Partis politiques et protection des renseignements personnels

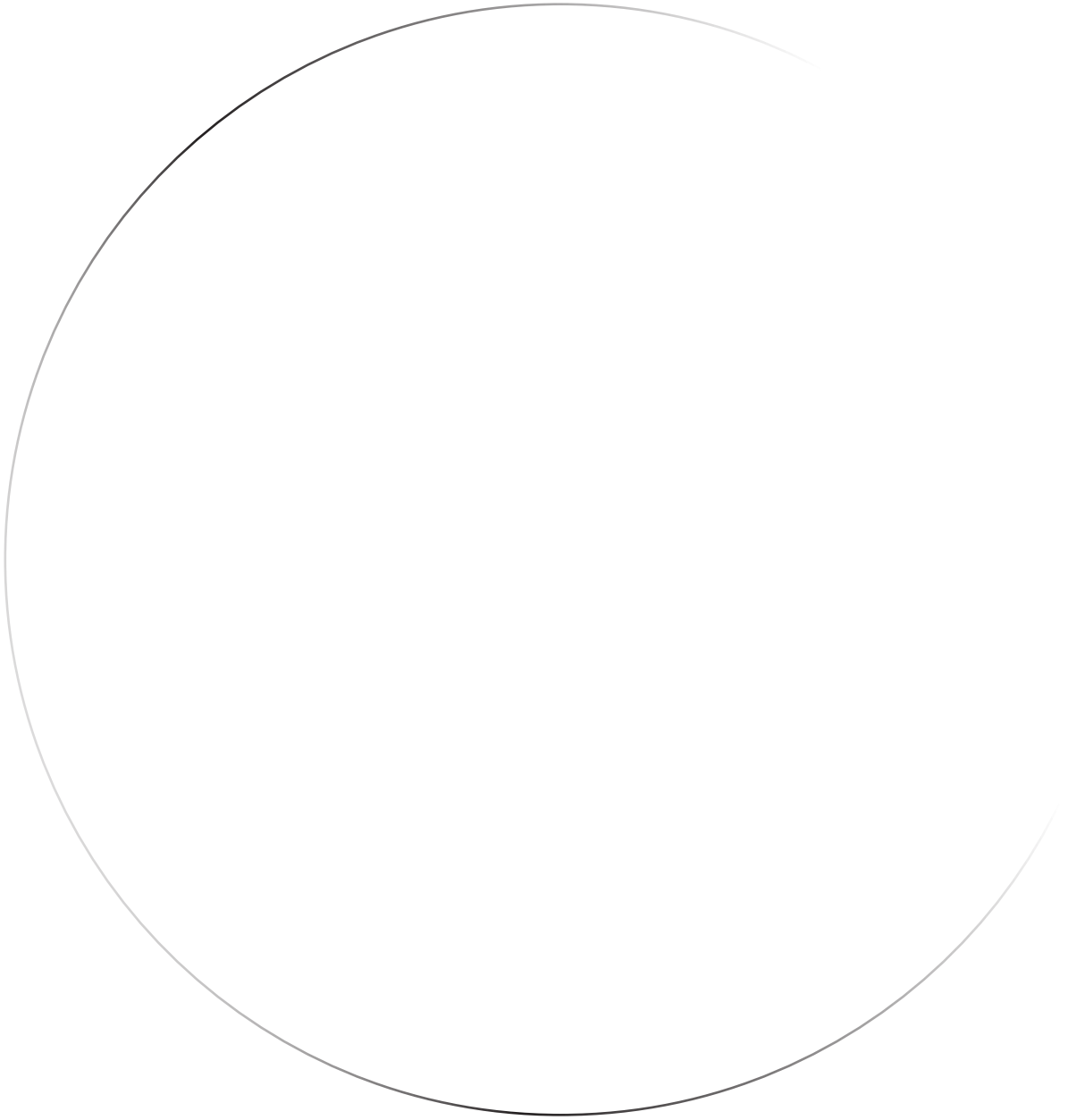
Exposé de la situation québécoise, perspectives comparées et recommandations

élections Québec

DGE-6359 (19-01)

Partis politiques et protection des renseignements personnels

Exposé de la situation québécoise, perspectives comparées et recommandations



élections Québec

Pour nous joindre :

Élections Québec
Édifice René-Lévesque
3460, rue de La Pérade
Québec (Québec) G1X 3Y5

De la région de Québec : 418 528-0422
De partout ailleurs : 1 888 ÉLECTION (1 888 353-2846)
Du lundi au vendredi, de 8 h 30 à 12 h et de 13 h à 16 h 30

Par courriel : info@electionsquebec.qc.ca
Par télécopie : 1 866 225-4095 (aucuns frais au Québec)

Les personnes sourdes ou malentendantes peuvent composer
sans frais le 1 800 537-0644.

Pour obtenir une copie de ce document, consultez
notre site Web : www.electionsquebec.qc.ca.

Dépôt légal – Bibliothèque et Archives nationales du Québec, 2019
Bibliothèque et Archives Canada
ISBN 978-2-550-83309-3 (version imprimée)
ISBN 978-2-550-83310-9 (version PDF)

Table des matières

Introduction

Depuis 2013, le directeur général des élections exprime des préoccupations à l'égard de la protection des renseignements personnels des électrices et des électeurs détenus par les partis politiques. Il recommande d'entreprendre une révision en profondeur de la *Loi électorale*[1] à ce sujet[2].

Ces recommandations sont le fruit d'une réflexion du directeur général des élections entreprise à la suite des procédures qu'il a intentées contre l'Institut Drouin[3]. Dans ce dossier, le tribunal a ordonné à cette entreprise de généalogie, en 2012, de détruire les fichiers qu'elle diffusait illégalement et qui avaient été colligés à partir de la liste électorale produite lors des élections générales provinciales de 2003.

En mars 2018, le *New York Times*[4] et le *Guardian*[5] révélaient que la firme britannique Cambridge Analytica[6] a illégitimement obtenu des renseignements concernant plus de 50 millions d'utilisateurs de Facebook et que ces renseignements ont été utilisés afin d'influencer la campagne du Brexit, au Royaume-Uni, ainsi que l'élection présidentielle américaine de 2016.

Dans les semaines qui ont suivi, ce scandale a fait écho jusqu'à l'Assemblée nationale du Québec, où les parlementaires ont exprimé leurs inquiétudes quant à la collecte de renseignements personnels sur les électrices et les électeurs par les partis politiques[7].

Le directeur général des élections est d'avis que ses préoccupations quant à la protection des renseignements personnels détenus par les partis politiques demeurent d'actualité. C'est pour cette raison qu'il souhaite susciter la réflexion sur ces questions en publiant cette étude, qui vise à examiner les façons dont les renseignements personnels détenus par les partis politiques sont encadrés à l'extérieur du Québec. Elle vise également à recenser les pratiques entourant la communication de la liste des électrices et des électeurs par les agences électorales et à comparer les pouvoirs qui sont dévolus aux autorités de surveillance pour s'assurer de la conformité des partis politiques quant à ces obligations, le cas échéant.

---

1. RLRQ, chap. E-3.3.
2. Les recommandations du directeur général des élections se trouvent dans ses rapports annuels de gestion 2012-2013 (p. 100), 2014-2015 (p. 122), 2015-2016 (p. 147), 2016-2017 (p. 128) et 2017-2018 (p. 133).
3. Voir la décision de la Cour supérieure, *Drouin* c. *9179-3588 Québec inc*. 2012 QCCS 2685, ainsi que l'appel rejeté par la Cour d'appel, *9179-3588 Québec inc. (Institut Drouin)* c. *Drouin* 2013 QCCA 2146.
4. Matthew Rosenberg, Nichols Confessore et Carole Cadwalladr, « How Trump Consultants Exploited the Facebook Data of Millions », *The New York Times*, 17 mars 2018. [https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html].
5. Carole Cadwalladr et Emma Graham-Harrison, « Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach », *The Guardian*, 17 mars 2018. [https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election].
6. Une description de l'affaire Cambridge Analytica est présentée à l'annexe 2.
7. Martin Croteau, « Scandale Facebook : des pouvoirs d'enquête accrus pour le DGEQ », *La Presse*, 7 avril 2018.

Enfin, cette étude vise à apporter un éclairage supplémentaire sur les enjeux qui sont soulevés par l'utilisation de renseignements personnels par les partis politiques, dans le contexte où il est nécessaire de préserver un équilibre entre le besoin des partis de joindre les électrices et électeurs et la protection de la vie privée de ces derniers.

L'étude qui suit est divisée en six chapitres. Les trois premiers font état de la valeur des données à l'ère numérique ; ils introduisent les principes reconnus en matière de protection des renseignements personnels et présentent certaines pratiques des partis politiques liées à l'utilisation de ces renseignements. Le quatrième chapitre décrit le cadre législatif applicable aux partis politiques au Québec. Les chapitres 5 et 6 examinent quant à eux l'encadrement applicable au Canada et à l'international. Le septième et dernier chapitre présente les enjeux qui sont soulevés par l'étude et propose neuf recommandations pour améliorer la situation.

1 Quelques considérations sur l'ère numérique

Aujourd'hui, la vie professionnelle, la vie sociale et la vie privée s'organisent autour des outils numériques, lesquels sont omniprésents dans le quotidien d'un individu.

Au sein de l'univers numérique, à l'échelle mondiale, chaque citoyen est en mesure d'échanger aisément des informations sur ses préférences, de commenter sans filtre l'actualité, d'affirmer ses opinions politiques, d'exprimer ses désirs et de révéler ses renseignements personnels d'une façon inédite. De la sorte, l'exposition d'une personne sur Internet — en partie volontaire, en partie involontaire, puisqu'elle laisse des traces sur les sites qu'elle consulte — prend une ampleur inattendue et peut engendrer des répercussions insoupçonnées.

À l'ère numérique, le respect de la vie privée semble de plus en plus fragilisé. Le citoyen formule des exigences parfois contradictoires : il accepte de se dévoiler davantage pour accéder à des services, valoriser son identité numérique et enrichir son réseau de relations, mais ne veut pas renoncer à un haut niveau de protection et de maîtrise de ses renseignements personnels, de son image et de sa réputation.

On constate souvent un écart révélateur entre les convictions d'une personne et ses pratiques courantes. D'une part, elle tient catégoriquement à la préservation de son intimité et manifeste une inquiétude au regard d'une appropriation abusive de ses données, d'un profilage indu ou d'une usurpation d'identité. D'autre part, sa façon d'agir s'avère beaucoup plus permissive : elle consent délibérément à la divulgation de renseignements personnels, selon le contexte et l'intérêt en jeu, et ce, sans la moindre garantie de protection. Voilà l'intrigant « paradoxe de la vie privée[8] », qui évoque une incohérence apparente et une ambivalence assumée.

La valorisation des données numériques

L'ère numérique se caractérise par sa capacité à bouleverser les règles du jeu et les positions établies. La collecte massive de renseignements personnels et les possibilités de recoupement des données sont amplifiées et recherchées par l'économie numérique, laquelle se déploie et tend à transformer les principaux secteurs d'activité professionnelle, commerciale, sociale et culturelle.

Les modèles d'affaires se fondent sur une valorisation intensive des données par un processus de traitement numérique. Cette dynamique pousse au regroupement de tout type de données et à leur croisement avec les renseignements personnels collectés. Le profilage permet d'affiner le ciblage et d'individualiser les offres sans que les personnes concernées aient manifesté leurs intentions ou énoncé explicitement

8. Susan B. Barnes, « A Privacy Paradox: Social Networking in the United States », *First Monday*, volume 11, numéro 9, 4 septembre 2006. [https://firstmonday.org/ojs/index.php/fm/article/view/1394/1312].

leurs préférences. Les modes de fonctionnement des algorithmes[9] qui traitent les données restent obscurs, alors qu'ils contribuent à anticiper les comportements, à cultiver les goûts et à infléchir les choix de chacun.

La collecte des données se fait de manière continue, par voie automatisée, sous une forme diffuse et insaisissable, ce qui permet aux organisations de développer une offre différenciée qui s'appuie sur une connaissance fine des besoins et de l'intérêt des individus. En ce sens, la publicité personnalisée peut être perçue comme apportant un service utile à son destinataire ou comme la contrepartie nécessaire d'un service apparemment gratuit. En règle générale, l'importance de la publicité dans le financement de l'économie numérique fait débat, puisqu'elle est basée sur une exploitation singulière et sur une marchandisation optimale des renseignements personnels des individus, ce qu'illustre l'adage « si c'est gratuit, c'est vous le produit ».

Depuis quelques années, les réseaux sociaux s'avèrent inéluctables au sein de l'univers numérique. Ils permettent aux usagers de se mailler autour d'intérêts communs, de suivre les activités de leurs amis et de leurs proches, de partager des contenus et de communiquer aisément les uns avec les autres suivant des modalités différentes selon le réseau utilisé. L'une des particularités de tous les réseaux sociaux est la création d'un profil, qui constitue le territoire numérique d'une personne sur le site concerné. Sur ce profil, l'individu met en scène sa personnalité, ses points de vue, ses faits et gestes quotidiens pour les exposer à son entourage et aux personnes intéressées, tout en contribuant à sa valorisation sociale et professionnelle. En raison de ce comportement, les sources et les types de renseignements personnels en circulation se sont considérablement élargis et enrichis.

Face à cette conjoncture, les grandes entreprises du numérique se sont engagées dans des stratégies de diversification, dont l'un des objectifs est de multiplier les données détenues sur chaque personne. Presque tous les usagers de l'univers numérique figurent dans les bases de données de Facebook[10], Google[11] ou Twitter[12]. Le principe directeur de ces plateformes numériques est de ne générer aucun contenu d'elles-mêmes. Elles laissent cette tâche à des partenaires et, surtout, aux utilisateurs, qui interagissent et mettent librement à la disposition de ces géants du Web des renseignements sur leur vie privée, tout en communiquant des informations sur les personnes qu'ils côtoient dans leur vie sociale. La valeur stratégique des données recueillies contribue à leur agrégation et à leur recoupement. Ce modèle table principalement sur les revenus provenant de publicités ciblées sur Internet, dont la gestion est assumée majoritairement par les grandes entreprises du numérique.

9. « Nombre de nos gestes quotidiens, d'achats, de déplacements, de décisions personnelles ou professionnelles se trouvent orientés par une infrastructure de calcul ». Loin d'être neutre, le calcul algorithmique importe les méthodes, les informations, les choix, les hypothèses de ceux qui l'ont mis en place. Les gigantesques infrastructures de calcul qui rythment nos activités, nos orientations, nos décisions et nos choix sont en réalité des plateformes qui visent avant tout la satisfaction d'intérêts particuliers. Voir Dominique Cardon, *À quoi rêvent les algorithmes : nos vies à l'heure des big data*, Seuil, 2015, introduction.
10. https://www.facebook.com/help/1735443093393986?helpref=hc_global_nav.
11. https://safety.google/.
12. https://about.twitter.com/fr/safety/enforcing-our-rules.html.

Les possibilités de valorisation des données ne se limitent cependant pas à la publicité et couvrent l'ensemble des usages numériques. Par exemple, Google[13] a développé d'autres services que son moteur de recherche — cartographie, infonuagique, messagerie, partage de vidéos, système d'exploitation, traduction, etc. — qui lui apportent une panoplie de données. Sa décision d'intégrer les diverses conditions d'utilisation et règles de confidentialité de chacun de ces services en une politique[14] unique de traitement des données lui permet d'agréger l'ensemble des informations, des traces et des renseignements qu'elle détient sur chaque personne, peu importe les services qu'elle utilise, afin d'établir plus précisément son profil.

