La protection des données et la responsabilité des syndicats

Présentation faite au Conseil fédéral à Victoriaville, le 3 mai 2023

Par Émilie Bouchard, conseillère syndicale à l'appui à l'arbitrage

Un syndicat détient plusieurs informations personnelles et souvent confidentielles concernant ses membres dans le cadre de ses activités.

L'utilisation des moyens technologiques par les syndicats, augmentée depuis la pandémie, occasionne plusieurs questionnements quant à la protection et la sécurité de ces données, notamment en cas de bris de sécurité.

La ***Loi sur la protection des renseignements personnels dans le secteur privé (LPRPSP)*** encadre la détention, la conservation et l'utilisation de renseignements personnels.

Elle s'applique aux entreprises qui ne sont pas des organismes publics et un syndicat constitue une entreprise selon cette loi.

Un syndicat doit donc respecter la **LPRPSP** quant aux **renseignements personnels** de ses **membres qu'il a en sa possession.**

Quels sont ces renseignements personnels?

Cette loi vise la protection de **tous les renseignements personnels**, c'est-à-dire :

Les renseignements qui concernent une personne physique et qui permettent de l'identifier (art.2).

Quelle que soit la nature du **support et la forme** :

- Écrit;
- Graphique;
- Sonore;
- Visuel;
- Informatique;
- ou autre.

En règle générale, les renseignements personnels détenus par un syndicat sont confidentiels.

Le syndicat ne sera pas obligé de respecter certaines dispositions (sections 2 et 3 de la loi)si les informations ont un caractère public.

Quels sont les renseignements considérés à caractère public?

La LPRPSP ne donne pas d'indication sur les renseignements qui sont publics contrairement à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

Article 57 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*

- ✓ le nom d'une personne;
- ✓ le titre d'emploi;
- ✓ et les coordonnées du lieu de travail (adresse et numéro de téléphone).

Sont des renseignements à caractère public.

Par conséquent, la prudence est de mise.

Les **coordonnées personnelles d'un membre du syndicat** sont des informations personnelles qui demeurent confidentielles, sauf exception selon la situation.

Les informations généralement les plus à risque :

- Les informations personnelles : les numéros d'assurance sociale, les numéros ou copies de permis de conduire, les dates de naissance, etc.;
- Les informations financières : les numéros de comptes bancaires, de cartes de crédit et débit, etc.;
- Les informations médicales : les numéros d'assurance maladie, les numéros de contrats ou de comptes médicaux.

Dossier d'un membre

L'article 4 de la LPRPSP permet à un syndicat de **constituer un dossier** sur autrui en raison d'un **intérêt sérieux et légitime**.

Seuls les **renseignements nécessaires** à l'objet du dossier doivent y être recueillis (art. 5 LPRPSP).

Dossier d'un membre

Le syndicat qui recueille des renseignements personnels auprès de ses membres doit les informer de la constitution d'un dossier à leur égard (art. 8 LPRPSP).

L’accès aux informations d’un membre

L’accès aux renseignements personnels devrait être limité aux **représentants syndicaux** qui ont **besoin de ces données** dans le cadre de leur travail (art. 20 LPRPSP).

Une évaluation des **fonctions de chacun** et des informations qu’ils ont besoin doit être faite.

Les personnes qui exercent un rôle **qui ne nécessite pas** ces renseignements **ne devraient pas avoir** systématiquement **accès** à celles-ci.

Conservation des renseignements

La Loi modernisant des dispositions ajoute des règles quant à la **destruction des informations**.

Un renseignement personnel conservé depuis **plus de sept (7) ans doit être détruit**.

Il ne peut plus être simplement conservé.

Dossier des membres détenu par moyen technologique

Lorsque la conservation des renseignements se fait à l'aide de moyens technologiques, il faut tenir compte également des règles prévues par la ***Loi concernant le cadre juridique des technologies de l'information***.

