Commission
d'accès à l'information
du Québec

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC

Dossier : 1005977-S

Nom de l'entreprise : Bell Mobilité

Date : 5 février 2020

Membre : M[e] Diane Poitras

DÉCISION

ENQUÊTE en vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé*[1].

APERÇU

[1] De plus en plus d'entreprises colligent des identifiants, tels que le numéro d'assurance sociale (NAS) ou le numéro de permis de conduire. L'objectif poursuivi par cette collecte est souvent de vérifier l'identité d'une personne.

[2] Toutefois, la Loi sur le privé pose des limites aux renseignements personnels que les entreprises peuvent recueillir. Elles ne peuvent colliger que les renseignements personnels nécessaires à l'objet d'un dossier qu'elles constituent au sujet d'une personne. Par exemple, lorsque la présentation d'une carte avec photo suffit à combler le besoin d'identification d'une personne, il n'est pas nécessaire de recueillir le numéro inscrit sur cette carte ni de la photocopier.

[3] C'est la question soulevée dans la présente décision : Bell Mobilité (l'entreprise) peut-elle recueillir un identifiant parmi le NAS, le numéro de permis de conduire ou le numéro d'une carte de crédit d'un nouveau client à un service postpayé[2] pour prévenir la fraude et le vol d'identité, s'assurer de sa solvabilité ou recouvrer éventuellement des sommes impayées?

---

[1] RLRQ, c. P-39.1, la Loi sur le privé.

[2] Un service postpayé réfère à l'utilisation d'un appareil et/ou de services de l'entreprise qui sont payés après leur utilisation, généralement de façon mensuelle, dans le cadre d'un forfait d'abonnement.

[4] Les identifiants comme le numéro de permis de conduire ou le NAS n'ont pas été créés pour servir d'identifiant universel. La loi ou des directives émises par l'émetteur de ces cartes restreignent d'ailleurs leur utilisation afin de préserver leur confidentialité et, par conséquent, leur fiabilité comme outil de validation de l'identité d'une personne dans un ou des contextes bien précis.

[5] Or, la collecte de plus en plus répandue de ces identifiants par des entreprises pour valider l'identité d'une personne dans d'autres situations que celles envisagées lors de leur création est susceptible d'avoir l'effet inverse, surtout dans le contexte numérique actuel.

[6] Plus ces renseignements sont recueillis et communiqués, plus le nombre de personnes qui y ont accès s'accroît. Cela augmente d'autant les risques de malversations, de vols de renseignements ou d'autres incidents de sécurité et, par conséquent, les risques de fraudes et de vols d'identité susceptibles d'en résulter. La fiabilité de ces renseignements comme moyen d'identifier un individu s'en trouve donc de plus en plus diminuée et les personnes concernées par ces identifiants sont exposées à des préjudices importants.

[7] Dans le contexte actuel, il existe une tension permanente entre la nécessité de prouver son identité de manière robuste et fiable dans un environnement numérique et le fait qu'il est de plus en plus facile de la contrefaire. L'absence de solution d'identification alternative au recours à ces « identifiants » constitue un enjeu important présentement, tant pour les entreprises que pour les citoyens.

[8] C'est dans ce contexte et à la lumière des éléments concrets soumis dans le présent dossier que la Commission d'accès à l'information (la Commission) conclut que la collecte d'un des numéros, au choix du client, parmi le permis de conduire, d'assurance sociale ou de carte de crédit est nécessaire pour permettre à l'entreprise de prévenir la fraude et le vol d'identité pour l'activation d'un service postpayé de l'entreprise.

[9] Toutefois, compte tenu que cette pratique contribue également à augmenter le risque d'atteinte à la protection des renseignements personnels des clients, voire de fraudes et de vols d'identité, la Commission recommande à l'entreprise de poursuivre ses recherches pour trouver un moyen alternatif à cette collecte, particulièrement pour remplacer la collecte du NAS et du numéro de permis de conduire.

[10] L'évolution constante des technologies et des moyens de s'identifier en cette ère numérique permet de croire que des solutions plus respectueuses de

la vie privée des citoyens et plus sécuritaires seront éventuellement à la disposition de l'entreprise.

[11] Le développement de telles solutions pourrait remettre en question la présente conclusion de la Commission quant à la nécessité de la collecte de ces renseignements personnels, dont le NAS et le numéro de permis de conduire.

[12] Dans l'intervalle, l'entreprise doit s'assurer de mettre en place des mesures de sécurité robustes pour assurer la confidentialité de ces renseignements.

CONTEXTE

[13] Les faits à l'origine de la plainte et de l'enquête de la Commission sont les suivants.

[14] Une cliente se présente à une boutique de l'entreprise afin de s'abonner à un service Internet haute vitesse. Voulant vérifier le prix d'un forfait avec l'un des deux produits offerts dans sa région, soit un *Turbo Stick* ou *Turbo Hub*, un représentant de l'entreprise propose d'activer l'appareil.

[15] Pour ce faire, il demande à la cliente de fournir son numéro de permis de conduire, son NAS ou le numéro d'une carte de crédit. Devant le refus de la cliente, le représentant de l'entreprise refuse de lui vendre un forfait Internet haute vitesse.

[16] S'adressant au bureau des plaintes de l'entreprise, la cliente propose une alternative à cette collecte de renseignements personnels : prépayer le *Turbo Hub* et le montant d'un mois de service. L'entreprise refuse et explique qu'elle doit nécessairement procéder à une vérification de crédit avant d'activer un appareil associé à un forfait Internet postpayé.

[17] La cliente porte plainte à la Commission concernant cette pratique relative à la collecte de renseignements personnels.

- **Résumé des motifs de la plainte**

[18] La cliente considère qu'elle ne devrait pas devoir fournir ces renseignements personnels simplement pour obtenir des informations au sujet des forfaits disponibles et leur prix. Elle soutient également qu'ils ne sont pas nécessaires afin de vérifier son crédit : son nom, son adresse et sa date de

naissance suffisent. Elle est cliente de Bell Canada depuis au moins 45 ans[3], a toujours payé ses comptes et habite à la même adresse depuis 32 ans. Compte tenu de ces faits et de son offre de prépayer l'appareil mobile et un mois de service, elle considère qu'il n'était pas nécessaire pour l'entreprise de procéder à une enquête de crédit.

[19] En outre, elle s'inquiète de la conservation et de la communication de ces renseignements par l'entreprise et par toute agence de crédit avec laquelle l'entreprise fait affaire, et ce, sans son consentement. Elle souligne qu'aucune entreprise n'est à l'abri d'erreurs ou d'incidents de sécurité et que le vol d'identité qui peut en résulter est susceptible d'avoir de graves conséquences pour elle. En comparaison, elle considère que les risques pour l'entreprise de faire affaire avec elle sont minimes. À son avis, cette pratique d'exiger des identifiants est abusive et crée les circonstances favorables aux vols d'identité.

- **Résumé de la position de l'entreprise**

[20] Pour sa part, l'entreprise considère avoir le droit de refuser un service postpayé lorsqu'un client ne consent pas à lui communiquer, à son choix, son numéro de permis de conduire, son NAS ou le numéro d'une carte de crédit et qu'il ne consent pas à ce qu'elle procède à une vérification de sa solvabilité.

[21] Elle considère avoir le droit de recueillir ces renseignements qui sont nécessaires aux divers objets du dossier qu'elle constitue au sujet d'un client lors de l'activation d'un service postpayé. Elle procède à diverses vérifications visant à contrer la fraude et le vol d'identité, à s'assurer de la solvabilité du client et à recouvrer des sommes qui lui sont dues à la suite de non-paiement de services ou de matériel.

