Facebook qui peuvent voir vos informations peuvent les partager s'ils utilisent des applications ». Lorsque Graph v2 a été lancé, en 2014, et que l'accès aux amis des utilisateurs-installateurs a été largement restreint, ce paramètre de réglage a été supprimé.

[24] Les utilisateurs de Facebook avaient aussi accès à d'autres paramètres de réglage :

1. Page « Paramètres de confidentialité ». Cette page permettait aux utilisateurs de limiter l'accès à leurs publications à un groupe précis et informait les utilisateurs que [TRADUCTION] « les personnes qui ont accès à vos informations peuvent les partager avec d'autres, notamment des applications ».

2. Désactivation de la plateforme. D'autres autorisations, paramètres et contrôles permettaient aux utilisateurs d'empêcher les applications d'avoir accès à des catégories précises d'informations les concernant, à part les informations publiques de leur profil. La désactivation permettait donc aux utilisateurs d'empêcher tout accès des applications à toutes les informations, y compris les informations publiques.

3. Suppression du compte. Les utilisateurs pouvaient supprimer leur compte Facebook et demander aux applications concernées de supprimer les informations les concernant.

3) Ressources de formation

[25] Facebook a fourni des ressources de formation à ses utilisateurs. Les ressources en question qui étaient disponibles durant la période visée étaient, entre autres :

1. Les pages d'aide. Facebook fournissait des ressources de formation sur divers sujets, notamment une ressource sur la confidentialité intitulée [TRADUCTION] « Contrôle de ce qui est communiqué lorsque des personnes qui ont accès à vos informations utilisent des applications », [TRADUCTION] « À propos de la plateforme Facebook », [TRADUCTION] « Vous pouvez gérer les informations que vos amis peuvent voir et partager dans les applications et les jeux à partir de

vos paramètres Applications », ainsi que d'autres pages sur la plateforme et les applications tierces.

2. Une visite virtuelle sur la confidentialité. Les nouveaux utilisateurs peuvent [TRADUCTION] « faire une visite virtuelle sur la confidentialité » pour se renseigner sur certains aspects de la confidentialité.

3. Les raccourcis de confidentialité. Lancé en 2012, le bouton « Raccourcis de confidentialité », était situé à côté du bouton « Accueil » sur la barre de titre de Facebook. En cliquant sur le bouton, l'utilisateur pouvait voir les trois raccourcis suivants : [TRADUCTION] « Qui peut voir mes publications? », [TRADUCTION] « Qui peut me contacter? », et [TRADUCTION] « Comment empêcher une personne de me déranger? » ainsi qu'un lien [TRADUCTION] « Voir tous les paramètres ».

4. Une vérification de la confidentialité. La vérification de la confidentialité, lancée en 2014, est un outil qui permet aux utilisateurs de passer en revue certains paramètres de confidentialité, la portée du partage de leurs informations et les applications auxquelles ils ont donné des autorisations d'accès.

5. Les « Privacy Basics ». Lancés en 2014, les Privacy Basics (ou l'ABC de la confidentialité) sont une interface modulaire qui répond aux questions fréquemment posées sur les moyens dont disposent les utilisateurs pour gérer les informations les concernant.

D. *Autres mesures prises par Facebook pour protéger la vie privée*

[26] Facebook appliquait deux autres mesures de confidentialité : 1) les contrôles contractuels et 2) l'observation.

[27] Facebook obligeait les développeurs d'applications à accepter la Politique de la plateforme Facebook et les Conditions de service avant qu'ils puissent lancer leurs applications sur sa plateforme.

[28] La Politique de la plateforme Facebook imposait aux développeurs d'applications des obligations contractuelles à l'égard des caractéristiques, de la fonctionnalité, de la collecte d'informations et de l'utilisation des applications sur la plateforme. Elle précisait par ailleurs que Facebook se réservait le droit de prendre des mesures coercitives. La Politique de la plateforme du 12 décembre 2012, applicable durant la période visée, prévoyait notamment :

[TRADUCTION]

1. Vous ne demanderez que les données nécessaires à l'exploitation de votre application.

2. Vous mettrez en place une politique de confidentialité indiquant aux utilisateurs lesquelles de leurs données vous utiliserez, ainsi que la façon dont vous utiliserez, afficherez, communiquerez ou transférerez ces données.

3. Les données des amis d'un utilisateur ne peuvent être utilisées que dans le contexte de l'expérience de l'utilisateur dans votre application.

4. S’agissant des données autres que les renseignements de base concernant un utilisateur, vous devez avoir le consentement explicite de l’utilisateur auprès duquel Facebook a recueilli ces données, avant d’utiliser ces données à toute fin autre que de les présenter à l’utilisateur sur votre application.

