Commission
d'accès à l'information
du Québec

Commission d'accès à l'information du Québec

Dossier :	1020846-S
Nom de la l'entreprise :	Fédération des caisses Desjardins du Québec
Date :	11 décembre 2020
Membre :	M[e] Cynthia Chassigneux

DÉCISION

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

APERÇU

[1] Les entreprises font de plus en plus l'objet d'attaques visant les renseignements personnels qu'elles détiennent.

[2] L'incident de sécurité survenu au sein de la Fédération des caisses Desjardins du Québec (Desjardins), qui a visé les renseignements personnels de 9,7 millions de personnes, illustre bien cette situation.

[3] Cet incident démontre l'importance que les entreprises doivent accorder à la sécurité afin de se prémunir contre les attaques visant les renseignements personnels qu'elles détiennent. Il démontre également que les attaques ne proviennent pas uniquement de l'externe. En effet, elles peuvent venir de l'interne, à la suite d'actions intentionnelles ou non, malveillantes ou non.

[4] C'est pourquoi une entreprise doit prendre un ensemble de mesures propres à assurer la sécurité des renseignements personnels qu'elle détient. Ces mesures doivent tenir compte de la sensibilité, de la quantité, de l'utilisation, de la répartition et du support des renseignements.

[5] Ces mesures de prévention, de détection et de contrôle doivent permettre de minimiser les risques. Elles doivent notamment être :

---

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

- administratives ou organisationnelles : par ex. formation et sensibilisation des employés, procédure pour accorder les accès et permissions requis, adoption de politiques, de directives;
- physiques : par ex. restriction de l'accès aux locaux, aux serveurs;
- techniques : par ex. chiffrement, mots de passe, journalisation, blocage des ports USB.

[6] Ces mesures doivent être documentées, mises en œuvre, surveillées, révisées régulièrement et diffusées à l'ensemble des employés.

[7] Cet incident met aussi en lumière la quantité de renseignements personnels qu'une entreprise peut conserver sur une personne physique. Il démontre l'importance pour une entreprise d'adopter des procédures visant à limiter l'accès à ces renseignements une fois que les fins pour lesquelles ils ont été recueillis sont accomplies ou encore à les détruire. En effet, l'incident vise les renseignements de près de 4 millions de membres ou de clients qui ne faisaient plus affaire avec Desjardins.

[8] Desjardins a manqué à plusieurs de ses obligations en matière de protection des renseignements personnels. Par exemple, informée de certaines vulnérabilités susceptibles d'affecter la protection des renseignements personnels qu'elle détient, elle a failli à son obligation de mettre en place avec diligence des mesures de protection et de détection proportionnelles à leur sensibilité et à leur quantité. Cela a permis à l'incident de se produire sur une période de 26 mois sans que Desjardins ne le détecte. L'entreprise en a été informée par le Service de police de Laval.

[9] Une fois alertée, Desjardins a pris un certain nombre de mesures pour éviter que pareille situation ne se reproduise et a proposé un plan d'action et un programme « cycle de vie des données ». La Commission d'accès à l'information (la Commission) s'en déclare satisfaite et s'assurera que leur déploiement soit complété au terme des échéanciers prévus.

[10] À cette fin, la Commission rend plusieurs ordonnances que Desjardins s'est engagée à respecter.

CONTEXTE

[11] Le 27 mai 2019, Desjardins déclare à la Commission avoir fait l'objet d'un incident de sécurité portant atteinte aux renseignements personnels d'environ

16 000 personnes[2]. Au final, ce sont quelque 9,7 millions de personnes[3] qui sont concernées par cet incident.

[12] Desjardins déclare que l'incident vise aussi bien des membres particuliers (les membres) que des entreprises clientes (les clients), actifs et inactifs. Elle précise que cet incident, en plus d'impliquer des membres et des clients situés au Québec, affecte également des personnes se trouvant dans les autres provinces et territoires du Canada, mais aussi à l'extérieur du Canada. Desjardins avise d'ailleurs les différentes autorités de protection des renseignements personnels ailleurs au Canada ainsi que l'Autorité des marchés financiers[4].

[13] Le 20 juin 2019, Desjardins tient une conférence de presse et publie un communiqué[5] reprenant les éléments déclarés à la Commission.

[14] On peut lire dans ce communiqué que Desjardins a été avisée de l'incident de sécurité par le Service de police de Laval alors que celui-ci faisait enquête dans le cadre d'un autre dossier[6]. Le communiqué indique notamment que :

- les renseignements personnels visés par l'incident concernent des membres et des clients;
- les personnes concernées seront avisées et que des mesures de protection ont été déployées pour l'ensemble des membres et des clients[7];
- les mots de passe, les questions de sécurité et les numéros d'identification personnels n'ont pas été compromis;

---

2 *Formulaire de déclaration d'un incident de sécurité portant atteinte à des renseignements personnels* transmis le 27 mai 2019, modifié les 20 juin et 10 décembre 2019, ci-après « Formulaire de déclaration ».

3 Réponse de Desjardins en date du 28 août 2020.

4 Formulaire de déclaration, précité, note 2.

5 « Déclaration de Desjardins concernant un accès non autorisé à certains renseignements de ses membres », Communiqué de presse, 20 juin 2019. Ce communiqué a été transmis à la Commission ce même jour avec une mise à jour du Formulaire de déclaration. Il convient de préciser que de nouveaux communiqués ont été diffusés par la suite au gré des découvertes quant à la portée de l'incident de sécurité.