Cette loi vise à assurer la sécurité juridique des communications effectuées par les personnes, les associations, les sociétés ou l'État.

Dossier des membres détenu par moyen technologique

Cette loi impose un **seuil de diligence**.

La personne qui détient des renseignements **doit prendre les mesures de sécurité propres à en assurer la confidentialité et voir à ce que les moyens technologiques convenus soient mis en place** pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance.

Dossier des membres détenu par moyen technologique

La confidentialité des renseignements doit être protégée **par un moyen approprié** au mode de transmission, y compris sur des réseaux de communication.

D’importants changements législatifs ont eu lieu à l’automne 2021

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

Elle vise autant la loi concernant les organismes publics que celle applicable aux entreprises privées.

Le législateur :

- renforce les exigences de protection des données;
- améliore la transparence de la transmission des informations;
- et accroît le niveau de confidentialité des données.

Entrée en vigueur

La majorité des dispositions entreront en vigueur le **22 septembre 2023** afin de permettre aux entreprises de se conformer aux nouvelles exigences.

Les modifications qui visent les syndicats

- La Loi modernisant des dispositions introduit de façon expresse le **principe de responsabilité de l'entreprise** qui recueille des renseignements.

Elle impose à son plus haut **dirigeant** le statut de **responsable** chargé de veiller au respect et à la mise en œuvre de la loi.

Ce dirigeant peut **déléguer ce rôle** à n'importe quelle personne, qu'elle soit à l'emploi ou non de l'entreprise.

Les modifications importantes qui visent les syndicats

- La *Loi modernisant des dispositions* prévoit également que les entreprises doivent **informer les personnes physiques du nom des tiers** ou des catégories de tiers auxquels elles peuvent **communiquer leurs renseignements personnels** afin de répondre aux fins pour lesquelles ils ont été recueillis.

À qui sont les outils?

Que les représentants du syndicat utilisent leurs ordinateurs portables personnels, ceux appartenant au syndicat ou à l'employeur, ils sont tenus de respecter ces obligations.

Si le syndicat utilise **les outils**, **les services** ou le **réseau informatique** de l'employeur, certaines obligations demeurent.

Il faudra déterminer à qui appartient la responsabilité de la mise en place de mesures de sécurité adéquates. Nous croyons que c'est à l'employeur de voir à ce que son système soit bien protégé.

Par ailleurs, pour s'assurer qu'un syndicat ne soit pas tenu responsable, **il doit vérifier les protections mises en place par l'employeur** avant d'utiliser ses systèmes ou ses outils pour la transmission, la conservation ou l'utilisation des renseignements personnels de ses membres.

Incident de confidentialité

Si **un incident découle des actes du syndicat**, comme l'oubli ou le vol du matériel en sa possession et l'envoi d'un courriel ou d'une télécopie de sa part, **même si les outils appartiennent à l'employeur**, le syndicat pourrait voir sa responsabilité engagée.

À tout le moins, il pourrait être forcé de démontrer qu'il a été diligent puisqu'il demeure avec des obligations de protection quant à l'utilisation et la transmission de données.

L'employeur pourrait également soutenir qu'il n'est pas responsable de l'utilisation que fait le syndicat de ses outils et systèmes.

Incident de confidentialité

Un **syndicat** qui **détient des renseignements personnels s'expose à des risques de <u>perte ou de vol</u> de ces informations** qui peuvent avoir des conséquences importantes sur les droits des membres et leur vie privée.

La notion de « bris de sécurité » est alors utilisée.

Incident de confidentialité

Il y a incident de confidentialité en cas d'accès, d'utilisation, de communication ou de perte non autorisées à l'égard d'un renseignement personnel ou en cas d'atteinte à la protection de celui-ci.

Incident de confidentialité

Certains incidents se qualifient cyberrisques et se résument à cinq (5) catégories :

1. les cyberattaques par des cyberterroristes (*hackers*) visant le vol de données : un des risques les plus importants;
2. les cyberarnaques par des cyberterroristes (*hackers*);
3. les virus informatiques et autres logiciels malveillants;
4. la perte ou le vol d'équipements informatiques;
5. l'erreur technologique (erreur humaine).