Dans l'univers numérique, ce qui est dit, écrit, fait et diffusé ne peut être assurément effacé ou, du moins, ne peut l'être sans avoir été inévitablement reproduit, exploité, sauvegardé ou copié. L'imprudence dont certaines personnes font preuve peut tenir au fait qu'elles ne perçoivent pas les risques et les conséquences d'une utilisation inappropriée de ces technologies. L'imbrication toujours plus étroite des diverses données numériques fait en sorte qu'elles ne renseignent plus seulement sur un individu, mais sur un réseau de personnes qui lui sont reliées. Ainsi, les données ne peuvent être simplement considérées en tant qu'entités autonomes. Il faut être conscient que l'affaiblissement de la protection de la vie privée d'une personne peut avoir une incidence inattendue sur celle des autres[15].

D'un usage consenti à une utilisation maîtrisée et responsable

L'univers numérique a fait évoluer la manière de contribuer à la vie démocratique et à l'exercice de la citoyenneté. L'appropriation et l'usage des outils numériques se sont rapidement imposés dans le quotidien des partis politiques. Les plateformes numériques et les réseaux sociaux favorisent la proximité avec les électrices et électeurs afin d'infléchir le suffrage dans le sens souhaité. Dans ce contexte, les partis politiques recourent de plus en plus à l'utilisation des renseignements personnels des électeurs en vue de mettre en œuvre leur stratégie électorale et leurs communications politiques.

L'utilisation du numérique lors de la campagne électorale de Barack Obama[16] en 2008 est devenue un véritable cas d'école pour la communication politique partout dans le monde. Nous présentons ci-dessous certaines de ses caractéristiques sous l'angle de l'usage des renseignements personnels des électrices et des électeurs. Cette façon de faire a inspiré plusieurs partis politiques.

13. https://www.google.ca/intl/fr_ca/about/products/.
14. https://www.google.com/intl/fr_ca/policies/terms/archive/20070416/.
15. Francesca Musiani, *Internet et vie privée*, Uppr Éditions, 2016, chapitre 2.
16. Terra Nova, *Moderniser la vie politique : innovations américaines, leçons pour la France*, janvier 2009. [Rapport de la mission d'étude de Terra Nova sur les techniques de campagne américaines]. [http://tnova.fr/system/contents/files/000/000/678/original/terranova-rapportmissionus.pdf?1436779596].

En 2006, la base de données Catalist[17] a été créée dans le but de répertorier plus de 220 millions d'Américains et d'exploiter jusqu'à 600 types de renseignements par personne à des fins électorales. L'équipe d'Obama a fait l'achat de fichiers afin d'agréger le maximum de données existantes — associatives, commerciales, politiques, sociétales, sportives, etc. — et y a ajouté les renseignements sur les électrices et les électeurs issus de la collecte militante lors des élections primaires et de la campagne électorale, ce qui représentait les deux tiers des informations recueillies.

L'équipe a ensuite employé la technique du microciblage. Elle a utilisé ces données afin de développer des messages personnalisés pour la communication numérique par texto, par courriel et sur les réseaux sociaux, mais aussi pour le porte-à-porte chez les sympathisants. Il ne s'agissait pas d'une campagne électorale fondée sur la sensibilité politique des électrices et des électeurs, mais d'une campagne motivée par la création d'un mouvement pour le changement et par la mobilisation directe de chaque citoyen. À la faveur d'une communication individualisée et ciblée, on visait prioritairement à susciter l'adhésion et l'appropriation : les électrices et les électeurs se transformaient en acteurs du changement et avaient le sentiment de faire intégralement partie de la campagne électorale de Barack Obama sur le terrain, sur les réseaux sociaux et dans l'univers numérique en relayant à leur entourage cette ambition de faire bouger les choses exprimée par les slogans « Change we can believe in » et « Yes we can ».

Au lieu de dévoiler une grande diversité, un traitement numérique de données appuyé sur de nombreuses traces individuelles finit par construire des groupes homogènes de citoyens. Au cours de cette campagne numérique, ce n'était pas forcément un politicien qui venait s'adresser à l'électeur ; c'était quelqu'un comme lui, un citoyen qui faisait face aux mêmes inquiétudes dans son quotidien. Comme sur les réseaux sociaux, ce n'était pas un inconnu qui interagissait avec l'électeur : c'était un proche, un ami, un collègue, un voisin, un membre de sa communauté numérique, qui lui était familier. En somme, quelqu'un avec qui l'électeur avait un lien de confiance et de proximité et avec qui il partageait des moments de sa vie et des renseignements personnels sans crainte.

Cette stratégie de communication politique ne relevait pas directement des militants et des sympathisants. L'organisation de la campagne était fortement encadrée par la plateforme numérique[18] MyBo de l'équipe de Barack Obama. Même si l'information sur les électrices et les électeurs circulait librement auprès des militants et des sympathisants, et ce, sans qu'on envisage les conséquences que cela pourrait avoir sur eux, rien n'indique qu'il y aurait eu un usage inapproprié des données. Cette campagne électorale a été rendue possible par l'exploitation de renseignements personnels et de données sensibles des électrices et électeurs[19], ce qu'un parti politique américain peut faire en toute légitimité.

17. https://www.catalist.us/data/.
18. Heather Havenstein, « My.BarackObama.com Social Network Stays Online after Election », *Computerworld,* 10 novembre 2008. [https://www.computerworld.com/article/2534052/web-apps/my-barackobama-com-social-network-stays-online-after-election.html].
19. James E. Katz, Michael Barris et Anshul Jain*, The Social Media President – Barack Obama and the Politics of Digital Engagement*, Palgrave Macmillan, 2013, chapitre 2.

Dès lors, les logiciels électoraux se sont popularisés, la collecte de données offrant des perspectives toujours plus poussées, orientées vers des modèles prédictifs propices à un ciblage de plus en plus fin[20]. Au Québec comme partout dans le monde, la question de la protection de la vie privée et des renseignements personnels est devenue un sujet de préoccupation à l'ère numérique, et ce, particulièrement en période électorale.

Ce contexte s'avère propice pour que le directeur général des élections poursuive son questionnement sur l'encadrement normatif requis afin d'assurer la protection des renseignements personnels détenus par les partis politiques ainsi que sur les mesures de gouvernance mises en œuvre dans le but d'assurer une utilisation maîtrisée des renseignements personnels des électrices et des électeurs.

20. Antonin Guyader, « Les enjeux du grand bouleversement », *Pouvoirs*, 2018/1, numéro 164, Seuil.

2 Les principes de protection des renseignements personnels

Avant de présenter les pratiques des partis politiques et d'examiner les régimes d'encadrement législatifs applicables, nous expliquerons en quoi consiste la protection des renseignements personnels. Dans le présent chapitre, nous présenterons les principes sous-jacents à la protection des renseignements personnels qui sont reconnus dans plusieurs législations internationales.

Dans le cadre de cette étude, nous utilisons les termes *renseignements personnels* et *données à caractère personnel* afin de désigner tous les renseignements qui concernent une personne physique et qui permettent de l'identifier, directement ou indirectement. Cette définition large et inclusive englobe tant des renseignements d'identité, comme le nom, l'adresse, la date de naissance, le numéro de téléphone, le numéro d'assurance maladie ou d'autres renseignements uniques à une personne, que des renseignements qui, en raison du contexte ou lorsque associés à d'autres renseignements, permettent d'identifier un individu et de révéler une information à son sujet.

Les principes reconnus au Québec et au Canada en matière de protection des renseignements personnels sont inspirés de ceux développés par l'Organisation de coopération et de développement économiques en 1980. Bien qu'il existe des différences dans la façon dont les pays ont transposé ces principes dans leurs lois respectives, ils se retrouvent généralement dans les législations en matière de protection des renseignements personnels ainsi que dans les normes sectorielles de bonnes pratiques.

Au Québec, ces principes se retrouvent dans la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[21], adoptée en 1982, ainsi que dans la *Loi sur la protection des renseignements personnels dans le secteur privé*[22], adoptée en 1993. Au Canada, en l'absence d'un encadrement légal s'appliquant aux entreprises, l'Association canadienne de normalisation a développé, en 1996, le *Code type sur la protection des renseignements personnels.* Il s'agit d'un code volontaire, conçu pour être appliqué par toute personne, toute entreprise et tout organisme public qui recueillent et utilisent des renseignements personnels. Les dix principes de cette norme ont par la suite été intégrés à la *Loi sur la protection des renseignements personnels et les documents électroniques*, adoptée en 2000, qui s'applique aux organisations du secteur privé au Canada, à l'exception de celles qui sont régies par une loi provinciale jugée essentiellement similaire[23].

21. RLRQ, chap. A-2.1.

22. RLRQ, chap. P-39.1.

23. Seuls le Québec, l'Alberta et la Colombie-Britannique ont des lois jugées essentiellement similaires.

Nous présenterons les notions relatives à la protection des renseignements personnels en fonction de ces dix principes plutôt que de faire référence aux lois applicables aux Québec. Cela permettra au lecteur de mieux comprendre en quoi consiste la protection des renseignements personnels, sans égard aux obligations légales et sans terminologie juridique.

Ces principes sont présentés sans tenir compte de la fonction des organisations, puisqu'ils ont été développés pour qu'ils soient appliqués par tout type de personne ou d'entité, peu importe la nature des renseignements personnels qu'elle détient et l'utilisation qu'elle en fait[24].

Responsabilité

Selon le principe de responsabilité, une organisation qui détient des renseignements personnels est responsable de tous les renseignements personnels dont elle assure la gestion et doit désigner une personne qui s'assure du respect des principes de protection des renseignements personnels.

Cela implique que cette organisation se dote de politiques et de procédures afin d'intégrer la protection des renseignements personnels à ses pratiques et à ses opérations courantes.

La personne responsable de la protection des renseignements personnels doit notamment veiller à ce que l'ensemble des membres de l'organisation respectent les politiques et les procédures établies, notamment à l'aide de formations et d'activités de sensibilisation. L'identité et les coordonnées de cette personne doivent être accessibles à toute personne qui fournit des renseignements personnels à l'organisation.

La responsabilité d'une organisation ne s'arrête pas aux renseignements qu'elle détient physiquement. Elle inclut également ceux qu'elle confie à des mandataires ou à des prestataires de service. Par exemple, une organisation qui confie la gestion ou l'hébergement de données à caractère personnel à un prestataire de service doit, par l'entremise de clauses contractuelles ou d'une entente, s'assurer que ce prestataire offre le même degré de protection des renseignements personnels qu'elle et qu'il ne peut les utiliser ou les communiquer d'une autre manière ou dans d'autres contextes que ceux prévus dans le contrat ou l'entente.

Détermination des fins de la collecte des renseignements

La détermination des fins de la collecte de renseignements est un principe fondamental de la protection des renseignements personnels. En effet, une organisation ne peut recueillir de renseignements personnels avant d'avoir déterminé à quelles fins ils seront utilisés.

La documentation de ces fins permet à l'organisation d'être transparente et de préciser, avant ou au moment de la collecte, à quelles fins les renseignements personnels seront utilisés.

---

24. Une description plus détaillée de ces principes se trouve à l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* (L.C. 2000, chap. 5).

Consentement

Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir.

Lorsque l'organisation ne peut recueillir de renseignements directement auprès de la personne concernée et qu'elle les recueille plutôt auprès d'un tiers, elle doit s'assurer que la personne concernée a consenti à ce que ce tiers puisse lui communiquer ses renseignements personnels ou que la loi autorise ce tiers à lui communiquer ces renseignements sans consentement.

Limitation de la collecte

Une organisation ne peut recueillir tous les renseignements qu'elle juge utiles. Elle doit se limiter aux seuls renseignements qui lui sont nécessaires pour accomplir les fins qu'elle a déterminées. La notion de nécessité implique que l'organisation restreint tant la quantité que la nature des renseignements qu'elle recueille en fonction de ses besoins.

La collecte de renseignements doit être effectuée par des moyens légitimes. Une organisation doit faire preuve de transparence et s'assurer qu'elle explique clairement quels renseignements elle recueille et à quelles fins elle le fait.

Limitation de l'utilisation, de la communication et de la conservation

Ce principe découle de celui du consentement. Il implique que les renseignements personnels détenus par l'organisation ne sont pas utilisés ou communiqués à d'autres fins que celles pour lesquelles ils ont été recueillis, sauf lorsque la personne concernée y consent ou qu'une loi l'autorise.

Ce principe implique également qu'une organisation détermine la durée de conservation des renseignements qu'elle obtient en fonction de l'usage auquel ils sont destinés et s'assure de les détruire lorsque cet usage a été réalisé.

Exactitude

Une organisation doit s'assurer que les renseignements personnels qu'elle détient sont exacts, complets et à jour afin de réduire les possibilités que des renseignements erronés portent préjudice à la personne concernée. La mise à jour des renseignements ne doit toutefois être effectuée que lorsque cela est nécessaire.

Mesures de sécurité

Selon ce principe, les renseignements personnels doivent être protégés par des mesures de sécurité qui correspondent au degré de sensibilité des renseignements.

L'organisation doit se doter de mesures qui lui permettent de prévenir la consultation, la communication ou l'utilisation non autorisée de renseignements personnels, ainsi que de réduire les risques de vol ou de perte de renseignements.

Transparence

Une organisation doit être transparente quant à la façon dont elle assure la gestion des renseignements personnels qu'elle détient et aux mesures qu'elle met en place pour les protéger. Elle doit rendre accessibles ses politiques et ses procédures visant à protéger ces renseignements.

Accès aux renseignements personnels

Lorsqu'une personne lui en fait la demande, une organisation doit l'informer de l'existence des renseignements qu'elle détient à son sujet et de l'utilisation qu'elle en fait. L'organisation doit aussi indiquer si elle a communiqué ces renseignements à des tiers. Elle doit également permettre à cette personne de les consulter ou d'en obtenir copie ainsi que d'en contester l'exactitude et d'en exiger la correction ou la destruction, le cas échéant.

Contestation

Toute personne doit être en mesure de se plaindre du non-respect des principes par l'organisation, le cas échéant. L'organisation doit donc établir des procédures pour recevoir les plaintes et y donner suite. Elle doit notamment établir des mécanismes internes pour évaluer ces plaintes et prendre les mesures appropriées lorsqu'une plainte est jugée fondée.

EN BREF

La protection des renseignements personnels obéit à une série de principes applicables, avec adaptation, à tout type d'organisation, publique ou privée. Ces principes se retrouvent d'ailleurs, sous différentes formes, dans les législations internationales relatives à la protection de la vie privée.

Essentiellement, ces principes reposent sur le droit de la personne concernée de consentir à la collecte, à l'utilisation et à la communication de ses renseignements personnels, et sur l'obligation, pour l'organisation qui détient ces renseignements, de limiter l'utilisation qu'elle en fait aux seules fins pour lesquelles la personne a fourni son consentement.

3 Aperçu des pratiques numériques des partis politiques au Québec

Les technologies numériques font désormais partie intégrante des plateformes électorales des principales formations politiques au Québec. En plus de façonner les nouvelles manières de mener les campagnes, ces technologies ont modifié les pratiques des partis en matière de communication avec les électrices et les électeurs et de mobilisation des sympathisants.

Les principaux partis politiques disposent désormais d'outils qui sont au cœur de leurs campagnes : les bases de données électorales. Ces bases de données offrent aux partis la possibilité de compiler un nombre important de renseignements personnels sur les électrices et les électeurs provenant de diverses sources. Au nombre des nouvelles façons de faire des partis, l'utilisation des réseaux sociaux occupe également une place importante, principalement pour la communication avec l'électorat.

