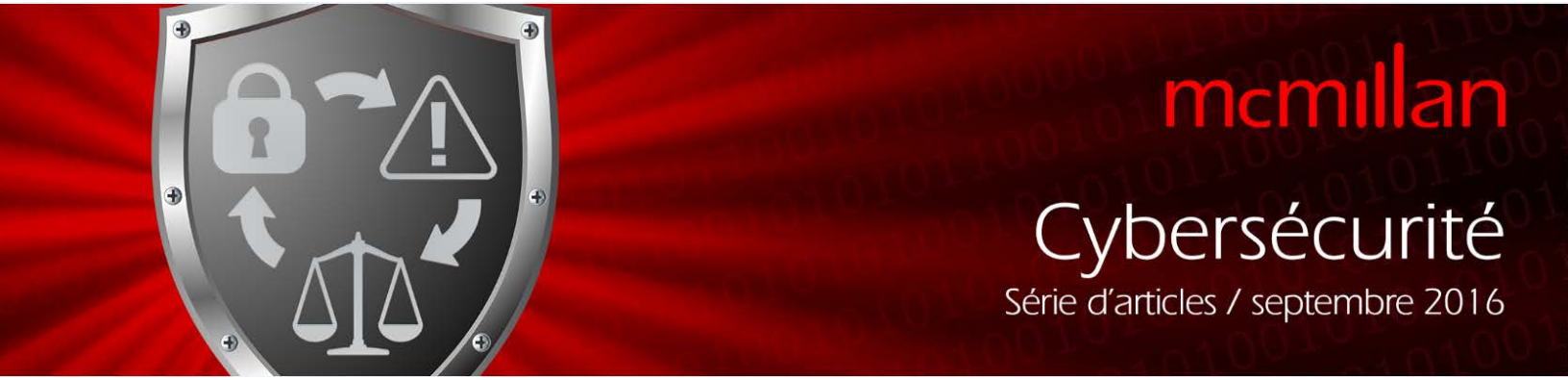

Transferts internationaux de données en provenance ou en direction du Canada

Transferts internationaux de données en provenance ou en direction du Canada à l'ère du Partenariat transpacifique et du Règlement général sur la protection des données: la mise en place de mesures de sécurité robustes protégeant les données personnelles doit être une priorité pour les entreprises canadiennes

Le régime canadien de protection des données personnelles est un régime complexe qui repose sur la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)[1]. Cette loi fédérale a été édictée en réponse, notamment, à la directive de 1995 relative à la protection des données (DPD)[2] de l'Union européenne. Certaines provinces, dont le Québec, l'Alberta et la Colombie-Britannique, ont adopté des lois essentiellement similaires à la LPRPDE, qui régissent la protection des données personnelles dans ces provinces. Ces lois fédérale et provinciales instaurent dans tous les secteurs d'activité un cadre de protection détaillé qui régit la collecte, l'utilisation et la communication des données personnelles.

Les entreprises canadiennes qui font affaire à l'extérieur du Canada, comme c'est souvent le cas dans le contexte actuel de la

---

[1] *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5.
[2] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, JO n° L 281 du 23/11/1995, p. 0031 à 0050
En ligne : *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fr:HTML*

mondialisation et de la cyberéconomie, doivent comprendre les lois nationales sur la protection des données, mais aussi les lois étrangères en cette matière qui sont susceptibles de s'appliquer à leurs employés, clients et fournisseurs.

La protection des données dans l'Union européenne

Outre-Atlantique, la DPD régit le traitement des données personnelles au sein des États membres de l'Union européenne. Les États-membres sont tenus d'adopter des lois qui posent des limites au transfert de données personnelles aux pays non-membres de l'Union européenne, sauf si ces pays fournissent un « **niveau de protection adéquat** » ou si les entités concernées ont mis en œuvre des mesures qui offrent le même niveau de protection (par exemple en utilisant des clauses contractuelles types ou des règles internes contraignantes).

