

# Confidentialité des données et sécurité de l'information

---

GRI 205-2; GRI 418-1

SASB: TC-TL-220a.1-2-3-4; TC-SI-220a.1-2-3-4; TC-TL-230a.1-2-3-4; TC-SI-230a.1-2-3-4

Nos clients, les membres de notre équipe et les investisseurs s'attendent à ce que nous fassions la preuve que nous recueillons les données de façon appropriée, les utilisons à des fins qui servent leurs intérêts et en assurons la protection. Notre approche de gouvernance de données englobe la protection et l'utilisation appropriée des données tout au long de leur cycle de vie, et nous considérons la gouvernance de données comme un facteur primordial à considérer dans toutes nos décisions relatives aux initiatives commerciales et aux technologies.

Le conseil d'administration de BCE Inc. a adopté une politique plus rigoureuse en matière de gouvernance de données en 2020, laquelle réunit les multiples politiques et programmes que nous avons mis en place dans les domaines interreliés de la protection de la vie privée, de la sécurité de l'information, de la gestion de l'accès aux données et de la gestion des dossiers. Tous les membres de l'équipe doivent suivre la formation obligatoire sur la gouvernance des données dans le cadre de leur formation et de leur révision du code de conduite en 2021. Nous avons également créé un site interne de gouvernance des données pour centraliser les ressources et répondre aux questions fréquemment posées aux membres de l'équipe. En 2022, nous avons continué d'examiner et de rationaliser notre inventaire de données.

# Confidentialité

## POURQUOI EST-CE IMPORTANT GRI 103

La sensibilisation des clients à l'importance de protéger leurs renseignements personnels et par leur les préoccupations utilisation de nos services en matière de protection de vie privée ont augmenté. Cela a conduit les législateurs et des organismes de réglementation. Des modifications aux lois sur la protection de la vie privée ont été proposées dans plusieurs juridictions canadiennes. L'utilisation, la collecte et la divulgation de renseignements personnels au Canada ont également fait l'objet d'une surveillance réglementaire accrue. Nos efforts constants dans ce domaine s'alignent sur notre impératif stratégique visant à promouvoir l'expérience

## CE QUE NOUS FAISONS

Nous apprécions la confiance que nous accordent nos clients en communiquant leurs renseignements personnels. Nous nous efforçons de faire preuve de transparence au sujet de nos pratiques en matière de protection de la vie privée et à rendre des comptes quant à la façon dont nous recueillons, utilisons et divulguons des renseignements personnels. Notre politique de confidentialité définit les informations que nous collectons, comment et pourquoi nous les collectons, les utilisons et parfois les divulguons, comment et quand nous pouvons demander le consentement éclairé de nos clients, comment les clients peuvent accéder à leurs informations personnelles et comment ils peuvent nous contacter s'ils ont des questions ou des préoccupations.

## Notre engagement en matière de protection de la vie privée

1. Nous nous engageons à vous rendre compte de la manière dont nous recueillons, utilisons et divulguons vos renseignements personnels.
2. Nous vous informerons des façons dont vos renseignements personnels sont recueillis, utilisés ou divulgués. Nous pouvons le faire en vertu de notre politique sur la protection de la vie privée, de nos conditions d'utilisation ou de nos sites Web.
3. Nous recueillons, utilisons ou divulguons vos renseignements personnels seulement si nous avons votre consentement ou dans des situations où votre consentement n'est pas nécessaire (comme une situation d'urgence)
4. Nous ne recueillons vos renseignements personnels que de manière juste et légale. Nous limitons la collecte de vos renseignements personnels aux fins qui vous ont été communiquées à l'avance.