6 Desjardins a précisé que l'enquête dans cet autre dossier visait une stratégie de vol d'identité et que « la piste d'une exfiltration non autorisée n'est pas envisagée à l'automne 2018 en raison de l'absence d'éléments pouvant laisser soupçonner cette dernière ». Réponse de Desjardins en date du 20 décembre 2019.

7 Il convient de préciser qu'en août 2020, la Commission a appris, dans les médias, que l'incident de sécurité visait également quelque 10 000 personnes clientes de Valeurs mobilières Desjardins. Desjardins soutient que ces personnes étaient comprises dans les chiffres divulgués en décembre 2019 et qu'elles ont été avisées par lettre en juin 2020.

- Desjardins n'a pas été victime d'une cyberattaque, mais que l'incident de sécurité est le fait d'un seul employé qui depuis a été congédié (l'Employé);
- les personnes concernées pourront souscrire à un service de surveillance de leurs dossiers de crédit et d'assurance[8].

[15] Sur la base de la déclaration de mai 2019 et des informations transmises en juin 2019, la Commission déclenche une enquête de sa propre initiative[9] quant aux pratiques de Desjardins en matière de protection des renseignements personnels.

[16] Également, la Commission signe, le 25 juillet 2019, une entente de collaboration avec le Commissariat à la protection de la vie privée du Canada afin de coordonner leurs actions relativement à leurs enquêtes respectives concernant cet incident.

OBJET DE L'ENQUÊTE

[17] L'enquête menée auprès de Desjardins porte sur les causes et circonstances ayant conduit à l'incident de sécurité déclaré en mai 2019. Elle porte, plus particulièrement, sur la gestion des accès aux renseignements personnels au sein de l'équipe d'où provient l'incident, sur les mesures de sécurité propres à assurer la protection des renseignements personnels qui étaient en place au moment de l'incident et sur celles qui ont été prises à la suite de celui-ci pour éviter qu'une telle situation ne se reproduise.

[18] Il convient de préciser que l'enquête ne porte pas sur le parcours des renseignements personnels après leur fuite, ni sur leur utilisation possible à des fins illégitimes par des personnes à l'extérieur de Desjardins.

AVIS D'INTENTION DE LA COMMISSION AU TERME DE L'ENQUÊTE

[19] Au terme de l'enquête, la Commission transmet, par courriel, un avis d'intention à Desjardins le 8 octobre 2020.

---

8 Au départ, le service de surveillance était offert pour une période de 12 mois. Cette période a été augmentée à 5 ans. Voir le communiqué de presse transmis le 20 juin 2019, mais aussi la réponse de Desjardins en date du 18 novembre 2019.

9 Loi sur le privé, article 81. Il faut noter que la Commission a répondu à plusieurs demandes formulées par les citoyens au lendemain de la divulgation au public de cet incident de sécurité.

[20] Dans cet avis, la Commission dresse plusieurs constats quant à la nature des renseignements visés par l'incident et à l'environnement de travail mis à la disposition de l'Employé par Desjardins. Elle constate également que le respect de plusieurs dispositions de la Loi sur le privé est mis en question par l'enquête.

[21] Plus spécifiquement, la Commission précise que selon les informations au dossier, elle pourrait conclure que Desjardins n'a pas respecté :

- l'article 10 de la Loi sur le privé en n'ayant pas pris les mesures nécessaires pour assurer la sécurité des renseignements personnels qu'elle détient au sujet des membres et des clients, actifs et inactifs, et pour prévenir l'utilisation non autorisée de ceux-ci, considérant notamment la quantité et la sensibilité des renseignements en cause;
- l'article 20 de la Loi sur le privé en ne limitant pas l'accès aux renseignements personnels des membres et des clients, actuels et anciens, déposés dans les répertoires partagés, situation faisant en sorte que l'Employé a pu avoir accès à des renseignements personnels qui n'étaient pas nécessaires à l'exercice de ses fonctions et pour lesquels il n'avait pas les droits d'accès;
- l'article 12 de la Loi sur le privé en n'ayant pas pris les mesures nécessaires pour limiter ou cesser l'utilisation des dossiers inactifs et, par le fait même, des renseignements personnels qui y figurent, une fois l'objet de ces dossiers accompli.

[22] Par ailleurs, cet avis informe Desjardins des ordonnances que la Commission pourrait prononcer pour éviter qu'un tel incident ne se reproduise, mais aussi pour apprécier la mise en œuvre des mesures propres à assurer la protection des renseignements personnels des membres et clients de Desjardins et exercer son pouvoir de surveillance quant à ces mesures.

OBSERVATIONS DE DESJARDINS

[23] Les 9 et 16 novembre 2020, Desjardins transmet ses observations à la Commission. Desjardins ne conteste pas les faits, mais souhaite apporter certaines nuances à des affirmations contenues dans l'avis d'intention. Desjardins ne remet pas en cause les conclusions de la Commission et s'est engagée à respecter les ordonnances énoncées dans l'avis d'intention. Elle indique toutefois que la mise en œuvre de certaines d'entre elles pourrait nécessiter plus de temps par rapport à ce qui est indiqué dans l'avis d'intention.

[24] Les principaux éléments que souhaite souligner Desjardins ont trait à l'environnement de travail mis à la disposition de l'Employé, mais aussi aux mesures de sécurité en place lors de l'incident de sécurité et à celles déployées à la suite de celui-ci.

ANALYSE

[25] Au regard des observations de Desjardins transmises en cours d'enquête[10] et à la suite de l'avis d'intention[11], la Commission examine les faits à l'origine de l'incident de sécurité ainsi que les pratiques de Desjardins

[26] Cette analyse se fait en vertu de la Loi sur le privé qui établit des règles relatives à la collecte, à l'utilisation, à la détention et à la communication de renseignements personnels à l'occasion de l'exploitation d'une entreprise[12].

