

## Le droit du secret bancaire au Canada

Par Shawn Smith, Wesley Ng, Stikeman Elliott S.E.N.C.R.L., s.r.l.,  
conjointement avec le conseiller en protection des  
renseignements personnels de Practical Law

© 2019 Thomson Reuters. Tous droits réservés.  
*Contenu intégral. Reproduit avec permission.*

---

THOMSON REUTERS  
**PRACTICAL LAW™**

# Le droit du secret bancaire au Canada

SHAWN SMITH AND WESLEY NG. STIKEMAN ELLIOTT LLP.  
CONJOINTEMENT AVEC UN CONSEILLER EN PROTECTION DES  
RENSEIGNEMENTS PERSONNELS DE PRACTICAL LAW

Pour en savoir plus, recherchez les [numéros d'identification de ressource inscrits en bleu](#) dans Westlaw.

Note de pratique qui porte sur les lois, règlements et directives régissant le secret bancaire au Canada sous le régime de la common law, de la Loi sur la protection des renseignements personnels et les documents électroniques (L.C. 2000, ch. 5) (la « LPRPDE ») et de la Loi sur les banques. Cette note donne des indications générales aux institutions bancaires appelées à traiter des données sur leurs clients au Canada à propos de la conformité aux obligations de secret bancaire, des circonstances permettant de communiquer des données sur leurs clients aux tiers et des mesures à prendre pour communiquer de l'information.

Le droit du secret bancaire interdit généralement aux institutions bancaires et à leurs dirigeants et employés de communiquer des données sur les clients aux tiers. Toutefois, les banques doivent habituellement communiquer des données sur les clients dans le cadre de leurs affaires courantes, notamment :

- Fournir des produits ou services aux clients.
- Faire des virements intersociétés.
- Impartir leurs fonctions à des tiers fournisseurs de service.
- Donner suite aux demandes des tribunaux et des organismes de réglementation.

Les banques mondiales qui exercent leurs activités dans des territoires dotés de lois sur le secret bancaire doivent trouver des solutions pratiques pour exercer leurs fonctions commerciales, faute de quoi elles s'exposent à des sanctions, notamment des amendes, mesures réglementaires, poursuites

privées et dans les cas graves, à des sanctions pénales pour avoir communiqué des données sur leurs clients en violation des lois sur le secret bancaire.

Cette note porte sur les lois, règlements et directives qui régissent le secret bancaire au Canada. Elle donne des indications aux institutions bancaires appelées à traiter des données sur leurs clients recueillies au Canada à propos de la conformité aux obligations de secret et d'impartition bancaires, des circonstances permettant de communiquer des données sur leurs clients aux tiers et des mesures à prendre pour communiquer de l'information.

Pour obtenir de l'information sur les lois sur le secret bancaire applicables aux banques mondiales, voir la note de pratique « Global Bank Secrecy Laws : Overview » ([WV-002-8052](#)).

## RÉGIME JURIDIQUE DU SECRET BANCAIRE AU CANADA

Contrairement à de nombreux territoires, le Canada n'a pas de législation particulière sur le secret bancaire. Toutefois, les banques qui recueillent des données sur leurs clients au Canada sont assujetties à certaines lois qui établissent collectivement le régime juridique applicable à la collecte, à l'utilisation et à la communication des données sur les clients, notamment :

- L'obligation de confidentialité en common law de la banque envers ses clients (voir la rubrique « Obligations en common law »).
- La Loi sur la protection des renseignements personnels et les documents électroniques (L.C. 2000, ch. 5) (voir la rubrique « LPRPDE »).
- Certaines dispositions de la Loi sur les banques (L.C. 1991, ch. 46) (la « Loi sur les banques ») (voir la rubrique « Loi sur les banques »).

## OBLIGATIONS EN COMMON LAW

Les tribunaux canadiens se sont appuyés sur l'arrêt de la Cour d'appel d'Angleterre *Tournier v. National Provincial and Union Bank of England* [1924] 1 K.B. 461 (C.A.), qui est l'arrêt de principe sur les obligations du banquier envers son client en common law. Selon l'arrêt *Tournier*, le banquier a une obligation contractuelle implicite envers son client de ne pas communiquer les données sur le client aux tiers, sauf dans certaines circonstances (voir la rubrique « Exceptions permettant de communiquer une information »).

## PERSONNES ET ENTITÉS VISÉES

L'obligation de protéger les données sur les clients en common law s'applique à la relation entre la banque et le client. Les banques mentionnées dans la Loi sur les banques et toute personne qui agit en qualité de banquier au Canada sont des banques.

L'obligation de protéger les données sur les clients incombe généralement à la banque, en sa qualité d'institution. Par conséquent, les banques doivent prendre des mesures pour s'assurer que leurs employés, administrateurs, dirigeants, mandataires et autres représentants conservent les données sur les clients conformément à l'obligation de common law.

L'obligation de protéger les données sur les clients en common law continue de s'appliquer même après la fin de la relation entre la banque et le client (*Tournier*, 1 K.B., p.473).