Le présent chapitre brosse un portrait des pratiques actuelles des partis politiques au Québec en matière de collecte et d'utilisation des renseignements personnels. Puisqu'aucun examen exhaustif de ces pratiques n'a été mené au Québec à ce jour, la recension présentée dans cette section s'appuie sur des sources d'information médiatiques et des pratiques documentées ailleurs au Canada, dont certaines pourraient avoir cours au Québec.

Cette recension ne couvre donc pas la totalité des pratiques des partis en matière de collecte et d'utilisation des renseignements personnels, mais en effectue un survol fondé sur des bases rigoureuses et objectives.

3.1 Les bases de données électorales

Le recours aux bases de données sur les électrices et les électeurs ne date pas d'hier. Élaborées initialement à partir des données sur les membres des partis[25], elles ont évolué au fil du temps, de sorte qu'elles comporteraient maintenant un nombre important de renseignements sur les électeurs. Ces données structurées permettraient aux partis d'effectuer le profilage d'un plus grand nombre de personnes, incluant celles qui ne font pas partie de ses partisans[26] et, « […] surtout, une personnalisation croissante de la communication électorale. L'objectif ultime étant de pouvoir faire vibrer les cordes sensibles particulières à chaque électeur ciblé[27] ». L'utilisation

25. Colin J. Bennett, *Voter Surveillance, Micro-Targetting and Democratic Politics: Knowing How People Vote Before They Do,* 11 avril 2014, p. 4. [https://ssrn.com/abstract=2605183].

26. *Loc. cit.*

27. Pierrot Péladeau, « Les partis politiques espionnent-ils vraiment votre « vie privée » ? », *Blogues*, *Journal de Montréal,* 21 août 2015. [https://www.journaldemontreal.com/2015/08/21/les-partis-politiques-espionnent-ils-vraiment-votre--vie-privee].

des nouvelles bases de données sur les électrices et électeurs remplacerait notamment le traditionnel « pointage » des électeurs sympathisants, opposants ou indécis, et ce, par des moyens plus rapides et efficaces[28].

Les principales formations politiques provinciales auraient investi, au cours des années, dans l'acquisition, le développement et l'adaptation d'outils informatiques leur donnant la possibilité de récolter et d'exploiter un maximum d'informations sur les électrices et les électeurs[29].

Dans la plupart des cas, les partis auraient eu recours à des prestataires de services spécialisés dans le développement de solutions informatiques, dans l'hébergement de serveurs ou dans l'analyse de mégadonnées. Dans certains cas, les bases de données seraient alimentées par des données géodémographiques disponibles sur le marché et qui permettent de classer les électrices et électeurs selon une panoplie de profils ou de styles de vie. En disposant de tels outils, « les partis politiques se servent des recherches les plus récentes en analyse comportementale pour adapter leurs messages, faire sortir le vote et atteindre leurs objectifs[30] ».

Ces bases de données constitueraient, pour les partis politiques, un outil essentiel pour optimiser le temps et les ressources consacrées au pointage, à la communication avec l'électorat ainsi qu'à sa mobilisation, dans un contexte où les ressources sont limitées[31].

C'est précisément ce que leur offriraient les bases de données sur l'électorat. En donnant aux partis la possibilité d'effectuer quantité de croisements entre les différents renseignements qu'ils recueillent sur les électrices et les électeurs, ces bases de données permettraient de cibler leurs préoccupations, d'établir des profils types et de les joindre à l'aide du moyen de communication le plus approprié.

Cette collecte de renseignements permettrait d'« […] ajuster les stratégies de persuasion, de cibler le message auprès de l'électeur et de le personnaliser. L'objectif ultime : repérer les électeurs indécis et identifier ceux et celles qui peuvent se laisser convaincre[32] ».

Les bases de données seraient d'autant plus utiles pour les partis dans le contexte actuel, où l'on observe un désengagement politique croissant, qui se traduit notamment par une baisse de la participation électorale[33]. Les partis sont de plus en plus nombreux et les électrices et électeurs semblent désormais plus sensibles aux idées soumises par les partis que portés vers une allégeance politique particulière. Dans ce contexte, « une [fine] connaissance du terrain [permettrait] aux politiciens de s'adapter à la montée de l'individualisme. Le citoyen est devenu un consommateur qui s'attend à

28. *Ibid.*

29. Martin Croteau, « Ce que les partis savent sur vous », *La Presse+,* 20 août 2018.

30. Institut de recherche en politiques publiques (IRPP), *Enjeux découlant des communications inappropriées reçues par les électeurs : rapport de table ronde,* mars 2013, p. 9. [https://on-irpp.org/2lyxY9e].

31. Janet Davison, « Robocalling and the Art of Finding Voters », *CBC News*, 29 février 2012. [http://www.cbc.ca/news/politics/story/2012/02/29/f-voter-identification.html].

32. Marc Godbout, « Les partis politiques recourent de plus en plus au profilage des électeurs », *Radio-Canada*, 30 septembre 2015. [https://ici.radio-canada.ca/nouvelle/737249/profilage-bases-donnees-partis-politiques-big-data].

33. Colin J. Bennett et Robin M. Bayley, *Les partis politiques fédéraux du Canada et la protection des renseignements personnels : une analyse comparative*, 28 mars 2012, p. 2. [Rapport préparé pour le Commissariat à la vie privée du Canada]. [https://www.priv.gc.ca/media/1757/pp_201203_f.pdf].

recevoir une offre personnalisée. L'électeur, dont l'allégeance est de plus en plus volatile, choisit son parti en fonction de ce qu'il y a pour lui, concrètement, dans les engagements d'une campagne[34] ».

Dans certains cas, le résultat des élections dépendrait également de la capacité des partis d'obtenir le vote d'un groupe important d'électrices et d'électeurs indécis dans les districts ou les circonscriptions clés[35], ou encore dans ceux où la lutte est serrée. Cela justifierait l'utilité, pour les partis, d'avoir accès à des bases de données qui « permettent la construction de profils détaillés d'électeurs individuels et le « micro-ciblage » de messages de plus en plus précis[36] ».

Selon les sources médiatiques et les études consultées, les bases de données sur l'électorat seraient hébergées et accessibles à partir d'applications Web. De plus, certains partis politiques auraient à leur disposition une version mobile de leurs bases de données, qui permettrait aux bénévoles d'accéder aux informations sur les électrices et les électeurs à partir d'un téléphone intelligent lorsqu'ils effectuent du porte-à-porte[37]. Ces versions mobiles permettraient également de recueillir des informations sur les électeurs en temps réel[38]. Ainsi, si un électeur exprime un intérêt pour un sujet en particulier, le bénévole peut saisir cette information directement dans son dossier[39].

Les bases de données sur l'électorat peuvent également être utilisées pour la gestion des campagnes, notamment pour l'affectation des bénévoles, la génération de listes d'appels téléphoniques dans une région donnée, l'organisation des opérations de porte-à-porte ou encore l'envoi de textos. Ces systèmes permettent notamment d'établir des itinéraires facilitant le porte-à-porte pour les bénévoles et d'optimiser l'organisation d'évènements. Notons que l'utilisation de plus en plus courante des appels automatisés par les partis politiques découlerait du fait que leur coût serait moins élevé que celui associé à d'autres modes de communication traditionnels[40].

Selon une source médiatique[41], les partis politiques au Québec ne détiendraient, dans leurs bases de données, que des informations qu'ils ont recueillies eux-mêmes, outre celles comprises dans la liste électorale transmise par le directeur général des élections.

Il est permis de penser, *a priori*, que les électrices et les électeurs fournissent des informations aux partis politiques de façon volontaire dans le cadre des campagnes électorales. Cependant, en effectuant des campagnes portant sur des enjeux

---

34. Alec Castonguay, « Les partis politiques vous espionnent », *L'Actualité*, 14 septembre 2015. [https://lactualite.com/societe/2015/09/14/les-partis-politiques-vous-espionnent].
35. Colin J. Bennett, *op. cit.*, p. 7.
36. Colin J. Bennett, « Voter Databases, Micro-Targetting, and Data Protection Law: Can Political Parties Campaing in Europe as They Do in North America? », *International Data Privacy Law*, vol. 6 nº 4, 2016, p. 261 [Traduction libre].
37. Hugo Joncas, « Partis politiques : ils vous ont tous fichés », *Journal de Montréal,* 28 juillet 2018. [https://www.journaldemontreal.com/2018/07/28/partis-politiques-ils-vous-ont-tous-fiches].
38. Marc Godbout, *op. cit.*
39. Martin Croteau, *op. cit.*
40. Institut de recherche en politiques publiques (IRPP), *op. cit.*, p. 8.
41. Antoine Robitaille, « Les partis vous espionnent-ils ? », *Journal de Montréal*, 24 mars 2018. [https://www.journaldequebec.com/2018/03/24/les-partis-vous-espionnent-ils].

particuliers, les partis ont la possibilité de récolter, sur leur site Web, les coordonnées des électrices et des électeurs et leur opinion ou leur intérêt sur ces enjeux[42], et ce, sans qu'ils en soient expressément informés. Dans certains cas, nous pouvons présumer que les électeurs n'ont pas toujours conscience de l'utilisation éventuelle des renseignements qu'ils fournissent lorsqu'ils s'expriment dans le cadre de ces campagnes.

Le nombre d'électrices et d'électeurs au sujet desquels des données exhaustives sont compilées varierait selon le parti politique. De même, la quantité et la nature des renseignements recueillis différeraient selon l'électeur et la méthode de collecte des données[43].

L'encadré qui suit présente un résumé des possibilités offertes par l'exploitation des bases de données sur l'électorat par les partis politiques et des avantages qui peuvent en découler.

Les possibilités offertes par les bases de données sur l'électorat[44]

- Suivi du nombre de membres, de donateurs et de sympathisants ;
- Optimisation du temps de collecte de données sur les électrices et les électeurs, notamment pour les ressources affectées sur le terrain par les militants et bénévoles ;
- Recension des préoccupations des citoyens et de leurs besoins ;
- Identification des sympathisants (pointage) ;
- Transmission de rappels aux partisans (dates de réunion et d'activités, adresses des lieux de scrutin, etc.) ;
- Suivi plus efficace du nombre d'électeurs qui sont allés voter et des rappels requis le jour du vote ;
- Communication ciblée ou personnalisation des messages communiqués lors d'appels téléphoniques ou de porte-à-porte (microciblage) ;
- Production de portraits détaillés du bassin d'électrices et d'électeurs potentiels ;
- Suivi des enjeux locaux et nationaux ;
- Recoupements de données afin de dresser des profils types d'électeurs (profilage) ;

42. Hugo Joncas, *op. cit.*

43. Marc Godbout, *op. cit.*

44. Institut de recherche en politiques publiques (IRPP), *op. cit.*, p. 4 ; Colin J. Bennett et Robin M. Bayley, *op. cit.*, p. 19 ; Martin Croteau, *op. cit.* ; Annabelle Blais et Alexandre Robillard, « L'arme secrète à 1 M$ de la CAQ », *TVA*, 4 octobre 2017 [https://www.tvanouvelles.ca/2017/10/04/larme-secrete-a-1-m-de-la-caq] ; Hugo Joncas, *op. cit.*

- Priorisation des efforts de mobilisation dans certains secteurs géographiques en fonction de caractéristiques socioéconomiques ciblées ou de résultats électoraux favorables obtenus dans certaines sections de vote, notamment dans des circonscriptions où la compétition est plus serrée (pour faire voter les partisans) ;
- Promotion de la participation à la démocratie en incitant les sympathisants à aller voter ;
- Mobilisation de la base militante de certains partis et appui à l'action politique au quotidien, au cours et en dehors de la période électorale.

3.2 Les sources et les données

Maintenant que nous avons décrit de façon globale les possibilités qu'offrent les technologies numériques aux partis politiques, nous présentons, dans cette section, de façon plus schématique et détaillée, les principales sources de renseignements qui seraient utilisées par les partis pour alimenter leurs bases de données sur les électrices et les électeurs, ainsi qu'une liste des renseignements que ces bases de données peuvent contenir.

Les sources

L'une des sources de renseignements qui alimentent les bases de données sur l'électorat est la liste électorale provinciale, qui est transmise aux partis politiques par le directeur général des élections. Cette liste contient :

- Le nom de l'électeur ou de l'électrice ;
- Son adresse ;
- Son sexe ;
- Sa date de naissance ;
- Son adresse à l'extérieur du Québec, lorsqu'il est autorisé à exercer son vote hors du Québec.

En plus des renseignements provenant des listes électorales provinciales, les partis politiques compileraient des renseignements sur les électrices et les électeurs à partir de diverses sources de données. L'encadré qui suit présente quelques exemples de sources. Rappelons qu'en l'absence d'un examen approfondi des pratiques des partis politiques au Québec, les informations concernant les sources de renseignements sont tirées de sources médiatiques et des pratiques recensées ailleurs au Canada. Les sources de renseignements citées ne sont pas nécessairement utilisées par tous les partis politiques.

Autres sources potentielles de renseignements des partis politiques[45]

- Listes publiques de numéros de téléphone achetées par les partis ;
- Appels téléphoniques de pointage (automatisés ou non) pour mobiliser l'électorat ou pour faire des sondages ;
- Renseignements sur les électeurs recueillis par les bénévoles sur le terrain (porte-à-porte, évènements, congrès, etc.) ;
- Données liées à l'adhésion au parti (carte de membre, participation à des congrès et évènements, réponses à des campagnes, bénévolat, etc.) ;
- Contributions versées aux partis politiques, notamment par l'entremise de l'outil « Recherche sur les donateurs », accessible à partir du site Web du directeur général des élections ;
- Sondages internes ;
- Prises de position publique (p. ex., lettres dans les journaux, commentaires dans des blogues) ;
- Pétitions et campagnes politiques portant sur des enjeux particuliers, à partir desquelles les partis politiques peuvent recueillir des numéros de téléphone cellulaire et des adresses de courriel ;
- Abonnement à des listes d'envoi du parti et inscription à des bulletins en ligne ;
- Résultats électoraux passés par section de vote ;
- Bases de données géodémographiques achetées auprès de tiers ;
- Données du recensement de Statistique Canada par secteur géographique.

45. Bennett 2014, *op. cit.*, p. 5 ; Hugo Joncas, *op. cit.* ; Martin Croteau, *op. cit.* ; Colin J. Bennett et Robin M. Bayley, *op. cit.*, p. 21, 38 et 40 ; Manon Cornellier, « Et les partis politiques, eux ? », *Le Devoir*, 29 mars 2018 ; Marc Godbout, *op. cit.*

Les renseignements sur l'électorat potentiellement compilés par les partis

Les partis politiques peuvent recueillir d'autres renseignements, notamment les données d'ordre démographique et socioéconomique en fonction de repères géographiques divers (bases de données géodémographiques), que les partis peuvent se procurer auprès de fournisseurs externes. Certaines formations politiques conserveraient également un historique des informations sur les électrices et les électeurs dans leurs systèmes, ce qui leur permettrait de suivre ces personnes d'élection en élection.

L'encadré qui suit présente les renseignements que les partis politiques peuvent compiler sur les électrices et les électeurs. Rappelons qu'en l'absence d'un examen approfondi des pratiques des partis politiques au Québec, les informations concernant les renseignements potentiellement compilés par les partis sont tirées de sources médiatiques et des pratiques recensées ailleurs au Canada. Les renseignements cités ne sont pas nécessairement compilés par tous les partis politiques.