1. Desjardins est assujettie à la Loi sur le privé

[27] Desjardins est une coopérative de services financiers qui exerce ses activités au Québec[13]. À ce titre, elle est soumise à la Loi sur le privé.

2. Les renseignements visés par l'incident de sécurité sont des renseignements personnels sensibles

[28] La Loi sur le privé prévoit que les renseignements qui concernent une personne physique et permettent de l'identifier constituent des renseignements personnels, et ce, quelles que soient la nature de leur support et la forme sous laquelle ils sont accessibles[14].

[29] Il ressort de l'enquête que l'incident de sécurité vise aussi bien des membres que des clients, actifs et inactifs.

---

[10] Desjardins a répondu aux questions écrites des analystes-enquêteurs de la Direction de la surveillance de la Commission en date des 18 novembre et 20 décembre 2019 et des 14 janvier, 13 mars, 23 juin, 5 et 29 août 2020. Desjardins a également répondu aux questions posées lors de rencontres, téléphonique ou en personne, qui ont eu lieu les 3 février, 30 juin, 16 et 17 juillet 2020. La Commission a pris connaissance de ces réponses et des documents transmis au soutien de celles-ci. Elle fonde la présente décision sur l'ensemble de ces éléments.

[11] Desjardins a répondu à l'avis d'intention de la Commission les 9 et 16 novembre 2020. La Commission a pris connaissance des observations de Desjardins et en tient compte dans la présente décision.

[12] Loi sur le privé, article 1.

[13] Desjardins est enregistrée au Registre des entreprises du Québec sous le numéro 1160196300.

[14] Loi sur le privé, articles 1 et 2.

a) Les renseignements personnels des membres

[30] Desjardins précise que « les renseignements personnels impliqués dans la fuite sont les suivants :

- nom et prénom;
- date de naissance;
- numéro d'assurance sociale;
- adresse de résidence;
- numéro de téléphone;
- adresse de courriel;
- certains renseignements au sujet des habitudes transactionnelles des membres (ex. type de produit, solde de compte, indicateur de forfait bancaire, nombre de cartes détenues, nombre d'hypothèques, utilisation d'AccèsD, indicateur de sollicitation, ancienneté du membre à la caisse, nombre de transactions sur [s]es différentes plateformes) »[15].

[31] Cette dernière catégorie est composée à la fois des renseignements fournis par le membre lorsqu'il transige avec Desjardins, mais aussi des analyses faites par les employés relevant du corps d'emploi « Affaires – Marketing » (ci-après « équipe marketing »), dont faisait partie l'Employé et qui se compose de plusieurs directions. Ces analyses sont réalisées à partir des bases de données auxquelles les employés de l'équipe marketing ont accès dans le cadre de leurs fonctions.

[32] Les renseignements personnels des membres visés par l'incident de sécurité vont donc au-delà des noms, prénoms, dates de naissance, numéros d'assurance sociale, adresses de résidence et de courriel et numéros de téléphone. Ils concernent également les habitudes transactionnelles d'un membre. Cet ensemble de renseignements est particulièrement sensible, ce qui a des incidences sur le niveau de protection que Desjardins devait mettre en place et assurer en tout temps à leur égard.

b) Les renseignements personnels des clients

[33] En plus d'offrir des produits et des services aux membres, Desjardins dessert également une clientèle d'affaires allant du travailleur autonome aux

---

[15] Réponses de Desjardins en date des 18 novembre et 20 décembre 2019.

grandes entreprises, en passant par des organismes à vocation communautaire. Parmi les renseignements des clients visés par l'incident de sécurité, on retrouve les renseignements personnels concernant les propriétaires et les dirigeants de ces entités ou encore les utilisateurs des services aux entreprises. Il en va ainsi de leurs :

- nom et prénom;
- date de naissance;
- numéro d'assurance sociale;
- adresse de résidence;
- numéro de téléphone;
- adresse de courriel;
- pourcentage de détention des actions dans Desjardins.

[34] Que ce soit pour les membres ou les clients, les renseignements précédemment décrits constituent des renseignements personnels, car ils permettent de faire connaître quelque chose (un renseignement) qui concerne une personne physique et permet de l'identifier.

[35] Aussi, seuls ou combinés, plusieurs de ces renseignements personnels peuvent être qualifiés de sensibles. Il en va notamment ainsi du numéro d'assurance sociale, qui constitue un identifiant unique prisé par les fraudeurs, ou encore des renseignements au sujet des habitudes transactionnelles, qui permettent d'établir le profil financier d'une personne en vue de lui proposer divers produits ou services offerts par Desjardins.

3. L'environnement de travail mis à la disposition de l'Employé par Desjardins a permis que l'incident de sécurité se produise

[36] Pour réaliser leurs mandats, les employés de l'équipe marketing, incluant l'Employé, pouvaient, à partir de leurs postes de travail et via un environnement virtuel, accéder :

- à un « outil de requête et d'analyse » comprenant une interface de requête et des répertoires partagés;
- aux différents entrepôts de données de Desjardins, en fonction de leurs droits d'accès. En l'espèce, deux entrepôts de données sont visés par l'incident : celui de données bancaires et celui de données de crédit.

a) L’entrepôt de données bancaires

[37] L’entrepôt de données bancaires[16] était segmenté en deux parties :

- une dite « confidentielle », à accès restreint, incluant les prénoms, noms, adresses, dates de naissance et numéros d’assurance sociale;
- une dite « non confidentielle », plus largement accessible, excluant ces renseignements personnels.