## PROTECTION DES DONNÉES SUR LES CLIENTS

L'obligation de protéger les données sur les clients en common law s'applique aux données obtenues par la banque auprès d'une source liée au client (personne physique ou morale), à l'exception de l'information publique (sauf si l'information devient publique en raison d'une faute de la banque), notamment les données concernant :

- l'identité du client;
- les investissements détenus et leur valeur;
- les dépôts et retraits;
- l'information sur les prêts;
- la valeur des investissements;
- l'information donnée par le client à propos de sa situation financière;
- la relation du client avec d'autres banques, le cas échéant.

L'obligation de protéger les données sur les clients en common law s'applique à l'information liée au client concerné. Les banques qui souhaitent anonymiser ou regrouper les données sur leurs clients avant de les communiquer, pour rendre impossible d'établir l'identité du client, doivent se conformer à la LPRPDE (voir la rubrique « Communication de renseignements personnels anonymisés »).

## EXCEPTIONS PERMETTANT DE COMMUNIQUER UNE INFORMATION

Selon l'arrêt *Tournier*, l'obligation de confidentialité de la banque envers son client en common law n'est pas absolue et des exceptions s'y appliquent dans les cas suivants :

- La communication d'information est exigée par la loi applicable (voir la rubrique « Communication d'information exigée par la loi »).
- La communication d'information est une obligation envers le public (voir la rubrique « Obligation envers le public de communiquer des données sur les clients »).
- La communication d'information est exigée dans l'intérêt de la banque (voir « Communication d'information exigée dans l'intérêt de la banque »).
- Le client a donné son consentement exprès ou implicite (voir la rubrique « Consentement exprès ou implicite du client »).

(Voir *Haughton v. Haughton* (1964), [1965] 1 O.R. 481 (C.S. Ont.);

*Guertin v. Royal Bank*, (1983) 43 O.R. (2d) 363 (C.S. Ont.).

La communication de bon nombre d'informations que les banques communiquent habituellement aux tiers, notamment les tiers fournisseurs de services et leurs entités apparentées, n'est pas autorisée par les exceptions définies dans l'arrêt *Tournier* (sauf l'exception du consentement). Les banques devraient demander le consentement écrit du client au lieu de s'en remettre aux autres exceptions définies dans l'arrêt *Tournier* pour communiquer les données nécessaires sur les clients et éviter qu'ils contestent leurs motifs de communication (voir la rubrique « Consentement exprès ou implicite du client »).

## Communication d'information exigée par la loi

Les tribunaux canadiens qui se sont prévalus de l'arrêt *Tournier* ont permis aux banques de communiquer des données sur leurs clients lorsque la communication était légalement requise, c'est-à-dire, en règle générale, imposée par une ordonnance judiciaire et par la législation (voir, par exemple, *Haughton* [1965] 1 O.R. 481 (en l'espèce, le tribunal a décidé que seule une ordonnance judiciaire peut obliger un directeur de banque à témoigner et que la citation à comparaître ne suffit pas à annuler l'obligation de confidentialité du banquier); *Royal Bank of Canada v. Art's Welding & Machine Shop (1980) Ltd.*, (1989), 34 C.P.C. (2d) 190 (B.R. Alb.) (en l'espèce, le tribunal a décidé que l'ordonnance judiciaire constituait une contrainte légale permettant la communication de données sur les clients).

Le paragraphe 628(1) de la Loi sur les banques, selon lequel la banque doit fournir au surintendant des institutions financières les renseignements qu'il exige, constitue un exemple de

communication d'information exigée par la loi (voir la rubrique « Loi sur les banques »).

L'exception de contrainte légale peut également comprendre la contrainte imposée par la loi d'un territoire étranger (voir *Park v. Bank of Montreal*, [1997] B.C.J. No. 787 (C.S. C.-B.)) (en l'espèce, le tribunal a conclu que la communication d'information par la succursale canadienne d'une banque coréenne au bureau du procureur coréen a eu lieu sous contrainte légale puisque la communication était exigée en application de la loi coréenne).

### Obligation envers le public de communiquer des données sur les clients

L'obligation de protéger l'intérêt public peut l'emporter sur l'obligation de secret bancaire en common law dans des circonstances limitées, notamment en cas de danger pour l'État ou le public (*Jubbal v. Royal Bank of Canada*, [1987] B.C.J. No. 1715) (C.S. C.-B.). Par exemple, les tribunaux ont jugé que les banques peuvent communiquer des données sur leurs clients dans le cadre de l'exception relative à l'intérêt public :

- Afin de prévenir la fraude, que ce soit en droit une fraude ou un dol (*deceit*) (*Canadian Imperial Bank of Commerce v. Sayani* (1993), 11 B.L.R. (2d) 28 (C.A. C.-B.)).
- Dans le cas du liquidateur de la Banque Commerciale du Canada, en vertu de la loi désormais connue comme la Loi sur les liquidations et les restructurations (voir *Canada Deposit Insurance Corp. v. Canadian Commercial Bank* (1989), 71 C.B.R. 239) (B.R. Alb.)).

