Tableau comparatif des lois sur la protection des renseignements personnels

par Karl Delwaide, Antoine Aylwin et Antoine Guilmain[1]

FASKEN

		Québec	Canada	Union Européenne	Californie
		Loi sur la protection des renseignements personnels dans le secteur privé	Loi sur la protection des renseignements personnels et les documents électroniques (« LPRPDÉ »)	Règlement Général sur la Protection des Données (« RGPD »)	California Consumer Privacy Act
1.	Entrée en vigueur et territorialité	• 1er janvier 1994 au Québec	• 1er janvier 2001 au Canada (applicable à toute organisation depuis le 1er janvier 2004)	• 24 mai 2016 (pleinement applicable depuis le 25 mai 2018) dans l'UE/EEE avec parfois une portée extraterritoriale	• 1er janvier 2020 en Californie
2.	Organisme responsable	• Commission d'accès à l'information du Québec	• Commissariat à la protection de la vie privée du Canada	• Autorité de contrôle propre à chaque État membre (CNIL, ICO, etc.) • Comité européen de la protection des données (qui remplace le G29)	• Procureur général de la Californie
3.	Champ d'application	• Toute « entreprise » (en vertu du *Code civil du Québec*) qui recueille, détient, utilise ou communique des renseignements personnels • Exclusion des organismes publics au sens de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ c A-2.1)	• Toute organisation qui recueille, utilise ou communique des renseignements personnels dans le cadre de ses activités commerciales • Exclusion des institutions fédérales sujettes à la *Loi sur la protection des renseignements personnels* (LRC 1985, c P-21) • Possibilité d'exclusion de l'application de la LPRPDÉ dans certaines provinces (par décret)	• Critère de l'établissement : le responsable du traitement ou le sous-traitant est établi dans l'UE/EEE • Critère du ciblage : le responsable du traitement est établi en dehors de l'UE/EEE mais ses activités de traitement concernent l'offre de biens ou services à des personnes[2] qui se trouvent sur le territoire de l'UE/EEE soit les activités de traitement concernent le suivi du comportement de personnes au sein de l'UE/EEE • Pas de distinction entre le secteur privé et le secteur public	• Toute entreprise privée, exerçant des activités dans l'État de Californie, qui recueille et vend des renseignements personnels à des fins commerciales, qui a des revenus annuels bruts excédant 25 millions $, qui traite annuellement les renseignements personnels d'au moins 50 000 personnes résidentes de la Californie ou qui tire au moins 50 % de ses revenus annuels de la vente de renseignements personnels • Voir également les autres lois californiennes concernant la protection des renseignements personnels (notamment concernant la notification)
4.	Renseignements personnels (ou « données personnelles »)	• Tout renseignement qui concerne une personne physique et permet de l'identifier • Quel que soit le support/format (écrit, graphique, sonore, visuel, informatisé ou autre) • Vise aussi les employés et candidats à un emploi	• Tout renseignement concernant un individu identifiable • Quel que soit le support/format • Régime particulier pour les « coordonnées d'affaires » (nom, poste, titre, adresse ou numéro de téléphone professionnels, etc.) • Vise uniquement les employés ou candidats d'entreprises fédérales	• Toute information se rapportant à une personne physique identifiée ou identifiable (y compris nom, numéro d'identification, données de localisation, identifiant en ligne et tout élément propre à l'identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale) • Quel que soit le support/format • Vise aussi les employés	• Identifiant, concernant, se rapportant à, permettant d'associer, ou pouvant raisonnablement être lié à, directement ou indirectement, un consommateur ou un foyer (y compris nom, pseudonyme, adresse postale, identificateur personnel unique, adresse de protocole Internet, adresse courriel, nom de compte, numéro de sécurité sociale, numéro de permis de conduire, numéro de passeport, informations biométriques, données de géolocalisation, informations professionnelles, éducation, etc.)

[1] Avocats chez Fasken (Montréal), groupe national Protection de l'information et de la vie privée. Les auteurs tiennent à remercier Natalia Fuentes Quintana, parajuriste, et Eliane Ellbogen, étudiante en droit, pour leur travail lors de la préparation de ce tableau. Ce document ne prétend pas à l'exhaustivité et ne constitue aucunement un avis juridique. La dernière mise à jour a été effectuée le 12 octobre 2018.

