LES ENJEUX DU PROJET DE LOI 64 POUR LES ENTREPRISES DU QUÉBEC

Par
Marco Estrela
Conseiller senior en cybersécurité

Patrick Naoum ing.
VPE alliances et solutions clients

12 novembre 2020
Capsules d'apprentissage ESI

ORDRE DU JOUR

- En quoi consiste le projet de loi 64?
- PL64 vs LPRPDE
- Ce qui retient l'attention
  - Entreprises
  - Individus
- Mise en application : 2022
- Comment s'y préparer?
- Comment ESI peut aider les entreprises du Québec à s'y conformer
- Notre atout : la solution DataStealth de Datex
- 5 pistes de réflexion

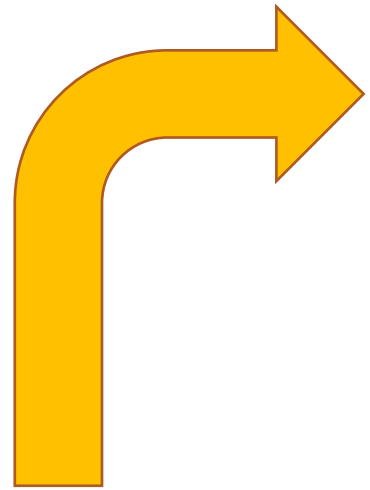
Projet de loi 64

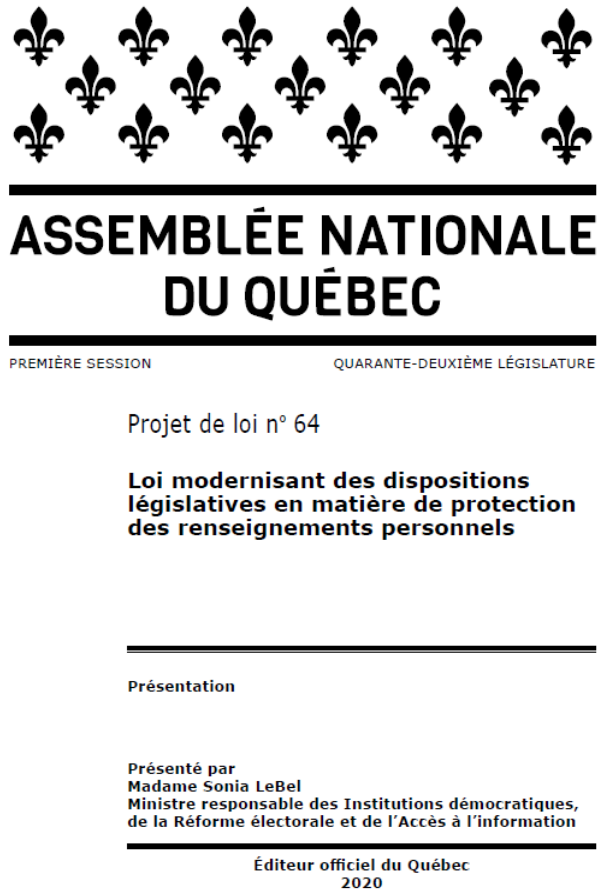
Projet de loi 64: Des sanctions de 25 M$ en cas de fuite de données personnelles

PARTAGEZ SUR FACEBOOK | PARTAGEZ SUR TWITTER | AUTRES

MARC-ANDRÉ GAGNON

Avec des sanctions pouvant atteindre 25 millions $, des entreprises comme Desjardins auront intérêt à protéger les données personnelles des Québécois, si le projet de loi présenté vendredi par la ministre Sonia LeBel est adopté.





ASSEMBLÉE NATIONALE DU QUÉBEC

PREMIÈRE SESSION — QUARANTE-DEUXIÈME LÉGISLATURE

Projet de loi n° 64

Loi modernisant des dispositions législatives en matière de protection des renseignements personnels

Présentation

Présenté par
Madame Sonia LeBel
Ministre responsable des Institutions démocratiques, de la Réforme électorale et de l'Accès à l'information

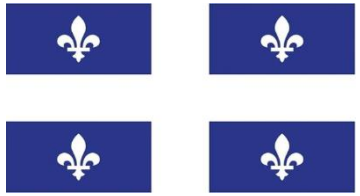
Éditeur officiel du Québec
2020

Le projet de loi a été **adopté à l'unanimité le 12 juin 2020** et sera sans doute en vigueur dès cet automne.

Résultat probable : les organismes publics et privés partout au Québec vont devoir effectuer des réformes majeures et auront des obligations considérablement accrues quant à la manière de protéger les données personnelles de leurs clients. ESI peut les aider dès maintenant!

PL64 vs LPRPDE

- LPRPDE (anglais : PIPEDA)
- Loi sur la protection des renseignements personnels et des documents électroniques
- Depuis : 18 juin 2015
- Portée : S'applique aux organisations qui recueillent, utilisent ou divulguent des renseignements personnels dans le cadre d'activités commerciales.
- Régit tout le Canada sauf la Colombie-Britannique, l'Alberta et le Québec qui ont leurs propres lois.
- Beaucoup moins mordante que le PL64.