### Communication d'information exigée dans l'intérêt de la banque

Les banques peuvent aussi communiquer des données sur les clients si leurs intérêts l'exigent. Toutefois, elles doivent interpréter cette exception de manière stricte (*Park v. Bank of Montreal*, [1997] B.C.J. No. 787 (C.S. C.-B.)). Les tribunaux ont conclu qu'une banque peut faire valoir cette exception dans des circonstances précises afin de protéger ses intérêts, notamment, par exemple :

- Informer les tiers de l'existence de la sûreté qu'elle détient sur le bien d'un client afin de protéger la sûreté (*Royal Bank of Canada v. Brattberg*, [1993] 8 W.W.R. 139 (B.R. Alb.); *Royal Bank of Canada v. Vincenzi*, [1994] B.C.W.L.D. 1221 (C.S. C.-B.)).
- Communiquer de l'information à propos du différend qu'elle a avec son client concernant une créance lorsque le client tente de contracter d'autres dettes (*Sayani*, 11 B.L.R. (2d) 28).

### Consentement exprès ou implicite du client

Les banques peuvent également communiquer des données sur le client avec le consentement du client. Les tribunaux ont

décidé que certains services personnalisés fournis par une banque lui procurent le consentement implicite du client à la communication des données du client. Par exemple, les tribunaux ont conclu que la banque à laquelle le client a consenti une sûreté sur ses biens a également consenti à ce que la banque en communique l'existence aux tiers intéressés (voir, par exemple, *Vincenzi*, [1994] B.C.W.L.D. 1221).

Toutefois, les banques doivent généralement tenter d'obtenir le consentement exprès écrit de communiquer des données sur leurs clients au lieu de faire valoir la notion de consentement implicite pour les besoins de la preuve. La banque obtient habituellement le consentement du client lorsqu'elle lui demande d'accepter ses conditions et sa politique de confidentialité usuelles au moment de l'ouverture du compte. Les conditions et la politique de confidentialité usuelles doivent énoncer les politiques et pratiques de la banque relativement à la collecte, à l'utilisation et à la communication des données sur les clients conformément aux pratiques du secteur au Canada.

### LOI SUR LES BANQUES

La Loi sur les banques régit les banques à charte du Canada. La charte d'une banque définit les types d'activités que la banque peut exercer et énonce ses obligations de gestion.

La Loi sur les banques n'interdit pas la communication de données sur les clients mais, conformément aux règles établies dans l'arrêt *Tournier*, plusieurs de ses articles protègent les données sur les clients de la communication, notamment ceux qui :

- attribuent aux administrateurs de la banque, dans le cadre de leur obligation de surveillance de la gestion et de l'activité commerciale de la banque, le mandat d'instituer des mécanismes visant à restreindre l'utilisation des renseignements confidentiels, notamment, en règle générale, les données sur les clients (alinéa 157(2)c) de la Loi sur les banques);
- exigent des administrateurs de la banque qu'ils désignent l'un des comités du conseil d'administration pour surveiller l'application des mécanismes visant à restreindre l'utilisation des renseignements confidentiels, notamment, en règle générale, les données sur les clients (alinéa 157(2)d) de la Loi sur les banques);
- obligent les banques et leurs mandataires à prendre les mesures suffisantes pour faire en sorte qu'aucune personne non autorisée n'ait accès aux renseignements qui sont contenus dans ses livres ou ne les utilise, notamment, en règle générale, les données sur les clients (alinéa 244d) de la Loi sur les banques).

Les banques assujetties à la Loi sur les banques doivent comprendre ces dispositions et veiller à prendre les mesures de protection nécessaires des données sur leurs clients. Les banques qui contreviennent aux dispositions qui précèdent sont passibles

d'une amende maximale de 500 000 \$ CA sur déclaration de culpabilité par procédure sommaire et de 5 000 000 \$ CA sur déclaration de culpabilité par mise en accusation (paragraphe 985(1) de la Loi sur les banques).

### LPRPDE

La LPRPDE régit la collecte, l'utilisation et la communication des renseignements personnels de quelque type qu'ils soient par certaines organisations du secteur privé, notamment les banques. Le renseignement personnel comprend généralement tout renseignement concernant un individu identifiable. D'après les conclusions des tribunaux canadiens et du Commissariat à la protection de la vie privée (le « CPVP ») un renseignement concerne un individu identifiable lorsqu'il y a une possibilité sérieuse qu'un individu puisse être identifié au moyen du renseignement, que ce renseignement soit pris seul ou en combinaison avec d'autres renseignements disponibles (voir le bulletin d'interprétation « Renseignements personnels » du CPVP).

La LPRPDE s'applique généralement aux banques qui recueillent des renseignements personnels au Canada, notamment les banques étrangères qui ont des bureaux, des succursales et des entités de leur groupe au Canada.

Pour plus d'information sur la LPRPDE, voir la note de pratique « Data Privacy Laws in Canada : PIPEDA » ([W-011-7386](#)).

### CHAMP D'APPLICATION

La LPRPDE s'applique aux renseignements personnels recueillis au Canada et ne s'applique généralement pas aux renseignements personnels recueillis à l'étranger. Toutefois, la LPRPDE est silencieuse sur sa portée territoriale et les tribunaux canadiens ont appliqué le critère des « liens véritables et étroits » de la common law pour déterminer si la LPRPDE devrait s'appliquer et établir la compétence du CPVP pour traiter une plainte concernant la protection de la vie privée qui a pris naissance à l'étranger. La question sous-jacente est de savoir s'il y a un lien suffisant entre le Canada et l'activité visée pour que le Canada applique sa loi.