Les renseignements sur les électeurs potentiellement compilés par les partis politiques[46]

- Nom et adresse ;
- Sexe et date de naissance ;
- Numéro de téléphone (domicile, cellulaire) ;
- Adresse de courriel ;
- Allégeance politique ;
- Historique de l'implication dans le parti (membre ou non, participation à des évènements, contributions politiques, réponses à des campagnes, bénévolat, etc.) ;
- Sympathisant ou opposant au parti ;
- Renseignements sur les champs et les enjeux politiques d'intérêt (environnement, santé, éducation, souveraineté, etc.) ;
- Commentaires et préoccupations recueillis par les bénévoles lors d'opérations de porte-à-porte, d'appels téléphoniques ou de tout autre évènement ;
- Langue parlée à la maison ;
- Langue privilégiée pour les communications avec le parti ;
- Origine ethnique ;

46. Hugo Joncas, *op. cit.* ; Martin Croteau, *op. cit.* ; Colin J. Bennett et Robin M. Bayley, *op. cit.*, p. 19, 21, 38 et 40 ; Manon Cornellier, *op. cit.*

- Situation familiale (célibataire, marié, divorcé, en union de fait, monoparental, etc.) ;
- Scolarité ;
- Caractéristiques et profil socioéconomique de l'électeur selon sa région, son quartier ou sa section de vote.

Par ailleurs, à partir des logiciels d'analyse de données, qui permettent d'effectuer des traitements techniques de profilage basés sur l'utilisation d'algorithmes[47], les partis politiques ont également la possibilité de segmenter l'électorat et d'établir des profils types et des profils probables d'électeurs[48]. Voici quelques exemples de l'utilité de tels traitements :

- Anticipation de l'intérêt de l'électrice ou de l'électeur pour certains sujets ;
- Évaluation des probabilités que l'électeur soit un sympathisant du parti ou qu'il vote pour lui en fonction de son adresse, des derniers résultats électoraux ou de données sociodémographiques ;
- En croisant les résultats avec des données sociodémographiques, comme celles issues du recensement, possibilité de prédire pour quel parti votera l'électeur dans un secteur particulier.

Les autres données

En plus des renseignements qu'ils recueillent au sujet des électrices et des électeurs, les formations politiques auraient en leur possession des renseignements concernant leurs contributeurs, leur personnel et les bénévoles qu'ils recrutent en période électorale. Ils en détiendraient également au sujet des candidates et des candidats qui se présentent ou qui envisagent de se présenter sous leur bannière dans le cadre d'une élection. Ces derniers feraient l'objet d'une attention particulière de la part des partis.

En effet, à l'approche d'une élection, les partis politiques effectueraient fréquemment des vérifications à propos de leurs candidats potentiels, « afin d'éviter que des renseignements personnels embarrassants soient révélés en pleine campagne électorale[49] ». De telles démarches deviendraient plus fréquentes et plus approfondies avec l'évolution des technologies. « Au palier fédéral, la plupart des partis politiques prévoient que le candidat autorise des organismes fédéraux comme l'Agence du revenu du Canada, l'Agence des services frontaliers du Canada et Citoyenneté et Immigration Canada à communiquer des renseignements aux partis politiques[50]. » Nous pouvons supposer que des pratiques similaires ont cours au Québec.

47. Un algorithme est une série d'instructions permettant d'obtenir un résultat. Les algorithmes effectuent des calculs à très grande vitesse et gèrent des données massives (*big data*). Voir Dominique Cardon, *op. cit.*
48. Hugo Joncas, *op. cit.* ; Martin Croteau, *op. cit.*
49. Colin J. Bennett et Robin M. Bayley, *op. cit.*, p. 22.
50. *Ibid.*

3.3 Les médias sociaux

« Les médias sociaux sont maintenant devenus un incontournable des campagnes électorales[51]. » Moins coûteux que les médias traditionnels, ils viennent compléter les autres moyens de communication généralement utilisés par les partis pour rejoindre l'électorat. Ils permettent de transmettre des messages ciblés à un auditoire plus large que les médias traditionnels.

Les partis utiliseraient la plateforme Facebook pour cibler des électrices et des électeurs par l'entremise d'achat de publicité ou par la diffusion de sondages sur des sujets d'intérêt. Ainsi, les publicités des partis pourraient être destinées à des groupes particuliers, appelés « audiences Facebook », en fonction, par exemple, de la langue, des champs d'intérêt ou du lieu de résidence (ville ou circonscription) des personnes[52].

En effet, « […] les formations politiques s'abonnent à des comptes *Facebook Business Manager*, les mêmes qu'utilisent les entreprises pour vous envoyer des publicités[53] ». « Ces abonnements corporatifs permettent aux utilisateurs d'acheter de la publicité en fonction « d'audiences » : des groupes de personnes correspondant au profil recherché[54]. »

Enfin, « [t]ous les sites Web des grands partis auraient des liens menant à un éventail de plateformes de médias sociaux. À divers degrés, ces sites encouragent l'échange de renseignements personnels. Par exemple, une personne qui clique sur le bouton « J'aime » sur Facebook voit s'afficher l'icône du parti en question sur sa page personnelle, ce qui revient à afficher, peut-être par inadvertance, ses convictions politiques[55] ».

Selon certaines sources médiatiques consultées[56], les partis politiques ne recueilleraient pas de renseignements personnels par l'entremise des réseaux sociaux.

EN BREF

L'aperçu des pratiques numériques des partis politiques dressé dans ce chapitre met en évidence l'importance qu'a prise, au fil des ans, la collecte de renseignements personnels.

Le nombre de données récoltées par les partis n'a cessé d'augmenter avec le déploiement des technologies numériques. L'accès à des données personnelles est devenu un outil de premier plan pour les partis politiques, tant pour la communication avec l'électorat que pour la promotion de la participation électorale.

---

51. Antonin-Xavier Fournier, « Les angles morts de la campagne électorale », *La Tribune*, 24 août 2018.
52. Hugo Joncas, *op. cit.*
53. *Ibid.*
54. *Ibid.*
55. Colin J. Bennett et Robin M. Bayley, *op. cit.*, p. 22.
56. Louis Lacroix, « Les partis politiques à l'ère des mégadonnées », *L'Actualité*, 23 mars 2018. [https://lactualite.com/politique/2018/03/23/les-partis-politiques-a-lere-des-megadonnees/] ; Martin Croteau, *op. cit.*

4 La protection des renseignements personnels sur les électrices et les électeurs au Québec

Dans ce chapitre, nous examinerons l'encadrement législatif applicable aux partis politiques provinciaux du Québec en matière de protection des renseignements personnels et, plus particulièrement, des renseignements relatifs aux électrices et aux électeurs. Nous nous limiterons aux obligations et aux autres dispositions prévues par des lois applicables au Québec.

Les partis politiques municipaux de même que les candidates et les candidats aux élections municipales ou scolaires peuvent également recevoir des renseignements sur l'électorat en période électorale, conformément aux dispositions prévues par la *Loi sur les élections et sur les référendums dans les municipalités*[57] et par la *Loi sur les élections scolaires*[58]. Bien que ces dispositions diffèrent de celles prévues par la *Loi électorale*, nous n'aborderons pas l'examen de ces lois dans la présente étude.

4.1 Historique législatif

Afin de mieux comprendre l'encadrement actuel des renseignements relatifs aux électrices et aux électeurs, il est utile de revoir l'historique des principales modifications législatives concernant l'utilisation et la communication de ces renseignements. Pour les fins de la présente étude, nous avons examiné les lois électorales adoptées depuis 1942.

Des listes électorales publiques

En 1942, la loi électorale conférait un caractère public aux listes électorales produites lors d'un recensement. Ces listes comprenaient le nom, le prénom, l'adresse et la profession de chaque électeur. Dans une section de vote urbaine, située dans une municipalité de plus de 5000 habitants, le recenseur devait également y inscrire, si possible, l'âge de l'électeur. Des copies des listes électorales devaient être transmises aux candidats et elles devaient être affichées dans des endroits accessibles au public pour des fins de révision[59].

57. RLRQ, chap. E-2.2.

58. RLRQ, chap. E-2.3.

59. *Loi concernant les élections à l'Assemblée législative*, S. Q. 1942, chap. 13, art. 50, 53 et 55.

L'âge devient un renseignement confidentiel

À partir de 1963, l'âge de l'électrice ou de l'électeur, qui était alors un renseignement obligatoire dans les sections de vote urbaines, ne devait plus apparaitre sur les listes électorales affichées dans les endroits publics. L'âge demeurait toutefois inscrit sur les listes qui étaient transmises aux candidats. Ce renseignement figurait également sur la liste électorale de la circonscription, accessible pour l'examen du public au bureau du président d'élection, l'équivalent actuel du directeur du scrutin. À cette époque, les listes électorales ont commencé à être distribuées à chaque électeur de la section de vote[60]. Étrangement, ces listes distribuées contenaient l'âge de l'électrice ou de l'électeur, même si ce renseignement n'était plus inscrit sur les listes affichées au public. Nous pouvons croire qu'il s'agissait d'une erreur du législateur, puisque deux ans plus tard, l'âge a été retiré de la liste distribuée aux électeurs[61].

Nous pouvons ainsi présumer que les listes électorales avaient un caractère public à des fins de contrôle. Il faut rappeler que les renseignements devaient être fournis au recenseur par l'électrice ou l'électeur lui-même, ou, sous certaines conditions, par une autre personne qui en faisait la demande. Puisque l'électeur n'avait pas à présenter de pièce d'identité, l'affichage et la distribution des listes électorales permettaient alors à toute personne qui doutait de la qualité d'un électeur inscrit de demander, en s'adressant à une commission de révision, de rayer cette personne de la liste électorale.

La transmission des listes électorales aux partis politiques

Ce n'est qu'à partir de 1972 que les listes électorales ont été transmises aux partis politiques, au moment de l'instauration du recensement annuel (qui a eu lieu jusqu'en 1989). Les listes électorales devaient alors être transmises au premier ministre et aux chefs de tous les partis reconnus à l'Assemblée nationale. Les députés indépendants avaient également le droit d'obtenir la liste électorale de leur circonscription[62].

La fin de l'affichage public

À partir de 1979, les listes électorales ne sont plus affichées dans les endroits publics[63].

La profession devient un renseignement confidentiel

À compter de la refonte de la *Loi électorale* de 1984, l'âge des électrices et des électeurs des sections de vote rurales devait obligatoirement être inscrit sur les listes électorales, comme dans les sections de vote urbaines. Cette nouvelle loi prévoyait également que la profession ne soit plus inscrite sur les listes électorales

60. *Loi électorale de Québec*, S. Q. 1963, chap. 13, art. 73 et 78.

61. *Loi électorale*, S. R. Q. 1964, chap. 7, art. 76, telle que modifiée par S. Q. 1965, chap. 12, art. 6.

62. *Loi électorale*, S. R. Q. 1964, chap. 7, art. 74, telle que modifiée par L. Q. 1972, chap. 6, art. 24.

63. *Loi électorale*, L. R. Q., chap. E-3, art. 75, telle que modifiée par L. Q. 1979, chap. 56, art. 262.

distribuées à chaque habitation de la section de vote, tout comme l'âge, qui n'était plus inscrit depuis 1965[64]. Ces renseignements continuaient toutefois d'être transmis aux candidates, aux candidats et aux partis politiques.

Les listes électorales deviennent confidentielles

Les listes électorales sont devenues confidentielles lors de la dernière refonte de la *Loi électorale*, en 1989. La *Loi* prévoyait ainsi des infractions de nature pénale pour quiconque communiquait la liste électorale contrairement à la *Loi* ou l'utilisait à des fins commerciales[65]. Malgré ces nouvelles dispositions, les listes électorales continuaient d'être transmises aux candidates, aux candidats et aux partis politiques, et la liste de section de vote, qui ne comprenait pas l'âge ni la profession, continuait d'être distribuée à chaque habitation[66].

Avec notre regard actuel, cela peut paraitre étrange que l'âge et la profession de l'électeur apparaissaient sur la liste électorale, d'autant plus qu'aucune pièce justificative n'était exigée lors du recensement. Nous pouvons toutefois penser que l'inscription de ces renseignements lors du recensement permettait d'authentifier la personne qui se présentait le jour du vote, puisqu'elle devait décliner l'ensemble des renseignements inscrits sur la liste électorale afin de s'identifier et d'exercer son droit de vote[67]. L'obligation de présenter une pièce d'identité avec photo n'a été introduite qu'en 1999[68]. Dans tous les cas, il semble que l'inscription de l'âge et de la profession sur les listes électorales avait été prévue à des fins de contrôle et que la transmission de ces renseignements aux candidates, aux candidats et aux partis politiques ne visait pas à leur permettre d'améliorer la communication avec les électrices et les électeurs.

La liste électorale permanente

En 1995, le directeur général des élections devient responsable de constituer un fichier des électrices et des électeurs qu'il peut mettre à jour à l'aide des renseignements communiqués par la Régie de l'assurance maladie du Québec et d'autres organismes publics. La liste électorale permanente a remplacé la nécessité d'effectuer un recensement au début de chaque période électorale. Depuis, la *Loi* prévoit que le fichier des électeurs contient le nom, l'adresse du domicile, le sexe et la date de naissance de chaque électeur[69].

Ainsi, la liste électorale permanente collige la date de naissance plutôt que l'âge de l'électrice ou de l'électeur et sa profession n'est plus recueillie. L'inscription du sexe et de la date de naissance était devenue nécessaire afin d'identifier avec précision les électeurs et de faciliter le recoupement de renseignements avec les organismes publics qui alimentent la liste électorale permanente.

---

64. *Loi électorale*, L. R. Q., chap. E-3.2, art. 85 et 94.
65. *Loi électorale*, L.R.Q., chap. E-3.3, art. 551, telle qu'en vigueur le 24 mars 1989.
66. *Ibid.*, art. 170 et 177, telle qu'en vigueur le 24 mars 1989.
67. *Loi électorale*, L. R. Q., chap. E-3.3, art. 157 et 337, telle qu'en vigueur le 24 mars 1989.
68. *Loi électorale*, RLRQ, chap. E-3.3, art. 337, telle que modifiée par L. Q. 1999, chap. 15, art. 18.
69. *Loi électorale*, RLRQ, chap. E-3.3, telle que modifiée par L. Q. 1995, chap. 23, art. 12.

Par la même occasion, la *Loi électorale* a été modifiée afin de restreindre l'utilisation et la communication des renseignements relatifs aux électrices et aux électeurs issus de la liste électorale permanente, incluant ceux transmis aux partis politiques, aux députés et aux candidats[70]. Ces restrictions, qui sont toujours en vigueur, seront décrites à la section 4.2.

La mise en place de la liste électorale permanente n'a pas modifié les modalités relatives à la communication des listes électorales aux candidates, aux candidats et aux partis politiques en période électorale, si ce n'est que la profession ne s'y retrouvait plus et que l'âge était remplacé par la date de naissance.

