_swissprivacy.law

Regards croisés sur la Loi 25 : un pas vers la conformité européenne pour le Québec ?

Azza Khelil, le 23 avril 2024

L'adoption de la *Loi 25* représente un pas significatif vers la conformité européenne en matière de protection des données. Quelles sont les modifications clés introduites par cette réforme ? Le Québec pourrait-il se voir reconnaître une décision d'adéquation de la Commission européenne vis-à-vis du droit européen ?

Nota bene : La présente contribution fait partie d'une série de deux contributions consacrées au cadre juridique canadien en matière de protection des données (cf. www.swissprivacy.law/295). Cette seconde contribution présente la Loi 25 adoptée récemment par le Québec en vue de moderniser son système.

I. Présentation de la *Loi 25*

En septembre 2021, le parlement québécois a adopté la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (Loi 25).

Dans une ère ou l'usage de la technologie est à son apogée, cette réforme a été élaborée afin de faire face aux inquiétudes croissantes des citoyens en matière de protection de la vie privée. Ainsi, sa mise en œuvre est tant destinée au secteur privé qu'au secteur public sur le territoire québécois. En effet, la Loi 25 modernise tant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels que la Loi sur la protection des renseignements personnels dans le secteur privé.

La mise en œuvre de cette loi est échelonnée sur trois ans. C'est en septembre 2023 que des dispositions primordiales sont entrées en vigueur. Afin de poursuivre leurs activités au Québec, de nombreuses entités ont dû aménager leurs pratiques de manière à se conformer aux nouvelles exigences légales.

La Loi 25 vise principalement à accroître la protection des individus visés. Pour ce faire, les obligations des entreprises et des organismes publics dans le cadre de leurs activités se sont vues considérablement renforcées. Sommairement, la Loi 25 requiert la mise place de nouvelles politiques et de pratiques de gouvernance encadrant la protection des données

personnelles afin d'octroyer la possibilité aux individus d'être plus impliqués dans la gestion de leurs données. Cela a pour effet de promouvoir une meilleure transparence du traitement et une confidentialité accrue.

II. Quelques obligations introduites par la *Loi 25*

Parmi ces nouvelles obligations, on retrouve entre autres celle de devoir dorénavant designer un responsable de la protection des renseignements personnels dans le secteur privé. Auparavant, il n'existait pas d'exigence formelle d'en désigner un, c'était plutôt une pratique en matière de gouvernance des données qui variait selon les entreprises. La responsabilité était souvent attribuée au cadre supérieur et relevait donc de la hiérarchie interne.

Le responsable du traitement des données est chargé de superviser les activités de traitement des données personnelles au sein de l'organisation. Il assure la sécurité de ces dernières en décidant des moyens du traitement des données eu égard à la nécessité et à la finalité.

Les coordonnées de cet individu doivent être accessibles au public ainsi qu'aux membres de l'organisation afin qu'ils puissent le contacter.

Ce dernier est également responsable de tenir un registre des incidents. Ce document consigne les différents faits relatifs à une violation grave de la sécurité des données ainsi que des mesures mises en place afin d'y remédier, le cas échéant. Cette première obligation témoigne d'un effort important du législateur afin de mettre en place des actions concrètes afin d'assurer la sécurité de l'information.

Quant aux différentes politiques de gouvernance, tant les entreprises que les organismes publics devront publier sur leur site web une politique claire quant à leurs mesures de protection des données. Cela rejoint cette idée de promouvoir une meilleure transparence du traitement vis-à-vis des citoyens. Le contenu diffère dépendamment de si l'on se trouve dans le secteur privé ou public, mais essentiellement, on retrouvera des directives concernant le type de données collectées lors des activités de l'entité ; la finalité d'une telle collecte ; la durée de conservation des données ; les mesures de protection mises en place afin d'assurer la sécurité des données ; un processus de traitement des plaintes, etc.

Notons par ailleurs que lorsque la finalité de la collecte des données est atteinte, ces dernières doivent être soit détruites soit anonymisées, c'est-à-dire qu'il doit être impossible d'identifier l'individu concerné.