Dans la décision rendue récemment dans l'affaire *A.T. c. Globe24h.com*, 2017 CF 114, la Cour fédérale a décidé qu'elle avait compétence pour prononcer une ordonnance extraterritoriale aux effets mondiaux contre un résident étranger, auquel elle a demandé de retirer d'Internet les documents qui contenaient des renseignements personnels sur des citoyens canadiens et contrevenaient à la LPRPDE.

La LPRPDE ne s'applique généralement pas aux renseignements personnels recueillis à l'étranger.

### PRINCIPES

Les dix principes relatifs à l'équité dans le traitement de l'information de la LPRPDE servent de fondement aux obligations de collecte, d'utilisation et de communication de renseignements personnels d'une banque au Canada. Ces principes sont les suivants :

- **Responsabilité.** Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, notamment les renseignements confiés à une tierce partie aux fins de traitement (premier principe, annexe 1, LPRPDE).
- **Détermination des fins de la collecte des renseignements.** L'organisation doit documenter les fins auxquelles les renseignements personnels sont recueillis et les préciser à la personne auprès de laquelle elle recueille des renseignements (deuxième principe, annexe 1, LPRPDE).
- **Consentement.** L'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'avec le consentement de la personne, sauf certaines exceptions limitées (troisième principe, annexe 1, LPRPDE).
- **Limitation de la collecte.** L'organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite (quatrième principe, annexe 1, LPRPDE).
- **Limitation de l'utilisation, de la communication et de la conservation.** L'organisation ne doit pas utiliser et communiquer les renseignements personnels à des fins autres que celles pour lesquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. Elle ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées (cinquième principe, annexe 1, LPRPDE).
- **Exactitude.** Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés (sixième principe, annexe 1, LPRPDE).
- **Mesures de sécurité.** L'organisation doit protéger les renseignements personnels au moyen de mesures de sécurité correspondant à leur degré de sensibilité (septième principe, annexe 1, LPRPDE).
- **Transparence.** L'organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne (huitième principe, annexe 1, LPRPDE).
- **Accès aux renseignements personnels.** Toute personne a le droit de consulter et de corriger les renseignements personnels qui la concernent, sauf certaines exceptions limitées (neuvième principe, annexe 1, LPRPDE).
- **Possibilité de porter plainte à l'égard du non-respect des principes.** L'organisation doit établir des procédures pour permettre à toute personne de se plaindre du non-respect des

principes énoncés ci-dessus (dixième principe, annexe 1, LPRPDE).

## TRANSFERTS DE DONNÉES

Dans certaines circonstances, les banques peuvent souhaiter faire des transferts transfrontaliers de renseignements personnels, notamment, par exemple, à leurs établissements ou sociétés mères à l'étranger ou à un tiers fournisseur de services. Aux termes de la LPRPDE, les banques demeurent responsables de tous les renseignements personnels transférés à des tiers au Canada ou à l'étranger. Les banques doivent, par voie contractuelle ou autre, veiller à ce que les tiers fournissent un degré de protection aux renseignements comparable au leur (voir « Facteurs liés à l'impartition »).

La LPRPDE n'interdit pas le transfert transfrontalier de renseignements personnels et ne fait pas de distinction entre les transferts nationaux et internationaux de données. Toutefois, le CPVP a déclaré que toute organisation située au Canada qui transfère des renseignements personnels vers un pays étranger doit prendre les mesures suivantes :

- Informer les personnes visées du transfert de leurs renseignements personnels vers le pays étranger.
- Informer les personnes visées du fait que leurs renseignements personnels pourraient être mis à la disposition du gouvernement ou des organismes d'application de la loi du pays étranger en vertu d'une ordonnance légale prononcée dans le pays en question.

Aux termes de l'article 245 de la Loi sur les banques, le surintendant des institutions financières et le ministre des Finances ont, dans certaines circonstances, les droits suivants :

- Interdire à la banque de transférer vers certains pays ou de traiter dans certains pays plusieurs livres, notamment ceux liés aux données sur ses clients.
- Ordonner à la banque de se livrer à ces activités uniquement au Canada.

Pour plus d'information, voir les lignes directrices du CPVP « Transfert transfrontalier de renseignements personnels » et la note de pratique « Cross-Border Personal Data Transfers (Canada) » ([W-009-4229](#)).

## LE CONSENTEMENT SELON LA LPRPDE

Selon la LPRPDE, il est généralement nécessaire d'informer la personne visée et d'obtenir son consentement avant de recueillir, d'utiliser et de communiquer ses renseignements personnels. Toutefois, la LPRPDE prévoit certaines exceptions où l'organisation n'est pas tenue d'obtenir le consentement.

