ASSEMBLÉE NATIONALE
DU QUÉBEC

COMMISSION DES FINANCES PUBLIQUES

LA FUITE DE DONNÉES PERSONNELLES CHEZ DESJARDINS

ASSEMBLÉE NATIONALE
DU QUÉBEC

COMMISSION DES FINANCES PUBLIQUES

LA FUITE DE DONNÉES PERSONNELLES CHEZ DESJARDINS

LES COLLABORATRICES ET COLLABORATEURS
DE LA COMMISSION DES FINANCES PUBLIQUES

SECRÉTARIAT DE LA COMMISSION

Stéphanie Pinault-Reid

Noémie Gauthier

SERVICE DE LA RECHERCHE

Xavier Mercier Méthé

Pour tout renseignement complémentaire sur les travaux de la Commission des finances publiques, veuillez vous adresser à la secrétaire de la Commission, M^{me} Stéphanie Pinault-Reid.

Édifice Pamphile-Le May
1035, rue des Parlementaires, 3^{e} étage
Québec (Québec) G1A 1A3

Téléphone : 418 643-2722
Sans frais : 1 866 337-8837

Courrier électronique : cfp@assnat.qc.ca

Ce document est mis en ligne dans la section Travaux parlementaires du site Internet de l'Assemblée nationale : assnat.qc.ca.

Dépôt légal – novembre 2019
Bibliothèque et Archives nationales du Québec
ISBN (Imprimé) : 978-2-550-85585-9
ISBN (PDF) : 978-2-550-85586-6

LES MEMBRES ET LES DÉPUTÉES ET DÉPUTÉS AYANT PARTICIPÉ

M. Simard (Montmorency), président

M. Asselin (Vanier-Les Rivières)
M. Barrette (La Pinière)
M. Chassin (Saint-Jérôme)
M. Émond (Richelieu)
M^me^ Foster (Charlevoix-Côte-de-Beaupré)
M. Gaudreault (Jonquière)
M. Lafrenière (Vachon)
M. Leitão (Robert-Baldwin)
M. Marissal (Rosemont)
M. Nadeau-Dubois (Gouin)
M. Ouellet (René-Lévesque)
M^me^ Rizqy (Saint-Laurent)
M. Thouin (Rousseau)

TABLE DES MATIÈRES

INTRODUCTION

CONTEXTE

Le 20 juin 2019, Desjardins a révélé avoir été victime d'une fuite majeure de renseignements personnels de ses membres. Nous savons aujourd'hui que tous les membres particuliers sont touchés par ce vol de renseignements personnels. Peu après, 6 millions de clients canadiens de Capitale One ont également subi une situation similaire. Au Canada, depuis que les entreprises assujetties à la *Loi sur la protection des renseignements personnels et les documents électroniques* sont tenues de divulguer tout incident au Commissariat à la protection de la vie privée du Canada, celui-ci a reçu 680 signalements touchant 28 millions de personnes[1]. L'importance des renseignements personnels dans l'économie actuelle en fait une marchandise convoitée par les fraudeurs. Le secteur financier semble particulièrement ciblé dans la mesure où les données en jeu sont potentiellement lucratives. Bien que les informations subtilisées puissent sembler banales, les conséquences sur les personnes peuvent être catastrophiques.

MANDAT DE LA COMMISSION

C'est dans ce contexte que, le 14 novembre 2019, l'Assemblée nationale a adopté, en vertu de l'article 146 de son règlement, une motion confiant à la Commission des finances publiques le mandat d'étudier la question de la fuite de données personnelles survenue chez Desjardins. Dans le cadre de ses travaux, la Commission a entendu les intervenants suivants : Desjardins, l'Autorité des marchés financiers (AMF), Equifax, l'Office de la protection du consommateur, l'Association des banquiers canadiens, José Fernandez, titulaire de la Chaire de recherche industrielle en cybersécurité et intelligence artificielle de Polytechnique Montréal.