[2] Le terme « personne » est privilégié dans le présent document par souci de simplicité, il ne correspond pas nécessairement à la terminologie utilisée dans chacune des législations à l'étude.

		Québec	Canada	Union Européenne	Californie
		Loi sur la protection des renseignements personnels dans le secteur privé	Loi sur la protection des renseignements personnels et les documents électroniques (« LPRPDÉ »)	Règlement Général sur la Protection des Données (« RGPD »)	California Consumer Privacy Act
5.	Renseignements sensibles	• Aucune définition de « renseignement sensible » • Garantir un niveau de sécurité adapté au degré de sensibilité	• Aucune définition de « renseignement sensible » • Garantir un niveau de sécurité adapté au degré de sensibilité	• Régime particulier pour les « catégories particulières de données personnelles » (incluant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données génétiques, les données biométriques, les données concernant la santé, la vie sexuelle ou l'orientation sexuelle) • Régime particulier pour les données relatives aux condamnations pénales et aux infractions • Pas de régime distinct pour les données financières	• Aucune définition de « renseignement sensible »
6.	Consentement	• Doit être manifeste, libre, éclairé et être donné à des fins spécifiques et ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé • Aucune précision concernant son retrait • Non nécessaire lorsqu'une exception s'applique	• Peut être explicite ou implicite selon les circonstances et la nature des renseignements, en tenant compte des attentes raisonnables de la personne concernée • Doit généralement être explicite pour le traitement de renseignements sensibles • Peut être retiré en tout temps sous réserve de restrictions prévues par une loi ou un contrat et d'un préavis raisonnable • Non nécessaire lorsqu'une exception s'applique (notamment dans le cadre d'une « transaction commerciale »)	• Doit être libre, spécifique, éclairé et univoque, sous une forme compréhensible et accessible et ne vaut que pour les finalités déterminées • Doit être « explicite » pour le traitement de catégories particulières de données • Peut être retiré à tout moment • Un autre fondement légal peut s'appliquer, tel que le caractère nécessaire pour l'exécution d'un contrat ou aux fins des intérêts légitimes du responsable du traitement	• Peut être tacite (en principe aucun consentement explicite n'est requis) • Peut être retiré en tout temps et doit pouvoir se faire de manière simple, évidente et accessible (« *opt-out* »)
7.	Enfants	• Aucune précision concernant les mineurs (sous réserve des dispositions du *Code civil du Québec* et d'autres articles ponctuels dans la Loi sur le secteur privé)	• Aucun âge minimum pour le consentement des mineurs, mais généralement valide à partir de 13 ans (selon les « Lignes directrices pour l'obtention d'un consentement valable »)	• Âge minimal de 16 ans pour le consentement des mineurs, sauf si le titulaire de la responsabilité parentale donne son autorisation • États membres peuvent prévoir un âge inférieur à 16 ans, mais pas en dessous de 13 ans	• Âge minimal de 16 ans pour le consentement des mineurs, sauf si la personne est âgée entre 13 et 16 ans et qu'elle donne son consentement explicite, ou si la personne est âgée de moins de 13 ans et que le titulaire de la responsabilité parentale donne son autorisation • Voir également *Children's Online Privacy Protection Rule* (COPPA)

