

# MINI\* FORMATION

C'EST GRATUIT!  


LOI 25 : COMMENT PROTÉGER  
TON ENTREPRISE ET LES  
RENSEIGNEMENTS  
PERSONNELS DE TES CLIENTS

Vendredi  
17 janv. 12h



AICHA TOHRY



PATRICIA FILIATRAULT



MÉLODIE LAMBERT



**LOI 25**

**MYTHES**

Vrai ou faux?

# Mythe #1

## Les petites entreprises ne sont pas concernées

Beaucoup pensent à tort que seules les grandes entreprises doivent se conformer aux réglementations sur la protection des données. En réalité, les lois s'appliquent souvent indépendamment de la taille de l'entreprise.



# Mythe #2

## Les données en dehors du Québec ne sont pas concernées par la Loi 25

La loi vise les renseignements personnels des résidents du Québec.



# Mythe #3

## Seules les données sensibles sont concernées

Les lois sur la protection des données s'appliquent généralement à toutes les données personnelles, pas seulement aux données dites "sensibles" comme le NAS ou la date de naissance.



# Mythe #4

## Je n'ai pas besoin de consentement si je n'ai pas l'intention de partager des données

Le consentement est souvent nécessaire même pour la collecte et le stockage des données, pas seulement pour leur partage.



# Mythe #5

## Une fois en conformité, toujours en conformité

Les lois sur la protection des données changent et évoluent, tout comme les entreprises. La conformité nécessite un effort continu.



# Mythe #6

## Les sanctions sont rares et mineures

Les amendes pour non-conformité peuvent être très importantes.





# Mythe #7

## La protection des données est uniquement le problème du service informatique

La protection des données est une responsabilité organisationnelle qui implique divers départements, y compris le service juridique, les ressources humaines, et la direction.



# Mythe #8

**Je n'ai pas besoin d'informer les utilisateurs si nous avons une violation de données**

Ça dépend des circonstances.



# Mythe #9

## Les entreprises BtoB (Business to Business) ne sont pas concernées

Il est faux de penser que les règles de protection des données ne s'appliquent qu'aux transactions BtoC (Business to Consumer). Les entreprises BtoB doivent également se conformer aux lois sur la protection des données lorsqu'elles traitent des données personnelles.



# Mythe #10

## Les OBNL (Organisations à but non lucratif) sont exemptées

Un autre mythe courant est que les organisations à but non lucratif sont exemptées des lois sur la protection des données. En réalité, les OBNL doivent aussi souvent se conformer aux mêmes lois que les entreprises à but lucratif.



# Mythe #11

## Il y a une durée de conservation spécifique pour les données

Certaines personnes pensent que les données peuvent être conservées indéfiniment. En réalité, plusieurs lois sur la protection des données spécifient que les données ne doivent être conservées que le temps nécessaire pour atteindre les objectifs pour lesquels elles ont été collectées.



# Mythe #12

## Avoir le consentement permet de collecter toutes les données souhaitées

Bien que le consentement soit un élément clé de la collecte de données, il ne donne pas carte blanche pour collecter n'importe quel type de données. Les données collectées doivent toujours être proportionnées et pertinentes par rapport à l'objectif pour lequel elles sont collectées.



# Mythe #13

## Je n'ai pas de e-commerce, donc la protection des données ne me concerne pas

Certaines personnes peuvent penser que les règles sur la protection des données s'appliquent uniquement aux entreprises en ligne ou aux plates-formes de commerce électronique. En réalité, les lois sur la protection des données peuvent s'appliquer à toute organisation qui collecte, stocke ou traite des données personnelles, qu'elle opère en ligne ou hors ligne.



# Mythe #14

## J'ai déjà mon 'pop-up' à cookies, donc je suis en conformité.

Avoir un pop-up pour les cookies est une étape vers la conformité, mais ce n'est pas suffisant en soi. Le simple fait d'informer les visiteurs que votre site utilise des cookies n'équivaut pas à une conformité totale. Vous devez également offrir la possibilité de refuser les cookies non essentiels et d'informer les utilisateurs de la manière dont leurs données seront utilisées.

De plus, la conformité va bien au-delà de la gestion des cookies et peut inclure des aspects tels que le traitement des données personnelles, les mesures de sécurité des données, les droits des personnes concernées, etc.





# Mythe #15

## J'ai déjà mis une case à cocher dans mon formulaire d'infolettre, donc je suis en conformité

Une case à cocher pour le consentement dans un formulaire d'abonnement à une infolettre est une autre étape positive vers la conformité avec certaines lois sur la protection des données. Cependant, elle ne garantit pas une conformité complète.

