Gouvernance des données

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 avions 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.

Confidentialité

POURQUOI C'EST IMPORTANT GRI 103

La sensibilisation des clients à l'importance de protéger leurs renseignements personnels et les préoccupations en matière de protection de la vie privée suscitées par leur utilisation des services sans fil, Internet et de courriel, en particulier, continuent d'augmenter. Cela a attiré l'attention des 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 client.

CE QUE NOUS FAISONS

Nous apprécions la confiance que nous accorde 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 nous nous engageons à rendre des comptes quant à la façon dont nous recueillons, utilisons et divulguons des renseignements personnels. Notre politique sur la protection de la vie privée indique les renseignements que nous recueillons, les raisons pour lesquelles nous les recueillons, la façon dont nous les utilisons et les personnes avec qui nous pouvons les partager, y compris la façon dont nous partageons les renseignements au sein du groupe d'entreprises Bell.

Bell et ses sociétés affiliées veillent depuis longtemps à garantir l'exactitude, la confidentialité, la sécurité et la protection des renseignements personnels des membres de leurs équipes respectives et des clients. Nous utilisons des mesures de protection techniques et administratives adaptées au caractère sensible des renseignements. Lorsque nous sommes informés d'une atteinte présumée à la vie privée, nous suivons des protocoles stricts pour enquêter sur le problème et l'évaluer, s'il y a lieu, pour élaborer et mettre en œuvre des stratégies d'atténuation afin d'éviter qu'une telle situation ne se reproduise. Depuis le 1er novembre 2018, nous sommes également tenus par la loi de signaler au **Commissariat à la protection de la vie privée du Canada** toute atteinte à la vie privée présentant un « risque réel de préjudice important » pour les individus concernés.

Chaque année, tous les membres de l'équipe Bell doivent lire et signer individuellement le **Code de conduite de Bell** afin de souligner l'importance de protéger les renseignements des clients et de ne les utiliser que dans le cadre de notre politique sur la protection de la vie privée.

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

La Politique de Bell sur la protection de la vie privée explique clairement comment et quand nous recueillons, utilisons et divulguons des renseignements personnels, y compris la façon dont nous partageons des renseignements au sein du groupe d'entreprises Bell. Nous expliquons également ce qui est considéré comme des renseignements personnels et ce qui ne l'est pas.

Nous recueillons des données personnelles uniquement avec le consentement du client et nous précisons clairement les fins pour lesquelles elles sont recueillies. Les clients ont la possibilité de retirer leur consentement à tout traitement supplémentaire de leurs données personnelles au-delà de l'objectif initial de collecte de données.

Nous nous efforçons d'assurer l'exactitude et l'exhaustivité des données personnelles qui figurent dans nos dossiers, de les tenir à jour et de ne conserver que la quantité minimale de données personnelles nécessaires pour atteindre l'objectif défini. De plus, nous ne conservons les données personnelles que pendant le temps nécessaire aux fins pour lesquelles elles ont été obtenues.

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. Nous ne conservons ces renseignements qu'aussi longtemps que nécessaire ou que la loi l'exige.**

Par ailleurs, Bell ne divulgue des renseignements confidentiels sur les clients aux organismes gouvernementaux que si elle est expressément tenue de le faire par une autorité judiciaire ou s'il s'agit d'un cas d'urgence menaçant la vie, la santé ou la sécurité d'une personne. Pour consulter notre rapport sur la transparence des demandes d'accès légal, veuillez consulter l'annexe 1 à la fin du présent document.

Vous trouverez de plus amples renseignements sur notre politique de protection de la vie privée, y compris les réponses à des questions fréquentes, en vous rendant sur notre site Web à la section **La confidentialité chez Bell**.

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

Nous fournissons aux membres de notre équipe les renseignements appropriés sur la protection de la vie privée et nous avons centralisé notre politique et nos ressources sur la protection de la vie privée sur le site Web interne de Bell. Cette politique fournit aux membres de l'équipe des directives claires quant aux responsabilités en ce qui a trait à la protection des renseignements personnels. Nous publions également de l'information sur notre intranet qui définit clairement, entre autres, les rôles, les processus et le soutien à la formation.

En 2020, Bell a continué d'investir des sommes considérables dans les gens, les processus et la technologie afin de protéger les renseignements confidentiels et personnels contre les menaces à la cybersécurité en constante évolution. Dans le cadre d'une initiative plus vaste de l'industrie, nous avons mis en œuvre un nouveau régime de vérification afin d'éviter que les numéros sans fil soient frauduleusement transférés et utilisés pour contourner d'autres protections de sécurité et accéder frauduleusement à des renseignements personnels. Nous fournissons aux membres de notre équipe de l'information et de la formation continue sur l'importance de protéger la vie privée de nos clients et des autres membres de l'équipe. 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 des renseignements personnels de Bell par l'intermédiaire de notre boîte Vie privée, qui fait constamment l'objet d'une surveillance.