5. Nous utilisons ou divulguons vos renseignements personnels pour les raisons pour lesquelles ils ont été recueillis, dans la mesure permise ou requise par la loi.
6. Nous corrigeons vos renseignements personnels lorsque vous nous informez d'erreurs ou que des mises à jour sont requises.
7. Nous faisons de notre mieux pour protéger vos renseignements personnels et nous nous assurons d'utiliser des mesures de protection physiques, techniques et administratives appropriées en fonction de la sensibilité de l'information. Si nous transférons vos renseignements personnels à nos fournisseurs, nous veillons à ce qu'ils soient protégés adéquatement.
8. Nous mettons à votre disposition de l'information sur nos politiques et pratiques en matière de gestion de l'information.
9. Nous vous donnerons accès aux renseignements personnels que nous détenons à votre sujet sur demande écrite, à moins que la loi ne l'interdise.
10. Nous sommes là pour vous écouter et vous aider. Pour toute préoccupation, veuillez nous écrire à l'adresse [privacy@bell.ca](mailto:privacy@bell.ca).

Bell et ses compagnies affiliées se concentrent depuis longtemps sur le maintien de l'exactitude, de la confidentialité, de la sécurité et de la confidentialité des renseignements personnels des clients et des membres de l'équipe. Pour ce faire, nous utilisons des mesures de protection techniques et administratives adaptées à la sensibilité de l'information. Lorsque nous prenons connaissance d'une atteinte présumée à la vie privée, nous suivons des protocoles stricts pour enquêter et évaluer le problème et, s'il y a lieu, élaborer et mettre en œuvre des stratégies d'atténuation afin d'éviter qu'une telle situation ne se reproduise à l'avenir. Depuis le 1er novembre 2018, la loi nous oblige également à signaler au [Commissariat à la protection de la vie privée du Canada](#) toutes les atteintes à la vie privée qui présentent un « risque réel de préjudice important » pour les personnes touchées. En 2022, nous avons mis à jour nos outils de suivi des atteintes pour améliorer nos capacités de production de rapports internes et externes.

Chaque année, tous les membres de l'équipe de Bell doivent examiner et signer individuellement le [Code de conduite commerciale de Bell](#).

## Consentement de l'utilisateur et objectif de la collecte de données

La politique de Bell sur la protection de la vie privée explique comment et quand nous recueillons, utilisons et divulguons des renseignements personnels, y compris la façon dont nous partageons des renseignements personnels au sein du groupe d'entreprises Bell.

Nous recueillons des renseignements personnels avec le consentement du client et précisons clairement la raison pour laquelle les renseignements recueillis sont utilisés. Nous ne conservons que la quantité d'information nécessaire aux fins pour lesquelles elle a été obtenue. Nous ne conservons ces renseignements qu'aussi longtemps que nécessaire ou que la loi l'exige.

De plus, Bell ne divulgue pas les renseignements confidentiels d'un client à des organismes gouvernementaux, à moins qu'ils ne soient requis ou autorisés par la loi (comme lorsqu'il est nécessaire d'enquêter sur la violation d'une loi ou de prévenir la fraude et de sécuriser nos réseaux) ou en cas d'urgence où il y a un danger imminent pour la vie ou la propriété. Pour consulter notre rapport sur la transparence des demandes d'accès légal, veuillez consulter l'annexe 1 à la fin du présent document.

Notre politique de confidentialité, y compris les réponses aux questions fréquemment posées, est disponible sur notre site Web [La protection de la vie privée chez Bell](#).

### Formation des membres de l'équipe et outils de protection de la vie privée

Nous fournissons aux membres de notre équipe des renseignements et une formation continue sur l'importance de respecter la confidentialité des renseignements personnels de nos clients et des membres de l'équipe. Nous publions des renseignements sur notre site intranet qui définissent clairement les rôles, les processus, le support de formation et plus encore. En 2021, nous avons mis en œuvre une formation obligatoire sur la gouvernance des données pour tous les employés dans le cadre de notre programme de formation semestriel sur le Code de conduite.