Cela fait plutôt référence à la Loi C28 (anti-pourriel).





**LOI 25**

**AICHA TOHRY**

Les grandes lignes

# C'est quoi, la Loi 25?

- Mise à jour de la *Loi sur la protection des renseignements personnels dans le secteur privé*.
- Introduction de nouveaux droits pour les usagers et de nouvelles obligations pour les entreprises
- Texte législatif très différent de ce qui est applicable en ce moment au Québec

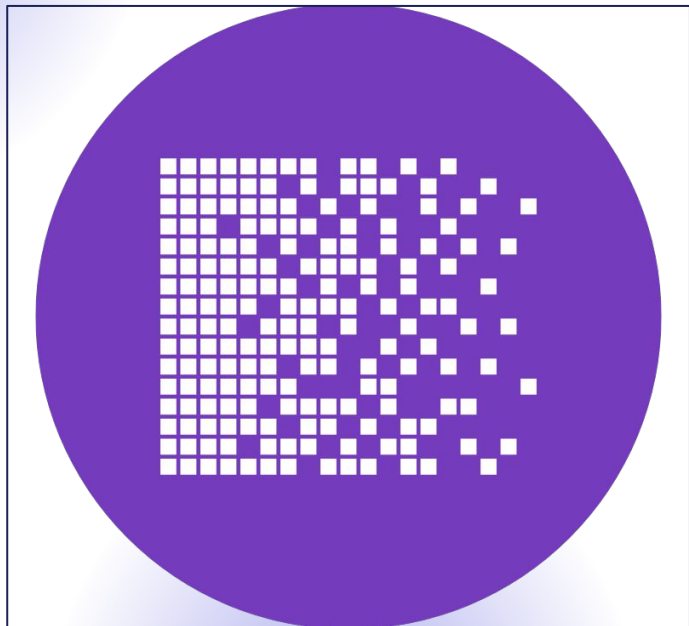
# À qui ça s'applique?

- La Loi fait référence aux entreprises:

*“l'exercice d'une activité économique organisée, quelle soit ou non à caractère commercial, consistant dans la production ou la réalisation de biens, leur administration ou leur aliénation, ou la prestation de services.”*

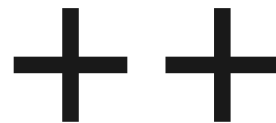
- Concerne les renseignements personnels (“RP”) des individus qui résident au Québec.

# RENSEIGNEMENT PERSONNEL



*"Tout renseignement qui concerne une personne physique et permet, directement ou indirectement, de l'identifier."*

Exclusions: renseignements personnels qui concernent l'exercice par la personne concernée d'une fonction au sein d'une entreprise



# Exemples de RP

Prénom

Nom

Date de naissance

---

Adresse courriel

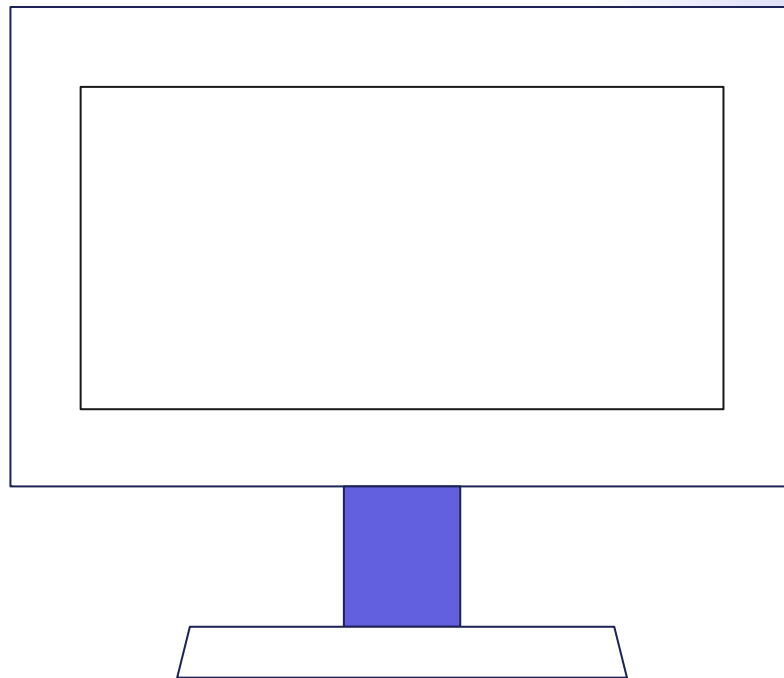
Adresse IP

Numéro de téléphone

---

# Concepts sous-jacents de la Loi 25

- Information et transparence
- Vie privée par défaut
- Responsabilisation face aux RP
- Contrôle sur ses RP