La Commission des finances publiques tient à remercier les personnes et les organisations qui ont participé à cette consultation. Leur contribution illustre à quel point l'enjeu de la protection des données personnelles dans le secteur financier émerge et devient une réalité cruciale pour les citoyennes et citoyens du Québec. Au-delà du cas particulier de Desjardins, il s'agit d'un risque bien présent pour l'ensemble de l'économie. Le présent rapport fait la synthèse des avis exprimés dans le cadre de ce mandat et expose les conclusions et les recommandations de la Commission.

[1] Commissariat à la protection de la vie privée du Canada. [*Un an après l'entrée en vigueur des déclarations obligatoires des atteintes à la protection des données : ce que nous avons appris et ce que les entreprises doivent savoir]* (Consulté le 31 octobre 2019).

SYNTHÈSE DES PROPOS RECUEILLIS

AUDITION

Les échanges entre les témoins et les membres de la Commission des finances publiques s'articulent principalement autour de cinq axes : les conséquences d'un vol de données sur les personnes touchées, les mesures de protection pour les victimes de fraude, l'encadrement légal et règlementaire des institutions financières, les mesures de protection des données personnelles mises en place par les institutions financières et l'identité numérique comme solution potentielle.

Les conséquences d'un vol de données

Les renseignements dérobés aux institutions financières servent généralement à identifier les clients. Le nom, l'adresse, la date de naissance, le numéro d'assurance sociale revêtent un intérêt considérable pour les fraudeurs. De plus, dans le cas des fuites de données chez Desjardins et Capitale One, certaines informations relatives aux avoirs détenus par les clients ont pu être volées.

Si ces données ne donnent pas accès aux comptes des personnes flouées, elles suffisent néanmoins à usurper leur identité.

Les institutions financières majeures sont vigilantes dans l'établissement de l'identité de leurs clients. Par contre, certains secteurs sont plus vulnérables. Les prestataires de services et d'autres commerces peuvent être visés par des fraudeurs. Le fait d'avoir des précisions sur les actifs d'une personne permet de cibler davantage les fraudes potentielles. Comme le rappelle un expert, un pourcentage d'individus victimes d'une fuite de renseignements personnels seront effectivement victimes d'une fraude. Toutefois, les conséquences d'un vol d'identité sont significatives sur la victime, et ce, même si celle-ci n'a aucune responsabilité dans la brèche de sécurité qui touche ses renseignements.

Le fait d'être victime d'une fuite de données n'affecte pas d'emblée le dossier de crédit d'un individu. C'est plutôt l'inscription de créances frauduleuses qui s'y répercute. Il en découle des difficultés pour les citoyennes et citoyens qui souhaitent avoir accès au crédit, à des prêts hypothécaires, à certains produits d'assurance, au logement et même à un emploi. Cela se produit souvent sans que la victime soit au fait de la situation. Il devient très difficile de rétablir le dossier de crédit de celle-ci par la suite. De plus, le fardeau de la preuve repose sur la victime. Dans le pire des cas, elle doit saisir elle-même les tribunaux pour contester le bien-fondé des inscriptions et de la créance. Ces démarches sont longues et fastidieuses.

Les mesures de protection des personnes victimes de fuites

Les personnes participant à la Commission font état de l'importance d'informer et de sensibiliser le public pour réduire le risque de fraudes liées aux fuites de données. Tant l'Autorité des marchés financiers que l'Office de la protection du consommateur diffusent de l'information sur les comportements à éviter afin d'aider le public à se prémunir contre d'éventuels actes malveillants lorsque des renseignements personnels ont été dérobés.

En plus de la sensibilisation, les personnes représentant l'industrie financière mettent de l'avant l'importance de la surveillance du dossier de crédit comme un moyen de protéger la population. L'inscription à un tel service repose toutefois sur l'individu. Celui-ci doit consentir aux services offerts au Québec par les entreprises de surveillance du crédit Equifax et TransUnion, qui se partagent le marché.