Les cas plus fréquents pour les syndicats sont la perte ou le vol d'équipements informatiques et l'erreur technologique.

Conséquences possibles

- la perte de documents importants;
- le vol d'identité pour des demandes de crédit;
- la fraude ou un vol de sommes importantes par virement bancaire ;
- ainsi que de fausses réclamations, que ce soit auprès d'autorités gouvernementales, d'assureurs privés ou de fournisseurs.

À faire rapidement en cas d'incident

Un syndicat diligent doit prendre les mesures, en cas d'atteinte, afin de **limiter immédiatement les conséquences** d'une perte ou d'un vol de renseignements personnels en s'assurant de **mettre fin à la pratique non conforme**, le cas échéant.

Nous suggérons également de **révoquer ou modifier les mots de passe ou les codes d'accès rapidement** ainsi que d'effectuer un contrôle des lacunes dans les systèmes de sécurité.

Le syndicat doit aviser rapidement la Commission d'accès à l'information et les personnes concernées de tout incident de confidentialité impliquant un renseignement personnel qu'il détient et **présentant un risque de préjudice sérieux**.
Il doit également tenir un **registre** des incidents.

Il s'agit d'une **nouvelle exigence** prévue par la loi.

Les recours

Une personne qui considère qu'un syndicat ne respecte pas ses obligations prévues par les différentes lois a plusieurs recours à sa disposition :

- Plainte à la Commission d'accès à l'information;
- Sanctions pécuniaires;
- Poursuites pénales;
- Recours civil.

Les recours

Pour **contrer un recours,** le syndicat devra mettre en preuve qu'une **politique** est mise en place puis appliquée et que **toutes les mesures nécessaires ont été instaurées et mises à jour**.

Aussi, il devra démontrer qu'il a **agi rapidement dès** qu'il a été mis **au fait** de la situation.

La responsabilité de l'employeur

En cas de vols de données des salariés, retraités, employés postulants, l'employeur doit agir **rapidement**;

Il doit divulguer l'incident aux employés, au syndicat, à la CAI, aux autorités concernées, à son assureur et contacter une compagnie aidant dans la gestion des incidents ;

Il doit mettre en place des mesures de protection et offrir des services de surveillance aux salariés.

Recours contre l'employeur

Dans le cas où l'employeur ne met en place aucune mesure ou encore si vous souhaitez protéger les droits des salariés, **déposez un grief**;

Les salariés pourront demander à être indemnisés pour le préjudice subi;

Les salariés devront établir la faute de l'employeur dans la conservation et la gestion des renseignements personnels.

Mesures de sécurité appropriées

La responsabilité d'un syndicat pourrait être engagée s'il n'a pas mis en œuvre les mesures de sécurité appropriées pour protéger son système d'information contre des atteintes, dans la mesure où cela a causé un préjudice.

Mesures de sécurité appropriées

Le syndicat doit prendre les **moyens appropriés** pour assurer la protection des renseignements personnels; on s'attend donc à un **seuil élevé de diligence**.

Mesures de sécurité appropriées

Les mesures à mettre en place vont dépendre du degré de sensibilité des renseignements en question et d'autres facteurs comme la quantité, le format et la répartition de ces renseignements.

Plus les renseignements sont sensibles,
plus les mesures doivent être importantes.

Mesures de sécurité appropriées

Il s'agit d'une obligation de moyens renforcée.

En résumé, un syndicat devra adopter toutes les mesures de sécurité jugées nécessaires par une « entreprise » **raisonnablement prudente et diligente**.

Mesures de sécurité appropriées

Pour les documents qui **ne sont pas électroniques**, par exemple sous forme **papier**, un syndicat doit mettre en place des méthodes de conservation comme :

- l'utilisation de **classeurs verrouillés**;
- ainsi qu'une **restriction** de **l'accès** aux documents et des personnes autorisées à les consulter.