# Information et transparence

- Obtention d'un consentement libre et éclairé et (pour les RP sensibles) explicite:
  - Politiques claires et simples publiées en ligne qui expliquent, entre autres, quelles sont les RP collectées, à quelles fins & la circulation des RP
  - Avoir les capacités requises pour donner le consentement: nécessité d'avoir l'autorisation d'un parent ou tuteur pour les mineurs de moins de 14 ans



# Vie privée par défaut

- *Privacy by design*
  - Lorsqu'on offre un produit ou un service technologique: plus haut paramètres de confidentialité activés
  - Collecte de RP qui se limite à ce qui est nécessaire pour les fins mentionnées
  - Fichiers témoins (*cookies*) qui permettent le profilage, la localisation, l'identification: désactivés par défaut (**témoins non-essentiels**)
  - Conservation pendant une durée précise

# Responsabilisation

- L'entreprise qui collecte les RP en est responsable
  - Personne ayant la plus haute autorité: responsable de la protection des RP (cette fonction peut être déléguée), dont les coordonnées doivent être affichées en ligne
- Responsabilité dans le cadre de la communication des RP aux tiers
  - Consentement à la communication (certaines exceptions s'appliquent)
  - Communication à l'extérieur du QC: Évaluation des facteurs relatifs à la vie privée qui doit être faite pour s'assurer que les RP seront protégés
- Entreprise doit veiller à la sécurité des RP (mesures techniques, organisationnelles, etc)

# Responsabilisation

- Incidents de sécurité
  - Avoir politiques en place
  - Conserver un registre sur les incidents de sécurité
  - Communiquer avec les personnes concernées et la CAI lorsque nécessaire suite à un incident de sécurité
  - Prendre les mesures nécessaires pour que ça ne se reproduise plus + diminuer les risques de préjudice

# Contrôle sur ses RP

- Droit d'accéder à ses RP
- Droit de modifier ses RP à des fins de rectification
- Droit de retirer son consentement à la communication ou à l'utilisation des RP
- Droit de faire cesser la diffusion de certains RP ou de demander la désindexation de certains hyperliens



**LOI 25**

# **MÉLODIE LAMBERT**

Comprendre les concepts

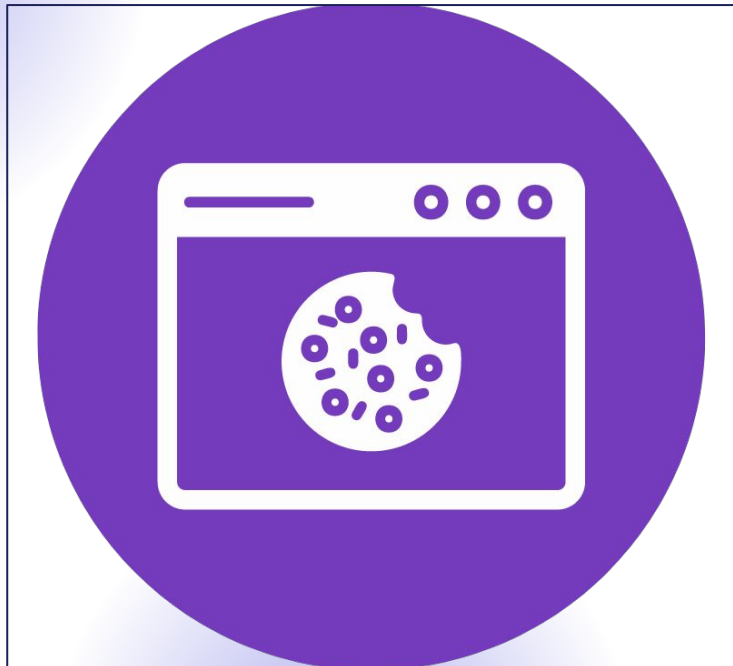


# LOI 25

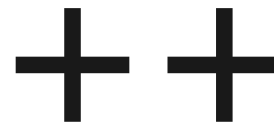
## OUTILS DE COLLECTE ET DE SUIVI

Cookie, pixel, balise: qu'est-ce que c'est, à quoi ça sert, et comment savoir si mon site les utilise?