5. Vous ne pourrez ni vendre ni acheter de données que quiconque aura obtenues auprès de Facebook.

[29] Les Conditions de service de Facebook du 11 décembre 2012 renfermaient des dispositions similaires sous la rubrique : [TRADUCTION] « Clauses spéciales applicables aux développeurs et exploitants d’applications et de sites Web ».

[30] Facebook dispose d’équipes d’employés chargés de détecter les violations des politiques de Facebook, de faire enquête sur celles-ci et de lutter contre elles. Les mécanismes que Facebook utilise consistent en un mélange de mesures automatisées et de mesures manuelles. Facebook utilise une « grille d’évaluation » pour guider ses pratiques d’observation. Les violations touchant les données de catégorie protégée font l’objet des mesures les plus sévères.

[31] Selon le dossier, Facebook a pris environ 6 millions de mesures coercitives entre le 1er août 2012 et le 13 juillet 2018, 38 869, en 2020, et 167 224, en 2021.

[32] Quoi qu’il en soit, la preuve n’indique pas clairement les raisons précises pour lesquelles des mesures coercitives ont été prises et, on peut donc difficilement déterminer la mesure dans laquelle Facebook a pris des mesures coercitives pour sévir contre la violation de ses politiques de confidentialité ou pour protéger les données concernant les utilisateurs.

[33] En outre, comme il a été mentionné plus haut, Facebook admet ne pas être en mesure, dans le cadre des initiatives prises pour voir au respect des politiques de sa plateforme, d’examiner le contenu des politiques de confidentialité que les développeurs d’applications présentent aux utilisateurs durant les étapes du processus GDP.

E. *Plainte déposée en vertu de la LPRPDE et enquête du commissaire*

[34] Le 19 mars 2018, le Commissariat a reçu une plainte (la plainte) en vertu du paragraphe 11(1) de la LPRPDE. Cette plainte soulevait des préoccupations au sujet de la conformité de Facebook à la LPRPDE à la suite de reportages sur une société d’experts-conseils britannique, Cambridge Analytica, qui aurait eu accès aux renseignements personnels des utilisateurs de Facebook à l’insu et sans le consentement de ces derniers. Le plaignant demandait au Commissariat [TRADUCTION] « de se pencher de façon générale sur la conformité de Facebook à la LPRPDE afin de s’assurer que les renseignements des utilisateurs canadiens de Facebook ne sont pas compromis et que Facebook prend des mesures adéquates pour protéger, à l’avenir, les données privées des Canadiens ».

[35] Le scandale de Cambridge Analytica a éclaté après qu’un développeur d’une application tierce a obtenu les renseignements personnels des utilisateurs de Facebook qui avaient installé son application grâce à l’accès à la plateforme Facebook et à l’API Graph. Les renseignements ont par la suite été communiqués, en contravention avec

les politiques de Facebook, à des tiers qui ont mis au point des modèles psychographiques dans le but de diriger des messages politiques vers des segments précis de la base d'utilisateurs de Facebook.

[36] En novembre 2013, M. Aleksandr Kogan, professeur à l'Université de Cambridge, a lancé sur la plateforme Facebook l'application TYDL. Cette application se présentait sous forme de test de personnalité. Avant le lancement de l'application TYDL, M. Kogan avait accepté la Politique de la plateforme Facebook et les Conditions de service. Grâce à cette plateforme, M. Kogan pouvait accéder aux renseignements du profil de chacun des utilisateurs qui avaient installé son application et accepté sa politique de confidentialité, incluant les renseignements sur les amis Facebook des utilisateurs-installateurs.

[37] Quelque 272 Canadiens utilisateurs de Facebook ont installé l'application TYDL et accordé les autorisations sollicitées. Ainsi, M. Kogan a pu avoir accès aux renseignements personnels des utilisateurs-installateurs et à ceux de leurs amis Facebook. Facebook estime que les 272 installations auraient permis la communication de données concernant plus de 600 000 Canadiens.

[38] En décembre 2015, des reportages médiatiques ont révélé que M. Kogan (et son entreprise, Global Science Research Ltd.) avait vendu des données sur des utilisateurs de Facebook à Cambridge Analytica et à une filiale, SCL Elections Ltd. Selon ces reportages, les données des utilisateurs de Facebook avaient servi pour aider les clients de SCL à diriger les messages politiques de leur client vers des électeurs éventuels aux élections primaires des candidats potentiels à la présidence des États-Unis, qui allaient avoir lieu peu de temps après.

[39] Après la parution de ces reportages, Facebook a retiré l'application TYDL de sa plateforme et a demandé à Cambridge Analytica de supprimer toutes les données qu'elle avait obtenues. Facebook n'a pas avisé les utilisateurs touchés et n'a pas expulsé M. Kogan, Cambridge Analytica ou SCL de sa plateforme.