Une obligation complémentaire instaurée par la Loi 25 énonce que les entités doivent établir un plan de réponse aux incidents de confidentialité. En principe, il faudra tout d'abord aviser un supérieur immédiat ou le responsable du traitement. La personne concernée devra également être informée de l'incident. L'autorité compétente devra également être signalée de l'incident si la violation présente un risque grave. Ensuite, il faut tenter de limiter le dommage causé et le réparer si possible. Puis, il faudra identifier les causes qui ont mené à cet incident et réduire au maximum les risques de récurrence.

La Loi 25 introduit également l'obligation de procéder à l'évaluation des facteurs relatifs à la vie privée (EFRVP) en certaines circonstances. Les organisations devront exécuter l'EFRVP lorsque les données personnelles sont communiquées à l'extérieur du Québec et pour tout projet d'acquisition, de développement et de refonte de système d'information ou de prestation électronique de services impliquant des renseignements personnels.

C'est la Commission d'accès à l'information du Québec qui veille au respect de l'ensemble des règles introduites par cette réforme législative.

En cas de contravention aux dispositions, des sanctions pénales sont prévues. Elles peuvent s'élever jusqu'à des millions de dollars canadiens. Ces dernières ont été rehaussées comparé au droit applicable antérieur. Cette réforme a réellement mis en place des peines fermes. Par exemple, une fuite de données engendre dorénavant l'obligation d'une divulgation publique de la faille en plus d'une annonce à l'autorité compétente afin qu'elle puisse prendre les mesures nécessaires.

Ainsi, la Loi 25 introduit plusieurs obligations qui assurent une protection plus robuste des données au Québec. Toutefois, cette réforme sert également à expliciter le cadre juridique de protection des données.

Par exemple, la loi clarifie les situations concrètes nécessitant le consentement explicite de la personne concernée. Il est également spécifié que c'est le consentement du titulaire de l'autorité parentale ou du tuteur qui est requis lorsque qu'un mineur a moins de 14 ans. Un autre cas illustratif concerne la description précise, dans la loi, du processus à suivre lors d'un traitement où le consentement n'est pas nécessaire. Cela inclut notamment de la communication d'information à des fins d'étude, de recherche ou de production de statistiques.

III. Le niveau de protection adéquat canadien en Europe

Avec l'avènement rapide des technologies numériques, le transfert transfrontalier de données devient une pratique de plus en plus répandue.

Il est convenu que si une entité québécoise traite des données personnelles d'un individu qui se trouve sur le territoire de l'Union européenne, cette dernière devra se conformer au Règlement général sur la protection des données (RGPD). Le RGPD étant un règlement qui s'impose de manière uniforme aux États membres de l'UE, sans nécessiter une transposition dans le droit national.

En matière de communication de données à l'étranger, l'art. 45 RGPD prévoit que celle-ci est possible du moment que l'État dans lequel les données sont communiquées bénéficie d'une décision d'adéquation. Vu l'importance des flux transfrontaliers de données, il est important de déterminer si le Canada est au bénéfice d'une telle décision. Sans cette reconnaissance, le pays devra fournir des garanties supplémentaires ou obtenir une autorisation spéciale, mettant un frein à la collaboration entre l'UE et les pays étrangers.

Tout d'abord définissons qu'est-ce qu'une décision d'adéquation. C'est une évaluation effectuée par la Commission européenne afin de déterminer si un pays tiers à l'espace économique européen assure un niveau de protection adéquat conformément au RGPD. Pour ce faire, c'est principalement la législation interne du pays qui est prise en compte, soit la force juridique et l'efficacité des lois nationales. D'autres critères sont également évalués tel que la capacité du Commissariat à la protection de la vie privée du pays à surveiller le respect de la loi ; les droits des individus ; la coopération du pays avec les autorités de l'Union européenne ; l'existence de recours juridiques (cf. www.swissprivacy.law/277).

En 2001, la Commission européenne a reconnu que le Canada offrait un niveau de protection adéquat par le biais de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). Or, comme nous l'avons analysé dans notre première contribution, le système canadien se distingue entre le secteur privé et le secteur public, mais également entre le système fédéral et les provinces. La LPRPDE est une loi fédérale qui ne couvre que le secteur privé. Ainsi, la décision de la Commission européenne est limitée au cadre de protection des données du secteur privé canadien. Elle ne concerne également que les activités commerciales des entreprises.