# LES COOKIES



Un cookie, aussi appelé “témoin de connexion”, c’est un petit fichier texte qui est stocké sur l’ordinateur ou l’appareil mobile d’un utilisateur quand il visite un site web et qui nous transmet des informations spécifiques liées au site web.



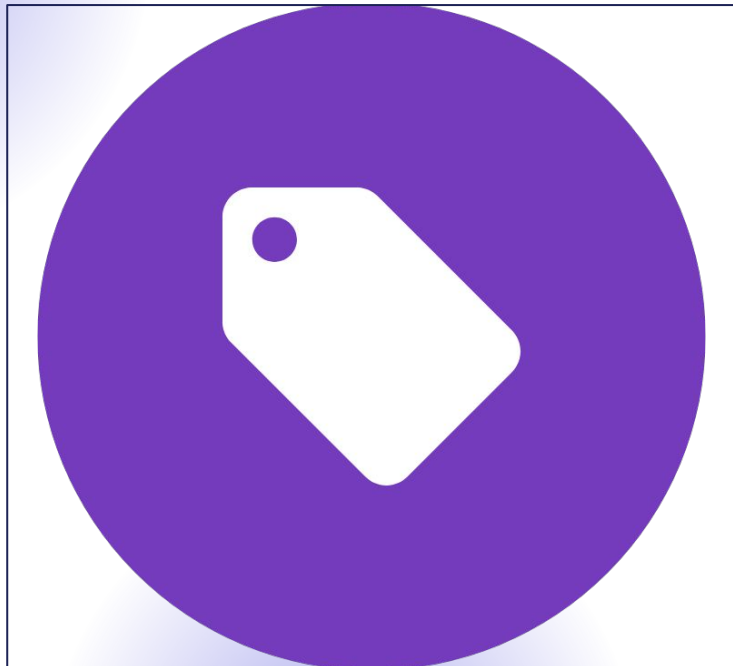
# Ne pas mettre tous les cookies dans le même panier!

Les cookies utilisés en marketing ne sont pas tous égaux, et ne sont pas considérés de la même façon aux yeux de la loi. C'est important de faire la distinction entre:

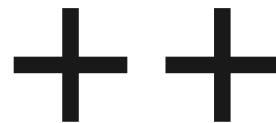
- Cookies de session VS cookies persistants
- Cookies de première partie VS tierces parties
- Cookies essentiels VS cookies non-essentiels



# LES BALISES



Une balise est un petit morceau de code, souvent JavaScript, qui est inséré dans le code source du site web pour recueillir des informations sur les interactions des visiteurs.



# Dans quel contexte est-ce qu'on utilise les cookies et balises?

Les principales plateformes de marketing que nous utilisons et qui intègrent les outils de suivi à nos autres outils d'entreprise sont Méta et son pixel ainsi que Google Analytics.

- Suivi du trafic et des interactions sur le site web
- Suivi des actions précises des visiteurs qui mènent à une conversion
- Pixel et balises de suivi des médias sociaux (ex: Méta Pixel)
- Pixel de suivi de remarketing
- Pixel de suivi de suivi des e-mails
- Pixel de suivi pour les tests A/B (ex. performance de pages de vente)



# LOI 25

## OBTENIR LE CONSENTEMENT

Les meilleures pratiques pour que  
nos clients acceptent les cookies!

# Les pop-ups

La loi 25 fait en sorte qu'on doit s'assurer du **consentement éclairé** de nos visiteurs avant de récolter les renseignements personnels et informations de suivi. Autrement dit, il faut s'assurer de leur transmettre l'information sur les données qu'on récolte en termes clairs et simples à comprendre, et ils doivent pouvoir nous autoriser à les récolter sans qu'il y ait d'ambiguïté.

C'est là que les pop-ups entrent en jeu.

Rien ne nous oblige spécifiquement à utiliser un pop-up pour demander le consentement à nos visiteurs, mais c'est de loin la méthode la plus efficace et simple à utiliser, c'est donc celle qu'on vous propose d'utiliser.

# Checklist Loi 25



[patriciafiliatrault.com/checklist-loi-25/](https://patriciafiliatrault.com/checklist-loi-25/)



# FORMATION POUR CONFORMER TON SITE WEB À LA LOI 25

TARIF RÉGULIER

**595\$** + taxes

TARIF POUR LA MISE À JOUR  
(17 au 24 janvier)

**395\$** + taxes

CODE PROMO : MISEAJOUR



PATRICIA FILIATRAULT



AICHA TOHRY



MÉLODIE LAMBERT



**\*BONUS\***  
1h avec les 3  
formatrices le  
21 fév. 11h