[22] L'entreprise affirme ne pas exiger de renseignements personnels lorsqu'un client souhaite seulement obtenir des informations au sujet de ses forfaits ou d'un de ses produits ou lorsqu'il achète un produit prépayé.

Avis d'intention et observations de l'entreprise

[23] À la suite de l'enquête de la Commission et d'un avis d'intention de décision défavorable, l'entreprise a pu présenter ses observations, par écrit et en personne. Elle a déposé au dossier plusieurs documents, dont un rapport

[3] L'entreprise souligne que Bell Mobilité et Bell Canada sont deux entreprises distinctes et qu'elle n'a pas accès à l'historique de crédit des clients de Bell Canada lors de l'activation d'un service.

d'expert au sujet de la fraude et du vol d'identité dans l'industrie des télécommunications sans fil. La Commission a pu bénéficier des explications de cet expert en cybercriminalité et de celles du directeur de la sécurité et de l'intégrité de l'entreprise lors d'une rencontre.

OBJET DE LA DÉCISION

[24] La présente décision concerne uniquement les demandes d'activation d'un service mobile postpayé lorsqu'il est demandé par un client présent en boutique. Bien que la situation à l'origine de la plainte soit un service Internet haute vitesse et une clé Turbo, les faits et les observations de l'entreprise ont porté sur ses pratiques concernant l'activation de tout service ou appareil postpayé, celles-ci étant les mêmes, peu importe le service ou l'appareil.

[25] Puisque ce sont ces pratiques de l'entreprise qui font l'objet de la présente décision et non seulement la situation à l'origine de la plainte, la Commission rejette l'affirmation voulant qu'elle n'ait pas contrevenu à la Loi sur le privé du seul fait qu'elle n'a pas recueilli les renseignements personnels de la cliente devant son refus de les fournir. L'entreprise admet qu'elle recueille systématiquement l'un de ces numéros lors de l'activation d'un service postpayé et c'est cette pratique qui fait l'objet de la présente décision.

[26] Ainsi, la Commission doit décider des questions suivantes :

- La collecte des renseignements personnels qu'effectue l'entreprise lors de l'activation d'un nouveau service postpayé est-elle nécessaire aux différents objets du dossier?
- L'entreprise peut-elle refuser d'activer un service postpayé au motif qu'une personne refuse de fournir un renseignement personnel?

[27] Si la Commission conclut que l'entreprise ne respecte pas la Loi sur le privé, elle doit déterminer si cette loi provinciale s'applique à l'entreprise en vertu des principes constitutionnels applicables[4]. En effet, l'entreprise soutient subsidiairement que la Loi sur le privé ne s'applique pas à elle parce que les entreprises de télécommunications sont soumises uniquement à la législation fédérale. Elle invoque également qu'il existe un conflit entre les législations fédérale et provinciale relatives à la protection des renseignements personnels et que la loi fédérale s'applique de façon prépondérante.

[4] L'entreprise a avisé le Procureur général du Québec conformément à ce que prévoit le *Code de procédure civile du Québec* (RLRQ, c. C-25.01).

ANALYSE

Première question : La collecte des renseignements personnels qu'effectue l'entreprise est-elle nécessaire aux différents objets du dossier liés à l'activation d'un nouveau service postpayé?

[28] La Loi sur le privé prévoit qu'une entreprise ne peut recueillir que les renseignements personnels nécessaires à l'objet du dossier qu'elle constitue au sujet d'un individu. Cette obligation vise à minimiser l'atteinte à sa vie privée.

[29] La nécessité de la collecte d'un renseignement personnel s'évalue en fonction de chaque finalité pour laquelle une entreprise envisage l'utiliser, en lien avec l'objet du dossier[5]. L'entreprise doit démontrer que chacun de ces objectifs est légitime, important et réel et que l'atteinte à la vie privée que constitue cette collecte de renseignements personnels est proportionnelle à chacun des objectifs poursuivis.

[30] Cette proportionnalité sera démontrée lorsque l'utilisation projetée est rationnellement liée à chaque objectif, que l'atteinte à la vie privée est minimisée et que la collecte est nettement plus utile à l'entreprise que préjudiciable à la personne concernée[6].

[31] L'entreprise affirme que la collecte de certains renseignements personnels lors de l'activation d'un service postpayé est nécessaire aux fins suivantes :

- **Aux fins d'ouverture d'un dossier** : nom, prénom, date de naissance (le client doit être majeur), adresse actuelle au Canada et numéro de téléphone valide;
- **Aux fins de vérification de l'identité de la personne** : l'entreprise demande de voir une pièce d'identité avec photo, au choix du client, de manière à valider le nom et la date de naissance fournis. Selon les éléments au dossier, l'entreprise ne recueille pas une copie de la pièce d'identité. La collecte des identifiants aux fins de validation de ces informations d'identité par le préposé en boutique n'est pas nécessaire. D'ailleurs, l'entreprise n'a pas soutenu que ce fût le cas;

---

[5] Voir notamment : *Laval (Société de transport de la Ville de)* c. *X.*, [2003] C.A.I. 667 (C.Q.), affaire *Laval*; *Grenier* c. *Centre hospitalier universitaire de Sherbrooke*, [2010] QCCQ 9397; *Synergie Hunt International inc.* c. *Trinque Tessier*, 2017 QCCQ 13747.

[6] Id.

- **Aux fins de prévention et de détection de la fraude et du vol d'identité** : l'entreprise recueille, au choix du client, le NAS, le numéro de permis de conduire ou d'une carte de crédit;
- L'un de ces trois numéros est aussi recueilli **aux fins de vérification de la solvabilité d'un client et du recouvrement de sommes impayées**. Elle procède également à une enquête de crédit.

[32] La Commission ne s'attarde pas aux deux premiers points qui ne sont pas remis en question par la plainte ou l'enquête. Elle examine donc s'il est nécessaire pour l'entreprise de recueillir les renseignements en cause dans le présent dossier pour :

- Informer un client du prix d'un service ou d'un appareil, tel que le soulève la plaignante dans sa plainte;
- Prévenir et détecter la fraude et le vol d'identité;
- Vérifier la solvabilité d'un client et recouvrer des sommes impayées.

1. Évaluation de la nécessité de la collecte pour informer un client du coût d'un produit

[33] L'entreprise convient que la collecte de renseignements personnels n'est pas nécessaire pour informer un client du prix d'un service ou d'un appareil. Elle affirme, déclarations sous serment à l'appui, ne pas exiger de renseignements personnels ni procéder à une enquête de crédit pour fournir de l'information à un client au sujet de ses produits.

[34] Toutefois, c'est ce qui s'est passé dans le cas de la cliente ayant porté plainte à la Commission. Le préposé à la boutique de l'entreprise à laquelle elle s'est présentée lui a proposé d'activer l'appareil convoité afin de vérifier le prix du forfait. Pour ce faire, le représentant de l'entreprise a exigé que la cliente fournisse son numéro de permis de conduire, son NAS ou le numéro d'une carte de crédit afin de procéder à une enquête de crédit. Aussi, lorsqu'elle s'est adressée au service à la clientèle et qu'elle a offert de payer l'appareil mobile et un mois de service, elle n'a pas été informée des alternatives à cette collecte de renseignements ni pourquoi son offre de prépaiement ne pouvait être acceptée.