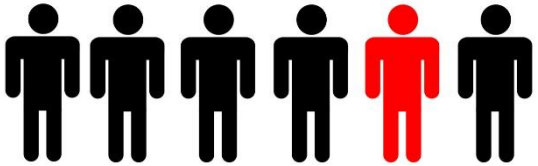
- PL64
- Loi modernisant des dispositions législatives en matière de protection des renseignements personnels
- Depuis : Adoption prévue automne 2020
- Portée : Tout système d'information, projet ou prestation de services électroniques impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction d'informations seront visés par le PL64

Ce qui retient l'attention

→ Pour l'entreprise :

- Les entreprises québécoises seront tenues de **divulguer** une atteinte à la protection des données à la Commission d'accès à l'information et aux personnes touchées.
- **Pénalités** salées : Sanctions de **5 000 $ à 50 000$** pour une personne physique, de **15 000 $ à 25 000 000$** pour une personne morale ou même, dans certains cas, un montant correspondant à 4 % du chiffre d'affaires mondial.
- Les entreprises fautives peuvent dorénavant être **poursuivies** en dommages-intérêts.
- Demande de **consentement** obligatoire.
- Les organisations doivent prendre les mesures requises afin de **réduire les risques**.
- **Nomination d'une personne responsable** de la protection des renseignements personnels au sein de chaque organisation assujettie, quelle que soit leur taille.
- Mise en œuvre de **politique de protection des données** dans l'entreprise.
- **Aucune technologie** permettant d'identifier, de localiser ou de **profiler un individu** n'est permise.

Ce qui retient l'attention



→ Pour l'individu :

- Droit à l'**oubli**.
- Droit de demander l'**origine** des données.
- Droit à la **portabilité** des données (copie de son dossier en format lisible!)
- Exigence des organisations qu'elles **détruisent ou rendent anonymes les renseignements** personnels lorsque les fins pour lesquelles ils ont été collectés sont atteintes.
- Droit de demander comment votre information a été **traitée par un moyen automatisé** (IA, ML, algorithmes, etc.) pour prendre une décision.

Mise en application

- Délai d’un an après son adoption
- Entrée en vigueur fort probablement en 2022
- 3 ans pour les exigences plus techniques

Comment s’y préparer?

- Mettez en place un processus de réponse aux incidents afin d’être prêts si le pire devait arriver.
- Révisez toutes vos politiques en matière de protection de renseignements personnels.
- Révisez tous vos contrats avec des tiers, surtout les sections sur comment ces derniers doivent se comporter en matière de manipulation de l’information.
- Révisez vos formulaires de consentement.
- Effectuez un audit des renseignements personnels que votre entreprise détient et assurez-vous d’avoir les mesures adéquates pour les protéger.

Comment ESI peut aider les entreprises du Québec à s'y conformer

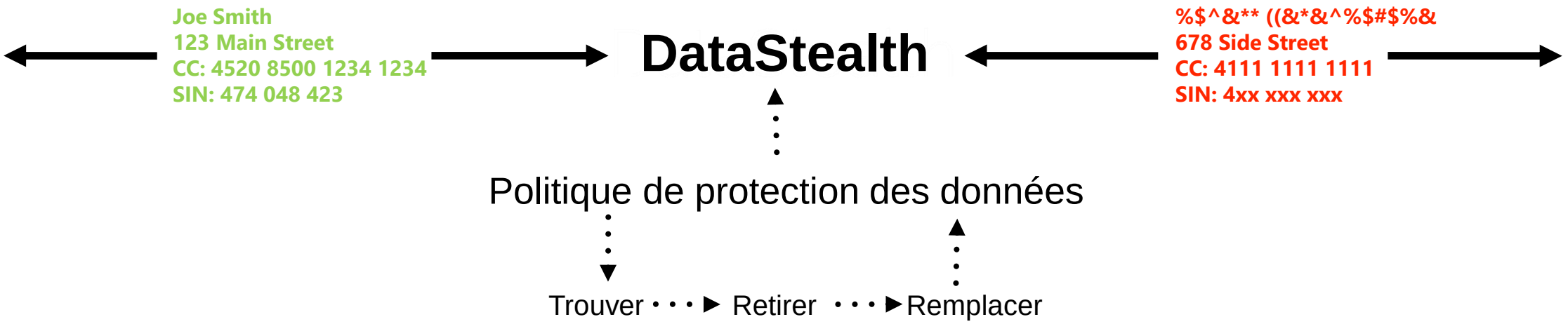
- **Établir l'applicabilité de la loi à votre entreprise** en collaboration avec notre réseau de conseillers juridiques
- Conseiller les clients pour **la mise en place d'une stratégie de sécurité complète** afin d'éviter des pénalités (entre autres!)
- Effectuer des **tests de sécurité** pour s'assurer que les brèches sont fermées
- **Gérer votre sécurité** avec notre équipe d'experts [SOC]
- Profiter du **SIRT ESI** comme service pour la réponse aux incidents
- **Mettre en place un SGSI** – Système de gestion de la sécurité de l'information – la solution « nucléaire »!