En 2022, Bell a continué d'investir considérablement dans le personnel, les processus et la technologie afin de protéger les renseignements personnels et confidentiels contre l'évolution des cybermenaces et d'améliorer nos capacités de gestion de la confidentialité et de production de rapports. Les membres de l'équipe et les clients sont également en mesure de répondre aux questions sur la protection de la vie privée et d'obtenir le soutien de l'équipe Protection de la vie privée de Bell par l'intermédiaire de notre boîte Vie privée, qui fait constamment l'objet d'une surveillance.

### Nombre de plaintes non résolues et fondées en matière de protection de la vie privée déposées auprès du Commissariat à la protection de la vie privée du Canada

2022	2021	2020
0	0	0

---

## Sécurité de l'information

### **POURQUOI C'EST IMPORTANT GRI 103**

Notre industrie, comme beaucoup d'autres, est soumise à des cybermenaces constantes. Nous devons être en mesure d'identifier et de traiter les risques de sécurité de l'information en temps opportun afin de protéger les systèmes et les renseignements et de contribuer à la réalisation de notre impératif stratégique pour promouvoir l'expérience client. Éviter des incidents importants liés à la sécurité de l'information peut également limiter l'augmentation des dépenses associées aux mesures correctives et aux responsabilités juridiques, ce qui est conforme à notre impératif stratégique de gérer avec agilité et selon une structure de coûts efficace.

### **CE QUE NOUS FAISONS**

Nous nous efforçons de protéger la sécurité de nos systèmes et les données de nos clients. Pour ce faire, nous mettons en œuvre des programmes de prévention, de détection et d'intervention liés aux menaces à la sécurité. Alors que nous offrons de la formation continue aux membres de l'équipe sur la protection des données, nous continuons également de contribuer à définir les pratiques de l'industrie en matière de sécurité et de gestion des risques.

### ***Notre objectif en matière de sécurité de l'information :***

***Être reconnu comme le leader de la sécurité de l'information dans notre industrie et comme partenaire de confiance pour nos clients.***

Chez Bell, nous cherchons à protéger nos réseaux, nos systèmes, nos applications, ainsi que les renseignements personnels qu'ils contiennent contre toute menace, notamment les cyberattaques, les accès non autorisés, les dommages causés par les incendies, et les catastrophes naturelles et autres événements. Nous nous efforçons de protéger la compétitivité des entreprises canadiennes qui utilisent les services de Bell en nous efforçant de maintenir la sécurité et la stabilité du réseau. Nous procédons à des investissements continus pour améliorer la performance et la disponibilité de nos services et de nos réseaux, et nous déployons des couches de contrôles de sécurité pour nous protéger contre les cybermenaces.

Les menaces à la cybersécurité continuent d'évoluer au fur et à mesure que de nouvelles technologies comme la 5G, l'informatique en nuage et l'IdO apparaissent. Le programme de sécurité de l'information de Bell traite de la confidentialité, de l'intégrité et de la disponibilité des technologies existantes et émergentes. L'intégration d'une attitude axée sur la sécurité et de protections appropriées dans tout ce que nous faisons décrit l'approche de sécurité dès la conception de Bell.

## Surveillance

Tous les membres du conseil de BCE ont la responsabilité d'identifier et de surveiller les principaux risques auxquels nos activités sont exposées et de chercher à assurer l'existence de processus qui visent à les identifier, les contrôler et les gérer de façon efficace. Bien que le conseil assume une responsabilité pleine et entière à l'égard du risque, il délègue la responsabilité de certains éléments du programme de surveillance des risques à des comités du conseil. Cela garantit que ces éléments (signalés au conseil régulièrement) sont traités avec une expertise, une attention et une diligence appropriées. Le comité du risque et de la caisse de retraite de BCE est responsable de la surveillance des risques et de la stratégie liés à la sécurité de l'information de Bell.