[35] Force est de constater que la politique de l'entreprise sur cette question n'est pas comprise correctement par tous ses employés de première ligne. Dans ce contexte, la Commission formule la recommandation suivante à l'entreprise :

Recommandation : Faire des rappels réguliers à tous ses employés affectés au service client et à l'activation de nouveaux comptes quant aux contextes qui autorisent la collecte, au choix du client, d'un de ces identifiants (NAS, numéro de carte de crédit ou de permis de conduire) et aux situations dans lesquelles une enquête de crédit peut être effectuée avec le consentement de la personne concernée.

2. Évaluation de la nécessité de la collecte pour prévenir et détecter la fraude et le vol d'identité

[36] Lors de l'activation d'un service ou de l'achat d'un produit sans fil postpayé, l'entreprise recueille, au choix du client, son NAS, le numéro de son permis de conduire ou de sa carte de crédit. Elle affirme vouloir ainsi détecter et prévenir la fraude et le vol d'identité ou de matériel.

[37] **La Commission conclut que ces objectifs sont légitimes, importants et réels. Aussi, dans le contexte actuel, cette collecte est proportionnelle à ces finalités.** L'entreprise pouvait donc recueillir l'un de ces numéros, au choix du client. Voici pourquoi.

- ***Les objectifs de détection et de prévention de la fraude et du vol d'identité et de matériel sont légitimes, importants et réels***

[38] Il ressort de la documentation soumise par l'entreprise et de ses observations que la fraude d'identité et le non-paiement de matériel mobile sont très élevés dans le secteur des télécommunications sans fil. L'entreprise en subit donc des pertes financières considérables. Il s'agit donc d'un problème réel et important.

[39] Aussi, le vol d'identité et la fraude à l'identité sont en croissance constante, notamment selon les données du Centre antifraude du Canada. D'ailleurs, la Gendarmerie royale du Canada considère que la croissance de ces crimes figure parmi l'une des plus rapides au monde.

[40] De plus, la mobilité du service offert par l'entreprise et l'accessibilité des appareils contribuent à faciliter ce genre de fraude. En effet, le service n'est lié à aucune adresse fixe. L'entreprise rappelle que les clients souhaitent repartir de la boutique avec un appareil mobile dont le coût varie d'une centaine à plus de mille dollars. Ces appareils sont également très prisés sur le marché noir.

[41] L'utilisation de ces appareils peut aussi faire grimper rapidement les coûts de services. L'entreprise souhaite donc offrir ce service rapide tout en minimisant ses pertes financières.

[42] C’est donc pour lutter contre ces phénomènes réels et importants que l’entreprise recueille les numéros d’identification précités au sujet d’un nouveau client qui souhaite bénéficier d’un service postpayé.

[43] Il est tout à fait légitime pour l’entreprise de vouloir limiter ses pertes financières en identifiant et en évitant ces tentatives de fraude et de vols. Les éléments concrets et factuels soumis par l’entreprise démontrent qu’il s’agit d’un problème répandu susceptible d’entraîner de lourdes conséquences financières pour l’entreprise. Ces objectifs poursuivis par cette collecte de renseignements personnels sont donc importants et réels.

- ***La collecte du renseignement personnel est proportionnelle aux objectifs de détection et prévention de la fraude et du vol d’identité et de matériel***

  - *Il existe un lien rationnel entre l’objectif poursuivi et la collecte des renseignements personnels*

[44] **D’abord, l’entreprise a démontré à la Commission qu’il existe un lien rationnel entre les objectifs poursuivis et la collecte du NAS, du numéro de permis de conduire ou celui d’une de carte de crédit.**

[45] En effet, le directeur de la sûreté et de l’intégrité de l’entreprise a expliqué à la Commission comment ces numéros sont utilisés pour détecter et prévenir les fraudes d’identité. Ils lui permettent de vérifier dans des banques de données internes et externes les cas identifiés de fraude, de vol d’identité ou des comptes sur lesquels des alertes sont actives. D’autres vérifications permettent de détecter les identifiants invalides ou falsifiés.

[46] Les statistiques soumises par l’entreprise démontrent clairement qu’elle peut détecter et prévenir un nombre important de fraudes et de vols d’identité grâce à la collecte et à l’utilisation de ces renseignements personnels. En fait, bien que ces fraudes puissent parfois être détectées sans ces numéros, ils permettent d’en détecter presque deux fois plus. Leur collecte est donc un moyen efficace pour l’entreprise, dans le contexte actuel, d’atteindre les objectifs poursuivis.

  - *L’atteinte à la vie privée de cette collecte est minimisée*

[47] **Deuxièmement, la Commission considère que l’atteinte à la vie privée que constitue cette collecte de renseignements personnels est minimisée.**

[48] En effet, la Commission comprend que le client peut choisir de ne pas fournir l'un des trois numéros demandés par l'entreprise en prépayant l'appareil et les services ou en donnant un dépôt de sécurité. L'entreprise a affirmé que ces renseignements ne sont pas demandés dans le cas d'un service prépayé.

[49] Aussi, si un client souhaite un service postpayé, l'entreprise ne recueille qu'un seul des numéros au choix du client.

[50] Enfin, des mesures de sécurité sont mises en place afin d'assurer la confidentialité de ces renseignements. Sans toutes les énumérer, en voici quelques exemples :

- Les numéros recueillis sont conservés dans des dossiers sécurisés dont l'accès est limité à certains employés. Ceux-ci suivent une formation complète et en continu sur la confidentialité de ces données et les droits des clients en matière de protection des renseignements personnels;
- Le numéro de carte de crédit est remplacé par de nouvelles données, appelées jetons (tokenisation). L'entreprise ne conserve donc aucun numéro de carte de crédit dans ses systèmes;
- Ces renseignements ne sont utilisés que pour la prévention du vol d'identité et de la fraude, la vérification de la solvabilité des clients et la perception des comptes impayés;
- Chaque année, tous les employés doivent relire et signer un code de conduite qui exige notamment l'utilisation appropriée et la confidentialité des renseignements personnels des clients;
- Des contrôles sont en place afin d'assurer l'utilisation conforme et la confidentialité des renseignements personnels.

[51] Mais surtout, l'entreprise affirme qu'actuellement elle ne dispose pas d'autre moyen que la collecte d'un de ces numéros afin de prévenir ou de détecter efficacement les fraudes d'identité. L'expert confirme cette affirmation. L'entreprise indique avoir évalué d'autres moyens d'atteindre ces objectifs, mais aucun n'est concluant pour l'instant. La seule alternative est de prépayer un appareil et le service, ce qui n'est pas à la portée de tous. L'entreprise affirme être à la recherche constante de nouveaux moyens fiables et efficaces de prévenir et de détecter la fraude et le vol d'identité et de matériel.

- ***La collecte des renseignements personnels est plus utile à l'entreprise qu'elle n'est préjudiciable aux clients***

[52] **Troisièmement, la Commission est d'avis que la collecte de ces numéros est plus utile à l'entreprise qu'elle ne porte préjudice au client.**

[53] Les numéros recueillis permettent à l'entreprise de détecter des milliers de tentatives de fraudes chaque année, et ce, avant de mettre en service des appareils sans fil. Cela lui évite des pertes financières importantes.

[54] Ces fraudes évitées sont aussi bénéfiques pour les personnes susceptibles d'en être victimes, notamment les fraudes d'identité. Si elles n'avaient pas été détectées, les personnes dont l'identité aurait été faussement utilisée auraient probablement dû composer avec les conséquences de cette fraude : prouver que ce ne sont pas elles qui ont acheté ou utilisé les services mobiles, faire modifier l'information erronée auprès de l'entreprise et possiblement des agences de crédit, etc.

[55] Selon l'expert en cybercriminalité et le directeur de la sûreté et de l'intégrité de l'entreprise, même si les entreprises collaborent avec les services de police pour lutter contre les vols et les fraudes à l'identité, les entreprises de télécommunications demeurent en première ligne pour tenter de lutter contre ce phénomène en ce qui concerne leurs services.