		Québec	Canada	Union Européenne	Californie
		Loi sur la protection des renseignements personnels dans le secteur privé	Loi sur la protection des renseignements personnels et les documents électroniques (« LPRPDÉ »)	Règlement Général sur la Protection des Données (« RGPD »)	California Consumer Privacy Act
8.	Droit d'accès	• Oui, sauf exception, y compris en cas de litige ou si susceptible de nuire sérieusement à un tiers • Demande d'accès par écrit avec preuve d'identité • Réponse dans un délai de 30 jours • Gratuit (avec possibilité d'exiger des frais raisonnables sous certaines conditions) • Obligation d'assistance de la part de l'entreprise	• Oui, sauf exception, y compris en cas de litige ou si les renseignements contiennent des informations sur des tiers ou encore pour des raisons d'ordre juridique, de sécurité ou commercial • Demande d'accès par écrit • Réponse dans un délai de 30 jours (avec possibilité de prorogation) • Possibilité d'exiger des frais sous certaines conditions • Obligation d'aide de la part de l'organisation sur demande de la personne concernée	• Oui, sauf exception, y compris pour des raisons d'ordre juridique ou de sécurité • Possibilité de confirmer l'identité de la personne concernée en présence de doutes raisonnables • Réponse par écrit ou à l'oral (lorsque la personne concernée en fait la demande) • Réponse dans les meilleurs délais et en tout état de cause dans un délai de 1 mois (avec possibilité de prolongation) • Gratuit (avec possibilité d'exiger des frais raisonnables sous certaines conditions) • Obligation de faciliter l'exercice du droit d'accès	• Oui, sauf exception, y compris si le traitement est ponctuel, les renseignements ne sont pas considérés comme étant personnels, la personne concernée a demandé l'accès plus de 2 fois dans les 12 derniers mois ou pour des raisons d'ordre juridique • Réponse dans un délai de 45 à 135 jours selon la complexité et la quantité de demandes • Gratuit (avec possibilité d'exiger des frais raisonnables si la demande est infondée ou excessive particulièrement en raison son caractère répétitif)
9.	Droit de correction (ou de rectification)	• Oui, si les renseignements sont inexacts, incomplets, équivoques, périmés, etc. • Exigences pour le droit d'accès applicables *mutatis mutandis*	• Oui, si les renseignements sont inexacts ou incomplets • Exigences pour le droit d'accès applicables *mutatis mutandis*	• Oui, si les données sont inexactes ou incomplètes • Exigences pour le droit d'accès applicables *mutatis mutandis*	• Facultatif, si les renseignements sont inexacts
10.	Droit à l'effacement (ou « à l'oubli »)	• Non	• Non	• Oui (sous certaines conditions)	• Oui (sous certaines conditions)
11.	Autres droits	• Droit de soumettre une demande d'examen de mésentente ou une plainte auprès de la Commission d'accès à l'information	• Droit de se plaindre du non-respect de la LPRPDÉ auprès de l'organisation et, si le problème persiste, auprès du Commissariat à la protection de la vie privée du Canada	• Droit à la limitation du traitement de données personnelles • Droit à la portabilité des données personnelles • Droit de s'opposer au traitement de données personnelles • Droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé • Droit de déposer une plainte auprès de l'autorité de contrôle compétente	• Droit de s'opposer à la vente ou à la communication de renseignements personnels à des tiers • Droit à la limitation du traitement de renseignements personnels • Droit à un traitement égal et à la non-discrimination dans l'exercice des droits • Droit à la portabilité des renseignements personnels