La transmission des listes électorales en dehors d'une période électorale

En 1995, le directeur général des élections recommandait qu'on l'autorise à transmettre annuellement la liste électorale aux partis politiques et aux députés indépendants en dehors d'une période électorale[71]. Cette proposition avait toutefois été remise en question par la Commission d'accès à l'information :

> « Selon cette même logique, la Commission s'interroge sur le sens et le bien-fondé de mettre à la disposition de tous les partis politiques, et ce une fois l'an, une version complète de cette liste, enrichie des modifications, radiations et ajouts enregistrés au cours des douze derniers mois. Au-delà de l'accroc à la finalité même de cette liste, cette distribution annuelle aux partis autorisés représentés à l'Assemblée nationale, à tout autre parti qui en ferait la demande et aux députés indépendants, représenterait un grave danger en ce qui a trait à la sauvegarde du caractère confidentiel de cette liste et des renseignements qu'elle contient. Les possibilités de fuite, de coulage ou de cession plus ou moins légitime de cette liste se trouveraient multipliées de façon inquiétante.
>
> Si l'Assemblée nationale décidait d'accepter la proposition du DGE de remettre annuellement la liste aux partis politiques, la Commission considère, compte tenu des dangers que représente cette distribution, qu'il sera essentiel d'amender la loi pour y inscrire des garanties de confidentialité plus contraignantes. Un engagement écrit à la confidentialité devrait être obtenu de toutes les personnes autorisées à recevoir et à utiliser la liste. La liste devrait, en outre, contenir une mise en garde à l'effet qu'il s'agit d'un document confidentiel ne devant faire l'objet de communication ou d'utilisation qu'aux fins de la tenue du scrutin. Enfin, il y aurait lieu d'instituer un régime pénal plus sévère et contraignant offrant des garanties de confidentialité les plus élevées possible[72]. »

70. *Ibid.*, art. 47.
71. Directeur général des élections, *Documents de réflexion : amendements à la Loi électorale*, 12 décembre 1995, p. 8.
72. Commission d'accès à l'information, *Mémoire relatif au document de réflexion proposant des amendements à la Loi électorale présenté à la Commission des institutions*, février 1996, p. 2-3.

En réponse à la proposition du directeur général des élections, le projet de loi nº 100 a été adopté en 1997, lorsque la liste électorale permanente est devenue opérationnelle. Ce projet de loi avait notamment pour objectif de permettre aux partis politiques et aux députés indépendants d'obtenir, une seule fois, une copie de la liste des électrices et des électeurs inscrits à liste électorale permanente afin d'en examiner le contenu et de vérifier la qualité des renseignements qu'elle contient. La liste contenait les mêmes renseignements que celle transmise en période électorale et pouvait être transmise sur un support informatique.

En réponse à l'avis de la Commission d'accès à l'information, la liste transmise devait contenir une mise en garde sur son caractère confidentiel. De plus, la personne désignée par le parti politique pour la recevoir devait s'engager à prendre les mesures appropriées pour protéger ces renseignements[73].

Cette transmission était alors justifiée afin de rassurer les parlementaires, qui étaient préoccupés par le risque que la liste électorale permanente contienne des renseignements inexacts ou qu'une électrice ou un électeur soit involontairement exclu de cette liste et ne puisse exercer son droit de vote. Lors de l'étude détaillée du projet de loi, le député de Laurier-Dorion, M. Christos Sirros, s'exprimait ainsi sur la nécessité d'obtenir un extrait de la liste électorale permanente :

> « […] il me semble tout à fait normal, et pertinent même, que la première liste produite soit examinée par les partis politiques afin de nous permettre de nous familiariser avec l'instrument et de vérifier, le cas échéant, les informations contenues sur le terrain[74]. »

En 1998, la *Loi électorale* a été modifiée afin de prévoir la transmission annuelle de cette liste aux partis politiques, aux députées et aux députés, selon les mêmes modalités qui avaient été prévues en 1997[75].

Lors des débats parlementaires entourant le projet de loi nº 450, le ministre de la Réforme électorale et parlementaire, M. Guy Chevrette, s'était exprimé sur les objectifs de cette modification :

> « En fait, ça a été discuté assez longuement, ça, au niveau des deux formations politiques, en particulier dans les comités consultatifs. Je sais que ça chatouille certaines structures, mais il n'en demeure pas moins que, pour faire un travail positif, si on veut améliorer la liste électorale, si on veut contribuer à ce que les électeurs ne soient pas oubliés, ou encore si on veut véritablement voir les mouvements d'électeurs à l'intérieur même d'une structure, je pense que les formations politiques ont besoin d'un instrument. On prend des mesures, on met des sanctions et on pense que ça n'a jamais prêté flanc, d'ailleurs, à de la grande exagération. Il y a toujours, peut-être, une exception ici et là, mais règle générale, les partis politiques ont été très sérieux avec les listes électorales, et je peux vous dire que je suis fier, moi,

73. L. Q. 1997, chap. 8, art. 26 à 28.

74. Assemblée nationale du Québec, *Journal des débats*, vol. 35, nº 85, 8 avril 1997.

75. *Loi électorale*, RLRQ, chap. E-3.3, tel que modifié L. Q. 1998, chap. 52, art. 3.

> en tout cas, de voir que nos présidents, bien souvent, qui ont une liste, avertissent tout leur monde, puis les listes circulent à très petit nombre puis pour des fins bien précises puis ils les font signer. Il y a beaucoup de responsabilisation qui a été faite là-dessus[76]. »

Nous pouvons ainsi comprendre que le législateur était soucieux du caractère confidentiel des renseignements relatifs aux électrices et aux électeurs, mais que l'objectif de cette transmission annuelle était de permettre aux partis politiques d'assurer un contrôle sur la qualité de la liste électorale permanente.

La proposition initiale du directeur général des élections était de transmettre la liste des électeurs aux partis politiques et aux députés indépendants, comme cela avait été prévu lors de la transmission unique en 1997. Les débats parlementaires n'expliquent pas pourquoi la transmission annuelle a été appliquée à tous les députées et députés.

La fin de la distribution des listes électorales aux électrices et électeurs

En 2001, la distribution des listes de section de vote à chaque habitation a été abolie. Elle a été remplacée par la transmission de l'avis à l'électeur, qui indique le nom des électrices et des électeurs inscrits à chaque adresse[77].

La transmission des listes électorales trois fois par année

La dernière modification à la *Loi électorale* concernant les listes électorales a été apportée en 2006 afin d'assurer une transmission plus fréquente de la liste électorale aux partis politiques et aux députées et députés. Depuis, cette liste est transmise en janvier, en avril et en septembre de chaque année. Cette modification législative prévoyait également que les candidates et candidats puissent recevoir la liste des électeurs inscrits au vote dans les installations d'hébergement et au vote au domicile de l'électeur qui ne peut se déplacer pour des raisons de santé[78].

Les débats parlementaires ne permettent pas d'expliquer les motivations des parlementaires pour hausser la fréquence de transmission ni les raisons justifiant l'envoi de la liste des personnes inscrites à ces nouveaux types de vote aux candidates et candidats.

---

76. Assemblée nationale du Québec, *Journal des débats de la Commission des institutions*, vol. 35, nº 135, 9 juin 1998.
77. *Loi électorale*, RLRQ, chap. E-3.3, art. 197, abrogée par L. Q. 2001, chap. 72, art. 12.
78. *Loi électorale*, RLRQ, chap. E-3.3, telle que modifiée par L. Q. 2006, chap. 17, art. 8 et 15.

4.2 Encadrement actuel au Québec

Au Québec, les partis politiques ne sont assujettis à aucune des deux lois générales qui encadrent la protection des renseignements personnels, soit la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, qui s'applique notamment aux renseignements détenus par un organisme public, et la *Loi sur la protection des renseignements personnels dans le secteur privé*, qui vise les renseignements personnels détenus par une personne qui exploite une entreprise au sens de l'article 1525 du *Code civil du Québec*[79].

Seule la *Loi électorale* encadre l'utilisation et la communication des renseignements relatifs aux électrices et aux électeurs par les partis politiques. Cet encadrement ne porte cependant que sur les renseignements inscrits sur les listes électorales qui sont communiqués aux partis politiques par le directeur général des élections. Tout autre renseignement personnel détenu par un parti politique, notamment ceux concernant ses bénévoles, ses candidates et candidats, ses membres et son personnel, n'est pas régi par la *Loi électorale*. Il en est de même des renseignements personnels qu'un parti a recueillis directement auprès des électrices ou électeurs ou qu'il a obtenus auprès d'un tiers.

Plus spécifiquement, la *Loi électorale*[80] interdit :

- d'utiliser les renseignements relatifs aux électeurs à d'autres fins que celles prévues par la *Loi* ;
- de communiquer ou de permettre la communication de ces renseignements à d'autres fins que celles prévues par la *Loi* ;
- de communiquer ou de permettre que ces renseignements soient communiqués à toute personne qui n'y a pas légalement droit.

Il faut souligner que la *Loi* ne définit pas expressément à quelles fins ces renseignements peuvent être utilisés par les partis politiques ni quelles sont les personnes qui ont légalement le droit d'obtenir ces renseignements. En pratique, les partis politiques confient les renseignements issus des listes électorales à des bénévoles et à des membres de leur personnel afin qu'ils les utilisent à des fins électorales, notamment pour communiquer avec les électeurs, recruter des membres, solliciter des appuis, favoriser la participation électorale, recruter des bénévoles ou solliciter des contributions politiques.

79. RLRQ, chap. CCQ-1991.

80. RLRQ, chap. E.3-3, art. 40.41.

Transmission des listes électorales par le directeur général des élections

Les partis politiques ainsi que les députées et députés à l'Assemblée nationale peuvent recevoir la liste des électeurs inscrits à la liste électorale permanente trois fois par année, en version électronique ou papier.

En période électorale, les candidates et candidats ont accès aux mêmes renseignements et peuvent recevoir la liste des personnes inscrites au vote en installation d'hébergement ou au vote au domicile de l'électeur. Ils peuvent également obtenir la liste des électrices et des électeurs qui ont voté par anticipation et de ceux ayant voté le jour du scrutin.

Autres obligations à respecter

Les députées, les députés et les personnes désignées par le parti politique pour recevoir la liste électorale doivent s'engager, par écrit, à prendre les mesures appropriées pour protéger le caractère confidentiel des renseignements relatifs aux électrices et aux électeurs et pour restreindre l'utilisation de cette liste aux seules fins prévues par la *Loi électorale*[81]. Il faut souligner que la *Loi* ne prescrit pas de mesure particulière à respecter ; les personnes et les partis politiques qui reçoivent les listes électorales peuvent donc déterminer elles-mêmes les mesures qu'ils prennent à cet effet.

La *Loi* ne prévoit aucune obligation similaire pour les candidates et candidats qui reçoivent la liste électorale en période électorale. Depuis 2014, ces personnes sont toutefois invitées à signer un engagement à la confidentialité avant de recevoir la liste électorale.

Rôle et pouvoirs du directeur général des élections

Le directeur général des élections est responsable de veiller à l'application de la *Loi électorale*. Il peut procéder à des vérifications pour s'assurer de son application. Il peut également, de sa propre initiative ou à la demande d'une personne, faire enquête sur toute infraction. Il peut intenter une poursuite pénale pour toute infraction à la *Loi électorale*[82].

Ses pouvoirs de vérification et d'enquête sont toutefois limités aux obligations et aux infractions prévues à la *Loi électorale*. Le directeur général des élections ne pourrait, par exemple, lancer un mandat de vérification relatif à la collecte de renseignements personnels par les partis politiques, puisqu'aucune disposition de la *Loi* n'encadre ces activités.

81. *Ibid.*, art. 40.38.3.

82. *Ibid.*, art. 485, 490.1, 491 et 569.

Infractions pénales et autres sanctions

La *Loi électorale* prévoit qu'une personne physique est passible d'une amende de 1 000 $ à 10 000 $ si elle utilise, communique ou permet que soient communiqués des renseignements relatifs aux électrices ou aux électeurs en contravention de la *Loi*. Les amendes vont de 3 000 $ à 30 000 $, s'il s'agit d'une personne morale[83].

La *Loi électorale* prévoit également qu'une personne physique est passible d'une amende de 5 000 $ à 10 000 $ si elle fait usage de la liste électorale à des fins commerciales ou lucratives. Les amendes vont de 10 000 $ à 30 000 $, s'il s'agit d'une personne morale[84].

EN BREF

Au cours des soixante-quinze dernières années, les renseignements sur les électrices et les électeurs sont passés du statut de renseignements publics à celui de renseignements confidentiels accessibles uniquement au directeur général des élections et à son personnel[85], aux partis politiques, aux députées et députés et, en période électorale, aux candidates et candidats. Ce changement est notamment dû à la mise en place de la liste électorale permanente, qui a permis au directeur général des élections d'effectuer un contrôle constant sur la qualité des listes électorales produites pour la tenue des scrutins. Ces mécanismes de contrôle ont ainsi réduit la nécessité d'assurer un contrôle public par les électrices et électeurs de même que par les partis politiques.

L'instauration de la liste électorale permanente, en 1995, a aussi conduit à des modifications législatives en matière de confidentialité en limitant l'accès à ces renseignements et les finalités pour lesquelles ils peuvent être utilisés ou communiqués.

La description des pratiques numériques des partis politiques a démontré que ces derniers recoupent les renseignements inscrits sur les listes électorales avec d'autres renseignements sur les électrices et les électeurs afin de communiquer avec eux. Nous pouvons nous demander si la *Loi électorale* encadre d'une manière adéquate ces pratiques, alors que les dispositions législatives pertinentes n'ont pas été modifiées depuis plus de 20 ans.

83. *Ibid.*, art. 551.1.1.

84. *Ibid.*, art. 551.2.

85. Conformément à l'article 62 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, les renseignements personnels ne sont accessibles qu'aux membres du personnel qui ont qualité pour les recevoir, lorsque ces renseignements sont nécessaires à l'exercice de leurs fonctions.

5 Encadrement au Canada

L'utilisation des renseignements personnels par les partis politiques telle que nous l'avons décrite au troisième chapitre n'est pas exclusive aux partis politiques du Québec. Dans le présent chapitre, nous examinerons l'encadrement légal applicable aux partis politiques du Canada et des autres provinces en matière de protection des renseignements personnels. Une description détaillée de ces modalités, incluant les références aux dispositions législatives correspondantes, est présentée à l'annexe 3.

5.1 Canada et autres provinces

Tout comme ceux du Québec, les partis politiques fédéraux et provinciaux ne sont pas assujettis aux lois générales qui encadrent la protection des renseignements personnels, qui s'appliquent aux organismes publics ou privés. Seuls les partis politiques de la Colombie-Britannique sont assujettis au *Personal Information Protection Act* qui, contrairement aux autres lois encadrant les organismes privés au Canada, ne s'applique pas seulement aux organisations à vocation commerciale. Le régime particulier de la Colombie-Britannique sera abordé à la section 5.2.

Restriction sur l'utilisation des listes électorales

La protection des renseignements personnels détenus par les partis politiques est donc uniquement encadrée par les lois électorales, qui restreignent l'utilisation des listes électorales et des renseignements issus du registre des électeurs.

De manière générale, les lois électorales canadiennes interdisent l'utilisation des renseignements inscrits aux listes électorales à des fins non prévues par la loi électorale ou limitent leur utilisation à la communication avec les électrices et les électeurs. Aucune de ces lois ne prescrit explicitement les utilisations qui sont autorisées, bien que certaines d'entre elles précisent que la communication avec les électeurs inclut la recherche d'appui, la sollicitation de contributions et le recrutement de membres.

En Colombie-Britannique, le directeur général des élections possède un pouvoir réglementaire lui permettant de restreindre les fins pour lesquelles les renseignements sur les électrices et les électeurs peuvent être utilisés. Ce règlement prévoit qu'un parti politique ou l'une de ses instances, un candidat ou un député peut utiliser ces renseignements afin de communiquer avec les électeurs, notamment afin de solliciter des appuis ou des contributions politiques ainsi que pour recruter des membres.

La loi de l'Ontario prévoit également que le directeur général des élections peut fournir des lignes directrices concernant l'utilisation des renseignements sur les électrices et les électeurs qui peuvent contenir des exigences supplémentaires.