Comme la Commission de l'Union européenne l'a établi il y a plus de 15 ans, la LPRPDE (y compris sa disposition prévoyant la reconnaissance d'une loi provinciale essentiellement similaire) satisfait à ce critère de « niveau de protection adéquat ». Ainsi, depuis 2001, les transferts de données personnelles de l'Union européenne vers le Canada sont jugés acceptables et, en principe, ne nécessitent aucune autre approbation de la part des autorités européennes chargées de la protection des données. Toutefois, au cours des dernières années, suivant les révélations continues concernant la facilité avec laquelle les pratiques de surveillance américaines peuvent capter des données provenant du Canada, plusieurs se sont demandé si ces événements pourraient mettre en péril la décision de la Commission de l'Union européenne relative au niveau adéquat.

L'invalidation de la « sphère de sécurité » Europe-États-Unis

Les États-Unis bénéficiaient d'un statut similaire à celui du Canada en tant que territoire offrant une protection adéquate, aux termes de la décision de la Commission 2000/520[3]. Dans cette décision, les

[3] 2000/520/CE : Décision de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et

transferts de données personnelles de l'Union européenne vers les États-Unis étaient acceptables lorsque l'organisation destinataire se conformait aux principes de la « sphère de sécurité » de la Communauté européenne et des États-Unis[4]. Cependant, la décision que la Cour de justice de l'Union européenne a rendue le 6 octobre 2015 dans l'affaire Schrems[5] a invalidé les principes de la « sphère de sécurité » et invalidé la décision d'adéquation de la Commission. Les organisations qui se fondaient auparavant sur les principes de la « sphère de sécurité » ont été prises au dépourvu et laissées en plan lorsque ce régime a soudainement été déclaré inopérant et que, dès lors, les transferts de données à partir de l'Union européenne vers les États-Unis basés sur ceux-ci sont devenus illégaux.

Bien que les États-Unis et la Commission européenne aient adopté en août dernier un nouveau programme appelé « Bouclier de protection des données UE-États-Unis », le groupe de travail de l'Article 29, qui regroupe les organismes européens de réglementation de données, a critiqué celui-ci en raison du manque de protection exercé par le gouvernement américain à l'égard des données de citoyens de l'Union européenne. En conséquence, et dans un contexte d'intensification des menaces pesant sur la sécurité des données, la démarche européenne et la localisation des données sont en voie de devenir un choix politique pertinent pour les pays qui se préoccupent de la faiblesse des garanties offertes à l'étranger.

Le nouveau régime européen

Le nouveau Règlement général sur la protection des données (RGPD), que le Parlement européen a adopté le 14 avril 2016, remplacera l'ancienne DPD. Lorsque le RGPD paraîtra officiellement dans le journal officiel de l'Union européenne, il s'appliquera directement à chaque État membre et harmonisera la protection des données à caractère personnel dans l'ensemble des pays de l'UE. Bien que nombre d'entreprises aient adopté des processus et des

---

par les questions souvent posées y afférentes, publiés par le ministère du Commerce des États-Unis d'Amérique, JO L 215 du 25/8/2000, p. 0007 à 0047
En ligne : *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:FR:HTML*

[4] Principes de la « sphère de sécurité » publiés par le ministère du Commerce des États-Unis d'Amérique, 21 juillet 2000.

[5] *Maximilian Schrems / Data Protection Commissioner,* affaire C-362/14.

procédures en matière de protection des données personnelles conformes à la DPD, le RGPD renferme un certain nombre de nouvelles protections pour les personnes concernées dans l'UE et prévoit de lourdes amendes et pénalités pour les organisations non conformes. Par conséquent les entreprises impliquées dans la collecte et le traitement de données personnelles de citoyens de l'Union vont devoir ajuster leurs processus et procédures.

Le RGPD permet les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale sous réserve de la conformité à un ensemble de conditions. À l'instar du mécanisme énoncé dans le DPD, le RGPD permet les transferts de données vers des pays dont le régime juridique, selon la Commission européenne, offre un niveau de protection « **adéquat** » quant aux données personnelles. Même en l'absence d'une décision d'adéquation, les transferts sont également permis vers des États en dehors de l'UE dans certaines circonstances, notamment dans le cadre de clauses types de protection des données ou de règles d'entreprise contraignantes (BCR).