### Circonstances où le consentement n'est pas nécessaire

Les banques peuvent recueillir et utiliser des renseignements personnels à l'insu d'un intéressé ou sans son consentement dans certaines circonstances, notamment les suivantes :

- La collecte du renseignement est manifestement dans l'intérêt de l'intéressé et le consentement ne peut être obtenu auprès de celui-ci en temps opportun (alinéa 7(1)a) de la LPRPDE).
- La collecte est raisonnable à des fins liées à une enquête sur la violation d'un accord ou la contravention au droit fédéral ou provincial et il est raisonnable de s'attendre à ce que la collecte effectuée au su ou avec le consentement de l'intéressé compromette l'exactitude du renseignement ou l'accès à celui-ci (alinéa 7(1)b) de la LPRPDE).
- Il s'agit d'un renseignement auquel le public a accès et son utilisation est conforme au Règlement précisant les renseignements auxquels le public a accès (DORS/2001-7) (13 décembre 2000) (le « Règlement ») (alinéa 7(1)d) de la LPRPDE).
- La collecte est faite en vue d'une communication exigée par la loi (sous-alinéa 7(1)e)(ii) de la LPRPDE).

Aux termes de la LPRPDE, les banques peuvent utiliser des renseignements personnels à l'insu de l'intéressé ou sans son consentement dans les cas suivants :

- L'organisation s'en sert pour répondre à une situation d'urgence mettant en danger la vie, la santé ou la sécurité de tout individu; (alinéa 7(2)b) de la LPRPDE).
- Il s'agit d'un renseignement contenu dans la déclaration d'un témoin et dont l'utilisation est nécessaire en vue de l'évaluation d'une réclamation d'assurance, de son traitement ou de son règlement (alinéa 7(2)b.1) de la LPRPDE).

L'organisation peut communiquer des renseignements personnels à l'insu de l'intéressé ou sans son consentement dans certaines circonstances, notamment les suivantes :

- La communication est faite en vue du recouvrement d'une créance que l'organisation a contre l'intéressé (alinéa 7(3)b) de la LPRPDE).
- La communication est exigée par assignation, mandat ou ordonnance d'un tribunal, d'une personne ou d'un organisme ayant le pouvoir de contraindre à la production de renseignements ou exigée par des règles de procédure se rapportant à la production de documents (alinéa 7(3)c) de la LPRPDE).
- La communication est faite à une institution gouvernementale qui a mentionné la source de l'autorité légitime étayant son droit d'obtenir le renseignement et le fait, selon le cas :
  - qu'elle soupçonne que le renseignement est afférent à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales;
  - qu'elle en a besoin aux fins de la collecte de renseignements en matière de sécurité, de la tenue d'une enquête ou du contrôle d'application du droit canadien, provincial ou étranger;
  - qu'elle en a besoin pour l'application du droit canadien



ou provincial;

- qu'elle en a besoin afin d'entrer en contact avec le plus proche parent d'un individu blessé, malade ou décédé, ou avec son représentant autorisé.

(alinéa 7(3)c.1) de la LPRPDE)

- La communication est faite à une institution gouvernementale et l'organisation :

- soit a des motifs raisonnables de croire que le renseignement est afférent à une contravention réelle ou éventuelle du droit canadien ou étranger;
- soit soupçonne que le renseignement est afférent à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales.

(alinéa 7(3)d) de la LPRPDE)

- Elle est faite à une autre organisation et est raisonnable en vue d'une enquête sur la violation d'un accord ou sur la contravention au droit canadien et la communication effectuée avec le consentement compromettrait l'enquête (alinéa 7(3)d.1) de la LPRPDE).
- Elle est faite à une autre organisation et est raisonnable en vue de la prévention, de la détection ou de la suppression d'une fraude et la communication effectuée avec le consentement compromettrait la capacité de prévenir la fraude, de la détecter ou d'y mettre fin (alinéa 7(3)d.2) de la LPRPDE).
- Elle est nécessaire aux fins d'identification de l'intéressé qui est blessé, malade ou décédé et est faite à une institution gouvernementale, à un proche parent de l'intéressé ou à son représentant autorisé et, dans le cas où la personne visée par le renseignement est vivante, l'organisation doit l'informer par écrit et sans délai de la communication du renseignement (alinéa 7(3)d.4) de la LPRPDE).
- Elle est faite à une personne qui a besoin du renseignement en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité de toute personne et, dans le cas où la personne visée par le renseignement est vivante, l'organisation doit l'informer par écrit et sans délai de la communication du renseignement (alinéa 7(3)e) de la LPRPDE).

La communication d'un renseignement personnel est également permise dans les cas suivants :

- Il s'agit d'un renseignement contenu dans la déclaration d'un témoin et dont la communication est nécessaire en vue de l'évaluation d'une réclamation d'assurance, de son traitement ou de son règlement; (alinéa 7(3)e.1) de la LPRPDE).
- Il s'agit d'un renseignement du Règlement auquel le public a accès (alinéa 7(3)h.1) de la LPRPDE).

Les exceptions qui précèdent sont interprétées de manière stricte dans les décisions du CPVP et des tribunaux canadiens et les circonstances dans lesquelles les organisations peuvent s'en prévaloir y sont précisées. Les banques doivent étudier attentivement la LPRPDE et la jurisprudence applicable avant de procéder à la collecte, à l'utilisation ou à la communication de renseignements personnels sans consentement.