En Alberta, au Manitoba et en Saskatchewan, la loi électorale permet aussi aux députées et députés d'utiliser ces renseignements dans l'exercice de leurs fonctions. Il s'agit des seuls cas où une loi canadienne permet une utilisation non électorale des renseignements sur l'électorat.

Restriction sur la communication des listes électorales

Outre celle du Québec, seule la loi électorale de l'Ontario restreint la communication des renseignements issus des listes électorales. En Ontario, il est interdit de communiquer ces renseignements à toute personne qui ne s'est pas engagée par écrit à respecter les obligations relatives à la confidentialité prévues par la loi. En pratique, cela suppose qu'un parti politique ayant reçu la liste électorale du directeur général des élections ne peut la communiquer à son personnel de campagne ou à ses bénévoles que si ces personnes ont signé un engagement à la confidentialité. À leur tour, ces personnes ne peuvent communiquer ces renseignements à d'autres personnes en l'absence d'un engagement écrit.

Transmission des listes électorales par l'administration électorale

Le tableau 1 fait état des destinataires autorisés à recevoir des listes électorales en période électorale et en dehors d'une période électorale ainsi que la fréquence de transmission de ces listes au fédéral et dans chacune des provinces. Les renseignements sur le Québec ont été inclus à des fins de comparaison.

En dehors d'une période électorale, à l'exception des lois de l'Île-du-Prince-Édouard et de la Saskatchewan, toutes les lois canadiennes prévoient que le directeur général des élections transmet la liste électorale aux partis politiques. Ces listes sont transmises annuellement, sauf en Colombie-Britannique, où la liste est transmise deux fois par année, ainsi qu'en Alberta, où la liste est plutôt transmise après une élection générale et deux ans plus tard, ainsi qu'après l'établissement d'une nouvelle carte électorale.

Les listes électorales des circonscriptions sont également transmises aux députées et députés à la même fréquence, à l'exception de trois provinces, Terre-Neuve-et-Labrador, l'Île-du-Prince-Édouard et la Saskatchewan, qui ne transmettent pas de liste aux députés. En Alberta, la liste électorale n'est accessible qu'aux députés indépendants.

Les partis politiques reçoivent les listes électorales de toutes les circonscriptions, sauf les partis politiques fédéraux, qui ne peuvent obtenir que celles des circonscriptions où ils ont présenté une candidate ou un candidat lors de la dernière élection. À cet effet, soulignons que la loi ne prévoit aucune disposition permettant à un nouveau parti politique d'obtenir des listes électorales en dehors d'une période électorale, sauf lorsqu'il s'agit d'une fusion de partis politiques.

Tableau 1 – Transmission des listes électorales au Canada

	Hors période électorale		En période électorale	
	Partis politiques	Députés	Candidats	Partis politiques
Canada	Annuellement	Annuellement	X	X
Terre-Neuve-et-Labrador	Annuellement		X	X
Nouvelle-Écosse	Annuellement	Annuellement	X	
Île-du-Prince-Édouard				X
Nouveau-Brunswick	Annuellement	Annuellement	X	
Québec	Trois fois par année	Trois fois par année	X	X
Ontario	Annuellement	Annuellement	X	X
Manitoba	Annuellement	Annuellement	X	
Saskatchewan			X	X
Alberta	Dans les jours suivant l'élection ainsi que deux ans plus tard et après l'établissement d'une nouvelle carte électorale	Dans les jours suivant l'élection ainsi que deux ans plus tard et après l'établissement d'une nouvelle carte électorale[86]	Candidats indépendants	X
Colombie-Britannique	Deux fois par année	Deux fois par année	X	

En période électorale, les listes électorales sont également accessibles aux partis politiques fédéraux ainsi qu'à ceux de Terre-Neuve-et-Labrador, de l'Île-du-Prince-Édouard, de l'Ontario, de la Saskatchewan et de l'Alberta. En Saskatchewan, les partis politiques ne peuvent toutefois obtenir que les listes des circonscriptions où ils présentent une candidate ou un candidat. Tous les candidats peuvent également obtenir la liste électorale de leur circonscription, sauf à l'Île-du-Prince-Édouard, où les listes électorales ne sont transmises qu'aux partis politiques. En Alberta, la loi prévoit que seuls les candidats indépendants peuvent obtenir la liste électorale du directeur général des élections. Nous pouvons donc comprendre que, dans ces deux provinces, les candidates et les candidats de partis ne peuvent obtenir la liste de leur circonscription que par l'intermédiaire de leur parti.

86. Seuls les députés indépendants peuvent obtenir les listes électorales.

Renseignements fournis par l'administration électorale

La nature des renseignements transmis aux partis politiques diffère selon les diverses lois canadiennes. Le tableau 2 fait état des renseignements qui sont inscrits sur les listes électorales transmises par le directeur général des élections au fédéral et dans chacune des provinces. Les renseignements sur le Québec sont inclus à des fins de comparaison.

Toutes les listes électorales transmises aux partis politiques contiennent le nom et l'adresse de l'électrice ou de l'électeur. Seules les listes du Nouveau-Brunswick (et du Québec) indiquent son sexe. Les listes du Manitoba et de l'Alberta indiquent également son numéro de téléphone. Les listes électorales fédérales ainsi que celles de la Nouvelle-Écosse, de l'Ontario, du Manitoba et de l'Alberta comprennent aussi un numéro d'identification unique désignant l'électeur.

En Nouvelle-Écosse, les listes électorales contiennent une indication précisant si l'électrice ou l'électeur a voté à chacune des élections générales ou partielles depuis 2009. En Colombie-Britannique, la liste révèle uniquement la participation de l'électeur à la dernière élection. En Ontario, la loi prévoit que les partis politiques peuvent obtenir la liste des personnes ayant voté après chaque jour du scrutin. Les autres lois canadiennes prévoient généralement la présence de représentants des candidates et des candidats dans les lieux de vote, ce qui leur permet de recueillir eux-mêmes les renseignements sur les personnes qui ont voté.

Tableau 2 – Renseignements inscrits sur les listes électorales au Canada

	Nom	Adresse	Sexe	Date de naissance	Numéro identificateur unique	A voté à la dernière élection	Téléphone
Canada	X	X			X		
Terre-Neuve-et-Labrador	X	X					
Nouvelle-Écosse	X	X			X	X[a]	
Île-du-Prince-Édouard	X	X					
Nouveau-Brunswick	X	X	X				
Québec	X	X	X	X			
Ontario	X	X			X		
Manitoba	X	X			X		X
Saskatchewan	X	X					
Alberta	X	X			X		X
Colombie-Britannique	X	X				X	

a. Les listes contiennent une indication précisant si l'électeur a voté à chacune des élections générales ou partielles depuis 2009.

Contrairement au Québec, aucune liste électorale au Canada ne contient la date de naissance des électrices et des électeurs, bien que les listes de la Nouvelle-Écosse indiquent leur catégorie d'âge. En Saskatchewan, l'année de naissance est indiquée seulement lorsque deux électeurs résidant à la même adresse portent le même nom. Les partis politiques de cette province peuvent également obtenir l'année de naissance de tous les électeurs, sur une liste transmise après l'élection, s'ils concluent une entente de confidentialité avec le directeur général des élections.

Les lois de Terre-Neuve-et-Labrador et de l'Alberta prévoient la transmission, en plus des listes électorales, des listes des électrices et des électeurs ayant voté par anticipation et celles des personnes inscrites au vote par correspondance. Ces dernières listes ne contiennent que le nom et l'adresse permanente de l'électeur, et non son adresse temporaire, à l'intérieur ou à l'extérieur de la province. Il en est de même en Ontario, où les partis politiques reçoivent une copie du registre des électeurs qui résident temporairement à l'extérieur de l'Ontario, qui n'indique que l'adresse permanente des électeurs. Rappelons qu'au Québec, les listes des électeurs inscrits au vote hors Québec incluent également leur adresse temporaire à l'extérieur du Québec.

Les principales obligations à respecter

D'une manière générale, les lois canadiennes prévoient peu d'obligations permettant de s'assurer que les partis politiques respectent le caractère confidentiel des renseignements issus des listes électorales. Dans les faits, les partis politiques fédéraux et ceux de Terre-Neuve-et-Labrador, de l'Île-du-Prince-Édouard et du Nouveau-Brunswick ont pour seule obligation de restreindre l'utilisation des renseignements sur les électrices et les électeurs à des fins électorales. Le tableau 3, à la page suivante, fait état des autres obligations à respecter par les partis politiques au fédéral et dans chacune des provinces. Les renseignements sur le Québec sont inclus à des fins de comparaison.

En Nouvelle-Écosse, les candidats doivent également détruire toute copie de liste électorale et s'assurer de la destruction de toute liste communiquée à des mandataires agissant en leur nom. Ils doivent attester de cette destruction auprès du directeur général des élections au plus tard dix jours après le jour du scrutin.

Au Manitoba et en Alberta, toute personne ou tout parti politique qui reçoit la liste électorale conformément à la loi doit s'assurer de prendre les mesures raisonnables afin de la protéger d'une perte ou d'une utilisation non autorisée. Ces personnes ont également l'obligation de signaler toute perte de renseignements au directeur général des élections. La loi ne prévoit toutefois pas d'autres mesures de sécurité particulières à respecter.

En Saskatchewan, un parti politique qui souhaite obtenir la liste électorale qui contient l'année de naissance doit conclure une entente qui prévoit qu'il met en place les meilleures pratiques en matière de sécurité et de protection de la vie privée.

Tableau 3 – Autres obligations à respecter par les partis politiques au Canada

	Destruction obligatoire après l'élection	Signalement des pertes de renseignements	Entente de confidentialité avec le DGE	Politique en matière de protection des renseignements personnels
Canada				
Terre-Neuve-et-Labrador				
Nouvelle-Écosse	X			
Île-du-Prince-Édouard				
Nouveau-Brunswick				
Québec				
Ontario				X
Manitoba		X		
Saskatchewan			X	
Alberta		X		
Colombie-Britannique				X

En Ontario, les partis politiques doivent élaborer et mettre en œuvre une politique pour s'assurer que leurs candidats, leurs députés, les membres de leur personnel et tout autre mandataire respectent les restrictions relatives à l'utilisation des renseignements sur les électrices et les électeurs. Cette politique doit respecter les lignes directrices émises par le directeur général des élections. Les députés indépendants et les candidats indépendants sont également tenus de satisfaire à cette obligation. Cette politique doit être transmise au directeur général des élections afin d'obtenir des renseignements provenant du registre permanent des électeurs.

En Ontario, les partis politiques de même que les candidats indépendants et les députés indépendants doivent, avant de communiquer des renseignements sur les électrices et les électeurs à toute personne, s'assurer qu'elle signe un engagement à respecter la confidentialité de ces renseignements. De plus, ils doivent tenir un registre de toutes ces communications, qui indique notamment si les renseignements ont été retournés ou détruits. Ils doivent déposer ce registre auprès du directeur général des élections après chaque transmission annuelle de la liste des électeurs de même qu'après chaque scrutin.

Toujours en Ontario, les partis politiques, les candidats indépendants et les députés indépendants doivent détruire les renseignements sur les électrices et les électeurs lorsque leur utilisation n'est plus autorisée et déposer des certificats de destruction auprès du directeur général des élections. Ils ne sont toutefois pas tenus de supprimer les renseignements intégrés aux bases de données électorales : seuls les documents fournis par le directeur général des élections et les copies supplémentaires doivent être détruits.

L'obligation d'élaborer une politique existe également en Colombie-Britannique, où les partis politiques, les députés et les candidats doivent soumettre une politique jugée acceptable par le directeur général des élections afin d'obtenir les listes électorales. Afin d'être acceptable, cette politique doit notamment comprendre des dispositions concernant les mesures de sécurité, la destruction des renseignements, la tenue d'un registre des personnes ayant accès aux renseignements et le signalement des atteintes à la vie privée. La politique doit également reconnaître le droit au directeur général des élections d'effectuer des vérifications de conformité.

En avril 2018, le gouvernement fédéral a déposé le projet de loi C-76[87] qui modifie la *Loi électorale du Canada* afin qu'un parti politique enregistré doive adopter une politique sur la protection des renseignements personnels et la publier sur un son site Internet. Une telle politique devrait notamment décrire les renseignements personnels détenus par le parti et leur source, les mesures de sécurité mises en place et l'utilisation que font les partis politiques de ces renseignements. Ce projet de loi a toutefois été critiqué, puisqu'il ne prévoit aucune norme minimale à respecter pour assurer la protection des renseignements personnels détenus par les partis politiques. Par ailleurs, il n'accorde aucun pouvoir à une autorité de surveillance pour s'assurer que les partis se conforment à la politique qu'ils adopteraient[88]. Ce projet de loi a été sanctionné le 13 décembre 2018 et entrera en vigueur en 2019.

Infractions pénales et autres sanctions

À l'exception de Terre-Neuve-et-Labrador, toutes les lois canadiennes à l'extérieur du Québec prévoient des infractions lorsqu'une personne utilise les renseignements sur les électrices et les électeurs à des fins non autorisées. Ces lois prévoient des amendes variant entre 2 000 $ (Île-du-Prince-Édouard) et 100 000 $ (Alberta). Elles prévoient également la possibilité de peines d'emprisonnement maximales d'un ou deux ans, sauf à l'Île-du-Prince-Édouard et au Nouveau-Brunswick, où cette infraction constitue également une manœuvre électorale frauduleuse ; cela a pour conséquence que la personne déclarée coupable ne peut être inscrite comme électrice ou être élue comme députée pendant une période de cinq ans.

Rôle et pouvoirs de l'autorité de surveillance

Bien qu'il revienne au directeur général des élections d'observer l'application de la loi électorale, le pouvoir de ce dernier varie selon les lois applicables. Ainsi, le directeur général des élections de l'Île-du-Prince-Édouard et du Nouveau-Brunswick ne possède aucun pouvoir de vérification ou d'enquête sur les infractions liées à l'utilisation des listes électorales. Les enquêtes sur ces infractions relèvent plutôt des services policiers.

87. *Loi modifiant la Loi électorale du Canada et d'autres lois et apportant des modifications corrélatives à d'autres textes législatifs*.

88. Colin Bennett, « A Data-Driven Election Can Be Ethical », *The Globe and Mail*, 13 août 2018. [https://www.theglobeandmail.com/opinion/article-a-data-driven-election-can-be-ethical/].

Ailleurs, un tel pouvoir est confié au directeur général des élections[89] ou à un commissaire aux élections[90]. Le commissaire aux élections du Manitoba et le directeur général des élections de la Colombie-Britannique agissent également à titre de poursuivant public.

En Alberta et en Nouvelle-Écosse, le directeur général des élections peut également conclure une entente de conformité avec toute personne qu'il considère avoir enfreint la loi. Cette entente peut imposer des conditions particulières pour que la personne se conforme à la loi, mais ne constitue pas une déclaration de culpabilité.

En Colombie-Britannique, en Alberta et en Nouvelle-Écosse, le directeur général des élections peut insérer des renseignements sur des électeurs fictifs dans les listes électorales afin de dépister les utilisations non autorisées de ces renseignements.

En Ontario et en Colombie-Britannique, le directeur général des élections peut, à la demande d'une électrice ou d'un électeur, retirer des renseignements des listes électorales afin d'assurer sa sécurité ou la protection de sa vie privée.

En Saskatchewan, le directeur général des élections a le pouvoir discrétionnaire de retirer des renseignements de toutes les listes électorales afin de protéger la vie privée et la sécurité des électrices et des électeurs. Ainsi, en décembre 2015, ce dernier a déterminé que les listes électorales utilisées par le personnel électoral, de même que celles transmises aux candidates, aux candidats et aux partis politiques en période électorale, ne contiendraient que le nom et l'adresse des électeurs. L'année de naissance n'est inscrite que lorsque deux électeurs portent le même nom à la même adresse[91].

