Protection des renseignements personnels

Fiche technique - Élections 2019

- Le vol de données chez Desjardins nous révèle une réalité trop longtemps ignorée : avec la mise en place des banques de données centralisées, les vols de fichiers contenant des renseignements personnels se multiplient depuis plusieurs années;
- Ces données ont une valeur sur le marché noir parce que des fraudeurs peuvent les utiliser pour usurper notre identité à des fins de fraude;
- Le défi : maintenant que les renseignements personnels ont été dérobés, il faut mettre en place des mécanismes de contrôle pour s'assurer que personne ne puisse effectuer une transaction à notre nom;
- Les lois fédérales sont laxistes et laissent aux banques le soin de déterminer quels contrôles elles mettent en place.
    - Si ça leur coûte cher de mettre en place des contrôles serrés, elles préfèreront ne rien faire et assumer les fraudes, quitte à exposer leurs clients à tous les désagréments liés au vol de leur identité.
- Le Bloc Québécois proposera des changements législatifs pour encadrer la pratique des banques et diminuer les fraudes :
    - Obligation d'instaurer des contrôles d'identité serrés pour éviter que des fraudeurs puissent utiliser des renseignements personnels volés pour usurper l'identité de quelqu'un et commettre des fraudes en utilisant son nom, à l'image des exigences en vigueur en Europe;
    - Obligation de faire une déclaration détaillée à même leurs déclarations annuelles du nombre de fraudes liées au vol d'identité détectées dans leur organisation de même que les pertes engendrées par ces fraudes.
    - Obligation de contacter toute personne dont l'identité aurait été utilisée frauduleusement au sein de l'organisation, qu'un compte ait été ouvert ou non.
    - Obligation d'assumer les frais que les victimes auront eu à payer pour recouvrer leur identité;
    - Mise en place d'une ligne de dénonciation anonyme pour les employés au courant de vols d'identité non déclarés en bonne et due forme et protection des lanceurs d'alerte.

■ Illustration

Le contexte : des vols de données de plus en plus fréquents

- Le 20 juin dernier, la direction de Desjardins a tenu une conférence de presse pour annoncer un important vol de données personnelles :
    - Un employé a subtilisé les renseignements personnels de 2,7 millions de personnes (2,4 millions de Québécois et 300 000 Canadiens) et 200 000 entreprises;
- Le vol de données chez Desjardins a fait grand bruit mais il n'est que le dernier d'une série d'évènements semblables;
    - En 2017, des pirates informatiques ont volé les dossiers de 146 millions de personnes (19 000 Canadiens) à l'agence de crédit américaine Équifax. On l'a appris six mois plus tard dans une fuite aux médias; jusque-là, Équifax avait préféré cacher l'information pour protéger sa réputation.
    - En 2018, des pirates informatiques ont volé les dossiers de 90 000 personnes à la Banque de Montréal et la CIBC. On l'a appris 3 mois plus tard lorsque les pirates eux-mêmes ont mis un message sur Internet pour rendre leur larcin public et demander une rançon aux banques, sous menace de vendre les fichiers à des fraudeurs. Jusque-là, les banques avaient préféré cacher l'information.
    - En juillet dernier, Capital One révélait le vol des données personnelles de 106 millions de ses clients dont près de 6 millions de Canadiens. Près d'un million de numéros d'assurance ont été piratés.
    - Il y a probablement des dizaines d'exemples semblables dont nous ignorons l'existence : en cas de vol de données, les banques sont tenues d'informer la police et le Commissariat à la vie privée mais rien ne les oblige à informer la population.

Le défi : empêcher que ces vols de données ne servent à commettre des fraudes

- Au fédéral, dans la foulée du vol chez Desjardins, le débat a beaucoup porté sur le numéro d'assurance sociale :
    - Plusieurs voudraient pouvoir changer de numéro dès maintenant, alors que la pratique actuelle veut qu'on ne puisse pas changer de N.A.S à moins d'avoir été victime d'une fraude par vol d'identité.
    - Plusieurs demandent à Ottawa de revoir la carte d'assurance sociale pour la rendre plus difficile à contrefaire, comme il l'a fait pour les passeports à la demande des Américains au lendemain des attentats du 11 septembre.
    - Ces deux demandes sont raisonnables et le Bloc Québécois demande à Ottawa d'y donner suite, mais ça ne suffira pas pour enrayer les fraudes.
- La meilleure façon de bloquer les tentatives d'usurpation d'identité, c'est de s'assurer que la personne qui veut faire une transaction est bien celle qu'elle prétend être.

- Il y a trois façons de contrôler l'identité de quelqu'un :
    1. Par ce qu'elle sait (ses renseignements personnels tels que nom, adresse, numéro d'assurance sociale, etc.). Ces contrôles d'identité sont de moins en moins fiables avec la multiplication des vols de renseignements. Forts de ces renseignements, les fraudeurs n'ont qu'à se fabriquer une fausse pièce d'identité et le tour est joué.
    2. Par ce qu'elle a (l'adresse IP de son ordinateur, que l'institution peut reconnaître si la transaction est faite à partir de la maison, son téléphone cellulaire, où l'institution peut envoyer un texto avec un code à entrer pour compléter la transaction, etc).
    3. Par ce qu'elle est (l'institution peut se doter de technologies qui reconnaissent les caractéristiques personnelles de quelqu'un : sa voix, son visage, son empreinte digitale, son écriture manuscrite, etc.).
- En 2016, l'Union européenne a adopté une règlementation (la Directive sur les Services de Paiement - DSP2) qui oblige les institutions financières à utiliser au moins deux de ces trois façons d'identifier quelqu'un avant d'autoriser une transaction.
- Au Canada, les banques n'ont aucune obligation semblable. Si elles estiment que ces mécanismes de contrôles leur coûteraient plus cher que la perte qu'elles assument actuellement en fraude, elles ont tout intérêt à ne rien faire.

La solution du Bloc : forcer les banques à contrer la fraude

- Le Bloc Québécois proposera un projet de loi pour contrer la fraude par usurpation d'identité. En particulier, nous modifierons la *Loi sur les banques* et la *Loi sur la protection des renseignements personnels et les documents électroniques* en :
    - S'inspirant de la règlementation européenne pour forcer les banques à mettre en place des mécanismes serrés de contrôle d'identité avant d'autoriser une transaction financière;
    - Augmentant les amendes pour inciter les banques à mieux protéger les renseignements personnels de leurs clients;
    - Obligation de faire une déclaration détaillée à même leurs déclarations annuelles du nombre de fraudes liées au vol d'identité détectées dans leur organisation de même que les pertes engendrées par ces fraudes.
    - Obligation de contacter toute personne dont l'identité aurait été utilisée frauduleusement au sein de l'organisation, qu'un compte ait été ouvert ou non.
    - Obligation d'assumer les frais que les victimes auront eu à payer pour recouvrer leur identité;
    - Mise en place d'une ligne de dénonciation anonyme pour les employés au courant de vols d'identité non déclarés en bonne et due forme et protection des lanceurs d'alerte.