#### **Obtention d'un consentement valable**

Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, sauf dans les circonstances précises énumérées. La forme du consentement peut varier selon les circonstances et la nature des renseignements, compte tenu des attentes raisonnables du client. Pour établir le type de consentement requis, les organisations doivent tenir compte du caractère sensible des renseignements. En règle générale, les organisations doivent obtenir un consentement explicite de l'intéressé lorsque les renseignements sont sensibles (voir le bulletin d'interprétation « Forme de consentement » et les « Lignes directrices pour l'obtention d'un consentement valable » du CPVP).

La LPRPDE ne définit pas précisément le renseignement sensible. Toutefois, les renseignements financiers sont généralement considérés comme sensibles (voir le bulletin d'interprétation « Forme de consentement » et les « Lignes directrices pour l'obtention d'un consentement valable » du CPVP).

#### **COMMUNICATION DE DONNÉES PERSONNELLES ANONYMISÉES**

Le CPVP adopte une position stricte sur l'anonymisation des renseignements personnels en vertu de la LPRPDE, en particulier les renseignements personnels sensibles comme les renseignements financiers. Dans une plainte déposée contre l'entreprise canadienne de télécommunications Bell Canada, le CPVP a conclu que Bell Canada avait contrevenu à la LPRPDE, malgré les mesures prises pour communiquer seulement des renseignements regroupés et anonymisés aux publicitaires. Le CPVP a conclu que Bell Canada aurait dû prendre des mesures proactives, comme interdire par contrat aux publicitaires d'utiliser des témoins de suivi, l'empreinte de l'appareil, les renseignements sur le compte ou d'autres méthodes de suivi, dans le but d'établir des liens entre les renseignements tirés du profil de publicité connexe et les renseignements regroupés afin de réidentifier les clients (voir le rapport de conclusions d'enquête en vertu de la LPRPDE n° 2015-001, paragraphes 48 à 52). Le CPVP s'est également demandé si le fait de générer des données anonymes et regroupées à partir de renseignements personnels particulièrement sensibles, comme les cotes de crédit, et de les utiliser à des fins de publicité ciblée est acceptable en toutes circonstances (voir le rapport de conclusions d'enquête en vertu de la LPRPDE n° 2015-001, paragraphes 53 à 58).

## COMMUNICATION DE DONNÉES SUR LES CLIENTS EN APPLICATION DES LOIS SUR LA PROTECTION DES DONNÉES ET DE LA COMMON LAW

Les banques qui sont appelées à traiter des renseignements personnels sur leurs clients sont soumises aux obligations de conformité de la common law et de la LPRPDE.

### ANALYSE DES DONNÉES VISÉES

Les organisations doivent analyser de manière distincte leurs obligations de traitement des données sur les clients et leurs obligations de conformité en application de la common law et de la LPRPDE. En effet, la common law et la LPRPDE protègent différentes catégories de données et s'appliquent dans des circonstances différentes. Par exemple :

- La LPRPDE s'applique de manière large à la collecte, à l'utilisation et à la communication de renseignements personnels, tandis que l'obligation de common law protège la communication des données sur les clients d'une banque.
- À la différence de l'obligation de common law, la LPRPDE s'applique aux renseignements sur les sociétés.

### CONFLITS ÉVENTUELS

Les banques peuvent être aux prises avec un conflit entre la common law et la LPRPDE, l'une permettant la communication d'information dans certaines circonstances, et l'autre non. Par exemple, la banque pourrait se trouver dans une situation où une exception de l'arrêt *Tournier* (sauf l'exception du consentement) permettant la communication de l'information s'applique, mais où l'exception ne s'applique pas sous le régime de la LPRPDE. En pareil cas, la banque doit obtenir le consentement exprès à la communication de l'information aux termes de la LPRPDE.

## FACTEURS LIÉS À L'IMPARTITION

### OBLIGATIONS DE COMMON LAW ET AUTRES FACTEURS

La banque qui impartit ses services à des tiers fournisseurs de services demeure responsable des activités imparties, y compris la communication non autorisée de données sur ses clients. Par conséquent, la banque doit procéder au contrôle diligent des tiers fournisseurs de services avant de retenir leurs services, pour s'assurer, entre autres, qu'ils peuvent protéger adéquatement les données sur les clients auxquelles elle peut leur donner accès.

Le Bureau du surintendant des institutions financières a publié la ligne directrice B-10 (la « ligne directrice »), qui énonce ses attentes à l'égard des entités fédérales, y compris les banques, qui recourent à l'impartition d'au moins l'une de leurs activités en faveur d'un fournisseur de services ou qui songent à le faire. Les banques canadiennes font généralement comme si la ligne directrice B-10 était juridiquement contraignante même si elle ne l'est pas.

En vertu de la ligne directrice, les banques doivent, entre autres :

- évaluer les risques de toute entente d'impartition existante ou proposée;
- élaborer un processus pour déterminer l'importance relative des ententes;
- mettre en œuvre un programme de gestion et de supervision des risques qui tient compte de l'importance relative des ententes;
- veiller à ce que le conseil d'administration, l'agent principal ou l'administrateur principal reçoive l'information nécessaire pour s'acquitter de ses fonctions en vertu de la ligne directrice;
- éviter d'impartir certaines activités à l'auditeur externe;
- prévoir des dispositions contractuelles dans lesquelles elles stipulent leurs exigences de confidentialité et de sécurité qui doivent satisfaire à une norme raisonnable dans les circonstances. Le marché ou l'entente d'impartition doit préciser :
  - qui est responsable des mécanismes de protection;
  - la portée de l'information à protéger;
  - les pouvoirs de chaque partie pour ce qui est de modifier les procédures et les exigences de sécurité;
  - quelle partie peut être tenue responsable des pertes pouvant résulter d'un manquement à la sécurité, de même que les exigences de notification en cas de manquement à la sécurité;
  - l'obligation du fournisseur de services de stocker les données sur les clients de la banque séparément des données fournies par d'autres clients.