5.2 Colombie-Britannique

La Colombie-Britannique est la seule province au Canada dont la loi encadrant la protection des renseignements personnels détenus par des organisations privées s'applique également aux partis politiques. En effet, le *Personal Information Protection Act* (PIPA)[92], en vigueur depuis 2004, s'applique à toute organisation qui détient des renseignements personnels, incluant toute personne, association non incorporée, syndicat, fiducie ou organisation à but non lucratif, sauf lorsque la loi prévoit une exception.

Il faut toutefois souligner que ce n'est qu'en 2011, à la suite d'une plainte d'un candidat, que le commissaire à la vie privée s'est prononcé pour la première fois sur l'application de cette loi aux partis politiques provinciaux. Il a alors conclu que ces derniers constituaient des associations non incorporées selon la loi[93].

89. En Nouvelle-Écosse, en Ontario, en Saskatchewan et en Colombie-Britannique.
90. Au Canada, au Manitoba et en Alberta.
91. Elections Saskatchewan, *Interpretation Bulletin ESKIB-2015/01*, 28 décembre 2015. [https://cdn.elections.sk.ca/upload/eskib-2015-01-voterslistprivacy_v10_final.pdf].
92. SBC 2003, chap. 63.
93. Office of the Information & Privacy Commissioner for British Columbia, *P11-01-MS: Summary of the Office of the Information and Privacy Commissioner's Investigation of the BC NDP's Use of Social Media and Passwords to Evaluate Candidates*. [https://www.oipc.bc.ca/mediation-summaries/1399].

Les obligations prévues par le PIPA

En vertu de cette loi, les partis politiques sont responsables de la protection de tous les renseignements personnels qu'ils détiennent, incluant ceux concernant les électrices et les électeurs, leurs candidates et candidats, leurs membres, leur personnel et leurs bénévoles.

Les partis politiques doivent notamment désigner une personne responsable de la protection des renseignements personnels, qui doit s'assurer que les procédures du parti respectent les obligations prévues par la loi.

Les partis politiques doivent également respecter les obligations suivantes[94] :

- Ils ne peuvent recueillir, utiliser ou communiquer des renseignements personnels sans le consentement des personnes concernées ;
- Ils doivent, au moment de la collecte des renseignements, informer les personnes des fins auxquelles ces renseignements seront utilisés ;
- Ils doivent limiter la collecte aux renseignements nécessaires à ces fins ;
- Ils ne doivent utiliser les renseignements personnels qu'aux seules fins pour lesquelles ils ont obtenu le consentement des personnes concernées ;
- Ils doivent restreindre la communication de ces renseignements à ces fins ;
- Ils doivent donner accès à tout renseignement qu'ils détiennent au sujet de tout individu qui en fait la demande ;
- Ils doivent prendre les mesures appropriées pour s'assurer que les renseignements personnels qu'ils détiennent demeurent exacts et à jour ;
- Ils doivent mettre en place des mesures de sécurité afin de prévenir les risques de collecte, d'utilisation, de communication ou de destruction non autorisée de ces renseignements ;
- Ils doivent détruire tout renseignement personnel lorsqu'il n'est plus nécessaire ;
- Ils doivent élaborer des politiques leur permettant de respecter ces obligations ainsi qu'une procédure pour gérer toute plainte à ce sujet. Ces politiques et cette procédure doivent être accessibles sur demande.

Rôle et pouvoirs de l'autorité de surveillance

Le commissaire à la vie privée et à l'information est responsable de veiller à l'application du PIPA. Le commissaire est une personne indépendante désignée par l'Assemblée législative. Il peut procéder à des vérifications pour s'assurer de la conformité des organisations assujetties à cette loi. Il peut également, de sa propre initiative ou à la demande d'une personne, faire enquête sur tout manquement à cette loi. À la suite d'une enquête, il peut émettre une ordonnance visant à rectifier tout manquement à la loi, pouvant aller jusqu'à la destruction de renseignements qui ont été recueillis en contravention à la loi.

---

94. Pour une description plus détaillée des obligations prévues par loi, voir Office of the Information & Privacy Commissioner for British Columbia, *A Guide to B.C.'s Personal Information Protection Act for Businesses and Organisations*, octobre 2015. [https://www.oipc.bc.ca/guidance-documents/1438].

En mai 2018, le commissaire, M. Michael McEvoy, a témoigné devant un comité parlementaire fédéral au sujet de l'assujettissement des partis politiques à une loi encadrant la protection des renseignements personnels. Il a alors émis les commentaires suivants.

> « Les partis politiques de ma province sont assujettis à la PIPA depuis son adoption en 2004. Au cours des 14 quatorze années écoulées depuis son adoption, je peux vous assurer que la démocratie a continué de prospérer sans entrave en Colombie-Britannique. Nous n'avons été informés d'aucune préoccupation ou suggestion laissant entendre que les lois protégeant les renseignements personnels des électeurs limitent la capacité des partis politiques ou des candidats d'atteindre les électeurs.
>
> Les partis politiques de la Colombie-Britannique peuvent recueillir des renseignements personnels sur les électeurs, et ils le font, mais en ayant les mêmes responsabilités et obligations juridiques raisonnables qui s'appliquent aux autres organismes.
>
> En règle générale, cela signifie que les partis politiques obtiennent des renseignements avec le consentement des électeurs, accompagnés d'une explication claire de la façon dont ces renseignements seront utilisés et de la raison pour laquelle ils le seront. J'ai utilisé les mots « en règle générale » et « avec le consentement » parce qu'il y a des dispositions légales qui permettent aux partis de recueillir des renseignements sans consentement, particulièrement pour obtenir la liste électorale et d'autres données sur les électeurs d'Elections BC. Toutefois, ces dispositions sont assorties d'une condition selon laquelle le parti qui reçoit l'information doit fournir au directeur général des élections une politique satisfaisante en matière de protection de la vie privée[95]. »

En septembre 2017, le commissaire a entrepris la tenue d'une enquête visant à examiner la conformité des trois principaux partis politiques à l'égard du PIPA. Cette enquête était motivée par de récentes modifications législatives, qui avaient permis aux partis politiques d'obtenir que les listes électorales comprennent une indication précisant si l'électeur a voté à la dernière élection, de même que par l'augmentation des capacités informatiques à analyser de grandes quantités de renseignements personnels.

Dans son rapport, paru le 6 février 2019, le commissaire y explique notamment que les partis politiques n'informent pas assez les personnes des raisons qui justifient la collecte de leurs renseignements personnels. Il émet dix-sept recommandations visant à améliorer la conformité des partis politiques[96].

---

95. Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, *Témoignages*, 1re session, 42e législature, 10 mai 2018, 0900. [http://www.noscommunes.ca/DocumentViewer/fr/42-1/ETHI/reunion-106/temoignages].

96. Office of the Information and Privacy Commissioner for British Columbia *Investigation Report P19-01. Full Disclosure : Political Parties, Campaign Data, and Voter Consen*t, 6 février 2019. [https://www.oipc.bc.ca/investigation-reports/2278].

5.3 Recommandations des autorités de surveillance

À la suite des incidents concernant des communications trompeuses avec les électrices et les électeurs survenus lors des élections générales fédérales de 2011, le directeur général des élections du Canada avait recommandé, en 2013, des modifications législatives en matière de protection des renseignements personnels[97].

Il avait notamment recommandé que la loi soit modifiée afin que les partis politiques soient assujettis aux principes de protection des renseignements personnels, ainsi que pour exiger des partis politiques qu'ils fassent preuve de diligence raisonnable lorsqu'ils donnent accès à leurs bases de données sur les électrices et les électeurs.

En avril 2018, lors d'une comparution devant un comité parlementaire, le commissaire à la protection de la vie privée du Canada, M. Daniel Therrien, a recommandé qu'une entité indépendante puisse examiner les pratiques des partis politiques afin de s'assurer que les droits des électrices et des électeurs en matière de respect de la vie privée soient respectés[98].

En juin 2018, le commissaire à l'information et à la protection de la vie privée de l'Ontario a recommandé d'assujettir les partis politiques à une réglementation et à une surveillance en matière de vie privée afin d'atténuer les risques associés à la collecte et à l'utilisation des renseignements personnels qu'ils détiennent[99].

En septembre 2018, dans le cadre d'une résolution conjointe, les commissaires fédéraux, provinciaux et territoriaux à l'information et à la protection de la vie privée, incluant le président de la Commission d'accès à l'information du Québec, ont demandé à ce que les lois canadiennes prévoient des obligations pour les partis politiques en matière de protection des renseignements personnels. Cette résolution était motivée ainsi :

> « Des évènements récents ont mis en lumière la manière dont les partis politiques recueillent et utilisent les renseignements personnels pour cibler de façon précise et unique des individus afin d'en retirer des avantages politiques. Des outils numériques collectent une grande quantité de renseignements personnels provenant de diverses sources, souvent à l'insu de l'intéressé ou sans son consentement. Ces pratiques de collecte de données massives de plus en plus sophistiquées soulèvent de nouvelles préoccupations en matière d'éthique et de vie privée, et mettent en évidence le besoin d'en accroître la transparence[100]. »

---

97. Élections Canada, *Prévenir les communications trompeuses avec les électeurs : recommandations du directeur général des élections du Canada à la suite de la 41e élection générale*, 2013, p. 34. [http://www.elections.ca/res/rep/off/comm/comm_f.pdf].

98. Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, *Témoignages*, 1re session, 42e législature, 17 avril 2018, 0850. [http://www.noscommunes.ca/DocumentViewer/fr/42-1/ETHI/reunion-99/temoignages].

99. Commissaire à l'information et à la protection de la vie privée de l'Ontario, *Trente années au service de l'accès à l'information et de la protection de la vie privée : rapport annuel 2017*, juin 2018, p. 47. [https://www.ipc.on.ca/wp-content/uploads/2018/06/ar-2017-f-web.pdf].

100. Commission d'accès à l'information, *Les gardiens du droit d'accès à l'information et du droit à la vie privée réclament que les partis politiques soient assujettis à la réglementation et à la surveillance en matière de protection de la vie privée*, 17 septembre 2018. [http://www.cai.gouv.qc.ca/les-gardiens-du-droit-dacces-a-linformation-et-du-droit-a-la-vie-privee-reclament-que-les-partis-politiques-soient-assujettis-a-la-reglementation-et-a-la-surveillance-en-matiere-de-p/].

Plus précisément, les commissaires ont souhaité l'adoption de lois qui :

- « exigent que les partis politiques respectent les principes de protection des renseignements personnels et de la vie privée reconnus mondialement ;
- habilitent un organisme indépendant afin qu'il vérifie la conformité à la vie privée et en assure le respect par les partis politiques, des règles relatives à la protection des renseignements personnels et de la vie privée entre autres, en réalisant des enquêtes à la suite de plaintes individuelles ;
- permettent de s'assurer que les Canadiens ont le droit d'accès à leurs renseignements personnels détenus par ou sous le contrôle des partis politiques[101]. »

En novembre 2018, le commissaire à la vie privée du Canada, M. Daniel Therrien, lors d'une comparution devant un comité parlementaire, réitérait ces recommandations en les justifiant ainsi :

> « En septembre, les commissaires à la protection de la vie privée de tout le Canada ont présenté une résolution conjointe exhortant les gouvernements à s'assurer que les partis politiques soient assujettis aux lois sur la protection de la vie privée.
>
> Les experts universitaires, la société civile et le public canadien étaient tous d'accord avec cette position, de même que le directeur général des élections.
>
> Le gouvernement, par contre, soutient que, bien que l'application des lois sur la protection de la vie privée aux partis politiques soit une question qui mérite d'être étudiée, les prochaines élections fédérales peuvent se dérouler sans y recourir.
>
> Le manque de surveillance exercée sur les pratiques de traitement des renseignements personnels des partis politiques canadiens devient malheureusement une exception par rapport aux autres pays et expose les élections canadiennes à une manipulation et à une utilisation non autorisée des renseignements personnels.
>
> En d'autres termes, sans une réglementation appropriée des données, il y aura un risque sérieux d'injustice dans le processus électoral lors des prochaines élections fédérales au Canada[102]. »

---

101. Commission d'accès à l'information, *Assurer la confiance et la confidentialité dans le processus électoral du Canada : résolution des commissaires fédéraux, provinciaux et territoriaux à l'information et à la protection de la vie privée*, 13 septembre 2018. [http://www.cai.gouv.qc.ca/documents/FPT-Resolution-on-privacy-and-political-parties-FRA-Final.pdf].

102. Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, *Témoignages*, 1re session, 42e législature, 1er novembre 2018, 1215. [http://www.noscommunes.ca/DocumentViewer/fr/42-1/ETHI/reunion-124/temoignages].

En décembre 2018, le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes a publié son rapport sur l'étude qu'il a entreprise à la suite de l'atteinte à la protection des renseignements personnels impliquant Cambridge Analytica et Facebook. Après avoir entendu des entreprises, des experts et des partis politiques fédéraux sur le sujet, le comité a recommandé :

> – « Que le gouvernement du Canada modifie la *Loi sur la protection des renseignements personnels et les documents électroniques* pour y assujettir les partis politiques tout en tenant compte de leurs obligations de mener des activités d'information et de sensibilisation démocratique.
> – Que le gouvernement du Canada octroie le mandat et l'autorité au commissaire à la protection de la vie privée ou à Élections Canada de mener des audits proactifs des partis politiques et des tierces parties politiques à l'égard de leurs pratiques relatives à la protection des renseignements personnels et d'émettre des ordonnances et des sanctions monétaires[103]. »

EN BREF

À l'exception de la Colombie-Britannique, qui est assujettie à une loi générale en matière de protection de la vie privée, l'encadrement des partis politiques au Canada et dans les provinces canadiennes est similaire à celui en vigueur au Québec.

Nous constatons toutefois que les listes électorales transmises aux partis politiques ailleurs au Canada contiennent moins de renseignements sur les électrices et les électeurs et qu'elles sont transmises à une fréquence moins élevée qu'au Québec.

L'examen de ces législations révèle cependant que les modifications législatives plus récentes ont permis un resserrement de la protection des renseignements sur les électrices et les électeurs. C'est notamment le cas en Colombie-Britannique, où des modifications ont été adoptées en 2015, et en Ontario, où des modifications ont été adoptées en 2016. Dans les deux cas, ces modifications prévoyaient notamment l'élaboration de politiques en matière de vie privée et un plus grand contrôle des accès aux listes électorales.

De même, les modifications législatives ayant mené à la mise en place de registres permanents des électeurs en Saskatchewan en 2016 et au Manitoba en 2017 ont été adoptées avec une préoccupation pour les risques liés à la protection des renseignements personnels. En Saskatchewan, la loi électorale permet au directeur général des élections de retirer des renseignements du registre des électeurs ou des listes électorales afin d'assurer la sécurité et la vie privée des électrices et des électeurs.

103. Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, *Démocratie menacée : risques et solutions à l'ère de la désinformation et du monopole des données*, décembre 2018, p. 28. [http://www.noscommunes.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-f.pdf].

6 Encadrement à l'extérieur du Canada

L'univers numérique est intimement lié au quotidien des individus, mais les préoccupations ne sont pas les mêmes partout dans le monde. Les questions posées au sujet de la protection des renseignements personnels sont liées à des choix de société.

Après avoir examiné l'encadrement canadien et québécois, nous vous proposons d'observer l'approche retenue dans certains pays d'Amérique du Nord, d'Océanie et d'Europe.