On observe qu'un pourcentage significatif d'individus touchés par des fuites de renseignement ne s'inscrit pas à ces services de surveillance, même lorsque les coûts sont payés par une institution financière. En revanche, des parlementaires font remarquer que les difficultés rencontrées par les membres de Desjardins, pour accéder aux services et être servis en français, nuisent à l'utilisation de ces services de surveillance.

Les entreprises offrant la surveillance du crédit alertent les personnes inscrites lorsqu'une transaction suspecte est portée à leur dossier. Les informations sur les transactions ne sont pas versées en temps réel. Il peut donc y avoir un délai entre le moment où une fraude est commise et celui où la personne en est avisée. Par ailleurs, il n'est pas possible de verrouiller un dossier de crédit pour bloquer toute nouvelle demande lorsque des renseignements personnels sont compromis. Bien que le dossier concerne les consommatrices et consommateurs et qu'il soit alimenté par leurs renseignements, ceux-ci ne sont pas en mesure de contrôler l'usage qu'en font les entreprises ou d'en restreindre l'accès.

Par ailleurs, les personnes représentant les institutions financières et de surveillance du crédit offrent des services supplémentaires d'assistance et de protection lorsque des inscriptions frauduleuses sont détectées. Afin de maintenir la confiance de la clientèle, l'institution peut rembourser des transactions frauduleuses, indemniser les personnes flouées ou les aider à rétablir leur dossier de crédit et leur identité. Des membres de la Commission s'étonnent qu'une procédure simple et rapide ne soit pas offerte automatiquement à toutes les victimes d'un vol d'identité, sans égard au maintien d'un rapport de clientèle ou au temps écoulé depuis la brèche.

L'encadrement légal et règlementaire

Contrairement à certains pays qui imposent des pénalités très sévères (qui s'élèvent parfois à des centaines de millions de dollars) selon la gravité de la fuite de données, les sanctions prévues à la *Loi sur la protection des renseignements personnels dans le secteur privé* s'élèvent à 10 000 $

maximum. Selon les membres de la Commission, ce montant n'apparaît pas dissuasif au regard de l'importance du chiffre d'affaires des institutions financières.

Le secteur financier est encadré par le Bureau du surintendant des institutions financières (BSIF) dans le cas des établissements sous juridiction fédérale. Desjardins relève de la législation québécoise et, de ce fait, est encadrée par l'Autorité des marchés financiers (AMF). Les deux régulateurs appliquent des exigences similaires, axées sur les mêmes conventions internationales.

L'Autorité des marchés financiers a un rôle de régulateur prudentiel; elle amène donc les institutions à adopter de bonnes pratiques dans la gestion des risques qui peuvent compromettre leur stabilité. Ainsi les risques technologiques, notamment ceux en lien avec les fuites de renseignements personnels, sont établis. Un questionnaire d'autoévaluation a été transmis à cet égard aux institutions financières en 2015. L'AMF s'affaire également à produire des lignes directrices qui permettent aux institutions de faire face à ces risques. Ces orientations n'impliquent pas de réglementation additionnelle, elles proposent plutôt l'application de standards internationaux en matière de sécurité des données. L'objectif est d'amener les institutions et leurs instances de direction à se responsabiliser.

Dans une situation comme celle qui affecte Desjardins, le rôle de l'Autorité des marchés financiers est de s'assurer que les mesures adoptées diminuent les risques menaçant la viabilité de l'institution. Bien que cela soit souhaitable, la communication d'incidents technologiques à l'AMF n'est pas obligatoire. Dans le cas qui occupe la Commission, l'AMF juge avoir été alertée rapidement et de manière transparente dans ce cas. Desjardins devra également fournir un rapport sur les actions réalisées et les correctifs nécessaires.

Pour leur part, les institutions financières assujetties à la législation canadienne doivent signaler les incidents liés à la technologie et à la cybersécurité, dans un délai maximal de 72 heures, au Bureau du surintendant des institutions financières, en vertu d'un préavis entré en vigueur en mars 2019.