Les dirigeants des unités d'affaires opérationnelles jouent un rôle central dans l'identification et la gestion proactives des risques au quotidien. Les dirigeants des unités d'affaires ont accès à plusieurs groupes de soutien de l'entreprise qui offrent une expertise indépendante pour renforcer la mise en œuvre des méthodes de gestion des risques.

Le groupe Sûreté de l'entreprise est responsable de tous les aspects de la sécurité. Nos professionnels de la Sûreté de l'entreprise ont une compréhension approfondie de l'entreprise, de l'environnement de gestion des risques et de l'environnement des intervenants externes, et ils établissent les normes pour l'entreprise dans nos politiques de sécurité et surveillent le rendement de l'entreprise par rapport à ces exigences. Ils collaborent également avec les dirigeants des unités d'affaires opérationnelles pour élaborer des stratégies et des plans d'action visant à atténuer les risques.

BCE a mis sur pied un Comité de surveillance de la santé et sécurité, de la sûreté, de l'environnement et de la conformité (comité de SSSEC), qui comprend plusieurs de nos plus hauts dirigeants, afin de superviser les progrès dans l'ensemble du programme de sécurité stratégique de BCE (y compris la sécurité de l'information).

Pour en savoir plus sur la culture de gestion des risques de Bell, consultez la section Gouvernance d'entreprise et gestion du risque de notre [Rapport annuel intégré](#).

## Cadre, politiques et certification

Afin de protéger les actifs existants, nous avons élaboré un cadre fondé sur les pratiques exemplaires et normes de l'industrie, y compris, mais sans s'y limiter, celles du Forum de la sécurité informatique, de l'Organisation internationale de normalisation (ISO), du National Institute of Standards and Technology (NIST) et des Normes de sécurité des données du secteur des cartes de paiements (SCP). Ce cadre comprend 10 piliers stratégiques en matière de sécurité de l'information et est soutenu par une série de politiques, de directives et de normes qui définissent les contrôles de sécurité pour protéger nos actifs et nos données.

En 2021, nous avons procédé à une évaluation externe du système et de la stratégie de gestion de la sécurité de l'information (SGSI) de Bell, renforçant ainsi notre conformité aux pratiques exemplaires et le leadership de l'industrie. Nous avons évalué et harmonisé 80 % de nos SGSI par rapport à la norme ISO, dans le but d'harmoniser nos SGSI à la norme ISO 27001 et d'obtenir la certification d'ici la fin de 2023. Nous procédons déjà à des vérifications de contrôle de l'organisme de services (SOC 1 et 2) sur certains services à l'échelle de Bell afin de garantir de manière indépendante la sécurité, la disponibilité et les contrôles de confidentialité à nos clients.

Nous nous appuyons sur un processus d'assurance robuste pour évaluer les projets, cerner les risques et établir des plans d'action afin de nous assurer que les systèmes sont déployés avec le niveau de sécurité approprié. En raison du caractère évolutif et de la sophistication des menaces à la sécurité de l'information partout dans le monde, nous adaptons rapidement nos politiques et procédures de sécurité.

### Piliers de la sécurité de l'information de Bell

1. Gestion et visibilité des actifs
2. Contrôle d'accès et authentification
3. Développement et exploitation de systèmes sécurisés
4. Sécurité des applications, du réseau et des points d'extrémité
5. Essais de sécurité
6. Politiques, exigences et hiérarchisation des risques
7. Gestion des risques liés aux fournisseurs
8. Compétences, éducation et sensibilisation en matière de sécurité
9. Renseignements sur les cybermenaces et détection de celles-ci
10. Intervention et reprise après incident



## Menaces et incidents

Nous avons une équipe interne de renseignements sur les cybermenaces qui détecte les menaces auxquelles Bell et nos clients sont exposés et qui complète les renseignements que nous recueillons d'autres sources de l'industrie. Par exemple, Bell est un membre fondateur de l'Échange canadien de menaces cybernétiques ([CCTX](#)), un forum national multisectoriel sur les menaces où les professionnels de la sécurité échangent des renseignements sur les menaces concrètes et des mesures d'atténuation avec leurs pairs.