[40] Les parties conviennent que M. Kogan et Global Science Research ont enfreint plusieurs dispositions de la Politique de la plateforme Facebook :

1. Les données des amis Facebook n'ont pas été utilisées uniquement pour améliorer l'expérience de l'application TYDL des utilisateurs-installateurs.

2. Les données des utilisateurs obtenues de Facebook ont été vendues.

3. Les données des utilisateurs ont été communiquées à une tierce partie.

4. L'application TYDL exigeait des autorisations pour accéder aux données des utilisateurs dont elle n'avait pas besoin pour fonctionner.

[41] En décembre 2015, M. Kogan a envoyé à Facebook un document censé être la politique de confidentialité de l'application TYDL. Cette politique renfermait des conditions qui enfreignent la Politique de la plateforme Facebook et les Conditions de service, notamment :

[TRADUCTION]

> 3. Objet de l'application. Nous utilisons cette application dans le cadre de recherches effectuées pour déterminer en quoi les données des utilisateurs de Facebook peuvent prédire diverses facettes de leur vie. Votre contribution et vos données nous aideront à mieux comprendre le lien entre la psychologie humaine et le comportement en ligne.
>
> […]
>
> 6. Renseignements recueillis. Nous recueillons les renseignements que vous aurez choisi de partager avec nous en utilisant cette application, ce qui peut inclure les noms, les données démographiques, les mises à jour de profil, les mentions « J'aime » qui paraissent sur votre journal et dans votre réseau.
>
> 7. Propriété intellectuelle. Si vous cliquez sur « OK », utilisez autrement l'application ou acceptez un paiement, vous permettez à GSR de […] transférer […], de vendre ou de céder (peu importe le moyen et les conditions) […] votre contribution et vos données. L'acceptation de ces conditions signifie que vous […] accordez à GSR une licence mondiale irrévocable, cessible, non exclusive, transférable et pouvant donner lieu à l'octroi de sous-licences pour utiliser vos données […].

[42] Il demeure incertain que cette politique ait été présentée aux utilisateurs qui ont installé l'application ou que d'autres versions aient été utilisées au fil du temps. Comme je l'ai mentionné plus haut, Facebook ne vérifiait pas le contenu des politiques de tiers.

[43] L'application TYDL a été lancée avec Graph v1 et est demeurée sur la plateforme pendant la transition à Graph v2. Après que Facebook a annoncé le passage à Graph v2, en avril 2014, M. Kogan a demandé le maintien des autorisations d'accès aux données selon le programme « App Review » de Facebook. Facebook a rejeté cette demande, car les données communiquées n'auraient pas servi à améliorer l'expérience des utilisateurs dans l'application.

[44] Au terme de son enquête, le 25 avril 2019, le commissaire a publié son rapport de conclusions et a jugé que Facebook avait enfreint la LPRPDE. Le 6 février 2020, le commissaire a déposé un avis de demande pour introduire la présente instance.

### F. *Enquête du commissaire de 2008–2009 sur Facebook et les applications tierces*

[45] De 2008 à 2009, le Commissariat a mené enquête précisément sur les pratiques de Facebook concernant la communication de renseignements personnels de ses utilisateurs aux applications tierces. Cette enquête se concentrait sur des questions semblables à celles en l'espèce. Au terme de son enquête, le commissaire a rendu un rapport qui exposait les recommandations suivantes :

1. limiter l'accès des développeurs d'applications aux renseignements des utilisateurs qui ne sont pas nécessaires au fonctionnement de l'application;

2. informer les utilisateurs des renseignements spécifiques qu'une application requiert et des fins y afférentes;

3. dans chaque cas, obtenir le consentement des utilisateurs à ce que les développeurs aient accès aux renseignements spécifiques;

4. interdire toute communication de renseignements personnels des utilisateurs qui n'ajoutent pas eux-mêmes une application (amis Facebook).

[46] En août 2009, le Commissariat a par écrit informé Facebook qu'il avait abandonné la recommandation nº 4 après « que Facebook m'a convaincu […] que de nombreuses applications sont conçues à des fins sociales et interactives ». Il mentionnait par ailleurs que, vu la mise en œuvre proposée du processus GDP par Facebook, il [TRADUCTION] « considérait que [s]es préoccupations générales relatives aux applications et aux données des amis ont été prises en compte de façon satisfaisante ».