[56] Les documents au dossier démontrent qu'un nombre important de fraudes à l'identité ont été évitées par l'entreprise, dont une grande proportion grâce à la collecte et à l'utilisation des numéros en question dans le présent dossier.

[57] La collecte de ces numéros est donc très utile à l'entreprise et aux clients pour lutter contre la fraude et le vol d'identité.

[58] Toutefois, contrairement à ce que soutient l'entreprise, cette collecte est aussi susceptible de porter préjudice aux clients.

[59] Comme le souligne la plaignante, la collecte de plus en plus répandue de ces identifiants par des entreprises est susceptible de compromettre leur confidentialité et, par conséquent, leur fiabilité.

[60] En effet, plus ces renseignements sont recueillis et communiqués par des entreprises, plus le nombre de personnes qui y ont accès augmente. Le nombre de banques de données contenant ces identifiants s'accroît avec chaque nouvelle collecte réalisée par une entreprise ou un organisme public. Cela augmente d'autant les risques de malversations, de vols de renseignements ou d'autres incidents de sécurité et, par conséquent, les risques de fraudes et de

vols d'identité susceptibles d'en résulter. Cela réduit la fiabilité de ces renseignements comme moyen d'identifier un individu.

[61] L'expert entendu dans le présent dossier convient de ce risque. Il considère qu'il est de plus en plus présent dans le contexte de l'environnement numérique et en l'absence de carte d'identité nationale ou de système de gestion de l'identité numérique. Il note une tension permanente entre la nécessité de prouver son identité de manière « robuste » dans un environnement où il est de plus en plus facile de la contrefaire.

[62] D'ailleurs, en ce qui concerne le NAS, le gouvernement du Canada invite les citoyens à protéger ce renseignement confidentiel et à ne jamais l'utiliser comme pièce d'identité[7]. Une section spécifique du site Internet d'Emploi et Développement social Canada rappelle un ensemble de mesures à prendre pour protéger ce renseignement confidentiel. On y indique de ne donner son NAS que lorsque la loi prévoit qu'une organisation a le droit de le recueillir. On y souligne que bien que ce ne soit pas illégal, il est fortement déconseillé de fournir son NAS pour s'identifier ou pour obtenir certains services énumérés, **dont un abonnement à un forfait mobile d'une entreprise de télécommunications**.

[63] Un Code de bonnes pratiques[8] consigne ces recommandations aux citoyens et précise aux entreprises leurs responsabilités concernant le NAS. On y indique qu'une entreprise ne doit jamais utiliser le NAS comme pièce d'identité ou numéro d'identification d'un client. Ce code prévoit aussi que le NAS ne devrait pas être une condition pour l'obtention d'un service ou d'un bien, à moins que la loi ne le prévoie. Toutefois, la loi n'interdit pas présentement ces utilisations.

[64] Invitée à commenter les recommandations de l'organisme émetteur du NAS, l'entreprise considère qu'elle les respecte presque toutes et que plusieurs recommandations ne s'appliquent pas vraiment à elle. Or, la Commission constate qu'il est explicitement prévu sur ce site que le NAS ne devrait pas être recueilli par une entreprise de télécommunications pour l'abonnement à un forfait mobile.

---

[7] Gouvernement du Canada. *Numéro d'assurance sociale – Code de bonnes pratiques*, Septembre 2013, en ligne : https://www.canada.ca/fr/emploi-developpement-social/services/numero-assurance-sociale/rapports/code-pratiques.html

[8] Id.

[65] La Commission rappelle également que le *Code de la sécurité routière*[9] vise à limiter l'utilisation du numéro de permis de conduire. En effet, l'article 61 prévoit que le titulaire d'un permis de conduire n'est tenu de le produire qu'à la demande d'un agent de la paix ou de la Société de l'assurance automobile du Québec et à des fins de sécurité routière uniquement.

[66] Ces mesures visent à limiter la collecte et l'utilisation du NAS et du numéro de permis de conduire aux situations pour lesquelles ils ont été créés ou qui sont expressément prévues par la loi. Elles témoignent de la nature sensible de ces renseignements et des conséquences qui peuvent résulter de leur utilisation inappropriée par des tiers. **La collecte de ces renseignements est donc susceptible d'avoir des effets préjudiciables sur leur titulaire, particulièrement le NAS et le numéro de permis de conduire.** En effet, ils sont beaucoup plus difficiles à remplacer qu'un numéro de carte de crédit en cas d'incident de sécurité.

[67] L'expert souligne qu'il faut considérer le niveau de maturité élevé des entreprises de télécommunications en matière de sécurité. Il considère que les moyens mis en œuvre par les entreprises de ce secteur d'activité sont nettement plus avancés et importants que ceux d'autres entreprises.

[68] La Commission prend surtout en considération le fait que l'entreprise a démontré qu'il n'existe présentement pas d'alternative efficace, portant moins atteinte à la vie privée des clients, pour lui permettre de lutter contre la fraude et le vol d'identité. Le Canada et le Québec ne disposent pas présentement d'un outil permettant à tous les citoyens de s'identifier autre que plusieurs cartes et numéros émis pour être utilisés uniquement dans un contexte précis. De plus, aucune méthode d'authentification liée à ces identifiants n'existe actuellement.

[69] Aussi, comme le souligne l'expert en cybercriminalité, plusieurs moyens actuellement utilisés pour contrer la fraude reposent sur la téléphonie mobile. On peut penser aux messages textes de validation envoyés par les banques, par exemple. Il conclut qu'il s'agit d'une raison supplémentaire pour s'assurer de l'identité du titulaire d'un appareil mobile.

[70] Enfin, tel qu'indiqué précédemment, un certain bénéfice collectif de prévention de la fraude et du vol d'identité résulte de cette collecte par l'entreprise.

---

[9] RLRQ, c. C-24.2.

[71] **Dans ce contexte, force est de conclure que la pratique actuelle de l'entreprise qui consiste à recueillir soit le NAS ou le numéro de permis de conduire ou d'une carte de crédit est proportionnelle aux objectifs de prévention et de détection de la fraude ou du vol d'identité et de matériel**.

Recommandation : La Commission recommande de poursuivre les recherches pour trouver une alternative à la collecte de ces identifiants, particulièrement pour le NAS et le numéro de permis de conduire; le développement d'une autre solution pourrait remettre en question sa conclusion quant à la pratique actuelle de l'entreprise.

[72] En effet, puisque cette pratique contribue également à augmenter le risque d'atteinte à la protection des renseignements personnels des clients, voire de fraudes et de vols d'identité, l'entreprise devrait poursuivre sa recherche d'une solution alternative à la collecte et à l'utilisation de ces identifiants.

[73] L'évolution constante des technologies et des moyens pour s'identifier en cette ère numérique permet de croire que des solutions plus respectueuses de la vie privée des citoyens et plus sécuritaires seront éventuellement à la disposition de l'entreprise. La pertinence et le besoin d'un moyen d'identification fiable à l'ère numérique, qui ne requièrent pas la collecte et la communication de renseignements personnels susceptibles de compromettre cette pièce en cas de vol ou de perte, font de plus en plus l'unanimité au sein de la société, tel qu'en témoigne l'actualité récente.

[74] La Commission insiste sur le fait que le développement de telles solutions pourrait remettre en question sa présente conclusion quant à la nécessité de la collecte de ces renseignements personnels (dont le NAS et le numéro de permis de conduire).