En 2022, un incident de cybersécurité s'est produit au sein de Bell Solutions techniques, et certains renseignements opérationnels sur l'entreprise et les employés ont été consultés. L'incident a été divulgué sur le site Web de Bell, un rapport d'atteinte à la vie privée a été déposé auprès du Commissaire à la protection de la vie privée du Canada, et les employés et clients concernés ont été avisés. Il n'y a pas eu d'enquêtes réglementaires ou de poursuites judiciaires à ce jour, réelles ou menacées.

## Sensibilisation et formation

La formation sur la sécurité de l'information a toujours fait partie de l'intégration des membres de l'équipe et de la formation obligatoire chez Bell.

En février 2021, nous avons lancé notre programme de formation sur la sécurité de l'information Soyez cyberavisé. Ce programme de formation comprend l'intégration à notre plateforme spécialisée Soyez cyberavisé et la réalisation de simulations d'hameçonnage. Le programme comprend quatre cours que les membres de l'équipe ont un an pour suivre une fois qu'ils sont intégrés. Ce programme élargit la formation obligatoire pour les membres de l'équipe et leur offre un catalogue complet de modules d'apprentissage pour une sensibilisation générale. En plus de la sensibilisation générale, elle renforce également les principes de sécurité dès la conception. Nous avons intégré 100 % des membres de l'équipe ciblés en 2022, et nous prévoyons que les membres de l'équipe termineront le cycle de formation d'ici la fin de 2023. En date du 31 décembre 2022, 88 %<sup>1</sup> des membres ciblés ont terminé le programme de formation complet. Nous avons ajusté l'objectif d'achèvement de la formation pour que 90 % des membres de l'équipe intégrés suivent la formation annuelle sur la sécurité de l'information Soyez cyberavisé. Notre taux de rapports de simulation d'hameçonnage

---

<sup>1</sup> PwC a produit une attestation d'assurance de portée restreinte à l'égard de notre indicateur de 2022. Veuillez consulter [l'énoncé d'assurance de PwC](#).

de 2022 est de 25 %<sup>2</sup>, et nous avons observé une augmentation de 155 % des simulations d'hameçonnage signalées par des employés pleinement formés par rapport aux employés non formés. Ces initiatives favorisent une culture de cybersécurité plus forte et une meilleure sensibilisation aux risques en matière de cybersécurité.

---

<sup>2</sup> PwC a produit une attestation d'assurance de portée restreinte à l'égard de notre indicateur de 2022. Veuillez consulter [l'énoncé d'assurance de PwC](#).

## Clients

Conformément à la position de Bell en tant que chef de file de longue date en matière de prestation de services de sécurité aux entreprises et organisations canadiennes, notre service géré de sécurité de l'IdO fournit une sécurité complète pour protéger les réseaux et les systèmes de nos clients lorsqu'ils adoptent les technologies IdO.

Notre gamme de services de sécurité est surveillée par le Centre de gestion de la sécurité de Bell, une équipe de professionnels de la sécurité qui assure la gestion des incidents, des politiques de gestion et la production de rapports sur tous les incidents liés à la sécurité en tout temps.

## Fournisseurs

### Diligence raisonnable des fournisseurs

Nous avons un vaste programme d'assurance des mesures de sécurité des fournisseurs qui évalue les partenaires tiers de plusieurs façons. Nous nous efforçons de comprendre les opérations des fournisseurs et la maturité de la sécurité afin de nous assurer que le développement des services et des produits se fait de façon sécuritaire; nous tirons parti des outils de l'industrie et des évaluations des fournisseurs pour évaluer les risques. Enfin, nous atténuons les risques en évaluant comment les fournisseurs accèdent à nos systèmes et à nos renseignements afin de mettre en place les contrôles appropriés.