Notons que l'art. 97 RGPD impose à la Commission de réexaminer ses décisions d'adéquation à chaque quatre ans. Ainsi, sa reconnaissance concernant le territoire canadien fut renouvelée le 15 janvier 2024 (cf. décision de la Commission Européenne). Cette exigence de réexaminer leur décision s'explique notamment par les mouvantes du cadre législatif du pays en

question, la Commission devant s'assurer qu'un niveau adéquat de protection est toujours assuré et substantiellement équivalent à celui du RGPD.

La Commission a entretenu avec le Canada de nombreuses discussions afin de remédier à quelques différences majeures dans le système de protection des données. Par exemple, le Canada n'autorisait que les citoyens ; les résidents permanents ou les personnes présentes sur le territoire d'accéder ou rectifier des données personnelles détenues par les organisations du secteur public. Dorénavant, ce droit est étendu à tous en vertu de la Loi sur l'accès à l'information. Le but étant d'obtenir un cadre législatif national qui converge de plus en plus vers celui de l'UE.

La Commission a donc conclu que le Canada par l'entremise de la LPRPDE continue d'assurer un niveau de protection substantiellement équivalent à celui du RGPD.

IV. Un niveau de protection québécois en Europe ?

Les décisions d'adéquation au RGPD concernent généralement des pays ou territoires autonomes. Il n'existe pas encore de reconnaissance à une subdivision interne telle qu'une province.

Étant donné que le Canada assure un niveau de protection adéquat par l'entremise de la LPRPDE, toutes les provinces canadiennes qui n'ont pas adopté leur propre législation et qui se conforment à la loi fédérale, bénéficieraient également de cette reconnaissance.

Mais qu'en-est-il des provinces qui ont élaboré leurs propres lois tel que le Québec ? Nous avons vu que LPRPDE continue de s'appliquer à moins que le gouverneur en conseil n'exempte l'application de la loi fédérale dans cette province. En effet, cette mesure serait accordée si les mesures de protections sont jugées équivalentes à celle du cadre fédéral.

La question est alors la suivante : est-ce que cette reconnaissance d'équivalence interne pourrait permettre à la Commission européenne de déclarer le Québec comme un territoire adéquat comme le reste du Canada ?

Malheureusement, le réexamen ne tient pas compte des réformes législatives proposées par la Loi 25 au Québec. Alors que de nombreuses dispositions quant à la collecte et la gestion des données personnelles proposées par la Loi 25 ont été inspirées par le droit de l'Union européenne. En effet, un des objectifs principaux de la loi était d'harmoniser la province du Québec aux standards internationaux. Ces différentes obligations de transparence, de consen-

tement et de divulgation s'apparentent aux principes généraux du RGPD.

V. Conclusion

En conclusion, l'adoption de la Loi 25 par le parlement québécois en septembre 2021 représente un progrès significatif vers la conformité européenne en matière de protection des données. Cette réforme vise à renforcer la protection des renseignements personnels au Québec, tant dans le secteur privé que dans le secteur public. Les obligations introduites par la loi, telles que la désignation d'un responsable de la protection des renseignements personnels dans le secteur privé, la publication de politiques de protection des données, la destruction ou l'anonymisation des données après atteinte de la finalité, ainsi que la mise en place de plans de réponse aux incidents, reflètent un engagement sérieux envers la sécurité et la transparence.

Il est important de noter que le Canada a déjà obtenu en 2001 une décision d'adéquation au RGPD par la Commission européenne, décision confirmée à la suite d'un réexamen en 2024. Cependant, la Loi 25, inspirée par les principes directeurs du RGPD, n'a pas été pris en considération par la Commission européenne pour une reconnaissance similaire.

Cette situation souligne l'importance de continuer à harmoniser les lois régionales avec les normes internationales afin de faciliter les échanges commerciaux et à assurer une protection adéquate des données. En définitive, alors que les décisions d'adéquation sont essentielles pour la libre circulation des données, il faut résoudre ces différences afin de garantir une protection uniforme des renseignements personnels dans un contexte mondial de plus en plus connecté.

Proposition de citation : Azza KHELIL, Regards croisés sur la Loi 25 : un pas vers la conformité européenne pour le Québec ?, 23 avril 2024 *in* www.swissprivacy.law/296