[75] Dans l'intervalle, la Commission recommande fortement à l'entreprise de mettre en place des moyens visant à sécuriser davantage ces identifiants, comme elle le fait pour le numéro de carte de crédit. En effet, le NAS et le numéro de permis de conduire sont des identifiants de nature quasi permanente qui sont difficiles à changer. Il s'agit de renseignements de nature sensible dont la divulgation non autorisée est susceptible de causer préjudice aux personnes qu'ils concernent.

[76] On peut penser à un encryptage ou à d'autres moyens permettant d'éviter leur utilisation ou leur communication en cas d'accès par une personne non autorisée ou ayant des intentions malveillantes.

Recommandation : L'entreprise devrait mettre en place des mesures visant à sécuriser davantage le NAS et le numéro de permis de conduire qu'elle détient au sujet de ses clients.

[77] Compte tenu que la Commission conclut que l'entreprise peut recueillir l'un de ces numéros pour prévenir et détecter la fraude et le vol d'identité ou de matériel, l'entreprise peut-elle aussi l'utiliser pour les autres finalités qu'elle a identifiées dans ses observations?

3. Évaluation de la nécessité de la collecte pour vérifier la solvabilité du client et recouvrer des sommes impayées

[78] Avant l'activation d'un appareil mobile, l'entreprise vérifie la solvabilité du client et si ce dernier lui doit des sommes pour des services antérieurs non payés.

[79] Après l'activation de l'appareil, elle doit parfois recouvrer des montants impayés de certains clients.

[80] **La Commission conclut que ces objectifs sont légitimes, importants et réels. Toutefois, le caractère systématique de cette collecte n'est pas proportionnel à ces finalités.**

[81] En conséquence, l'entreprise ne pourrait recueillir de façon systématique le NAS ou le numéro de permis de conduire ou de carte de crédit d'une personne aux seules fins de vérifier sa solvabilité ou de recouvrer des sommes dues.

[82] **Toutefois, l'entreprise peut, à certaines conditions, utiliser le renseignement recueilli à ces autres fins.** Voici pourquoi.

- ***La vérification de la solvabilité des clients et la perception de sommes impayées sont des objectifs légitimes, importants et réels***

[83] Tel qu'indiqué précédemment, il est tout à fait légitime pour l'entreprise de vouloir limiter ses pertes financières. Évaluer la solvabilité d'un nouveau client et disposer d'informations suffisantes afin de recouvrer les sommes qui lui sont dues en cas de non-paiement d'un appareil ou de services mobiles rendus contribuent à limiter ses pertes financières.

[84] Chaque année, l'entreprise refuse d'activer plusieurs milliers de comptes parce qu'ils sont associés à d'anciens comptes radiés ou suspendus pour non-paiement. Ces comptes sont identifiés grâce à une vérification dans ses

propres fichiers. Cette vérification permet aussi d'identifier des demandes d'activation d'un nouveau service ou d'ouverture d'un nouveau compte par un client actuel de l'entreprise, dont le compte a été autorisé sous réserve d'un dépôt de sécurité.

[85] Avant l'activation d'un compte, l'entreprise vérifie également la solvabilité du client auprès d'Équifax. Tel qu'indiqué précédemment, l'entreprise souhaite éviter des pertes financières compte tenu de la valeur des appareils mobiles et du fait que les clients peuvent rapidement faire grimper le coût des services utilisés sans avoir à les payer avant leur utilisation. Le nombre de clients et de nouvelles demandes d'activation étant très élevé, les risques de pertes financières susceptibles de résulter du non-paiement de matériel ou de services postpayés sont importants en l'absence de vérification de solvabilité.

[86] Dans ce contexte, la Commission conclut que l'objectif de vérification de solvabilité et de recouvrement en cas de non-paiement de matériel ou de services est légitime, important et réel.

- ***La collecte de renseignements n'est pas proportionnelle aux objectifs de vérification de la solvabilité et de recouvrement des sommes dues***

  - *L'existence d'un lien rationnel entre l'objectif poursuivi et la collecte des renseignements personnels*

[87] **La Commission considère qu'il existe un lien rationnel entre la collecte du NAS ou du numéro de permis de conduire ou d'une carte de crédit et l'objectif d'identifier les demandes d'activation associées à des comptes en souffrance, radiés ou suspendus pour non-paiement. Il en est de même des renseignements obtenus à la suite d'une enquête de crédit.**

[88] En effet, selon les documents soumis par l'entreprise, ces numéros permettent d'identifier davantage de demandes d'activation associées à des comptes en souffrance, radiés ou suspendus pour non-paiement dans ses fichiers internes.

[89] Aussi, l'enquête de crédit permet de mieux connaître la solvabilité d'un éventuel client et les risques encourus par l'entreprise. Elle lui permet de déterminer si elle acceptera ou non l'activation d'un compte pour des services postpayés et si un dépôt est requis.

[90] **Par contre, la Commission ne considère pas que les éléments au dossier démontrent le lien rationnel entre la collecte systématique d'un des numéros au choix du client et l'enquête de crédit réalisée par Équifax.**

[91] Une analyse réalisée en 2014 visant à évaluer l'impact du NAS sur l'efficacité d'une telle vérification, produite au dossier par l'entreprise, démontre qu'un très faible pourcentage de dossiers n'a pu être correctement identifié sans cet identifiant. L'entreprise n'a fourni aucun détail sur l'impact du numéro de permis de conduire ou d'un numéro de carte de crédit sur la possibilité d'identifier le bon dossier de crédit.

[92] Ce premier critère n'est donc pas rencontré. Cette collecte n'est pas davantage proportionnelle en vertu du second critère pour les motifs qui suivent.

- *L'atteinte à la vie privée que constitue cette collecte systématique de renseignements personnels n'est pas minimisée*

[93] D'abord, il existe d'autres moyens que la collecte systématique de l'un de ces numéros pour permettre à l'entreprise de vérifier la solvabilité d'un client ou pour recouvrer des sommes dues. D'ailleurs, l'entreprise reconnaît pouvoir procéder sans ces numéros, bien que ses démarches soient plus efficaces avec l'un de ces identifiants.

[94] Pour la vérification de la solvabilité auprès d'Équifax, les informations fournies par l'entreprise indiquent que la très grande majorité de ces recherches sont fructueuses sans le NAS. L'entreprise convient que le NAS n'est pas indispensable pour lancer une enquête de crédit, mais elle soumet que même un faible pourcentage de cas où il est impossible d'identifier le bon dossier de crédit du client a un grand impact pour elle compte tenu de son volume d'affaires.

[95] Elle ajoute que sa situation diffère des autres contextes dans lesquels la Commission a conclu que la collecte systématique du NAS n'était pas nécessaire à la réalisation d'enquêtes de crédit. Elle souligne le prix des appareils mobiles, son obligation de respecter l'atteinte d'objectifs qualitatifs imposés par voie législative aux entreprises de télécommunications à titre de service essentiel à la population et le grand nombre de fraudes auxquelles elle est confrontée.

[96] La Commission ne voit pas en quoi ce contexte justifie une collecte systématique de ces renseignements alors qu'un pourcentage très élevé d'enquêtes de crédit est réalisé avec succès sans ces numéros. D'ailleurs, l'entreprise Équifax indique sur son site Internet que cet identifiant est facultatif.

[97] Par exemple, on peut s'interroger sur la nécessité d'exiger l'un de ces numéros pour obtenir le bon dossier de crédit de la demanderesse dans la mesure où elle habite à la même adresse depuis 32 ans. Peut-être que l'un de

ces identifiants sera nécessaire, dans certaines situations, pour bien identifier le bon dossier de crédit. Toutefois, la collecte systématique de ces renseignements n'est pas proportionnelle à cet objectif.