### Exigences contractuelles

Les sous-traitants de données tiers sont tenus de mettre en œuvre des mesures adéquates pour assurer la sécurité de l'information. Nous tenons les fournisseurs responsables au moyen de clauses contractuelles qui exigent que les contrôles appropriés soient mis en place pour protéger les données et les systèmes de Bell.

Lorsqu'un fournisseur gère des renseignements confidentiels qui appartiennent à une entreprise de Bell, à un client de Bell ou à un des membres de notre équipe, il doit respecter toutes les lois applicables sur la protection de la vie privée du territoire où il se trouve, ainsi que les obligations contractuelles énoncées dans l'entente. Bell se réserve le droit d'évaluer et de surveiller les pratiques des fournisseurs en matière de protection de la sécurité de l'information. Les fournisseurs doivent immédiatement aviser Bell de toutes les atteintes à la vie privée réelles ou suspectes, des incidents de sécurité de l'information ou des pertes de données de Bell, et le fournisseur doit aider Bell à gérer les conséquences de ces événements.

## Collaboration et partenariats externes

En tant que membre du chapitre canadien du Forum de la sécurité informatique, un organisme à but non lucratif dirigé par ses membres, Bell contribue à l'évolution des pratiques de sécurité et de gestion des risques. Nous respectons également diverses normes et cadres de sécurité internationaux, entre autres la norme de bonnes pratiques du Forum de la sécurité informatique, le cadre NIST et les normes de sécurité des données du secteur des cartes de paiement (normes PCI).

Bell est un membre fondateur de l'Échange canadien de menaces cybernétiques (CCTX), qui vise à aider les organisations publiques et privées à partager de l'information sur les cybermenaces et l'atténuation dans divers secteurs d'activité au Canada. Bell est également un membre fondateur du Comité consultatif canadien pour la sécurité des télécommunications (CCCST), où nous travaillons ensemble pour favoriser l'adoption de pratiques exemplaires et améliorer la sécurité et la résilience du monde connecté du Canada avec d'autres fournisseurs canadiens de services de télécommunications, ministères et organismes d'application de la loi.

Bell est reconnue comme un chef de file canadien en matière de sécurité par IDC Canada. IDC Canada évalue les fournisseurs de services de sécurité en fonction de leurs capacités actuelles et de leurs stratégies futures pour la prestation de services de sécurité. Le leadership de Bell a été reconnu dans les rapports d'IDC Canada de 2015, 2016, 2017, 2018, 2019 et 2022.<sup>3</sup>

Nous visons également à aligner notre programme sur la norme ISO 27001 d'ici la fin de 2023.

---

<sup>3</sup> [IDC MarketScape : Rapport d'évaluation des fournisseurs canadiens de services de sécurité de 2022.](#)

# Rapport sur la transparence des demandes d'accès légal de 2022

Bell ne divulgue des renseignements confidentiels sur les clients aux autorités policières ou organismes gouvernementaux que lorsqu'elle est expressément tenue de le faire par une autorité compétente ou s'il s'agit d'un cas d'urgence menaçant la vie, la santé ou la sécurité d'une personne. Vous trouverez ci-dessous un sommaire des demandes auxquelles Bell a répondu en 2021.

## Demands des autorités judiciaires et des agences gouvernementales

	NOMBRE DE DEMANDES	NOMBRE DE CLIENTS <sup>4</sup>	REMARQUES
URGENCES OU CIRCONSTANCES PRESSANTES (Y COMPRIS POUR SOUTENIR LES APPELS AU 9-1-1)	59,463.00	60,106.00	Divulgations faites pour aider les autorités publiques dans des situations impliquant une menace grave ou imminente pour la vie ou les biens sans l'autorisation d'un juge. (Régies par les dispositions pertinentes du Code criminel, y compris les articles 184.1, 184.4 et 487.11, , et autre lois pertinentes et, règles de common law)

