CFP – 002M
C.P. – Fuite de données personnelles chez Desjardins

Consultations particulières et auditions publiques sur la question de la fuite de données personnelles chez Desjardins

2019/11/21

Allocution d'Éric Prudhomme,
Directeur général (Québec)

Devant la Commission des finances publiques de l'Assemblée nationale du Québec

ASSOCIATION DES BANQUIERS CANADIENS
CANADIAN BANKERS ASSOCIATION

Bonjour! Je remercie la Commission pour cette occasion de m'adresser à vous cet après-midi.

Je m'appelle Eric Prud'homme. Je suis le directeur général de la direction du Québec de l'Association des banquiers canadiens (ABC). À mes côtés se trouve ma collègue Angelina Mason, avocate en chef et vice-présidente des affaire juridiques de l'ABC. L'Association est la voix de 70 banques membres, soit des banques canadiennes ainsi que des filiales et des succursales de banques étrangères exerçant des activités au Canada. Les banques, qui emploient 275 000 personnes au Canada dont près de 45 000 au Québec, contribuent à l'essor et à la prospérité économiques du pays. L'ABC préconise l'adoption de politiques publiques favorisant le maintien d'un système bancaire solide et dynamique, capable d'aider les Canadiens à atteindre leurs objectifs financiers.

Nous tenons à préciser que le Mouvement des caisses Desjardins n'est pas membre de l'ABC, vu que l'Association représente des institutions bancaires sous réglementation fédérale, assujetties à la *Loi sur les banques*.

Les banques sont conscientes de la confiance que les Canadiens leur accordent pour garder en sécurité les dépôts ainsi que les renseignements personnels et financiers. Elles emploient des équipes de professionnels hautement qualifiés en matière de cybersécurité et de protection des données et investissent lourdement dans la technologie et les mesures de sécurité. Entre 2007 et 2017, les six plus grandes banques canadiennes ont investi 84,5 milliards de dollars dans la technologie, dont une grande partie en solutions destinées aux mesures de sécurité. Malgré l'évolution soutenue des cybermenaces, les banques canadiennes maintiennent un excellent bilan en matière de protection de leurs systèmes et de leurs clients.

À titre d'institutions financières sous réglementation fédérale, les membres de l'ABC sont déjà assujettis à des exigences strictes en matière de cybersécurité et de protection des renseignements personnels établies par des lois et des règlements, ainsi qu'à une surveillance réglementaire. La protection des renseignements personnels ayant toujours été une pierre angulaire des activités bancaires, les mesures solides à cette fin font partie intégrante des politiques et des pratiques des banques depuis longtemps.

Le secteur bancaire a été le premier à aller au-delà d'une déclaration de principes et à adopter plutôt, dès 1986, un code de conduite complet pour la protection des renseignements personnels. Les valeurs de ce code se reflètent aujourd'hui dans la *Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)* fédérale, qui régit, entre autres, la façon dont les organisations recueillent et communiquent les renseignements personnels qui leur sont confiés. Les banques font partie de la première cohorte d'organisations assujetties à la LPRPDE depuis janvier 2001, et elles maintiennent un excellent dossier de conformité à cette loi.

Toutes les banques ont prévu une politique en matière de renseignements personnels et ont nommé un responsable de la conformité pour veiller à ce que cette politique soit respectée et que les renseignements personnels des clients soient protégés et tenus à jour, comme l'exige la loi. Nous sommes d'avis que la LPRPDE fonctionne bien : elle a permis d'atteindre un bon équilibre entre la protection des renseignements personnels d'un individu et l'usage légitime des renseignements personnels par les organisations. Basée sur des principes et technologiquement neutre, la LPRPDE fournit les dispositions nécessaires pour encadrer les innovations, les nouvelles technologies et les modèles de gestion nouveaux. Cette loi est formulée de façon à pouvoir maintenir son mandat à l'avenir.