Pour en savoir plus sur la protection de la vie privée des clients, consultez le **Rapport 2020 sur notre but et la responsabilité d'entreprise**.

Notre engagement en matière de protection de la vie privée (suite)

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.**

Sécurité de l’information

POURQUOI C’EST IMPORTANT GRI 103

Notre industrie, comme de nombreuses autres industries, est constamment confrontée à des cybermenaces. Nous devons être en mesure d’identifier et de contrer les risques en matière de sécurité de l’information en temps opportun afin de protéger les systèmes et l’information, et de contribuer à l’exécution de notre impératif stratégique visant à 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 engageons à protéger 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 notre 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.

Chez Bell, nous nous efforçons de protéger nos réseaux, nos systèmes, nos applications, ainsi que les renseignements personnels qu’ils contiennent contre toute menace telle que les cyberattaques, les accès non autorisés, les dommages causés par les incendies, et les catastrophes naturelles et autres événements. Nous mettons tout en œuvre pour 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 robuste programme de sécurité de l’information de Bell traite de la confidentialité, de l’intégrité et de la disponibilité des technologies existantes, ainsi que des technologies 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.

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.

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 identifier, à contrôler et à gérer les risques 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 sont traités avec une expertise, une attention et une diligence appropriées, et ces comités tiennent le conseil informé dans le cours normal des affaires. Le comité du risque et de la caisse de retraite de BCE est responsable de la surveillance des risques et de la stratégie liée 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 d'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**.

Cadre, politiques et certification

Pour protéger les actifs existants, nous avons élaboré un cadre basé sur les meilleures pratiques et normes de l'industrie, y compris, sans s'y limiter, celles du Forum de la sécurité informatique, de l'Organisation internationale de normalisation (ISO) et de l'Institut national des normes et de la technologie. (NIST). 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 (SGI) de Bell, renforçant ainsi notre conformité aux meilleures pratiques et le leadership de l'industrie. Nous évaluons actuellement nos systèmes de gestion de la sécurité de l'information par rapport à la norme ISO dans le but d'harmoniser nos SGI avec la norme ISO 27001. 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.

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. Cependant, dans le cadre de notre évolution, nous avons lancé notre programme Soyez cyberavisé en 2020. 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, le programme Soyez cyberavisé ciblera les rôles techniques à l'échelle de l'entreprise avec une formation spécifique à la sécurité qui sera lancée en 2021, renforçant les principes de sécurité dès la conception.

Le programme Soyez cyberavisé a déjà été offert à 20 % des employés et nous nous attendons à ce qu'il soit offert à tous les membres de l'équipe ciblés d'ici la fin de 2021.

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 du fournisseur 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 la norme de sécurité des données de l'industrie des cartes de paiement (norme 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 (CSTAC), 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.

Annexe 1 : Rapport sur la transparence des demandes d'accès légal de 2020

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 résumé des demandes auxquelles Bell a répondu en 2020.

Demandes des autorités judiciaires et des agences gouvernementales

	NOMBRE DE DEMANDES	NOMBRE DE CLIENTS[1]	REMARQUES
URGENCES OU CIRCONSTANCES PRESSANTES (Y COMPRIS POUR SOUTENIR LES APPELS AU 9-1-1)	**52 008**	**52 603**	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, ainsi que d'autres statuts pertinents et la common law)

[1] Nombre de clients divulgué; basé sur le nombre de clients touchés

DEMANDES LÉGISLATIVES	**560** **412**	**1 187** **38 297**	Demandes auxquelles les destinataires sont contraints de répondre faites par des organismes gouvernementaux en vertu de l'autorité expresse des lois fédérales ou provinciales Renseignements de base sur l'abonné[2]
ORDONNANCE DE LA COUR/ MANDAT	**8 035** **4** **35 627**	**14 687** **4** **467 610**	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 Demandes d'agences étrangères (ordonnées par le tribunal), p. ex., Loi sur l'assistance mutuelle dans les affaires pénales Renseignements de base sur l'abonné[2]

[2] Les renseignements de base 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[3]

	NOMBRE DE DEMANDES	NOMBRE DE CLIENTS[4]	REMARQUES
AGENCES GOUVERNEMENTALES	**1 085**	**4 382**	Renseignements publics de base sur l'abonné pour une ligne sur fil ou l'identification d'un fournisseur de services
ORGANISMES D'APPLICATION DE LA LOI	**12 262**	**37 991**	Renseignements publics de base 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.

Divulgation 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 aux lois pertinentes sur la protection des renseignements personnels, y compris l'alinéa 7(3)(d) de la LPRPDE.

[3]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)**
[4] Nombre de clients divulgué; basé sur le nombre de clients touchés