### LPRPDE

En vertu de la LPRPDE, les organisations demeurent responsables de tous les renseignements personnels communiqués à des tiers, y compris à l'étranger (premier principe, article 4.1.3, annexe 1, LPRPDE). Les banques doivent procéder à un contrôle diligent des tiers fournisseurs de services préalable à l'attribution du mandat pour s'assurer qu'ils peuvent protéger adéquatement les renseignements personnels. Si elle veut procéder efficacement, la banque doit passer en revue le personnel du service de la protection des renseignements personnels et de la sécurité des données, les groupes administratifs et commerciaux concernés et le fournisseur et collaborer avec eux pour :

- Repérer les types de renseignements personnels qu'elle doit transférer en fonction de la portée des travaux proposés, afin de comprendre le degré de sensibilité des renseignements personnels.
- Envisager des façons d'atténuer les risques au moyen d'une proposition d'utilisation limitée des renseignements personnels



par le fournisseur dans le respect des obligations commerciales.

- Examiner les politiques, les procédures, les contrôles internes et le matériel de formation du fournisseur afin d'évaluer sa capacité à :
  - déceler et gérer l'évolution des risques pour la sécurité des données;
  - former et surveiller adéquatement ses employés et sous-traitants concernés;
  - observer les politiques de confidentialité et de sécurité de l'information de l'organisation;
  - se conformer aux lois, règlements et normes sectorielles applicables.
- Examiner les mesures de sécurité applicables aux renseignements personnels chez le fournisseur, notamment le recours éventuel au chiffrement.
- Examiner les antécédents du fournisseur en matière de confidentialité et de sécurité des données, notamment les mesures de mise en application par les autorités, les litiges ou les incidents de sécurité (comme les atteintes à la sécurité des données).
- Comprendre les lois du territoire du fournisseur afin de repérer d'autres facteurs de risque susceptibles de se répercuter sur l'intégrité, la sécurité et la confidentialité des renseignements personnels.

Les banques devraient aussi prendre des mesures de protection contractuelles qui garantissent un niveau de protection de la confidentialité similaire à celui auquel elles s'engagent envers leurs clients. Des conditions contractuelles rigoureuses obligent notamment le fournisseur à adopter des mesures de sécurité raisonnables pour la protection des données sur les clients, y compris souscrire aux obligations suivantes :

- Protéger les données sur les clients au moyen d'antivirus, de pare-feu, d'outils de protection et de désinfection conformes aux meilleures pratiques du secteur et adopter et mettre à jour des mesures de sécurité, ainsi que des méthodes et procédures de sauvegarde conformes aux meilleures pratiques du secteur.
- Recueillir, utiliser et communiquer des données sur les clients conformément aux lois sur la protection des renseignements personnels applicables, à seule fin de permettre au tiers d'exécuter ses obligations contractuelles ou de se libérer de ses obligations contractuelles.
- S'acquitter de ses obligations contractuelles afin de permettre à la banque de se conformer aux obligations qui lui incombent en application des lois sur la protection des renseignements personnels applicables.
- Autoriser la banque à vérifier la conformité au contrat de ses

pratiques de protection des renseignements personnels.

- Aviser promptement la banque de la réception d'une demande d'accès aux données sur les clients, d'une plainte en rapport avec ces données ou d'un avis de non-conformité à une loi sur la protection des renseignements personnels applicable.
- Prendre les mesures raisonnables de soutien suivantes :
  - répondre aux demandes d'accès, de modification, de correction ou aux demandes similaires relativement à ces renseignements;
  - enquêter sur les plaintes liées à la réception, à l'utilisation ou à la communication de renseignements, limiter leurs effets et y donner suite;
  - répondre aux demandes ou consignes formulées par une autorité gouvernementale relativement à ces renseignements.
- Détruire promptement toutes les copies des renseignements dont il a la possession ou le contrôle à la demande de la banque ou lorsqu'il n'a plus besoin des renseignements pour s'acquitter de ses obligations contractuelles.

## APPLICATION ET PÉNALITÉS

### CONTRAVENTIONS À LA COMMON LAW

La banque à laquelle il est reproché d'avoir enfreint les droits à la protection des renseignements personnels d'un client sur le fondement de l'arrêt *Tournier* s'expose à des poursuites en dommages pécuniaires ou au prononcé d'une mesure injonctive par un tribunal. Des recours similaires peuvent également être exercés au moyen de mécanismes substitutifs de résolution des différends. Les actions collectives sont de plus en plus utilisées au Canada pour faire valoir des réclamations contre les banques et d'autres grandes entreprises dont les violations auraient, selon les allégations, porté préjudice à de multiples clients. Les banques s'exposent également à des poursuites fondées sur d'autres délits de common law, notamment l'abus de confiance et l'atteinte à la vie privée (voir, par exemple, *Jones v. Tsige*, 2012 ONCA 32. La Cour d'appel de l'Ontario a accordé 10 000 \$ CA de dommages-intérêts à un homme dont l'ex-épouse et employée de banque avait consulté sans autorisation les renseignements bancaires personnels de la nouvelle conjointe de son ex-époux).