[98] Quant à l'identification des demandes d'activation associées à des comptes en souffrance, radiés ou suspendus pour non-paiement, les documents soumis par l'entreprise visent à démontrer qu'un nombre considérable de ces vérifications sont concluantes grâce à la collecte de l'un de ces identifiants. L'entreprise admet toutefois que certains de ces cas auraient pu être identifiés même sans le numéro recueilli, sans toutefois les chiffrer.

[99] D'ailleurs, un seul identifiant est requis, au choix du client, lors d'une nouvelle demande d'activation. Si le client donne un autre numéro que celui qui est indiqué aux dossiers de l'entreprise, ce renseignement ne peut faciliter la recherche ni son efficacité.

[100] Dans ce contexte, la Commission considère que l'atteinte à la vie privée que constitue la collecte systématique d'un de ces numéros aux fins de réaliser une évaluation de la solvabilité du client n'est pas minimisée.

[101] En ce qui concerne la nécessité de la collecte d'identifiants pour percevoir des sommes dues à l'entreprise, le seul élément soumis à la Commission dans le cadre du présent dossier est une affirmation de l'entreprise voulant que les agences de crédit et de recouvrement avec lesquelles elle fait affaire se fient aux identifiants personnels dans leurs efforts de recouvrement et pour identifier les clients.

[102] Sans autre précision ni élément factuel au dossier que cette affirmation, la Commission ne peut davantage conclure que la collecte systématique de ces renseignements personnels est proportionnelle aux fins de recouvrement de sommes impayées.

- *La collecte de ce renseignement est susceptible de porter davantage préjudice au client que d'être utile à l'entreprise*

[103] Contrairement à l'objectif de prévention de la fraude et du vol d'identité, l'objectif de vérifier la solvabilité des clients et de recouvrer des sommes dues ne profite pas au client. L'entreprise soutient le contraire et explique que d'éviter ces pertes financières contribue à conserver des prix compétitifs et raisonnables pour ses produits, ce qui profite aux consommateurs. Elle ajoute qu'elle doit respecter des objectifs qualitatifs imposés par voie législative aux entreprises de télécommunications à titre de service essentiel à la population.

[104] L'entreprise rappelle que les clients souhaitent repartir de la boutique avec un appareil mobile dont les coûts sont parfois élevés. L'utilisation de cet appareil peut aussi faire grimper rapidement les coûts de service. L'entreprise souhaite donc offrir ce service rapide tout en minimisant ses pertes financières.

[105] La Commission considère que cet argument, dont l'ampleur n'a pas été démontrée, doit être apprécié à la lumière d'autres considérations, notamment le fait que cette collecte est susceptible d'être préjudiciable aux clients.

[106] En effet, tel qu'indiqué précédemment, la collecte de plus en plus répandue de ces identifiants par des entreprises augmente leur circulation et, par conséquent, les risques de malversations, de vols de renseignements ou d'incidents de sécurité. Ce constat est d'autant plus vrai lorsque l'entreprise communique ces renseignements à un tiers, par exemple afin de réaliser une enquête de crédit ou recouvrer des sommes dues. Il s'ensuit un plus grand danger pour le client d'être victime de fraude et de vol d'identité, particulièrement dans le contexte où l'entreprise conserve le NAS et le numéro de permis de conduire sans leur attribuer une mesure particulière accrue de sécurité, contrairement à ce qu'elle fait avec le numéro de carte de crédit.

[107] Comme le souligne l'expert en cybercriminalité, la fraude et le vol d'identité engendrent des conséquences négatives pour les personnes qui en sont victimes. Ces conséquences sont financières, administratives et psychologiques. Il indique que ce sont les préjudices financiers indirects et à retardement causés par l'inexactitude des dossiers administratifs qui s'avèrent les plus pénalisants. Par exemple, les victimes peuvent se voir attribuer des scores de crédit négatifs calculés sur la base d'activités frauduleuses menées à leur insu et en leur nom. Il peut être ardu de rétablir ensuite leur réputation financière.

[108] L'expert souligne aussi que les impacts émotionnels et psychologiques sur les victimes d'une fraude ou d'un vol d'identité sont démontrés scientifiquement, même s'il s'agit de crimes sans violences : honte, perte d'estime de soi, colère, sentiment d'isolement social et perte de confiance envers autrui et les institutions, perte de sommeil, tensions familiales et stress font partie des manifestations de ces conséquences.

[109] Dans ce contexte, la Commission ne peut conclure à la nécessité de la collecte systématique de l'un de ces numéros pour l'objet du dossier qui consiste à réaliser une évaluation de la solvabilité du client. Les explications de l'entreprise voulant qu'elle devrait changer ses façons de faire, former son personnel ou que la rapidité de son service au client en boutique pourrait s'en

ressentir, puisque certaines vérifications seraient moins efficaces, ne justifient pas l'atteinte à la vie privée que constitue cette collecte pour tous les clients.

CONCLUSION AU SUJET DE LA COLLECTE

[110] L'entreprise peut recueillir, au choix du client, soit le NAS, le numéro de permis de conduire ou un numéro de carte de crédit aux seules fins de prévenir et détecter la fraude et le vol d'identité.

[111] L'entreprise ne peut recueillir de façon systématique l'un de ces renseignements aux seules fins de vérifier la solvabilité du client ou de recouvrer des sommes impayées.

[112] Mais dans la mesure où elle est autorisée à recueillir l'un de ces numéros pour prévenir et détecter la fraude et le vol d'identité, la Loi sur le privé lui permet-elle de les utiliser pour ces autres fins? Pour les motifs qui suivent, la Commission conclut que oui, à certaines conditions.

L'ENTREPRISE PEUT, À CERTAINES CONDITIONS, UTILISER L'IDENTIFIANT RECUEILLI, AUX FINS DE VÉRIFICATION DE LA SOLVABILITÉ ET DE RECOUVREMENT

[113] La Loi sur le privé prévoit qu'une entreprise peut utiliser un renseignement personnel qu'elle détient à une fin **pertinente** à l'objet du dossier ou si elle obtient le **consentement du client**[10].

- **Utilisation aux fins de vérifier la solvabilité du client avec le consentement de la personne concernée**

[114] L'entreprise affirme qu'elle procède à la vérification de crédit uniquement avec le consentement de la personne concernée. Cette pratique est conforme à ce que prévoit la Loi sur le privé.

[115] En effet, puisqu'il s'agit d'une collecte de renseignements personnels auprès d'un tiers et qu'elle implique la communication de renseignements personnels à ce tiers (ex. : Équifax), la Loi sur le privé exige le consentement de la personne concernée[11].

[10] Art. 13 de la Loi sur le privé : « Nul ne peut communiquer à un tiers les renseignements personnels contenus dans un dossier qu'il détient sur autrui ni les utiliser à des fins non pertinentes à l'objet du dossier, à moins que la personne concernée n'y consente ou que la présente loi ne le prévoie. »

[11] Articles 6 et 13 de la Loi sur le privé.

[116] La Commission constate que la politique sur la protection de la vie privée de l'entreprise et la formation donnée aux employés précisent l'obligation d'obtenir un consentement exprès avant d'utiliser des renseignements personnels pour procéder à une vérification de crédit. Le formulaire de consentement utilisé par l'entreprise devrait donc préciser qu'elle utilise et communique l'un des numéros recueillis aux fins de vérification de la solvabilité. Afin que ce consentement soit libre, le client devrait pouvoir refuser que ce renseignement soit utilisé à ces fins.