		Québec	Canada	Union Européenne	Californie
		Loi sur la protection des renseignements personnels dans le secteur privé	Loi sur la protection des renseignements personnels et les documents électroniques (« LPRPDÉ »)	Règlement Général sur la Protection des Données (« RGPD »)	California Consumer Privacy Act
12.	Responsable de la protection des renseignements personnels	• Aucune obligation spécifique	• Obligation de désigner une personne qui devra s'assurer du respect de la LPRPDÉ tout en divulguant son identité	• Obligation de désigner un « délégué à la protection des données » dans certaines circonstances, dont le traitement à grande échelle de catégories particulières de données ou impliquant un suivi régulier et systématique à grande échelle des personnes concernées • Obligation de désigner un « représentant » dans un contexte extraterritorial sous certaines conditions	• Aucune disposition spécifique
13.	Obligations de transparence	• Informer la personne concernée de l'objet du dossier, de l'utilisation qui sera faite des renseignements ainsi que des catégories de personnes qui y auront accès au sein de l'entreprise, et de l'endroit où sera détenu le dossier ainsi que des droits d'accès ou de rectification	• Faire en sorte que les politiques et pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne sous une forme généralement compréhensible • Informer la personne concernée du genre de renseignements personnels que possède l'organisation, y compris une explication générale de l'usage auquel ils sont destinés, incluant des précisions additionnelles • Être en mesure d'expliquer à la personne concernée à quelles fins sont destinés ces renseignements	• Fournir à la personne concernée une multitude d'informations au moment où les données en question sont obtenues (finalités du traitement, fondements légaux, destinataires, transfert de données, durée de conservation, droits applicables, coordonnées du responsable du traitement ou du délégué à la protection des données, etc.) • Fournir toute information d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples	• Informer la personne concernée des types de sources à partir desquelles les renseignements personnels sont recueillis, les fins commerciales de la collecte ou de la vente, les destinataires tiers et les droits prévus par la loi • Fournir les renseignements sous une forme facilement utilisable et transférable
14.	Mesures de sécurité	• Mise en place des mesures de sécurité propres à assurer la protection des renseignements personnels et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support	• Mise en place des mesures de sécurité, y compris des moyens matériels, administratifs et techniques, selon le degré de sensibilité des renseignements, leur quantité, leur répartition, leur format ainsi que les méthodes de conservation • Obligation de sensibiliser le personnel à l'importance de protéger le caractère confidentiel des renseignements personnels	• Mise en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque (y compris la pseudonymisation et le chiffrement des données, selon les besoins)	• Mise en place des mesures de sécurité raisonnables selon la nature des renseignements • Dé-identification et/ou pseudonymisation des renseignements personnels, par la mise en place de mesures techniques et organisationnelles, lorsque le traitement n'est pas expressément permis par la loi

		Québec	Canada	Union Européenne	Californie
		Loi sur la protection des renseignements personnels dans le secteur privé	Loi sur la protection des renseignements personnels et les documents électroniques (« LPRPDÉ »)	Règlement Général sur la Protection des Données (« RGPD »)	California Consumer Privacy Act
15.	Notification en matière de sécurité	• Notification facultative (formulaire disponible en ligne)	• Notification au Commissariat à la protection de la vie privée le plus tôt possible de toute atteinte à la protection des données présentant un « risque réel de préjudice grave » • Notification aux personnes concernées le plus tôt possible de toute atteinte présentant un « risque réel de préjudice grave » à leur endroit • Tenue d'un registre des atteintes à la protection des données et donner accès à ce registre au Commissariat à la protection de la vie privée à la demande de celui-ci	• Notification à l'autorité de contrôle dans les meilleurs délais et, si possible, 72 heures au plus tard après avoir pris connaissance de l'incident dans certaines circonstances • Communication à la personne concernée dans les meilleurs délais si la violation est susceptible d'engendrer un risque élevé pour les droits et libertés, sous certaines conditions	• Voir *California Security Breach Information Act*
16.	Transfert vers des territoires tiers	• À l'extérieur du Québec • Oui, notamment par voie contractuelle, en prenant les moyens raisonnables pour s'assurer que les renseignements ne seront pas utilisés à des fins non pertinentes à l'objet du dossier ni communiqués à des tiers sans le consentement des personnes concernées	• À l'extérieur du Canada • Oui, par voie contractuelle ou autre, sous réserve qu'un degré comparable de protection aux renseignements personnels soit fourni • Mention aux personnes concernées que leurs renseignements personnels pourraient être envoyés dans un autre pays aux fins de traitement, et que les tribunaux, organismes d'application de la loi et agences de sécurité nationale de ce pays pourraient y accéder (selon les « Lignes directrices sur le traitement transfrontalier des données personnelles »)	• À l'extérieur de l'UE/EEE • Oui, s'il existe une « décision d'adéquation » ou d'autres garanties appropriées en vertu du RGPD, telles que les clauses contractuelles types approuvées par la Commission européenne, les règles d'entreprise contraignantes, l'application d'un code de conduite ou d'un mécanisme de certification	• À l'extérieur de la Californie • Oui, si la collecte ou la vente des renseignements personnels sont entièrement effectuées à l'extérieur de la Californie et relativement à des personnes situées à l'extérieur de la Californie
17.	Autres obligations et modalités	• Régime particulier pour les « listes nominatives » (soit une liste de noms, de numéros de téléphone, d'adresses géographiques de personnes physiques ou d'adresses technologiques où une personne physique peut recevoir communication d'un document ou d'un renseignement technologique)	• Obligation de faire enquête sur toutes les plaintes et, si une plainte est jugée fondée, l'organisation doit prendre les mesures appropriées, y compris la modification de ses politiques et de ses pratiques au besoin	• Mise en œuvre de la protection des données dès la conception (« *privacy by design* ») et par défaut (« *privacy by default* ») • Registre des activités de traitement requis, sauf pour une organisation ou une entreprise comptant moins de • 250 employés sous certaines conditions • Analyse d'impact relative à la protection des données requise dans certaines circonstances	• Une entreprise peut offrir des incitations financières pour la collecte, la vente ou l'effacement des renseignements personnels dans la mesure où la personne concernée donne son consentement pour participer au programme incitatif (« *opt-in* »)