[38] L’Employé avait seulement accès à la partie non confidentielle de cet entrepôt. Il n’avait donc pas accès aux prénoms, noms, adresses, dates de naissance et numéros d’assurance sociale contenus dans cette base de données.

b) L’entrepôt de données de crédit

[39] L’entrepôt de données de crédit n’était pas segmenté. Ainsi, l’ensemble des renseignements qu’il contient étaient accessibles à tout employé ayant les accès requis[17], ce qui était le cas de l’Employé.

[40] Par le biais de cet entrepôt, l’Employé avait accès aux renseignements personnels suivants : prénoms, noms, adresses, numéros de téléphone, courriels, numéros d’assurance sociale et dates de naissance. Il avait donc accès à des renseignements personnels auxquels il n’avait pas accès par le biais de l’entrepôt de données bancaires.

[41] Les prénoms, noms, adresses, dates de naissance et numéros d’assurance sociale ne faisaient donc pas l’objet du même niveau de protection selon l’entrepôt de données dans lequel ils se trouvaient.

[42] L’accès aux différents entrepôts de données est accordé en fonction du rôle de chaque employé au sein de Desjardins. Les employés n’avaient donc pas tous les mêmes droits d’accès à ces entrepôts. L’Employé avait accès à la partie non confidentielle de l’entrepôt de données bancaires et à l’entrepôt de données de crédit, mais pas à la partie confidentielle de l’entrepôt de données bancaires.

c) Les répertoires partagés et leurs sous-répertoires

[43] Les employés de l’équipe marketing avaient aussi accès à des répertoires partagés. Dans ces répertoires, les employés pouvaient entre autres :

---

[16] En cours d’enquête, Desjardins a indiqué qu’en plus de l’Employé, plusieurs personnes avaient accès à cet entrepôt de données.

[17] En cours d’enquête, Desjardins a indiqué qu’en plus de l’Employé, plusieurs personnes avaient accès à cet entrepôt de données.

- déposer les résultats de leurs recherches effectuées par le biais des entrepôts de données auxquels ils avaient accès;
- transférer, manuellement ou automatiquement sur une base régulière, des données extraites des entrepôts auxquels ils avaient accès, incluant ceux à accès restreint.

[44] Ces répertoires contiennent des sous-répertoires accessibles à tous et des sous-répertoires à accès restreint. Selon Desjardins, les résultats de recherches contenant des informations confidentielles auraient dû être déposés dans les sous-répertoires à accès restreint, comme prescrit par ses directives, et non dans ceux accessibles à tous. Desjardins reconnaît que l'utilisation des dépôts de données dans les répertoires partagés de l'équipe marketing était contraire aux encadrements en place au moment de l'incident et aux meilleures pratiques de travail[18].

[45] Par conséquent, des résultats de recherches et des données provenant d'entrepôts à accès restreint ont été déposés dans les répertoires communs accessibles à l'ensemble de l'équipe marketing. Ce faisant, des renseignements personnels étaient accessibles à tous les employés de cette équipe, et ce, peu importe leurs droits d'accès aux entrepôts de données.

[46] En ayant accès aux répertoires partagés et, par le fait même, aux résultats de recherches qui y étaient déposés, l'Employé a pu, à l'aide de ses propres scripts, compiler les données des entrepôts de données auxquelles il avait accès avec celles auxquelles il n'avait pas accès. Il a alors pu constituer des fichiers d'extraction qu'il a fait transiter sur son poste de travail via l'outil de partage de fichiers. Par la suite, il a pu les exporter sur des périphériques amovibles de stockage de type clés USB.

[47] Les scripts utilisés par l'Employé lui ont permis de compiler les renseignements personnels décrits aux paragraphes [30] et [33] concernant les membres et les clients, actifs et inactifs, de Desjardins. C'est ce que Desjardins nomme « le stratagème ».

[48] Au regard de ce qui précède, la Commission constate que certains employés de l'équipe marketing n'ont pas respecté une des directives de Desjardins indiquant que le dépôt d'informations confidentielles, comme celles issues d'entrepôts de données à accès restreint, n'est permis que dans un répertoire dont les accès sont restreints aux seules personnes autorisées[19]. Elle

---

[18] Réponse de Desjardins en date du 9 novembre 2020.

[19] *Directive Mouvement sur l'utilisation des technologies*, 2013 (révisée en 2016).

constate également que les mesures en place au moment de l'incident pour contrôler l'accessibilité et la sécurité des renseignements personnels n'étaient pas efficientes.

[49] L'enquête démontre, en effet, qu'un certain laps de temps s'est écoulé avant que Desjardins ne se rende compte de l'incident de sécurité, celui-ci ayant possiblement débuté en mars 2017.

4. Les mesures en place au moment de l'incident n'étaient pas efficientes

[50] Une personne qui exploite une entreprise doit prendre des mesures pour assurer la protection des renseignements personnels qu'elle détient. Ces mesures doivent être administratives ou organisationnelles, physiques et techniques. Elles doivent être documentées, mises en œuvre, surveillées, révisées régulièrement et être diffusées à l'ensemble des personnes travaillant au sein de l'entreprise.

[51] Bien que Desjardins ait adopté un cadre de gestion en matière de protection des renseignements personnels, sa mise en œuvre et les mesures de surveillance et de contrôle de son efficacité n'étaient pas suffisantes. Cette lacune a contribué à ce que l'incident de sécurité puisse se produire.

a) Les mesures visant à limiter l'accès aux renseignements personnels n'étaient pas adéquates

[52] La Loi sur le privé prévoit qu'un renseignement personnel n'est accessible à tout employé qui a qualité pour le connaître qu'à la condition que ce renseignement soit nécessaire à l'exercice de ses fonctions[20].