<sup>4</sup> Nombre de clients divulgué; basé sur le nombre de clients concernés

DEMANDES LÉGISLATIVES	496	1206	Demands auxquelles les destinataires sont contraints de répondre faites par des organismes gouvernementaux en vertu de l'autorité expresse des lois fédérales ou provinciales
	324	36,844	Renseignements de base sur l'abonné <sup>5</sup>
ORDONNANCE DE LA COUR/ MANDAT	9,899	15,320	Divulgations effectuées conformément aux ordonnances de communication, aux citations à comparaître, aux assignations à comparaître et aux mandats de perquisition émis par un juge ou un autre officier de la justice
	7	18	Demands d'agences étrangères (ordonnées par le tribunal), p. ex., Loi sur l'assistance mutuelle dans les affaires pénales
	36,775	470,041	Renseignements de base sur l'abonné <sup>2</sup>

<sup>5</sup> Les renseignements essentiels sur l'abonné font référence au nom et à l'adresse du client et/ou à l'identification du fournisseur de services.

## Services tarifés du Conseil de la radiodiffusion et des télécommunications canadiennes<sup>6</sup>

	Nombre de demandes	Nombre de clients <sup>7</sup>	Commentaires
Agences gouvernementales	1352	2462	Renseignements publics essentiels sur l'abonné pour une ligne sur fil ou l'identification d'un fournisseur de services
Organismes d'application de la loi	17222	34830	Renseignements publics essentiels sur l'abonné pour une ligne sur fil ou l'identification d'un fournisseur de services

**Ordonnances rejetées ou contestées** : Nous ne faisons pas le suivi des ordonnances rejetées ou contestées. Notre processus et notre pratique de gouvernance en matière d'accès légal consistent à valider toutes les demandes et à collaborer avec la partie demanderesse pour réduire la portée ou à retirer la demande si elle est jugée trop vaste ou invalide.

**Divulgarion volontaire** : Bell ne divulgue pas volontairement des renseignements personnels à moins qu'elle ne participe à une enquête sur un manquement aux lois canadiennes (p. ex. un crime contre Bell). Une telle divulgation, le cas échéant, est faite conformément à la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), y compris l'alinéa 7(3)(d).

<sup>6</sup> Référence aux tarifs du CRTC : [Requêtes tarifaires \(8740\) | CRTC](#)

Tarifs généraux de Bell Canada : [Tarifs de Bell Canada | BCE Inc.](#)

Article 2175 – Nom et adresse du client : [2175.pdf \(bce.ca\)](#)

Article 2177 – Identification du fournisseur de services : [2177.pdf \(bce.ca\)](#)

<sup>7</sup> Nombre de clients divulgué; basé sur le nombre de clients concernés

*Si cette fiche d'information contient des déclarations prospectives, y compris sur nos perspectives commerciales, plans, objectifs, cibles, buts, priorités stratégiques, engagements, ainsi que d'autres déclarations qui ne renvoient pas à des faits historiques, ces déclarations ne représentent pas une garantie du rendement ni des événements futurs, et nous mettons en garde le lecteur contre le risque que représente le fait de s'appuyer sur ces déclarations prospectives. Les déclarations prospectives sont l'objet de risques et d'incertitudes et reposent sur des hypothèses donnant lieu à la possibilité que les résultats ou les événements réels diffèrent de façon significative des attentes exprimées ou sous-entendues dans ces déclarations prospectives. Veuillez consulter le dernier rapport de gestion annuel de BCE Inc., mis à jour dans les rapports de gestion trimestriels ultérieurs de BCE Inc., pour obtenir plus d'information au sujet de ces risques, incertitudes et hypothèses. Les rapports de gestion de BCE Inc. sont disponibles sur son site Web à [bce.ca](http://bce.ca), sur SEDAR à [sedar.com](http://sedar.com) et sur EDGAR à [sec.gov](http://sec.gov).*