[47] Le 21 septembre 2010, le commissaire alors en fonction a fait parvenir à Facebook une lettre finale de suivi au sujet de Facebook et des applications tierces :

> [TRADUCTION]C'est avec plaisir que je constate la réorganisation de la plateforme qui accueille des applications tierces pour améliorer le respect de la vie privée grâce à la mise en place du modèle d'autorisations. Lors de notre enquête, nous avions conclu que les applications tierces pouvaient avoir accès aux renseignements concernant les utilisateurs, sans consentement valable et sans mesure de protection appropriée. Le nouveau modèle d'autorisations oblige les applications à informer les utilisateurs des catégories de renseignements dont elles ont besoin pour fonctionner, à fournir un lien vers les politiques de confidentialité des développeurs et à obtenir le consentement exprès des utilisateurs pour accéder aux renseignements. Facebook a mis en œuvre les moyens techniques pour empêcher les applications tierces d'accéder à l'information sans consentement et dispose maintenant des mécanismes de surveillance voulus.
>
> Je suis convaincu que, grâce à la mise en œuvre du modèle d'autorisations, Facebook a honoré ses engagements envers le Commissariat. Quoi qu'il en soit, nous avons décelé, pendant la mise à l'essai de la nouvelle plateforme qui accueille les applications, certains risques pour ce qui est de la surveillance des applications et des instructions que Facebook donne aux développeurs. Nous serions reconnaissants à Facebook de prendre rapidement les mesures pour atténuer ces risques et j'encourage 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.

## III. Questions en litige

A. *La demande du commissaire est-elle inappropriée du fait qu'il a omis d'obtenir le consentement de chacun des plaignants?*

B. *Facebook a-t-elle omis d'obtenir le consentement valable des utilisateurs et des amis Facebook des utilisateurs lorsqu'elle a partagé leurs renseignements personnels avec des applications tierces?*

C. *Facebook a-t-elle omis de protéger suffisamment les renseignements concernant ses utilisateurs?*

D. *Si Facebook a enfreint la LPRPDE, est-elle protégée par le principe de la préclusion résultant d'une déclaration ou de l'erreur provoquée par une personne en autorité?*

E. *Quelle est la réparation appropriée?*

## IV. Analyse

[48] D'emblée, il me semble utile de noter les principes de base des audiences tenues sous le régime de l'alinéa 15a) de la LPRPDE.

[49] Les instances visées à l'alinéa 15a) de la LPRPDE sont des instances *de novo*. À la base, la question à trancher est de savoir si Facebook a enfreint la LPRPDE et, dans l'affirmative, de déterminer la réparation qui peut être accordée en vertu de l'article 16 de la LPRPDE. Il appartient au demandeur de prouver qu'il y a eu manquement à la LPRPDE (*Kniss c. Canada (Commissaire à la protection de la vie privée)*, 2013 CF 31, au paragraphe 28). En l'espèce, la charge de preuve revient au commissaire. Le rapport du commissaire peut certes être déposé en preuve, mais il ne fait l'objet d'aucune retenue judiciaire (*Englander c. Telus Communications Inc.*, 2004 CAF 387, [2005] 2 R.C.F. 572 (*Englander*), aux paragraphes 47–48).

[50] La partie 1 de la LPRPDE régit la protection des renseignements personnels dans le secteur privé. L'objet de cette partie, tel qu'énoncé à l'article 3 de la LPRPDE, est de mettre en équilibre la protection des renseignements concernant les utilisateurs, d'une part, et le droit des organisations de recueillir, d'utiliser et de communiquer des renseignements personnels, d'autre part :

> **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.

[51] La LPRPDE est considérée comme une loi quasi constitutionnelle, car la faculté d'une personne d'exercer un droit de regard sur les renseignements personnels la concernant est intimement liée à son autonomie, à sa dignité et à son droit à la vie privée (*Alberta (Information and Privacy Commissioner) c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401*, 2013 CSC 62, [2013] 3 R.C.S. 733, au paragraphe 19; *Nammo c. TransUnion of Canada Inc.*, 2010 CF 1284, [2012] 3 R.C.F. 600, au paragraphe 74; *Bertucci c. Banque royale du Canada*, 2016 CF 332, au paragraphe 34). Ce statut quasi constitutionnel est un indicateur à considérer dans l'interprétation de la LPRPDE, mais il n'a pas pour effet de modifier l'approche traditionnelle d'interprétation des lois (*Renvoi relatif au paragraphe 18.3(1) de la Loi sur les Cours fédérales*, 2021 CF 723, [2021] 3 R.C.F. 503, au paragraphe 39; *Lavigne c. Canada (Commissariat aux langues officielles)*, 2002 CSC 53, [2002] 2 R.C.S. 773, au paragraphe 25).

[52] Finalement, vu que la LPRPDE vise à mettre en équilibre deux intérêts concurrents, la Cour doit user de souplesse, de sens commun et de pragmatisme pour interpréter cette loi (*Englander*, au paragraphe 46).

A. *La demande du commissaire est-elle inappropriée du fait qu'il a omis d'obtenir le consentement de chacun des plaignants*?

[53] Facebook a soulevé à titre préliminaire une question d'ordre procédural, et a soutenu que la présente demande est frappée de « nullité » du fait que le commissaire a omis d'obtenir le consentement de tous les plaignants sous le régime de la LPRPDE.