[53] Desjardins avait donc l'obligation de prendre des mesures pour limiter et contrôler l'accès aux renseignements personnels visés par l'incident, notamment compte tenu de la quantité et de la nature sensible des renseignements personnels contenus dans les entrepôts de données et les répertoires partagés.

[54] Or, l'enquête révèle que les mesures en place n'étaient pas adéquates.

[55] Desjardins disposait de certains moyens visant à restreindre l'accès aux renseignements personnels qu'elle détenait pendant la période durant laquelle l'incident de sécurité s'est produit. Par exemple :

---

[20] Loi sur le privé, article 20.

- les autorisations d'accès aux renseignements personnels étaient basées sur les principes du moindre privilège, visant à n'accorder à un employé que les accès requis à l'exercice de ses fonctions, du besoin de savoir dans le cadre des fonctions et de l'autorisation du propriétaire de l'information;
- pour qu'un employé puisse accéder aux différentes ressources dont il avait besoin pour effectuer ses tâches, son supérieur immédiat devait en faire la demande auprès du responsable de la gestion des accès;
- les employés devaient prendre connaissance d'un certain nombre de documents précisant les règles de confidentialité, dont les droits et obligations de chacun, le fait que l'accès à l'environnement de travail est accordé uniquement dans le cadre des fonctions exercées au sein de Desjardins ou encore les modalités de sauvegarde et d'utilisation des technologies. Ils devaient signer annuellement une attestation à l'effet qu'ils avaient pris connaissance du *Code de déontologie* de Desjardins[21].

L'Employé avait signé, tous les ans depuis son embauche, cette attestation ainsi que l'engagement relatif aux conditions d'utilisation de l'entrepôt de données bancaires.

[56] Par ailleurs, l'Employé avait obtenu les autorisations requises pour accéder à certains entrepôts de données, environnements et répertoires partagés dans l'exercice de ses fonctions. Ainsi, à titre de conseiller principal en stratégie d'affaires au sein de l'équipe marketing, l'Employé avait accès :

- à la partie non confidentielle de l'entrepôt de données bancaires;
- à l'entrepôt de données de crédit;
- au Comptoir clientèle, qui ne contient pas de renseignements personnels;
- à des environnements d'intelligence d'affaires; et
- aux répertoires partagés par l'équipe marketing.

[57] Toutefois, comme décrit aux paragraphes [43] et suivants, l'Employé a eu accès à des renseignements personnels qui n'étaient pas nécessaires à

---

[21] *Code de déontologie,* décembre 2018. On peut lire dans ce code que « Vous ne devez accéder qu'aux renseignements confidentiels exigés par vos fonctions et uniquement dans la mesure requise par vos fonctions. […] Vous ne devez pas faire usage de renseignements confidentiels pour votre propre bénéfice ou celui d'une autre personne. Les obligations mentionnées dans le présent article subsistent même après que vous ayez cessé d'occuper votre fonction ou votre emploi. ».

l’exercice de ses fonctions. En effet, ayant accès aux répertoires partagés avec les autres employés de l’équipe marketing, l’Employé a pu, à l’aide de ses propres scripts, compiler des données auxquelles il avait accès avec les résultats de recherches et les transferts provenant des autres employés de son équipe qui étaient déposés dans les répertoires communs plutôt que dans les répertoires protégés par des droits d’accès restreint. Il a alors pu les faire transiter sur son poste de travail et les exporter sur des périphériques amovibles de stockage.

[58] Par conséquent, la Commission considère que, malgré les directives en place pendant la période durant laquelle l’incident de sécurité s’est produit, Desjardins n’a pas pris les mesures nécessaires pour limiter l’accès aux renseignements personnels des membres et des clients, actifs et inactifs, déposés dans les répertoires partagés, ce qui a permis à l’Employé d’avoir accès à des renseignements personnels qui n’étaient pas nécessaires à l’exercice de ses fonctions et pour lesquels il n’avait pas les droits d’accès.

[59] Desjardins a donc manqué à l’obligation qui lui incombe d’adopter des mesures visant à limiter l’accès aux seuls renseignements personnels nécessaires aux employés dans le cadre de leurs fonctions, en vertu de l’article 20 de la Loi sur le privé.

b) Le contrôle des mesures propres à assurer la sécurité des renseignements personnels n’était pas suffisant

[60] La Loi sur le privé prévoit que toute personne qui exploite une entreprise doit prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits. Ces mesures doivent être raisonnables compte tenu, notamment, de la sensibilité, de la finalité, de la quantité, de la répartition et du support des renseignements personnels[22].

[61] Desjardins avait donc l’obligation de mettre en place des mesures de prévention, de détection et de contrôle visant à assurer la protection des renseignements personnels auxquels avaient accès les employés de l’équipe marketing dont faisait partie l’Employé.

[62] Or, l’enquête révèle que les mesures en place n’étaient pas suffisantes.

[63] Desjardins a adopté des politiques, guides et autres documents visant à assurer la protection des renseignements personnels. Toutefois, Desjardins n’a

[22] Loi sur le privé, article 10.

pas exercé un contrôle actif de ces mesures. Desjardins reconnaît ne pas avoir « assuré une mise en œuvre complète et intégrée de ces mesures »[23].