Dans les très rares cas de fuite de données, les banques sont tenues de signaler certaines atteintes à la sécurité mettant en cause des données personnelles au Commissariat à la protection de la vie privée du Canada (CVPC), et d'aviser les personnes affectées par l'atteinte en question ainsi que les organisations susceptibles d'atténuer les dommages causés par l'incident. Dans l'avis aux personnes atteintes, les banques doivent inclure suffisamment d'information pour permettre à ces personnes de comprendre l'importance, pour elles, de l'atteinte et de prendre, si cela est possible, des mesures en vue de réduire le risque de préjudice qui pourrait en résulter ou d'atténuer un tel préjudice. Dans les cas où l'atteinte pourra produire d'importants dommages, les banques surveillent les activités sur le compte afin de détecter un piratage de renseignements personnels potentiel ou actuel, et d'arrêter toute activité non autorisée le cas échéant. Par ailleurs, dans certains cas, les banques indemnisent le titulaire du compte pour la perte de fonds due à des opérations non autorisées. Également, les banques font appel aux agences de crédit afin de réduire le risque de dommage.

Parallèlement, les banques sont assujetties à l'obligation de signaler les incidents liés à la technologie et à la cybersécurité établie par le Bureau du surintendant des institutions financières (BSIF). Lorsqu'une institution financière sous réglementation fédérale fait face à un incident lié à la technologie ou à la cybersécurité qui pourrait avoir des conséquences importantes sur ses activités habituelles, elle est tenue de le signaler au BSIF dans un intervalle de 72 heures. Aussi, les banques doivent communiquer des mises à jour au BSIF à mesure que de nouveaux renseignements deviennent disponibles, notamment au sujet de leurs plans de redressement à court et à long terme, et lui soumettre un compte-rendu sur les leçons apprises. En outre, le BSIF s'attend à ce que l'équipe de direction de chaque banque passe en revue ses politiques et ses pratiques en matière de gestion des cyberrisques afin de les garder en phase avec le changement de circonstances et l'évolution des risques.

La cybersécurité et la résilience sont des priorités collectives pour les banques au Canada. Il n'y a aucun avantage concurrentiel à procéder individuellement. Avec l'augmentation des opérations effectuées électroniquement, les réseaux et les systèmes deviennent de plus en plus interconnectés, ce qui amplifie la collaboration entre les banques, les gouvernements, les forces de l'ordre et d'autres secteurs. Aujourd'hui au Canada, 72 % des consommateurs utilisent principalement les services bancaires en ligne et mobiles. Une hausse par rapport aux 52 % d'il y a tout juste 4 ans.

Les banques canadiennes ont activement participé aux consultations qui ont mené au développement de la Stratégie nationale de cybersécurité et appuient fermement la démarche intégrée public-privé envers la cybersécurité et la cyberrésilience au pays. Les banques maintiennent leur collaboration avec les organismes gouvernementaux dans l'échange de connaissances récentes, y compris le nouveau Centre canadien pour la cybersécurité, et participent activement à des projets avec d'autres organisations comme l'Échange canadien des menaces cybernétiques (ECMC). Ces actions favorisent grandement la collaboration entre les secteurs public et privé, assurent la protection des consommateurs et, par conséquent, mènent à la création d'un cyberenvironnement plus résilient et plus sécurisé.

Une des principales priorités du Centre canadien pour la cybersécurité est de veiller à ce que les secteurs clés au Canada soient cyberrésilients. Pour ce faire, le Centre devra encourager un environnement de collaboration et agir comme point de contact vers lequel les secteurs public et privé pourront se tourner pour obtenir conseils et directives en la matière.

L'ABC est d'avis que la sensibilisation à la cybersécurité est essentielle. Éduquer la population est la responsabilité commune du gouvernement et du secteur privé. Veiller à ce que les individus participent activement aux efforts de lutte contre les cybermenaces passe par des connaissances générales du sujet et par une prise de conscience individuelle de la responsabilité de chacun dans cet enjeu. Le secteur bancaire sera heureux de collaborer davantage avec les gouvernements sur les initiatives publiques de sensibilisation et de responsabilisation, comme l'ajout de la cybersécurité aux efforts de promotion de la littératie financière.

Pour conclure, j'aimerais rappeler que les banques attachent une grande importance à la protection des données personnelles des citoyens. En effet, parallèlement à l'évolution rapide de la technologie et à l'adoption des outils bancaires numériques par un nombre croissant de consommateurs, les banques poursuivent leur recherche de solutions technologiques susceptibles d'améliorer la protection des renseignements personnels de leurs clients. Un simple exemple serait les solutions d'identification et d'authentification numériques. Le secteur bancaire canadien continuera à collaborer et à investir dans la protection des données personnelles et financières, et à appuyer le travail des gouvernements en vue de protéger les Québécois, et les Canadiens dans leur ensemble.

Merci de votre temps! Nous serons heureux de prendre vos questions.