[54] La plainte a été déposée par trois parlementaires, mais le commissaire a obtenu le consentement d'un seul de ces parlementaires avant d'introduire la présente demande. Selon Facebook, le commissaire devait obtenir le consentement des trois parlementaires.

[55] À l'appui de sa thèse, Facebook invoque le libellé de l'alinéa 15a) de la LPRPDE et l'application du paragraphe 33(2) de la *Loi d'interprétation*, L.R.C. (1985), ch. I-21. L'alinéa 15a) de la LPRPDE prévoit que le commissaire peut intenter un recours devant la Cour « avec le consentement du plaignant ». Le paragraphe 33(2) de la *Loi d'interprétation* dispose que « [l]e pluriel ou le singulier s'appliquent, le cas échéant, à l'unité et à la pluralité». À partir du mot « plaignant », à l'alinéa 15a), Facebook avance que le commissaire doit obtenir le consentement de chacun des plaignants.

[56] Je ne suis pas d'accord. En l'espèce, il était loisible au commissaire de considérer le même texte signé par trois individus distincts comme trois plaintes distinctes. Ainsi, l'obtention du consentement d'un seul de ces individus répond à cette condition de l'alinéa 15a).

B. *Facebook a-t-elle omis d'obtenir le consentement valable des utilisateurs et des amis Facebook des utilisateurs lorsqu'elle a partagé leurs renseignements personnels avec des applications tierces?*

[57] Les principes du consentement valable sont énoncés à titre de troisième principe prévu à l'article 4.3 de l'annexe 1 de la LPRPDE. Cette annexe est incorporée dans les dispositions essentielles de la LPRPDE par le paragraphe 5(1).

[58] Selon l'article 4.3.2 de l'annexe 1, il faut informer la personne au sujet de laquelle on recueille des renseignements et obtenir son consentement. Cet article prévoit en outre que la norme applicable au consentement valable est l'« effort raisonnable » déployé par l'organisation pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés et que cette information doit être énoncée de façon que la personne puisse la « comprendre raisonnablement ».

> **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.

[59] L'article 4.3.4 prévoit que « [l]a forme du consentement que l'organisation cherche à obtenir peut varier selon les circonstances et la nature des renseignements ».

[60] En 2015, l'article 6.1 a été ajouté à la LPRPDE de façon à codifier davantage ces principes :

> **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.

[61] Les dispositions applicables sur le consentement et la raisonnabilité des efforts des organisations pour obtenir un consentement valable ne sont guère contestées.

[62] Les faits essentiels ne sont guère contestés non plus. Les deux parties s'entendent dans l'ensemble sur les politiques et les ressources que Facebook avait mises en place durant la période visée, lorsque l'application TYDL était fonctionnelle sur la plateforme Facebook.

[63] Le litige tire son origine de la qualification de ces faits. La question que la Cour doit résoudre consiste à déterminer si Facebook a déployé des efforts raisonnables pour s'assurer que les utilisateurs de Facebook et les amis Facebook de ces utilisateurs avaient été informés des fins pour lesquelles les renseignements les concernant seraient utilisés par les applications tierces.

[64] Le commissaire avance que Facebook n'a pas obtenu le consentement valable de ses utilisateurs avant de communiquer les renseignements les concernant à l'application TYDL. Il soutient que Facebook s'est fiée aux développeurs de l'application pour obtenir le consentement de tiers et que ce consentement n'est pas valable au sens de la LPRPDE.

[65] Bien qu'elles puissent se fier à des tiers pour obtenir le consentement, les organisations doivent prendre des mesures raisonnables pour s'assurer que ce consentement est valable. Selon le commissaire, le processus GDP de Facebook, qui oblige les développeurs à 1) présenter un écran d'installation qui dresse la liste des catégories de renseignements que leur application recevrait; et 2) fournir un lien vers leur politique de confidentialité, ne répond pas aux critères du consentement valable. Bien que Facebook se soit assurée de l'existence des politiques de confidentialité et que sa Politique de la plateforme et ses Conditions de service obligeaient les applications tierces à dévoiler les fins pour lesquelles les renseignements étaient requis, elle ne vérifiait pas en réalité le contenu des politiques des tiers. Facebook a donc négligé de s'assurer que ses utilisateurs comprenaient raisonnablement les fins pour lesquelles leurs renseignements seraient utilisés et que, pour cette raison, leur consentement n'était pas valable.