### LOI SUR LA PROTECTION DES DONNÉES

#### LPRPDE

Les plaintes déposées en vertu de la LPRPDE peuvent être engagées par un individu ou par le CPVP. Après le dépôt de la plainte, le CPVP peut enquêter et produire un rapport détaillé de ses conclusions et recommandations. Ce rapport n'a pas force

obligatoire à l'égard des banques. Toutefois, si les banques ne mettent pas en œuvre les recommandations, le CPVP peut présenter une demande d'ordonnance de mise en œuvre des recommandations à la Cour fédérale. Après que le CPVP a produit un rapport ou avisé la personne concernée de la fin de l'examen, cette dernière peut former une demande en dommages-intérêts devant la Cour fédérale.

La Cour fédérale peut ordonner à une organisation de faire ce qui suit :

- Revoir ses pratiques.
- Publier un avis correctif.
- Verser au plaignant des dommages-intérêts, notamment en réparation de l'humiliation subie.

Quiconque prend part aux activités suivantes ou entrave l'action du CPVP dans le cadre d'une vérification ou de l'examen d'une plainte pourrait également commettre une infraction et encourir, sur déclaration de culpabilité par mise en accusation, une amende maximale de 100 000 \$ CA pour :

- Violation des dispositions applicables à la conservation des renseignements qui font l'objet d'une demande d'accès.
- Représailles contre l'employé qui :
  - signale au CPVP une contravention ou un soupçon raisonnable de contravention à la LPRPDE;
  - refuse de contrevenir à la LPRPDE; ou
  - se conforme de bonne foi aux obligations législatives.

#### À PROPOS DE PRACTICAL LAW

Practical Law offre un savoir-faire juridique qui donne aux avocats un meilleur point de départ. Notre équipe spécialisée d'avocats rédacteurs crée et tient à jour des milliers de ressources utiles dans tous les grands champs de pratique. Nous repoussons les limites de la recherche législative et juridique classique pour vous procurer les ressources nécessaires à une pratique plus efficace, à l'amélioration de votre service à la clientèle et à l'ajout de valeur.

Si vous n'êtes pas déjà abonné, nous vous invitons à faire l'essai de nos services en ligne, à l'adresse [legalsolutions.com/practical-law](https://legalsolutions.com/practical-law). Pour plus d'information ou planifier une formation, appelez le 1-800-733-2889 ou écrivez à [referenceattorneys@tr.com](mailto:referenceattorneys@tr.com).

02-19

© 2019 Thomson Reuters. Tous droits réservés. L'utilisation des sites Web et des services de Practical Law est assujettie aux conditions d'utilisation (<http://static.legalsolutions.thomsonreuters.com/static/agreement/westlaw-additional-terms.pdf>) et à la politique de confidentialité (<https://a.next.westlaw.com/Privacy>).

## À propos de Stikeman Elliott

Stikeman Elliott est un chef de file mondial en droit des affaires canadien et la référence des entreprises canadiennes et des sociétés étrangères exploitant leurs activités au Canada. Nos bureaux sont situés à Montréal, Toronto, Ottawa, Calgary, Vancouver, New York, Londres et Sydney. Nous offrons des conseils hautement stratégiques et innovateurs à nos clients et leur proposons des solutions concrètes. Le cabinet possède un bilan exceptionnel en matière d'opérations transfrontalières aux États-Unis et à l'échelle internationale dans des dossiers multiterritoriaux d'envergure et est un chef de file dans ses principaux champs de pratique, notamment les fusions et acquisitions, les valeurs mobilières, le litige commercial, le droit bancaire et le financement, la concurrence et les investissements étrangers, la fiscalité, les restructurations, l'énergie, le droit minier, l'immobilier, le développement de projets, l'emploi et travail et les régimes de retraite.

Pour plus d'information sur Stikeman Elliott, consultez notre site Web au [www.stikeman.com](http://www.stikeman.com).

### Contactez-nous

**Shawn Smith**

sasmith@stikeman.com

**Wesley Ng**

wng@stikeman.com

Suivez-nous



Abonnez-vous aux publications sur divers sujets juridiques provenant de la section Notre savoir de Stikeman Elliott à [stikeman.com/fr-ca/savoir](http://stikeman.com/fr-ca/savoir)

---

Cette publication a pour but de donner des renseignements généraux sur des questions et des nouveautés d'ordre juridique à la date indiquée. Les renseignements en cause ne sont pas des avis juridiques et ne doivent pas être traités ni invoqués comme tels. Veuillez prendre connaissance de notre avis de non-responsabilité complet à <https://www.stikeman.com/fr-ca/avis-juridique>.

Stikeman Elliott LLP

Montréal Toronto Ottawa Calgary Vancouver New York London Sydney

**Stikeman Elliott**