[64] Par exemple, pendant toute la période durant laquelle l'incident de sécurité s'est produit :

- les mesures mises en place par Desjardins ne lui permettaient pas de connaître l'ensemble de l'historique des manipulations réalisées par l'Employé, le nombre d'extractions de renseignements qu'il a pu réaliser et le nombre de personnes concernées par l'incident de sécurité;
- la journalisation et la surveillance au niveau des applications étaient partiellement en place et la surveillance était essentiellement passive, car elle se faisait uniquement à la suite d'un incident;
- le blocage des ports USB n'était pas activé pour les employés de l'équipe marketing;
- il n'y avait aucune limite physique quant au volume de données pouvant être téléchargées sur des périphériques amovibles de stockage;
- les revues d'accès à la partie confidentielle de l'entrepôt de données bancaires se faisaient sur une fréquence de 12 à 18 mois et il n'y en avait pas pour l'entrepôt de données de crédit.

[65] De plus, Desjardins était informée des possibles menaces externes et internes en raison de différentes analyses réalisées au cours de la période durant laquelle l'incident s'est produit. Ces analyses ont été réalisées à l'interne, mais aussi à l'externe, notamment à la suite d'une demande de l'Autorité des marchés financiers. Ces analyses visaient notamment à évaluer la maturité des pratiques de Desjardins en matière de sécurité ou encore à identifier et à encadrer les risques pouvant mener à une fuite d'information.

[66] Certaines recommandations contenues dans ces analyses concernaient justement des vulnérabilités qui ont été exploitées par l'Employé pour exfiltrer les renseignements personnels : l'utilisation de dispositifs de stockage amovibles, compte tenu du risque très élevé de fuite d'information par vecteurs physiques, tels que des clés USB; l'accès aux bases de données; la gestion de l'octroi des droits d'accès; la poursuite de la mise en place, tant vis-à-vis de l'externe que de l'interne, de la stratégie de prévention des fuites de données, intentionnelles ou non (DLP pour « data loss prevention »).

---

[23] Réponse de Desjardins en date du 9 novembre 2020.

[67] Or, la mise en place de plusieurs de ces recommandations n'était pas effectuée ou terminée en mai 2019, lorsque Desjardins a été informée de l'incident de sécurité par le Service de police de Laval. C'est notamment le cas du blocage des ports USB et du déploiement de la stratégie DLP.

[68] Par conséquent, compte tenu de la connaissance qu'avait Desjardins des risques possibles quant à la sécurité des renseignements personnels à l'interne, elle aurait dû réaliser davantage de contrôles actifs de la sécurité des renseignements personnels et sensibles qu'elle détient et mettre en place plus rapidement des mesures visant à pallier les vulnérabilités identifiées dans les analyses réalisées au cours de la période durant laquelle l'incident s'est produit.

[69] Desjardins a donc manqué à son obligation, prévue à l'article 10 de la Loi sur le privé, puisqu'elle n'avait pas pris les mesures nécessaires pour assurer la sécurité des renseignements personnels qu'elle détient au sujet des membres et des clients, actifs et inactifs, compte tenu notamment de la quantité et de la sensibilité des renseignements auxquels les employés de l'équipe marketing pouvaient avoir accès.

[70] Desjardins a indiqué à la Commission qu'elle a pris certaines mesures et qu'elle entend en appliquer d'autres d'ici à la fin du quatrième trimestre 2021 pour éviter que pareille situation ne se reproduise. Ces mesures sont décrites dans un plan d'action[24] qui présente une vue d'ensemble des activités à mettre en place pour renforcer la sécurité physique et de l'information de Desjardins, mais aussi la protection des renseignements personnels qu'elle détient. La Commission s'assurera que ces mesures sont complétées et mises en œuvre selon cet échéancier.

c) Les mesures visant à limiter ou à cesser l'utilisation des renseignements personnels une fois l'objet du dossier accompli étaient insuffisantes

[71] La Loi sur le privé prévoit que l'utilisation des renseignements contenus dans un dossier n'est permise, une fois l'objet du dossier accompli, qu'avec le consentement de la personne concernée, sous réserve de délais prévus par la loi ou par un calendrier de conservation établi par règlement du gouvernement[25].

---

[24] Dans le cadre de la présente décision, la Commission réfère au plan d'action de Desjardins daté du 9 juin 2020. Dans ses observations transmises le 16 novembre 2020 à la suite de l'avis d'intention de la Commission, Desjardins a précisé l'état d'avancement de certaines des mesures prévues dans ledit plan.

[25] Loi sur le privé, article 12.

[72] Desjardins devait donc prendre des mesures pour limiter ou cesser l'utilisation des dossiers inactifs.

[73] Or, l'enquête révèle que des renseignements personnels contenus dans des dossiers inactifs sont concernés par l'incident de sécurité, soit presque 4 millions de dossiers. Desjardins reconnaît ce fait et précise qu'un dossier est considéré comme inactif lorsque le membre cesse complètement de faire affaire avec elle[26].

[74] Desjardins a une politique[27] et une directive[28] énonçant plusieurs principes quant à la conservation des renseignements personnels. Elle a également précisé avoir respecté les délais de conservation prévus dans les différentes lois et différents règlements, fédéraux et provinciaux, applicables aux produits et services qu'elle offre aux membres et aux clients[29].

[75] Ainsi, pour ce qui est de l'entrepôt de données bancaires, « il y avait une épuration après 20 ans pour ce qui est du volet de détention de produit et transactionnel »[30]. Toutefois, malgré les questions posées lors de l'enquête, Desjardins n'a pas été en mesure de préciser le calendrier de conservation des comptes inactifs.

[76] Par ailleurs, même si aujourd'hui les utilisateurs de l'entrepôt de données bancaires semblent n'avoir accès qu'aux dossiers actifs et inactifs des 8 dernières années, l'enquête révèle que Desjardins ne semble pas disposer de mesures visant à limiter ou cesser l'utilisation de renseignements personnels, une fois l'objet du dossier accompli, pour l'ensemble des bases de données et répertoires mis à la disposition de ses employés.