[66] Pour ce qui est précisément de l'application TYDL, le commissaire soutient que Facebook n'a présenté aucune preuve de l'information que recevaient ses utilisateurs lors de l'installation de l'application TYDL. Facebook n'a produit que des captures d'écran d'autres applications pour donner une idée de la politique de confidentialité qui aurait pu avoir été présentée aux utilisateurs-installateurs. Vu l'incapacité de Facebook de fournir les captures d'écran précises de l'application TYDL, il est impossible de conclure que le consentement valable ait jamais été obtenu. Le commissaire prétend,

de toute façon, que les écrans qui auraient peut-être été présentés aux utilisateurs ne permettaient pas à ces derniers de savoir à quelles fins les renseignements les concernant seraient utilisés. La politique en question prévoit seulement que les renseignements seraient utilisés à des fins de recherche, et non pour dresser des profils psychographiques ou pour cibler des messages politiques.

[67] En gros, les mesures de protection de la vie privée de Facebook sont, selon le commissaire, obscures, truffées d'ambiguïtés intentionnelles pour créer une illusion de contrôle, de déclarations rassérénantes sur les engagements de Facebook à la confidentialité et d'images de cadenas et de dinosaures studieux susceptibles de donner un faux sens de sécurité aux utilisateurs qui consultent les politiques et les ressources de formation pertinentes. D'un côté, le commissaire critique les ressources de Facebook parce qu'elles sont trop complexes et utilisent trop de vocabulaire juridique, ce qui les rend inutiles pour assurer le consentement valable; de l'autre, il estime que, dans certains cas, les ressources sont démesurément simplistes et qu'elles taisent trop de choses.

[68] Facebook, quant à elle, soutient que la combinaison de ses politiques applicables à l'échelle du réseau, des contrôles utilisateur et des ressources de formation constitue un effort raisonnable au sens de la LPRPDE. Facebook et le souscripteur de l'affidavit de la défenderesse sont d'avis que les politiques sont rédigées en langue simple, sont faciles à comprendre et représentent un avancement au sein de l'industrie. Facebook estime que la suggestion du commissaire voulant qu'elle vérifie concrètement la politique de confidentialité de chacune des applications est peu pratique, voire irréalisable, car elle nécessiterait un personnel juridique formé pour passer en revue individuellement les millions de politiques de confidentialité.

[69] Facebook soutient en outre que l'évaluation du caractère raisonnable de ses politiques de confidentialité doit prendre en compte l'enquête de 2008–2009 du Commissariat sur ses pratiques en matière de confidentialité et les pourparlers qui ont suivi. Facebook prétend qu'elle pouvait raisonnablement se fier aux observations du commissaire selon lesquelles le processus GDP était un moyen efficace d'obtenir un consentement valable.

[70] Selon Facebook, la responsabilité du transfert d'informations par M. Kogan en violation des politiques de confidentialité de Facebook et de la politique de confidentialité de l'application TYDL censément fournie aux utilisateurs revient à M. Kogan, et non à Facebook.

[71] Pour soupeser ces deux qualifications opposées, la Cour dispose de bien peu de preuve, à part les photos des pages Web pertinentes tirées de l'affidavit déposé en faveur de Facebook. Il n'y a aucune preuve d'expert qui permettrait à la Cour de savoir ce que Facebook pourrait raisonnablement faire différemment, aucune preuve subjective des utilisateurs de Facebook quant à leurs attentes de confidentialité ni aucune preuve indiquant que les utilisateurs ne comprennent pas les questions en jeu lorsqu'ils utilisent Facebook. De telles preuves ne sont pas nécessaires, à strictement parler, mais elles auraient pu permettre à la Cour de mieux évaluer le caractère raisonnable du consentement valable dans un domaine où la norme de raisonnabilité et les attentes des utilisateurs dépendent autant du contexte et sont en constante évolution.

[72] Par ailleurs, le commissaire ne s'est pas prévalu des larges pouvoirs que lui confère l'article 12.1 de la LPRPDE pour contraindre Facebook à produire des éléments de preuve. Les avocats du commissaire ont expliqué qu'ils n'ont pas exercé les pouvoirs que leur confère cet article parce que Facebook ne s'y serait pas conformée ou n'aurait rien eu à offrir. Tel est peut-être le cas; mais, en fin de compte, il appartient au commissaire d'établir le manquement à la LPRPDE sur la foi de la preuve, et non à partir d'hypothèses et de déductions tirées de faits essentiels aussi clairsemés. Si Facebook avait refusé de produire des éléments contrairement à ce qu'elle était tenue de faire en vertu de la LPRPDE, le commissaire aurait de bon droit pu contester ce refus.

[73] Le commissaire critique la preuve par affidavit de Facebook parce qu'elle passe sous silence les « partenariats » que Facebook a établis avec d'autres entreprises et ne traite que de la relation entre Facebook et les développeurs d'applications tierces.