Mesures de sécurité appropriées

Pour les documents qui sont **conservés par moyen technologique,** un syndicat doit mettre en place :

- un **contrôle d'accès** effectué au moyen d'un procédé de **visibilité réduite**

ou

- un procédé qui **empêche une personne non autorisée** de prendre connaissance d'un renseignement personnel

ou selon le cas,

- **d'avoir accès autrement** à un document ou aux composantes qui permettent d'y accéder.

Mesures de sécurité appropriées

Lorsque le salarié du syndicat est à la maison :

Il doit s'assurer qu'il **ne laisse pas à la vue des données** confidentielles et qui pourraient être portées à la connaissance d'autres membres de la famille et des visiteurs du domicile.

Il doit redoubler de **prudence** lors de **l'envoi de données** par courrier électronique, télécopieur ou lors de la transmission d'informations par téléphone.

En fait, avec les adaptations nécessaires à la réalité du **télétravail**, le salarié a les **mêmes obligations** que le salarié **œuvrant dans les locaux** de l'employeur relativement à l'accès, la protection et la sécurité de l'information et des renseignements personnels.

Les pratiques à privilégier

- Placer l'équipement de bureau partagé, comme les télécopieurs, les photocopieurs, les boîtes à courrier individuelles ou communes et les casiers de traitement de documents à des endroits non accessibles au public.

- Utiliser, dans la mesure du possible, uniquement le matériel appartenant au syndicat pour la conservation, l'utilisation ou la transmission des données. À défaut de pouvoir, des mesures strictes doivent être appliquées.

Les pratiques à privilégier

- Garder sous clé dans des armoires, classeurs ou autres endroits à accès autorisé, seulement les dossiers contenant des renseignements personnels sur les membres ;

- S'assurer que le réseau sans fil que le syndicat utilise offre une authentification et une communication sécurisées ;

- Vérifier préalablement, dans la mesure où le syndicat utilise les systèmes appartenant à l'employeur, que des mesures sont mises en place par ce dernier pour assurer la protection des renseignements et permettre de prévenir les risques d'atteinte.

Les pratiques à privilégier

- Prévoir une politique et une procédure relatives à la sécurité des informations. Les mettre à jour, les distribuer et les expliquer à chaque nouveau membre de l'exécutif;

- Ne recueillir que les informations personnelles qui sont nécessaires pour l'exercice des fonctions d'un syndicat. Il faut donc que le syndicat détermine précisément les renseignements qu'il a besoin d'obtenir de ses membres et se limite à la conservation de ceux-ci ;

- Obtenir le consentement des membres concernant les informations personnelles, surtout pour la communication de celles-ci. Le consentement peut être donné verbalement.

Les pratiques à privilégier

- Informer les membres de l'application de cette politique;
- Informer les membres du nom des tiers à qui le syndicat transfère leurs renseignements personnels;
- Nommer une personne du comité exécutif qui sera responsable de la protection des données et de l'application de la procédure;
- Limiter l'accès aux renseignements personnels et déterminer quelles sont les personnes qui y auront accès;
- S'assurer que l'envoi de courriels qui contient des renseignements personnels est limité aux personnes autorisées et qu'ils sont transmis aux bons destinataires.

Les pratiques à privilégier

- Détruire les renseignements personnels qui sont conservés depuis plus de sept (7) ans ;
- Crypter les ordinateurs portatifs, les clés USB et les autres dispositifs portatifs ;
- Se munir de logiciels et de mesures de protection et les tenir à jour ;
- Installer des systèmes de détection et de prévention des intrusions et les surveiller.