Le partage de données entre les institutions financières en cas d'incidents se fait dans le respect des lois protégeant la confidentialité des renseignements personnels. Dans certaines circonstances, un plus grand partage de l'information pourrait limiter la portée de la fraude.

Les mesures de protection prises par les institutions financières

Les institutions financières investissent des centaines de millions de dollars dans les nouvelles technologies et dans les systèmes de protection des renseignements personnels de leur clientèle. Les mesures de sécurité du secteur financier sont supérieures à la moyenne des entreprises et des institutions.

Les brèches de sécurité proviennent d'attaques extérieures ou de personnes à l'interne qui utilisent les données à des fins non autorisées. Les mesures technologiques visant à contrer des attaques externes

sont élaborées et semblent efficaces pour détecter et bloquer les accès non autorisés. Les brèches internes, en revanche, sont plus difficiles à détecter et à freiner. Elles comptent pour près du tiers des événements détectés.

Des procédures et des mesures technologiques existent pour prévenir les brèches internes. Les membres du personnel font l'objet d'enquêtes avant leur embauche. Des parlementaires insistent sur l'importance de procéder à de telles enquêtes de manière régulière après l'embauche, puisque la situation d'un individu peut évoluer. Les accès aux renseignements sont également limités selon les besoins liés à la fonction de l'employé. Des programmes de journalisation permettent également de détecter des accès inhabituels à certains renseignements de la part des membres du personnel.

Il demeure que certaines personnes, par leur fonction, doivent avoir accès à un grand éventail de données. Selon des personnes du milieu, contrer les menaces internes s'avère difficile. Il faut s'interroger sur les intentions de la personne qui accède à des renseignements. Une plus grande surveillance par des moyens technologiques est possible, mais pose des enjeux éthiques en matière de protection de la vie privée du personnel.

Les institutions financières collaborent avec les autorités policières et signalent un nombre important de transactions qui pourraient s'avérer frauduleuses. Ce sont les policiers qui font ensuite enquête et qui sont à même d'établir la nature criminelle des actes. Les enquêtes policières peuvent révéler des brèches de sécurité qui n'ont pas été détectées par une institution financière. Dans le cas de Desjardins, par exemple, ce sont des informations transmises par le Service de police de Laval qui ont permis de mettre à jour la fuite de donnée touchant ses membres.

Les institutions financières peuvent limiter les dommages causés par une brèche de sécurité, notamment en congédiant le personnel fautif et en saisissant du matériel. Il apparaît toutefois essentiel que ces actions n'entravent pas le travail d'enquête des policiers et ne compromettent pas leur capacité d'amasser une preuve suffisante pour intenter des poursuites.

L'identité numérique comme solution

Les fuites de données personnelles se multiplient et mettent en lumière un problème de fond : les données d'identification actuellement utilisées au Québec ne sont pas adaptées à l'environnement technologique et sont semées à tout vent. La protection du public passe par l'adoption de l'identité numérique. Celle-ci serait utilisée à la fois par les secteurs publics et le secteur privé. Elle permettrait d'authentifier une personne de manière sécurisée sans avoir à dévoiler ses renseignements personnels, notamment sa date de naissance ou son numéro d'assurance sociale. Le support pourrait être une carte à puce ou un téléphone intelligent.

Plusieurs intervenantes et intervenants mentionnent leur intérêt pour le principe d'identité numérique. La circulation des données et l'interconnexion des systèmes témoignent d'une tendance forte. Il ne faut pas entraver la circulation des données, mais plutôt en assurer la sécurité. Cette question transcende la concurrence.