- **Utilisation de ces renseignements aux fins de recouvrement ou de perception de sommes impayées autorisée sans le consentement de la personne concernée**

[117] En ce qui concerne le recouvrement ou la perception de sommes impayées, la Commission conclut que l'identifiant recueilli peut être utilisé sans qu'il ne soit nécessaire d'obtenir le consentement du client.

[118] Il s'agit d'une **utilisation pertinente** à l'objet pour lequel ce renseignement est recueilli, soit la prévention de la fraude, du vol d'identité ou de matériel.

[119] En effet, une absence de paiement dans le contexte d'un service postpayé implique que des appareils et des services de l'entreprise sont utilisés par le client sans la contrepartie due selon le contrat conclu entre eux. L'utilisation de l'identifiant aux fins d'identifier si une personne qui souhaite activer un service postpayé lui doit de l'argent ou pour percevoir ces sommes est donc en lien direct avec l'objectif de prévention de la fraude et du vol de matériel pour lequel il peut être recueilli.

Question 2 : L'entreprise a-t-elle refusé d'activer un service postpayé parce que la plaignante a refusé de fournir les informations demandées? Si oui, la Loi sur le privé le permet-elle?

[120] La Loi sur le privé prévoit qu'une entreprise ne peut refuser un bien ou un service pour le motif qu'une personne refuse de fournir un renseignement personnel, sous réserve de quelques exceptions, notamment :

- lorsque le renseignement est nécessaire à la conclusion ou à l'exécution d'un contrat;

- si la collecte du renseignement est autorisée par la loi[12].

[121] Puisque l'entreprise a démontré, dans le contexte actuel, la nécessité de la collecte d'un des identifiants en cause aux fins de prévenir la fraude et le vol d'identité dans les contrats de service postpayés, elle peut refuser l'activation d'un tel service lorsqu'une personne refuse de fournir l'un de ces renseignements.

[122] Toutefois, elle invite l'entreprise à rappeler régulièrement à ses employés et représentants affectés au service client et à l'activation de nouveaux comptes sa politique en matière de refus d'activation de services postpayés et la possibilité pour un client qui ne souhaite pas fournir l'un des identifiants demandés de prépayer l'appareil et le service.

ANALYSE DES ARGUMENTS CONSTITUTIONNELS

[123] L'entreprise soutient subsidiairement que la Loi sur le privé ne s'applique pas à elle parce que les entreprises de télécommunications sont uniquement soumises à la législation fédérale. Elle précise que ces arguments sont invoqués uniquement si la Commission conclut que ses pratiques actuelles sont contraires aux articles 5 ou 9 de la Loi sur le privé.

[124] Bien que la présente décision n'arrive pas à cette conclusion et ne comporte aucune ordonnance, la Commission soumet brièvement, à titre d'*obiter,* son avis sur les arguments constitutionnels soulevés.

[125] Comme l'a souligné le Procureur général du Québec dans une lettre déposée au dossier, les ouvrages, entreprises et affaires fédérales ne sont pas des « enclaves » soustraites de l'application de toute loi provinciale valide :

> En règle générale, les entreprises fédérales, comme les autres entreprises privées exploitées dans la province, doivent

[12] L'article 9 de la Loi sur le privé prévoit : « Nul ne peut refuser d'acquiescer à une demande de bien ou de service ni à une demande relative à un emploi à cause du refus de la personne qui formule la demande de lui fournir un renseignement personnel sauf dans l'une ou l'autre des circonstances suivantes : 1° la collecte est nécessaire à la conclusion ou à l'exécution du contrat; 2° la collecte est autorisée par la loi; 3° il y a des motifs raisonnables de croire qu'une telle demande n'est pas illicite.
En cas de doute, un renseignement personnel est réputé non nécessaire. »

> fonctionner dans le cadre que forment les lois provinciales et payer les taxes provinciales imposées dans la province.[13]

[126] Le Procureur général du Québec considère que le respect par l'entreprise de la Loi sur le privé dans le contexte du présent dossier n'emporte pas de conséquences fâcheuses au point d'entraver la compétence fédérale sur les télécommunications. Il ajoute que même si cette loi imposait des conditions plus sévères à l'entreprise, leur respect n'aurait pas pour conséquence qu'elle soit en contravention avec la loi fédérale en matière de protection des renseignements personnels. Au contraire, l'objet de protection de la vie privée partagé par ces lois fédérale et provinciale serait rencontré.

[127] La Commission partage cette position.

[128] De plus, contrairement à ce que prétend l'entreprise, la décision *Air Canada* c. *Constant*[14] ne constitue pas un précédent permettant de conclure à l'application de la doctrine de l'exclusivité des compétences[15] en l'espèce, au motif que la Loi sur le privé « *entrave de façon grave et importante la compétence du Parlement (fédéral) à exercer sa compétence exclusive à leur égard* »[16].

[129] D'abord, la question en litige dans cette décision concernait l'accès aux dossiers de sélection et d'embauche des candidats agents de bord d'une entreprise œuvrant en matière d'aéronautique. C'est donc uniquement dans ce contexte que la Cour évalue la doctrine de l'exclusivité des compétences. Celui-ci diffère du présent dossier qui porte sur la collecte et l'utilisation de renseignements personnels concernant des clients d'une entreprise de télécommunications.

[130] Mais surtout, dans l'affaire *Air Canada* la Cour conclut que le simple fait que la Loi sur le privé « touche » à un élément vital et essentiel d'une entreprise relevant de la compétence exclusive du Parlement suffit à la rendre inapplicable à l'entreprise et que le test de l'entrave ne s'applique pas. Cette conclusion

---

[13] *Air Canada* c. *Colombie-Britannique*, [1989] 1 R.C.S. 1161, à la page 1191.
[14] 2003 CanLII 1018 (QC CS).
[15] Selon la doctrine de l'exclusivité des compétences, une loi validement adoptée par un ordre de gouvernement ne peut empiéter indûment sur le « contenu essentiel et irréductible » de la compétence exclusive réservée à l'autre palier de gouvernement au point « d'entraver » sa capacité à exercer ses pouvoirs à l'égard des éléments essentiels de sa compétence. Voir notamment : *Banque de Montréal* c. Marcotte, 2014 CSC 55; *Banque canadienne de l'Ouest* c. *Alberta*, 2007 CSC 22.
[16] Observations amendées de l'entreprise, par. 165.

s'appuie essentiellement sur la décision rendue dans l'affaire *Bell Canada* c. *Québec (CSST)*[17].

[131] Or, les décisions rendues par la Cour suprême par la suite ont réaffirmé que le critère à appliquer est celui de l'entrave, soulignant que ce critère plus exigeant est davantage fidèle à notre régime fédéral[18].

[132] De plus, contrairement aux prétentions de l'entreprise, la Commission ne croit pas que les règles visant la protection des renseignements personnels applicables en l'espèce visent un aspect essentiel et vital de l'entreprise au point d'entraver la compétence fédérale de légiférer en matière de télécommunications. En effet, le test doit viser la compétence de légiférer sur ces éléments vitaux et essentiels et non l'impact sur les activités de l'entreprise.

[133] La Loi sur le privé vise la protection des renseignements personnels et non les aspects intrinsèques liés à la gestion et à l'exploitation des entreprises de télécommunications au sujet desquels le Parlement fédéral peut légiférer.