[77] Par conséquent, la Commission conclut que Desjardins n'a pas pris les mesures nécessaires pour limiter ou cesser l'utilisation des dossiers inactifs et, par le fait même, des renseignements personnels qui y figurent, une fois l'objet de ces dossiers étant accompli.

[78] Desjardins indique être en train de développer un calendrier de conservation et un processus visant à limiter, archiver, détruire, masquer ou anonymiser les renseignements personnels détenus par Desjardins. Ce programme « cycle de vie des données » se fera en trois étapes de six mois et

---

26 Réponse de Desjardins en date du 18 novembre 2019.
27 *Politique sur la protection des renseignements personnels*, 2005 (dernière révision 2019).
28 *Directive Mouvement sur la gestion des documents*, 2017.
29 Réponse de Desjardins en date du 18 novembre 2019.
30 Réponse de Desjardins en date du 23 juin 2020.

devrait être complété fin juin 2022[31]. La Commission s'assurera que ces mesures sont complétées et mises en œuvre selon cet échéancier.

d) Les autres mesures organisationnelles mises en place avant l'incident de sécurité

[79] Avant l'incident de sécurité, en plus des éléments décrits précédemment, Desjardins avait :

- adopté plusieurs directives visant à établir une « stratégie globale de protection des renseignements personnels [incluant] un ensemble de moyens touchant aux ressources humaines, aux processus et aux technologies » [32]. Desjardins indique cependant que la mise en œuvre de celles-ci « n'était pas complète et intégrée au moment de l'incident »[33];
- nommé un Chef de la sécurité de l'information, un Chef de la protection des renseignements personnels, un comité de gestion de la sécurité Mouvement (tactique) regroupant les parties prenantes de l'écosystème de gestion de la sécurité et un comité d'évolution de la sécurité Mouvement (stratégique). Relativement au Chef de la protection des renseignements personnels, Desjardins indique que son positionnement hiérarchique a été revu afin de lui permettre d'avoir un impact plus transversal[34].

[80] Desjardins avait également adopté différentes mesures de prévention, dont les suivantes :

- enquêtes de sécurité : Desjardins indique qu'elle procéde à de telles enquêtes au moment de l'entrée en fonction des nouveaux employés, lors de certains mouvements de personnel et en cours d'emploi pour certains postes et que l'Employé a fait l'objet de telles enquêtes;
- signature d'engagements quant à la confidentialité et aux modalités d'utilisation des ressources mises à la disposition des employés : Desjardins indique qu'au moment de leur intégration, les employés doivent prendre connaissance d'un certain nombre de documents. Parmi ces documents, on retrouve la *Politique sur la protection des*

---

31 Dans le cadre de la présente décision, la Commission réfère au programme « cycle de vie des données » de Desjardins soumis le 16 novembre 2020.
32 Réponse de Desjardins en date du 18 novembre 2019.
33 Réponse de Desjardins en date du 9 novembre 2020.
34 Réponse de Desjardins en date du 5 août 2020.

renseignements personnels, la *Directive sur l'utilisation acceptable des technologies* et le *Code de déontologie* de Desjardins;

- formation et sensibilisation : Desjardins indique que tous les employés doivent suivre une formation quant à la sécurité de l'information et à la protection des renseignements personnels lors de l'embauche. Cette formation se déroule en ligne et les employés doivent répondre à certaines questions au cours de celle-ci. Desjardins indique également que des campagnes de sensibilisation sont réalisées tout au long de l'année auprès des employés pour rappeler les messages clés et les bonnes pratiques en matière de sécurité et de protection des renseignements personnels[35].

5. Les mesures prises par Desjardins à la suite de l'incident de sécurité

[81] Après avoir été informée de l'incident de sécurité par le Service de police de Laval, Desjardins a pris plusieurs mesures visant à informer les membres et clients touchés par l'incident de sécurité et à leur offrir un programme de protection (protection des actifs, services d'accompagnement, remboursement des frais) – que leur dossier soit actif ou inactif – et une inscription aux services de surveillance d'Équifax, incluant une assurance permanente en cas de vol d'identité à hauteur de 50 000$[36]. Desjardins a également offert, à tous ses membres utilisateurs d'*AccèsD*, un accès illimité à leur dossier de crédit auprès de TransUnion[37].

[82] Par ailleurs, Desjardins a aussi pris un certain nombre de mesures pour circonscrire la portée de l'incident et en a adopté de nouvelles pour éviter qu'un tel évènement ne se reproduise. Ces mesures sont énoncées dans son plan d'action[38]. D'autres, relatives à la conservation des renseignements personnels, sont décrites dans son programme « cycle de vie des données »[39].

[83] Sans passer en revue l'ensemble de ces mesures, les éléments suivants peuvent être soulignés parce qu'ils sont en lien avec certains aspects soulevés dans le cadre de la présente décision et visent à renforcer la protection des renseignements personnels au sein de Desjardins :

---

35 En cours d'enquête, Desjardins a transmis le plan d'intégration des nouveaux employés, ainsi que la liste des formations et des activités de sensibilisation adressées aux employés, avant et après l'incident de sécurité.

36 Réponses de Desjardins en date des 18 novembre 2019 et 20 décembre 2019. Voir également https://www.desjardins.com/renseignements-personnels/index.jsp.