Des groupes réfléchissent à la question de l'identité numérique au Québec. Ils sont composés de personnes issues de différentes industries et d'institutions publiques. La technologie nécessaire est disponible et éprouvée. Plusieurs pays européens disposent d'un système d'identité numérique, notamment la Belgique, l'Espagne et l'Estonie. Il serait possible d'appliquer un tel système tant à l'échelle du Québec qu'à l'échelle du Canada. Cependant, les méthodes de sécurité retenues doivent être faciles à utiliser et viser l'inclusion de tous et toutes, notamment des personnes âgées, mineures et des personnes plus vulnérables.

OBSERVATIONS

Les parlementaires souhaitent poursuivre leur réflexion sur l'enjeu de la protection des données personnelles lors des consultations particulières qui se tiendront dans le cadre des projets de loi qui seront déposés par le gouvernement.

De plus, les parlementaires observent que :

- Desjardins a tenté de remettre en perspective la fuite de données personnelles de ses clients en la qualifiant de phénomène mondial.
    - À cet égard, les parlementaires jugent que Desjardins devrait :
        - Assumer sa pleine responsabilité relativement à cette fuite ;
        - Continuer de travailler sur les services offerts à ses clients victimes de la fuite de leurs données personnelles ;
        - Mieux prévenir des événements similaires dans le futur en ciblant, notamment, davantage le contrôle exercé sur les accès sur les bases de données et la cybersécurité.
- Malgré 90 ans de présence au Québec et une part de marché qui s'élève à 70 % dans la province, Equifax n'a pas été en mesure de fournir, dès le départ, un service en français aux membres de Desjardins touchés par la fuite de données.
    - Les parlementaires estiment que cela est inacceptable, toutefois, ils notent qu'Equifax s'est engagé à offrir un meilleur service aux francophones.
- Plusieurs membres de Desjardins qui souhaitent s'inscrire au service de surveillance de crédit offert par Equifax ont fait face à des problèmes qui ont pu retarder leur inscription.
    - Les parlementaires sont d'avis que la date d'échéance pour l'inscription à ce service devrait être plus flexible que celle prévue, pour véritablement permettre à tous les clients qui souhaitent s'y inscrire de pouvoir le faire.
- La protection de données personnelles est un enjeu complexe et d'une très grande importance, son amélioration doit être prioritaire pour le gouvernement du Québec.
- Plusieurs intervenants ont proposé l'identité numérique comme une solution de remplacement aux méthodes « archaïques » d'identification personnelle, compte tenu de la prolifération des

transactions numériques. Ils ont également souligné qu'il s'agirait d'une manière concrète de lutter contre les vols d'identité.

  - Les parlementaires prennent acte de cette proposition et ils jugent, à cet égard, que les différents paliers de gouvernements doivent se pencher sur l'amélioration de ces méthodes.

  - Ils considèrent d'ailleurs la pertinence de la création d'une identité numérique québécoise.

  - De plus, ils croient que l'on devrait envisager d'obliger les entreprises et l'État à supprimer toute données périmées, et ce, dès que la personne concernée en fait la demande.

  - Finalement, ils croient que la divulgation publique obligatoire des fuites de données des entreprises privées devrait être une solution à évaluer.

- Il est difficile pour les consommateurs victimes de fraude reliée au vol de données de corriger leur cote de crédit. Par ailleurs, les moyens pour le faire sont méconnus.

  - Les parlementaires estiment que les Québécois doivent être mieux informés sur les recours dont ils disposent pour reprendre le contrôle de leurs données personnelles.

Enfin, les membres de la Commission demandent au président de la Commission des finances publiques de formuler, par écrit, à Desjardins, toutes les questions complémentaires que les membres de la Commission souhaitent poser, et ce, dans les 15 jours suivants le dépôt du rapport à l'Assemblée nationale.

DIRECTION GÉNÉRALE
DES AFFAIRES PARLEMENTAIRES

Édifice Pamphile-Le May
1035, rue des Parlementaires
3e étage, Bureau 3.15
Québec (Québec) G1A 1A3

Téléphone : 418 643-2722
Télécopieur : 418 643-0248
commissions@assnat.qc.ca

100%
BIOGAZ
EcoLogo
Papier fabriqué au Québec