[74] La Cour n'est saisie d'aucune question concernant ces « partenariats » ou les pratiques de Facebook en matière de confidentialité en lien avec ces derniers. En l'espèce, l'avis de demande et le rapport de conclusions sur lequel il se fonde mettent en cause les mesures de confidentialité prises par Facebook relativement aux applications tierces, et non aux partenariats. Le Commissariat a de fait mené une enquête distincte en 2019 sur certains partenariats de Facebook. Cette enquête s'est terminée en 2021 sans que le commissaire formule de conclusions.

[75] L'un des éléments de preuve sur lequel le commissaire se fonde est un relevé statistique que Facebook a préparé pour une présentation interne, en octobre 2013, qui montre que 46 p. cent des développeurs d'applications n'avaient pas consulté la Politique de la plateforme ou les Conditions de service depuis qu'ils avaient lancé leur application. Le commissaire prétend que cet élément de preuve montre l'inefficacité des mécanismes de contrôle de Facebook.

[76] L'importance qu'il convient d'accorder à cet élément de preuve n'est pas claire, car tout ce qu'il montre c'est que les développeurs n'ont pas consulté les politiques « depuis » le lancement de leur application, et non qu'ils ne les ont jamais consultées. Cette constatation est particulièrement éloquente, car le commissaire admet lui-même que la plupart des dispositions pertinentes de la Politique de la plateforme sont demeurées essentiellement inchangées durant la période visée. En conséquence, je n'accorde que peu de poids à cet élément de preuve.

[77] En l'absence de preuve, le commissaire, dans ses observations, invite à de multiples reprises la Cour à tirer des « inférences », dont la plupart sont dénuées de fondement en droit ou au vu du dossier. Par exemple, la Cour a été invitée à tirer une inférence défavorable d'une revendication de privilège non contestée visant certains documents par le souscripteur de l'affidavit produit par Facebook.

[78] La Cour est ainsi réduite, à partir des photos de diverses politiques et ressources de Facebook, 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.

[79] J’en conclus que le commissaire n’est pas parvenu à s’acquitter de la charge qui lui incombait de prouver que Facebook a enfreint la LPRPDE pour avoir omis d’obtenir des consentements valables.

C. *Facebook a-t-elle omis de protéger suffisamment les renseignements concernant ses utilisateurs?*

[80] L’article 4.7 de l’annexe 1 de la LPRPDE définit le septième principe, applicable aux mesures de sécurité. Il prévoit que « [l]es renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité ».

[81] L’article 4.7.1 de l’annexe 1 dispose, entre autres, que « [l]es 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 ».

[82] L’occurrence d’une atteinte à la protection des données ne signifie pas que les mesures de sécurité d’une organisation sont inadéquates selon la LPRPDE; de même, l’absence d’une telle atteinte ne signifie pas que les mesures de sécurité d’une organisation sont adéquates.

[83] Facebook soutient que, une fois que l’utilisateur a autorisé Facebook à communiquer des renseignements à une application, l’obligation de Facebook concernant les mesures de sécurité selon la LPRPDE prend fin. De l’avis de Facebook, la LPRPDE ne l’oblige pas à s’assurer que l’utilisation ultérieure des renseignements en question par l’application est légale. Si une application manque à ses propres obligations, la responsabilité incombe à cette application, et non à Facebook.

[84] À titre subsidiaire, Facebook soutient que la combinaison de ses mesures de sécurité, incluant les ententes contractuelles avec les développeurs d’applications, est suffisante pour l’application de la LPRPDE.

[85] Le commissaire réplique que Facebook conserve le contrôle des renseignements communiqués aux applications tierces parce qu’elle a le droit contractuel de demander les renseignements aux applications. Le commissaire maintient que les mesures de sécurité de Facebook sont inadéquates.

[86] Je suis d’accord avec Facebook : ses obligations de sécurité prennent fin une fois que les renseignements sont communiqués aux applications tierces. Dans l’arrêt *Englander*, la Cour d’appel a noté que les mesures de sécurité imposées aux organisations sont liées à la façon de « gérer » les renseignements personnels « une fois qu’ils sont en leur possession » (au paragraphe 41).

[87] La limite des obligations de sécurité ressort clairement du contexte donné par d’autres dispositions de la LPRPDE. L’article 4.1 de l’annexe 1 expose le principe de la responsabilité. L’article 4.1.3 prévoit qu’une « organisation est responsable des renseignements personnels qu’elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement », mais ne prolonge pas cette responsabilité sur les renseignements communiqués en toutes circonstances.

[88] Selon l'article 7.2 de la LPRPDE, il incombe à l'organisation de prendre des mesures de sécurité pour d'éventuelles transactions commerciales. L'organisation qui communique des renseignements personnels à une autre organisation doit conclure un accord aux termes duquel l'organisation qui reçoit les renseignements s'engage « à les protéger au moyen de mesures de sécurité correspondant à leur degré de sensibilité ». Si l'organisation avait l'obligation générale de protéger les renseignements communiqués aux tiers, en vertu de ce principe de sécurité, cette disposition serait inutile.