37 Réponse de Desjardins en date du 9 novembre 2020.

38 Précité, note 24.

39 Précité, note 31.

- création du Bureau de la sécurité afin de fusionner, entre autres, l'ensemble des activités liées à la sécurité de l'information, à la sécurité physique, à la conformité et à la protection des renseignements personnels des membres et des clients[40];
- mise en place d'un Centre d'intelligence en sécurité et d'une équipe de sécurité dédiée aux menaces internes;
- augmentation de la fréquence des enquêtes de sécurité pour certains postes, dont les postes ayant des accès à haut privilège, compte tenu de la capacité d'extraction et de manipulation de masse des données confidentielles, ce qui était le cas du poste occupé par l'Employé. Les enquêtes seront renouvelées aux trois ans et non plus aux cinq ans;
- retrait des accès aux entrepôts de données bancaires et de crédit et réattribution de ceux-ci afin de réduire le nombre et les catégories d'employés ayant accès à ces bases de données;
- rencontre des gestionnaires et des employés ayant à accéder aux entrepôts de données bancaires et de crédit dans l'exercice de leurs fonctions pour leur rappeler les exigences en matière de sécurité et de modalités d'accès;
- blocage des médiums de stockage externes / amovibles pour tous les secteurs et toutes les directions;
- déploiement plus rapide de plusieurs processus de sécurité dont l'implantation était en cours ou à venir;
- mise en place d'un espace virtuel interne restrictif ne permettant plus de sauvegarder ou de télécharger des données sur le réseau ou sur un poste de travail;
- mise en place d'un processus de douane (c'est-à-dire une autorisation du supérieur immédiat) pour la sortie de fichiers hors de cet environnement;
- mise en place d'une surveillance active des journaux et des flux sortants;
- révision de la segmentation des entrepôts de données bancaires et de crédit, mais aussi des procédures du corps d'emploi « Affaires –

[40] En cours d'enquête, Desjardins mentionne qu'afin « d'envoyer un message clair à l'ensemble de l'organisation, un budget de 150 millions de dollars a été octroyé au Bureau de Sécurité, des ressources spécialisées ont été recrutées et [Desjardins] s'est assurée de retenir les services d'experts externes et internationaux afin de guider l'organisation vers les meilleures pratiques de l'industrie ». Réponse de Desjardins en date du 5 août 2020.

Marketing », notamment par le retrait du processus d'appariement à l'aide du numéro d'assurance sociale et par le fait que la date de naissance n'est plus utilisée dans les fichiers de sortie;

- mise en place du programme « cycle de vie des données » en vue de détruire, d'archiver, de masquer ou d'anonymiser les renseignements personnels détenus par Desjardins;
- révision de plusieurs politiques et directives et de la formation des employés.

[84] La Commission a pris connaissance de l'ensemble des mesures que Desjardins entend mettre en œuvre d'ici juin 2022. Considérant l'importance de ces mesures et le délai pour leur déploiement complet, Desjardins devra faire, sur une base régulière, une reddition de compte sur leur mise en œuvre, mais également faire réaliser une vérification indépendante. La Commission pourra ainsi apprécier la mise en œuvre des mesures annoncées propres à assurer la protection des renseignements personnels des membres et clients de Desjardins et exercer son pouvoir de surveillance quant à ces mesures.

[85] Desjardins s'est engagée à respecter les ordonnances de la Commission.

CONCLUSION

[86] À la lumière de ce qui précède, la Commission considère que Desjardins n'a pas respecté les articles 10, 12 et 20 de la Loi sur le privé en ce qui a trait au contrôle des mesures de sécurité, à l'accessibilité aux renseignements personnels et à l'utilisation faite de ceux-ci une fois l'objet du dossier accompli.

POUR CES MOTIFS, la Commission :

[87] **ORDONNE** à Desjardins de lui transmettre, tous les six mois à la suite de la réception de la présente décision, un état d'avancement détaillé du déploiement de l'ensemble des mesures décrites au plan d'action soumis à la Commission le 9 juin 2020, jusqu'à leur mise en place complète, prévue pour fin 2021. Desjardins devra informer la Commission de toutes les modifications qui pourraient être apportées à ces mesures et des motifs de ces modifications;

[88] **ORDONNE** à Desjardins de lui transmettre, tous les six mois à la suite de la réception de la présente décision, un état d'avancement détaillé des différentes mesures visant à limiter, à archiver, à détruire, à masquer ou à anonymiser les renseignements personnels détenus par Desjardins, telles que décrites au programme « cycle de vie des données » soumis à la Commission le 16 novembre

2020, jusqu'à leur déploiement complet, prévu pour juin 2022. Desjardins devra informer la Commission de toutes les modifications qui pourraient être apportées à ces mesures et des motifs de ces modifications;

[89] **ORDONNE** à Desjardins de lui transmettre, dans les deux ans suivant la réception de la présente décision, une évaluation par un auditeur externe indépendant, dont l'identité devra être approuvée par la Commission, relative à l'ensemble des mesures déployées et propres à assurer la protection des renseignements personnels des membres et clients, actuels et anciens, détenus par Desjardins. Cette évaluation devra notamment, mais non limitativement, porter sur :

- les mesures relatives à l'accessibilité aux renseignements personnels détenus par Desjardins et par son personnel ainsi qu'à la surveillance de celles-ci;
- les mesures de sécurité mises en place et propres à assurer la sécurité des renseignements personnels et la surveillance de celles-ci;
- les mesures relatives à la conservation et à l'utilisation des renseignements personnels une fois l'objet du dossier accompli;

[90] **INVITE** Desjardins à expliquer, lors de la transmission du rapport d'évaluation visé au paragraphe précédent, les raisons pour lesquelles elle accepte ou refuse de suivre les recommandations qui y seront contenues et, le cas échéant, à communiquer à la Commission le calendrier pour leur mise en œuvre.

« Original signé »

Cynthia Chassigneux
Membre de la Commission, section de surveillance