	Québec	Canada	Union Européenne	Californie
	Loi sur la protection des renseignements personnels dans le secteur privé	Loi sur la protection des renseignements personnels et les documents électroniques (« LPRPDÉ »)	Règlement Général sur la Protection des Données (« RGPD »)	California Consumer Privacy Act
18. Conservation des données	• Aussi longtemps que nécessaire pour la réalisation des fins déterminées ou pour permettre à une personne concernée d'épuiser les recours prévus par la loi • Maintien des dossiers sur autrui à jour et exacts au moment où l'entreprise les utilise pour prendre une décision relative à la personne concernée • Absence de calendrier de conservation établi par règlement du gouvernement	• Aussi longtemps que nécessaire pour la réalisation des fins déterminées ou pour permettre à une personne concernée d'épuiser les recours prévus à la loi • Maintien des renseignements personnels de manière aussi exacte, complète et à jour que l'exigent les fins auxquelles ils sont destinés	• Aussi longtemps que nécessaire et limitée au strict minimum	• Aussi longtemps que nécessaire pour permettre à une personne concernée d'exercer son droit d'accès à l'information, soit pour une période maximale de 12 mois
19. Sanctions	• 1 000 $ à 10 000 $ en cas de contravention aux dispositions de la loi • 5 000 $ à 50 000 $ en cas de contravention aux règles de transfert des renseignements personnels à l'extérieur du Québec • Montants doublés si récidive	• 10 000 $ ou 100 000 $ notamment en cas d'entrave à une vérification ou à l'examen d'une plainte ou en cas de contravention de tenir et conserver un registre de toutes les atteintes aux mesures de sécurité qui ont trait à des renseignements personnels dont une entreprise a la gestion.	• Jusqu'à 10 millions € ou 2 % du chiffre d'affaires annuel mondial ou 20 millions € ou 4 % du chiffre d'affaires annuel mondial (le montant le plus élevé étant retenu) selon la nature de l'infraction	• Amende maximale de 7 500 $ pour une infraction intentionnelle à la loi
20. Autres recours	• Recours à la Commission d'accès à l'information (compétence exclusive en principe) • Recours auprès des tribunaux de droit commun (incluant par voie d'actions collectives)	• Recours au Commissariat à la protection de la vie privée du Canada • Recours auprès des tribunaux de droit commun (incluant par voie d'actions collectives)	• Recours auprès de l'autorité de contrôle compétente • Recours auprès des tribunaux de droit commun (incluant par voie d'actions collectives)	• Recours civil en cas d'atteinte à la protection des renseignements personnels • 30 jours pour remédier à l'atteinte sinon responsable des dommages de 100 $ jusqu'à concurrence de 750 $ par personne concernée et par incident ou le total des dommages réels (le montant le plus élevé sera retenu), selon la nature et gravité de l'infraction

FASKEN

Contacts

Karl Delwaide
Associé
+1 514 397 7563
kdelwaide@fasken.com

Antoine Aylwin
Associé
+1 514 397 5123
aaylwin@fasken.com

Antoine Guilmain
Avocat
+1 514 397 5164
aguilmain@fasken.com