NOTRE CARTE CACHÉE POUR AIDER LES CLIENTS AVEC LE PL64 :

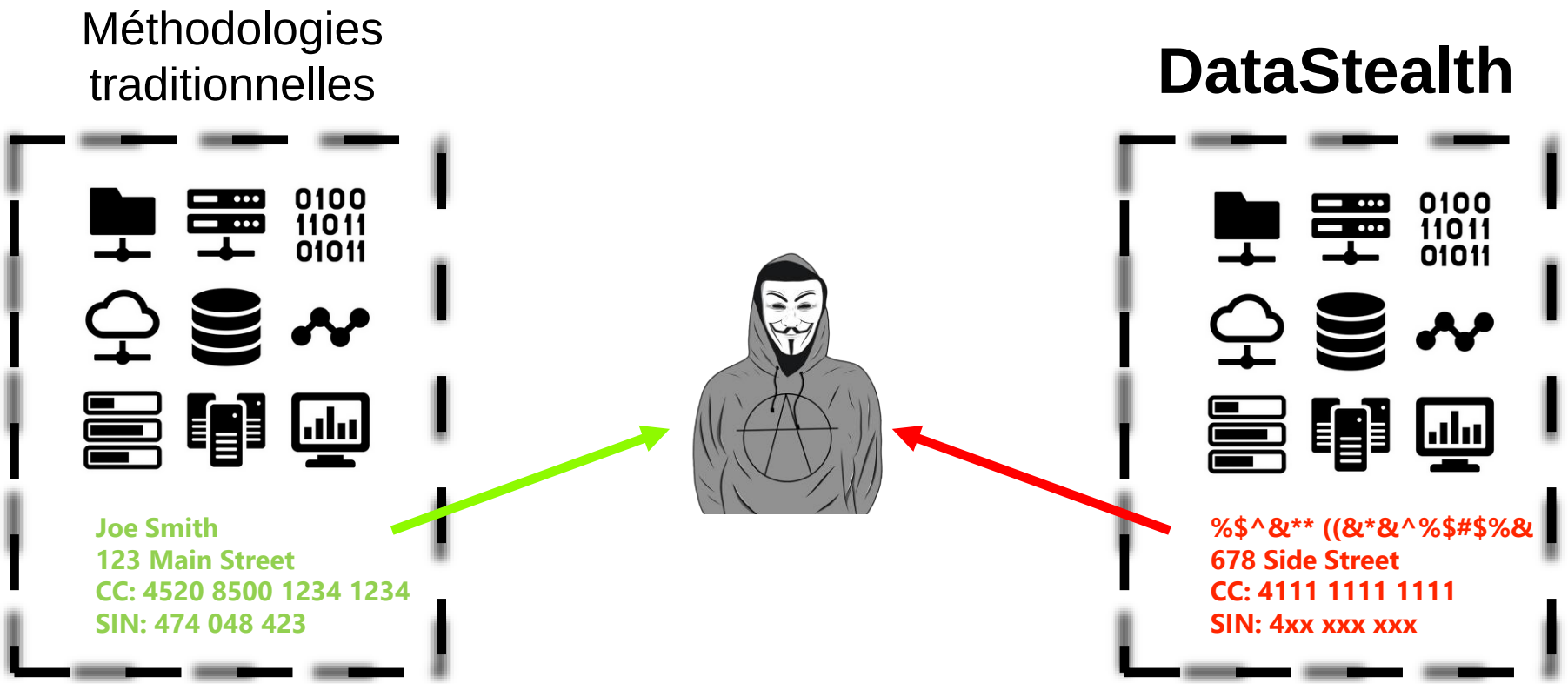
→ Comment DataStealth peut aider avec PL64?

- Élimination de toutes les informations nominatives (PII)
- Droit à l'oubli en « un seul clic »
- Communication transfrontalière de données (*data residency*)
- Pas de données à voler, donc pas de divulgation de brèches de sécurité
- *Tokenisation* vs. chiffrement

La plateforme DataStealth



Changement de paradigme



DataStealth résout des problèmes complexes

- Lois et conformité
  - PCI, RGPD, LPRPDE, ISO 27001, Projet de loi 64
- Sécurité et vie privée
  - Gestion des données tests (dev), Masquage de données dynamique, « data residency », anti-hameçonnage
- Gouvernance
  - Accès, audit, journalisation, surveillance
- Intégration
  - Salesforce, Okta, Veeam, AWS, Azure, Google Cloud

5 PISTES DE RÉFLEXION

1. Le PL64 deviendra loi tôt ou tard
2. Toutes les entreprises publiques et privées seront assujetties à ces nouvelles règles du jeu
3. Vous pouvez vous préparer dès maintenant
4. Avec une planification adéquate, vous investirez seulement dans ce qui est nécessaire pour conformer votre entreprise
5. ESI et son réseau de conseillers juridiques sont là pour vous conseiller

ESI Technologies

Toronto – Montréal – Québec – É.-U.

Marco Estrela, conseiller cybersécurité
Cell: 514-236-0056