[134] C'est d'ailleurs l'approche adoptée dans l'affaire *Banque de Montréal* c. *Marcotte*[19] dans laquelle la Cour suprême conclut à l'application de dispositions de la *Loi sur la protection du consommateur*[20] aux banques en ces termes :

> [68] […] Les dispositions de la L.P.C. n'empêchent pas les banques de prêter de l'argent ou de convertir des devises; elles exigent seulement que ces frais de conversion soient mentionnés au consommateur.
>
> [69] […] Les dispositions qui prévoient la mention des frais et les recours possibles ont effectivement une incidence sur la façon dont les banques exercent un certain aspect de leurs activités, mais, comme nous l'avons vu précédemment, cette incidence ne saurait être assimilée à une entrave. Il est difficile d'imaginer comment ces dispositions pourraient forcer le Parlement à légiférer de manière à les écarter, à défaut de quoi, sa capacité de réaliser l'objectif pour lequel la compétence exclusive sur les banques lui a été attribuée serait entravée. […]

[135] De plus, la Cour suprême affirme qu'en l'absence de textes législatifs conflictuels de la part de l'autre ordre de gouvernement, les tribunaux devraient

---

[17] [1988] 1 R.C.S. 749.
[18] *Banque canadienne de l'Ouest* c. *Alberta*, précitée note 15, par. 48.
[19] Préc., note 10.
[20] RLRQ, c. P-40.1.

éviter d'empêcher l'application de mesures considérées comme ayant été adoptées en vue de favoriser l'intérêt public[21]. Les lois visant la protection des renseignements personnels, un des éléments constitutifs du droit à la vie privée, font certainement partie de mesures visant à favoriser l'intérêt public.

[136] Enfin, les faits au dossier ne permettent pas davantage de conclure que l'application de l'article 5 de la Loi sur le privé entraîne un conflit opérationnel ou d'intention avec la *Loi sur la protection des renseignements personnels et les documents électroniques*[22].

[137] En effet, l'entreprise soutient que la LPRPDE l'autorise à recueillir l'un des identifiants en cause aux fins décrites dans la première partie de la présente décision. La Commission en arrive à la même conclusion, dans le contexte actuel.

[138] La Commission ne croit pas non plus qu'il existe un conflit d'intention entre la Loi sur le privé et la LPRPDE : la loi provinciale n'empêche pas la réalisation de l'objectif de la loi fédérale.

[139] D'abord, il apparaît incongru de conclure que la Loi sur le privé, qui vise la protection des renseignements personnels détenus par les entreprises, entrave ou empêche la réalisation de l'objectif de protection des renseignements personnels également poursuivi par la LPRPDE. C'est là l'objectif premier de la LPRPDE.

[140] Contrairement à ce que soutient l'entreprise, elle ne considère pas davantage que l'application de la Loi sur le privé, dans le présent dossier, contrecarre un objectif d'uniformité et de cohérence des règles applicables aux entreprises fédérales qui serait poursuivi par la LPRPDE.

[141] Dans la mesure où la Loi sur le privé est jugée similaire[23] à la LPRPDE, la Commission ne voit pas en quoi son application entrave ou contrecarre l'objectif d'uniformité et de cohérence. Si les règles sont essentiellement similaires, les entreprises sont donc assujetties à des règles similaires et cohérentes. À tout le moins, les conclusions de la Commission dans le présent dossier ne mettent pas en cause une telle cohérence ou uniformité des règles pour l'entreprise.

---

[21] *Banque canadienne de l'Ouest* c. *Alberta*, précitée note 15, par.37.
[22] L.C. 2000, c.5, ci-après LPRPDE.
[23] Le *Décret d'exclusion visant des organisations de la province de Québec,* DORS/2003-374.

[142] D'ailleurs, la Commission souligne que l'entreprise affirme respecter la législation fédérale et les lois provinciales dans le passage suivant de sa politique sur la protection de la vie privée :

> 18. Quelles sont les lois applicables à la collecte, à l'utilisation et à la divulgation de mes renseignements personnels? Nos pratiques sont conçues pour être conformes aux lois canadiennes fédérales, provinciales et territoriales applicables, […].

[143] La Commission rappelle les enseignements de la Cour suprême invitant à favoriser une interprétation visant la conciliation des lois provinciales et fédérales applicables à une situation donnée, surtout lorsque les deux lois poursuivent, par des moyens semblables, le même objet et la même finalité.

[144] La LPRPDE et la Loi sur le privé visent le même objectif de protection des renseignements personnels détenus par les entreprises et comportent des règles essentiellement similaires. Elles peuvent donc coexister.

CONCLUSION

[145] La Commission considère que l'entreprise a démontré que la collecte d'un identifiant, parmi le NAS, le numéro de permis de conduire ou le numéro de carte de crédit, dans le contexte actuel, est nécessaire à la prévention de la fraude et du vol d'identité dans le contexte de l'activation d'un service postpayé.

[146] Par contre, l'entreprise n'a pas démontré la nécessité de recueillir de façon systématique ce renseignement aux fins de vérification du crédit d'un client ou pour percevoir des sommes impayées en lien avec un service postpayé.

[147] Toutefois, elle peut utiliser ce renseignement pour percevoir des sommes impayées en lien avec le contrat. Elle peut aussi l'utiliser et le communiquer afin de vérifier sa solvabilité, avec le consentement de la personne concernée. Ce consentement devrait préciser que l'entreprise utilise et communique l'un des numéros recueillis aux fins de vérification de la solvabilité. Afin que ce consentement soit libre, le client devrait pouvoir refuser que ce renseignement soit utilisé à cette fin.

[148] Compte tenu que cette collecte contribue également à augmenter le risque d'atteinte à la protection des renseignements personnels des clients, voire de fraudes et de vols d'identité, la Commission considère que l'entreprise devrait poursuivre ses recherches pour trouver un moyen alternatif à la collecte

de ces identifiants, particulièrement pour le NAS et le numéro de permis de conduire.

[149] De plus, la Commission recommande fortement à l'entreprise de mettre en place des moyens visant à sécuriser davantage ces identifiants, comme elle le fait pour le numéro de carte de crédit. On peut penser à un encryptage ou à d'autres moyens permettant d'éviter leur utilisation ou leur communication en cas d'accès par une personne non autorisée ou ayant des intentions malveillantes.

[150] Enfin, la Commission recommande à l'entreprise de faire des rappels réguliers à tous ses employés affectés au service client et à l'activation de nouveaux comptes quant aux contextes qui autorisent la collecte d'un de ces identifiants et aux situations dans lesquelles une enquête de crédit peut être effectuée, avec le consentement de la personne concernée, de manière à éviter qu'une situation comme celle à l'origine de la plainte ne se reproduise.

POUR CES MOTIFS, LA COMMISSION :

[151] **RECOMMANDE** que l'entreprise poursuive ses recherches pour trouver un moyen alternatif à la collecte du NAS ou du numéro de permis de conduire aux fins de prévenir et de détecter la fraude et le vol d'identité ou de matériel dans le contexte de l'activation d'un service postpayé;

[152] **RECOMMANDE** que l'entreprise mette en place des moyens visant à sécuriser davantage le NAS et le numéro de permis de conduire qu'elle détient au sujet de ses clients;

[153] **RECOMMANDE** que l'entreprise effectue des rappels réguliers à tous ses employés affectés au service client et à l'activation de nouveaux comptes quant aux contextes qui autorisent la collecte, au choix du client, d'un de ces identifiants (NAS ou numéro de permis de conduire ou de carte de crédit) et aux situations dans lesquelles une enquête de crédit peut être effectuée, avec le consentement de la personne concernée.

«Original signé»

Diane Poitras
Juge administratif

BORDEN LADNER GERVAIS
(M[e] Stéphane Richer)
Procureurs de l'entreprise

BERNARD ROY (JUSTICE-QUÉBEC)
(M[e] Samuel Chayer)
Procureur général du Québec