Les pratiques à privilégier

- En cas d'atteinte, agir rapidement. Limiter immédiatement l'atteinte aux renseignements personnels (mettre fin à la pratique non autorisée, récupérer les dossiers, éteindre le système qui fait l'objet de l'atteinte, révoquer ou changer les codes d'accès informatiques et corriger les lacunes des systèmes de sécurité matériels ou électroniques);

- Aviser rapidement les personnes visées par l'atteinte afin de diminuer le préjudice potentiel.

Plan d'intégration des bonnes pratiques

1. <u>Responsabilité de la gestion des données</u>

- Déterminer qui est responsable de la gestion des renseignements personnels, d'en assurer la protection et de traiter les demandes d'accès. Nommer une personne du comité exécutif qui sera responsable de la protection des données et de l'application de la procédure.
- À moins qu'une personne soit identifiée responsable, la loi prévoit que c'est le plus haut dirigeant, donc le président du syndicat.

Plan d'intégration des bonnes pratiques

2. <u>Dossiers format papier</u>

Si vous avez un local syndical :

- Évaluer qui a accès au local syndical;
- Évaluer si le local syndical peut être verrouillé ou l'accès restreint ;
- Se munir de classeur verrouillé et y mettre tous les dossiers format papier des membres.

Plan d'intégration des bonnes pratiques

2. <u>Dossiers format papier</u>

Si vous n'avez pas de local syndical :

- Évaluer qui a accès à l'endroit où sont conservés les documents;
- Évaluer si cet endroit peut être verrouillé ou l'accès restreint;
- Se munir de classeur verrouillé et y mettre tous les dossiers format papier des membres.

Plan d'intégration des bonnes pratiques

- Identifier le type de renseignements personnels (catégorie de dossiers) que le syndicat détient en format papier et établir un registre des dossiers;
- Déterminer un classement physique qui assure le respect de la confidentialité et qui permet au syndicat de se retrouver;
- Débuter les travaux de classement en commençant par les dossiers contenant des renseignements personnels plus sensibles (congédiement, invalidité, harcèlement, santé et sécurité, données financières);

Plan d'intégration des bonnes pratiques

- Lors du classement, faire un ménage de chacun des dossiers ;
- Détruire les renseignements personnels qui sont conservés depuis plus de sept (7) ans et qui ne sont plus utiles pour le travail du syndicat ;
- Pour chaque type de dossier, déterminer les membres de l'exécutif qui sont autorisés à y avoir accès.

Plan d'intégration des bonnes pratiques

3. <u>Dossiers électroniques</u>

- Évaluer qui a accès aux dossiers électroniques;
- Identifier le type de renseignements personnels (par catégorie de dossiers) que le syndicat détient électroniquement;
- Déterminer un classement qui assure le respect de la confidentialité et qui permet au syndicat de se retrouver;
- Débuter les travaux de classement en commençant par les dossiers contenant des renseignements personnels plus sensibles (congédiement, invalidité, harcèlement, santé et sécurité, données financières).

Plan d'intégration des bonnes pratiques

3. <u>Dossiers électroniques</u>

- Lors du classement, faire un ménage de chacun des dossiers ;
- Détruire les renseignements personnels qui sont conservés depuis plus de sept (7) ans et qui ne sont plus utiles pour le travail du syndicat;
- Pour chaque type de dossier, déterminer les membres de l'exécutif qui sont autorisés à y avoir accès.

Plan d'intégration des bonnes pratiques

3. <u>Dossiers électroniques</u>

- Prioriser l'utilisation de matériel attitré exclusivement aux activités du syndicat ;

- Se munir de logiciels et de mesures de protection pour chacun des outils et les tenir à jour et s'assurer que l'employeur s'acquitte de ces mêmes obligations.

Plan d'intégration des bonnes pratiques

4. <u>Mise en place de la politique</u>

- Préparer une politique qui respecte les paramètres de la loi et la mettre à jour. Une politique type sera préparée dans les prochaines semaines et sera disponible pour les syndicats;
- Aviser les membres de la politique mise en place;
- La communiquer et l'expliquer à chaque nouvelle personne de l'exécutif du syndicat.

Merci!