[89] L'article 4.7.3 de l'annexe 1 dresse la liste des méthodes de protection des renseignements, notamment la prise de « moyens matériels » (« par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux »); de « mesures administratives » (« par exemple des autorisations sécuritaires et un accès sélectif »); et de « mesures techniques » (« par exemple l'usage de mots de passe et du chiffrement »). Aucune de ces mesures de sécurité n'a à voir avec la protection de renseignements dont le contrôle échappe à l'organisation.

[90] Le commissaire, dans ses observations, avance qu'il est essentiel d'adopter des mesures pour assurer le respect des politiques par les tiers dans un contexte numérique en constante évolution, vu la grande quantité de renseignements personnels que les géants de la technologie, telle Facebook, traitent et la facilité avec laquelle ces renseignements passent d'une entité à l'autre. En revanche, Facebook, dans ses observations, souligne le rôle que jouent les médias sociaux au chapitre de la promotion de la liberté d'expression dans la société moderne; que Facebook a, de plusieurs façons, remplacé les lieux de rassemblements publics, les kiosques à journaux, les ventes de débarras et les premiers rendez-vous galants. Ces observations militent 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 non en faveur d'une interprétation dénuée de tout principe que la Cour pourrait faire de la loi actuelle qui s'applique également aux géants des réseaux sociaux, aux banques locales et aux concessionnaires automobiles.

[91] Quoi qu'il en soit, même si les obligations en matière de sécurité devaient s'appliquer à Facebook après qu'elle a communiqué des renseignements à des tiers, la preuve est trop mince pour pouvoir conclure que les accords contractuels et les mesures prises pour encourager le respect de ses politiques constituent des mesures de sécurité adéquates. Les parties commerciales s'attendent raisonnablement dans leurs opérations contractuelles à un niveau minimal d'honnêteté et de bonne foi (*Bhasin c. Hrynew*, 2014 CSC 71, [2014] 3 R.C.S. 494, au paragraphe 60). Pour les mêmes raisons que celles concernant le consentement valable, le commissaire n'est pas parvenu à s'acquitter de la charge de montrer qu'il était déraisonnable de la part de Facebook de s'en remettre aux développeurs d'applications tierces pour agir de bonne foi et respecter en toute honnêteté leurs accords contractuels.

D. *Si Facebook a enfreint la LPRPDE, est-elle protégée par le principe de la préclusion résultant d'une déclaration ou de l'erreur provoquée par une personne en autorité?*

[92] À titre subsidiaire, Facebook invoque la préclusion résultant d'une déclaration et l'erreur provoquée par une personne en autorité. S'agissant de la préclusion résultant d'une déclaration, Facebook fait fond sur la décision de la Cour suprême du Canada

dans l'arrêt *Canadian Superior Oil c. Hambly*, [1970] R.S.C. 932, aux pages 939–940. Pour ce qui est de l'erreur provoquée par une personne en autorité, elle fait fond sur la décision de la Cour suprême du Canada dans l'arrêt *Lévis (Ville) c. Tétreault; Lévis (Ville) c. 2629-4470 Québec inc,* 2006 CSC 12, [2006] 1 R.C.S. 420, au paragraphe 26.

[93] L'idée maîtresse de ces observations est que, si Facebook a enfreint la LPRPDE, elle l'a fait parce qu'elle a été induite en erreur par les déclarations du commissaire à la suite de l'enquête du Commissariat de 2008–2009. Facebook soutient que le Commissariat a sanctionné et approuvé expressément son processus GDP après l'avoir mis à essai juste après avoir conclu son enquête. En conséquence, le commissaire ne peut alléguer maintenant que ce même processus enfreint la LPRPDE.

[94] Le commissaire s'inscrit en faux et avance que Facebook n'a pas mis en œuvre son processus GDP tel qu'elle avait promis et que le commissaire avait sanctionné.

[95] Puisque j'ai conclu que le commissaire n'est pas parvenu à établir que Facebook a enfreint la LPRPDE, je suis d'avis qu'il n'est pas nécessaire d'aborder cette question.

E. *Quelle est la réparation appropriée?*

[96] Vu la décision sur le fond, il n'est pas nécessaire d'examiner la réparation ou la portée de la réparation demandée par le commissaire.

[97] La demande est rejetée. Les parties ont convenu que les dépens adjugés à la partie qui aurait gain de cause pour l'essentiel dans le présent appel devraient être fixés à 80 000 $, incluant les taxes et les intérêts.

JUGEMENT dans le dossier T-190-20

LA COUR REND LE JUGEMENT suivant :

1. La demande est rejetée.

2. Les dépens fixés à 80 000 $, incluant les taxes et les intérêts, sont adjugés en faveur de Facebook.