Aux termes de la DPD, seules des personnes situées dans des pays tiers approuvés pouvaient recevoir des données à caractère personnel de personnes concernées de l'UE, et les décisions étaient rendues pour chaque pays. Le RGPD étend la portée de ces décisions sur le caractère adéquat et permet les transferts non seulement à des pays tiers approuvés, mais également à des territoires approuvés ou à des secteurs déterminés dans un pays tiers, voire à une organisation internationale. Lorsque la Commission européenne confère (ou retire) cette décision d'adéquation, sa décision lie tous les États membres de l'UE.

L'interdiction du TPP sur la création de restrictions en matière de transfert de données

Dans l'autre hémisphère, 12 pays bordant l'océan Pacifique ont signé l'Accord de partenariat transpacifique (TPP) le 4 février 2016, à savoir les États-Unis, le Japon, la Malaisie, le Vietnam, Singapour, Brunéi, l'Australie, la Nouvelle-Zélande, le Canada, le Mexique, le Chili et le Pérou. Fait intéressant, la Chine ne figure pas parmi les signataires.

Aux termes du TPP, les parties à l'accord sont tenues d'adopter ou de maintenir « un cadre juridique assurant la protection des renseignements personnels des usagers du commerce électronique » et, ce faisant, de « prendre en compte les principes et les lignes directrices énoncés par les organismes internationaux concernés ». Une note de bas de page précise que cette obligation peut être remplie de diverses façons, notamment « en adoptant ou en maintenant des mesures comme des lois d'ensemble pour protéger la vie privée, les renseignements personnels ou les données personnelles, des lois sectorielles visant la protection de la vie privée ou des lois prévoyant l'application d'engagements volontaires en matière de vie privée pris par les entreprises ».

Le TPP a pour principal objectif de faciliter le commerce mondial. Sur le plan de la protection des données personnelles et de la vie privée, le TPP permet les flux de données transfrontaliers et **interdit les exigences en matière de localisation de données**. Chaque pays membre du TPP est tenu d'autoriser « le transfert transfrontières de renseignements par voie électronique, y compris les renseignements personnels, lorsque cette activité s'inscrit dans le cadre d'activités commerciales exercées par une personne visée ». On pose comme hypothèse que le transfert de données à des fins commerciales devrait suffire, de telle sorte que les données personnelles devraient circuler librement entre des entreprises de pays membres du TPP, sans égard au ressort en cause.

En l'absence d'un « objectif légitime de politique publique », les pays **doivent obligatoirement** autoriser ce transfert transfrontières de données effectué dans le cours des affaires. En particulier, le TPP interdit les lois non financières qui exigent la localisation des données (c'est-à-dire des lois exigeant que les serveurs informatiques des entreprises soient situés dans un pays).

Le RGPD et le TPP, des forces contraires

En interdisant la création de restrictions en matière de transfert de données entre les pays signataires, le TPP a créé un conflit potentiel avec la DPD et le RGPD (qui restreignent les transferts de données aux seuls pays, territoires ou secteurs dont les lois satisfont aux critères du niveau de protection « adéquat »). À la lumière des obligations découlant du TPP, il y a donc un risque que la Commission

européenne révoque sa décision d'adéquation de 2001 relative au Canada.

Les entreprises canadiennes qui travaillent avec des organisations situées en Europe devront agir de façon proactive pour établir des mesures de protection rigoureuses qui répondent aux exigences du RGPD (par exemple les clauses contractuelles types de protection des données ou les règles d'entreprise contraignantes). Si la décision d'adéquation visant le Canada est effectivement révoquée, les entreprises qui auront mis en place cette protection de rechange demeureront des destinataires « sûrs » de données à caractère personnel de personnes de l'Union européenne.

par Elisa Henry, Darcy Ammerman et Michael Reid

Pour en savoir plus sur le sujet, veuillez communiquer avec les personnes suivantes :

Montréal	Elisa Henry	514.987.5083	elisa.henry@mcmillan.ca
Ottawa	Darcy Ammerman	613.691.6131	darcy.ammerman@mcmillan.ca
Vancouver	Michael E. Reid	778.328.1634	michael.reid@mcmillan.ca

Mise en garde