6.1 États-Unis

Régime d'encadrement

Aux États-Unis, l'encadrement normatif de la protection des renseignements personnels résulte d'une juxtaposition de lois sectorielles et non d'un cadre général[104]. C'est une approche centrée sur la réparation du préjudice subi, qui vise un équilibre entre l'atteinte à la vie privée et la libre circulation des données. Cette manière de faire laisse une grande place à l'autorégulation. L'agence indépendante de contrôle des pratiques commerciales (Federal Trade Commission) a mis en place un code de bonnes pratiques, mais il n'est que facultatif. La seule exigence fixée aux entreprises américaines est de communiquer leurs conditions générales d'utilisation des données[105].

En ce qui concerne le *Privacy Act*[106], il établit les règles et un code de conduite que seule l'administration publique fédérale américaine est tenue de respecter lors de la collecte et du traitement des renseignements personnels des citoyens.

Les partis politiques ne sont assujettis à aucun encadrement pour la protection des renseignements personnels. Ils sont libres de collecter, traiter, conserver et communiquer des renseignements personnels sur les électeurs, les candidats et les donateurs, et ce, sans qu'ils aient à obtenir leur consentement[107]. La communication politique semble protégée par le droit constitutionnel découlant de la jurisprudence en vertu du premier amendement portant sur la liberté d'expression[108].

---

104. Jacky Richard, *Le numérique et les droits fondamentaux*, 2014, p. 72. [https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf].
105. Federal Trade Commission, *Privacy & Data Security – Update: 2017*, 2017, p. 1. [https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf].
106. *The Privacy Act of 1974*, 5 U. S. C. chap. 5, § 552a. – *Records Maintained on Individuals.* [https://www.law.cornell.edu/uscode/text/5/552a].
107. Ace Electoral Knowledge Network, « Élections et technologie », *ACE Project*. [http://aceproject.org/ace-fr/topics/et/default].
108. Winston J. Maxwell, *La jurisprudence américaine en matière de liberté d'expression sur Internet*. [https://www.hoganlovells.com/~/media/a8a5a7b6d1094edd84d509f9259840bf.ashx].

Opérations électorales

Le système électoral américain s'avère atomisé, hétérogène et sans véritables normes nationales[109]. Les États-Unis n'ont pas de commission électorale nationale responsable de l'organisation des scrutins.

La constitution américaine donne aux États fédérés la pleine compétence sur l'encadrement des élections. Chaque État décide des procédures électorales sur son territoire. Les élections sont administrées par près de 14 000 entités locales indépendantes ; les bulletins de vote, les dispositifs de scrutin, les règles et les procédures ne sont pas uniformisés[110].

En 2002, le Congrès américain a adopté la première loi fédérale portant spécifiquement sur l'administration électorale, le *Help America Vote Act*[111]. Elle fixe quelques normes et obligations nationales en matière de vote, mais conditionne la plupart d'entre elles à la décision des États de les mettre en œuvre. La commission d'assistance électorale (U.S. Election Assistance Commission) est chargée d'accompagner les États qui en font la demande.

Il n'existe pas de liste électorale unique et l'inscription d'un citoyen est volontaire. La loi impose à chaque État la responsabilité d'établir des listes électorales centralisées et actualisées de façon à éviter les votes multiples, les radiations arbitraires, les refus injustifiés et les votes illégaux[112]. Selon l'État concerné, la liste électorale peut comporter de nombreuses données sur les électrices et les électeurs. En Californie[113], par exemple, la liste précise, pour chaque électeur :

- Ses prénoms ;
- Ses noms ;
- Son adresse ;
- Son adresse de courriel ;
- Son numéro de téléphone ;
- Sa date et son lieu de naissance ;
- Son origine ethnique ;
- Son allégeance politique ;
- Son choix de mode de votation.

109. Élisabeth Vallet, « L'heure du jugement : le système électoral américain en question », *Politique américaine*, 2005/2 (nº 2), p. 82. [https://www.cairn.info/revue-politique-americaine-2005-2-page-79.htm].
110. Robert A. Pastor, « États-Unis : une administration électorale décentralisée, anachronique et satisfaite d'elle-même », *ACE Project*. [http://aceproject.org/ace-fr/topics/em/electoral-management-case-studies/the-united-states-decentralized-to-the-point-of].
111. *Help America Vote Act of 2002* – 116 Stat. 1666. [http://legislink.org/us/stat-116-1666].
112. *Ibid.*, art. 303.
113. *Voter List Information – California*. [http://voterlist.electproject.org/states/california].

De façon générale, les listes électorales peuvent être vendues aux partis politiques, aux candidates et candidats à une élection, à des chercheurs, à des organismes sans but lucratif et à des citoyens pour des fins non commerciales[114].

Il y a une spécificité, aux États-Unis, qui tient à l'identification à un parti au moment de l'inscription sur la liste électorale. Dans la plupart des États, une électrice ou un électeur précise son allégeance politique en s'inscrivant comme républicain, démocrate ou indépendant (identification à aucun parti). Cela lui permet de voter lors des primaires — selon l'allégeance politique qu'il a exprimée — afin de désigner la candidate ou le candidat d'un parti lors d'une élection.

6.2 Australie

Régime d'encadrement

En 1988, l'Australie a adopté le *Privacy Act*[115] pour encadrer le traitement des renseignements personnels de ses citoyennes et citoyens. Cette loi se fonde sur les principes usuels de protection des renseignements personnels que sont tenus de respecter les entreprises du secteur privé, les organisations à but non lucratif et les milieux de la santé en tenant compte du contexte particulier de leur milieu d'activité[116].

Les partis politiques australiens ne sont pas assujettis au *Privacy Act*. Au moment de l'adoption de cette loi, leur exclusion a été justifiée en invoquant le motif de la liberté des communications politiques, laquelle est essentielle à la vie démocratique australienne, conformément à la constitution du pays. Le commissaire à la protection de la vie privée et divers intervenants avaient néanmoins manifesté leur désaccord au regard de cette exclusion[117].

À la suite d'enquêtes journalistiques sur le traitement inapproprié de données et de renseignements personnels par les partis politiques au début des années 2000, des pressions citoyennes ont été exercées sur les pouvoirs publics afin que les partis politiques soient également régis par le cadre législatif de protection de la vie privée. En 2006, une loi a été déposée au Parlement pour mettre fin à cette exclusion, mais elle n'a pas été adoptée[118].

En 2008, après plusieurs mois de travaux commandés par un comité sénatorial, la commission de la réforme législative (Australia Law Reform Commission) procédait à un examen approfondi du *Privacy Act* et recommandait notamment que les partis politiques soient tenus de respecter les obligations, les principes et les pratiques découlant de cette loi, tout en reconnaissant certaines exceptions, dans le but de renforcer la confiance des citoyens[119].

---

114. United States Elections Project, *US Voter List Information*. [http://voterlist.electproject.org/].
115. *Privacy Act 1988*. [https://www.legislation.gov.au/Series/C2004A03712].
116. Office of the Australian Information Commisioner, *Australian Privacy Principles*. [https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles].
117. Colin J. Bennett et Robin M. Bayley, *op. cit.*, p. 10.
118. Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice (ALRC Report 108)*, vol. 2, mai 2008, p. 1416. [https://www.alrc.gov.au/publications/41.%20Political%20Exemption/introduction].
119. *Ibid.*, p. 1413.

Le gouvernement australien a toutefois rejeté cette recommandation et a maintenu le non-assujettissement des partis politiques. Il a précisé que les renseignements personnels ne pouvaient être utilisés par les partis politiques qu'à des fins électorales ou lors d'un processus référendaire et qu'en aucun cas ces renseignements ne pouvaient faire l'objet d'un usage commercial.

Opérations électorales

Sous le *Commonwealth Electoral Act* de 1918, l'organisation des élections fédérales et des référendums relève de la commission électorale (Australian Electoral Commission). Les élections des États et des collectivités locales sont du ressort de commissions électorales distinctes mises en place par chacun des États et des territoires australiens.

La commission électorale maintient une liste électorale permanente des citoyennes et citoyens autorisés à voter et transmet cette liste aux partis politiques, aux membres du Parlement et aux candidates et candidats lors des élections.

La liste électorale précise les données suivantes sur les électrices et les électeurs[120] :

- Nom ;
- Prénom ;
- Adresse.

Un citoyen peut examiner la liste électorale dans les locaux de la commission électorale, mais il ne peut en obtenir un exemplaire sous aucune forme. La loi n'autorise l'usage des données de la liste électorale qu'à des fins électorales et de communication politique. Toute autre utilisation est susceptible d'être sanctionnée par une amende[121].

6.3 Nouvelle-Zélande

Régime d'encadrement

En Nouvelle-Zélande, le *Privacy Act* s'applique à toute personne ou tout groupe de personnes, incorporé ou non, du secteur public ou privé, qui détient des renseignements personnels, à l'exception des députées et députés, des tribunaux et des médias. Les partis politiques sont ainsi assujettis à cette loi et doivent se conformer aux principes usuels de protection de la vie privée[122].

Le commissaire à la protection de la vie privée s'emploie à créer et à promouvoir une culture dans laquelle les renseignements personnels sont protégés et respectés. Il est habilité à enquêter sur les plaintes pour violation de la vie privée, à valoriser l'éducation citoyenne et à procéder à l'examen des diverses lois quant à leurs incidences sur la vie privée des citoyens.

---

120. *Commonwealth Electoral Act 1918*, art. 83 et 90B. [https://www.legislation.gov.au/Details/C2018C00259].
121. Australian Electoral Commision, *About the Commonwealth Electoral Roll*. [https://www.aec.gov.au/Enrolling_to_vote/About_Electoral_Roll/].
122. New Zealand Privacy Commissioner, *Privacy Act & Codes*. [https://www.privacy.org.nz/the-privacy-act-and-codes/privacy-act-and-codes-introduction/].

Opérations électorales

Les électrices et les électeurs doivent s'inscrire pour voter[123]. Chaque fois qu'il déménage, un citoyen doit remplir un nouveau formulaire d'inscription. Si le citoyen est d'origine maorie, il peut choisir de s'inscrire sur la liste électorale maorie ou sur la liste électorale générale. La liste qu'il choisit a des incidences sur la façon dont il pourra voter lors des élections législatives[124].

Une citoyenne ou un citoyen peut demander d'être inscrit sur la liste électorale confidentielle s'il ne veut pas que soient divulgués ses renseignements personnels dans l'espace public. Dans ce cas, la commission électorale protégera la confidentialité de ses informations[125].

Les listes électorales diffusées publiquement contiennent les renseignements suivants sur les électrices et les électeurs :

- Prénoms ;
- Nom ;
- Adresse ;
- Profession ;
- Origine (si maorie) ;
- Groupe d'âge.

Les partis politiques, les candidats, les députés et les chercheurs scientifiques peuvent obtenir, sur demande, les listes électorales sur tout type de support. En outre, tout citoyen peut consulter ou acheter une copie imprimée d'une liste électorale[126].

123. New Zealand Electoral Commission, *Enrol and Vote for the First Time*. [https://www.elections.org.nz/voters/get-ready-enrol-and-vote/enrol-and-vote-first-time].
124. New Zealand Electoral Commission, *Enrol and Vote as New Zealand Maori – Te Reo*. [https://www.elections.org.nz/voters/get-ready-enrol-and-vote/enrol-and-vote-new-zealand-maori-te-reo].
125. New Zealand Electoral Commission, *Concerned about Your Personal Safety ?* [https://www.elections.org.nz/voters/get-ready-enrol-and-vote/concerned-about-your-personal-safety].
126. New Zealand Electoral Commission, *Enrolling to Vote: Application*. [https://www.elections.org.nz/sites/default/files/plain-page/attachments/Enrolment%20Form%20ROE1_MAR13.pdf].

6.4 États membres de l'Union européenne

L'Union européenne attache une grande importance au respect de la vie privée et à la protection des données à caractère personnel des citoyennes et citoyens dans les traités, les lois et les règlements[127]. Les renseignements personnels sont considérés comme des « données nominatives imprescriptibles, inaliénables, insaisissables et incessibles[128] ».

Règlement général sur la protection des données

L'avènement des réseaux sociaux et le modèle de l'économie numérique fondé sur l'exploitation de tout type de données ont posé de nouveaux enjeux et défis aux législations européennes de protection des renseignements personnels[129].

En 2016, le Parlement européen a adopté le *Règlement général sur la protection des données*[130] (RGPD) afin de disposer d'une législation uniforme et actualisée en matière de protection des données sur tout le territoire de l'Union européenne. Ce règlement a modernisé le cadre juridique européen et a remplacé les textes législatifs nationaux qui avaient été mis en place pour transposer la *Directive européenne sur la protection des données* de 1995[131].

---

127. Adoptée en 2000, la *Charte des droits fondamentaux de l'Union européenne* (http://www.europarl.europa.eu/charter/pdf/text_fr.pdf) consacre, dans ses articles 7 et 8, le droit au respect de la vie privée et le droit à la protection des données à caractère personnel au rang des droits fondamentaux. La *Charte* est intégrée au *Traité de Lisbonne* (https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:C:2007:306:FULL&from=FR), en 2007, et revêt alors un caractère juridiquement contraignant, tant pour les institutions de l'Union européenne que pour les États membres.

128. Georges Châtillon, *Les données personnelles : enjeux juridiques et perspectives*, 28 février 2004. [https://www.pantheonsorbonne.fr/diplomes/master-droit-du-numerique/bibliotheque-numerique-du-droit-de-ladministration-electronique/droit/protection-des-donnees/les-donnees-personnelles-enjeux-juridiques-et-perspectives-rapport-de-georges-chatillon/].

129. Le considérant 6 du *Règlement général sur la protection des données* expose le contexte qui a présidé à l'élaboration et à l'adoption de ce texte : « L'évolution rapide des technologies et la mondialisation ont créé de nouveaux enjeux pour la protection des données à caractère personnel. L'ampleur de la collecte et du partage de données à caractère personnel a augmenté de manière importante. Les technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère personnel comme jamais auparavant dans le cadre de leurs activités. De plus en plus, les personnes physiques rendent des informations les concernant accessibles publiquement et à un niveau mondial. Les technologies ont transformé à la fois l'économie et les rapports sociaux, et elles devraient encore faciliter le libre flux des données à caractère personnel au sein de l'Union et leur transfert vers des pays tiers et à des organisations internationales, tout en assurant un niveau élevé de protection des données à caractère personnel » (https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=fr).

130. *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46*. [https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=fr].

131. *Directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, 24 octobre 1995. [https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:31995L0046]. Il s'agit du premier véritable ensemble législatif cohérent sur la protection des données pour l'Union européenne. Il tentait d'établir un équilibre entre la protection des libertés individuelles et les nécessités des échanges communautaires. La directive imposait des principes fondamentaux et prévoyait la mise en place d'autorités de contrôle indépendantes.

Depuis le 25 mai 2018, le RGPD est applicable dans chacun des 28 États membres de l'Union européenne. Il s'applique à toutes les organisations privées et publiques — incluant les partis politiques et les mouvements associatifs — qui collectent, traitent et exploitent des données sur les citoyens européens[132].

Ce texte normatif instaure une législation harmonisée en fixant des règles précises et neutres[133] sur le plan technologique, en responsabilisant davantage l'ensemble des acteurs à toutes les étapes de la collecte et du traitement des renseignements personnels, en donnant aux personnes la capacité d'agir par un renforcement de leurs droits et en imposant des sanctions en cas de non-conformité.

Le RGPD comprend quelques mesures phares :

- il réitère, actualise et opérationnalise les grands principes formant le socle de la protection des renseignements personnels énoncés dans les textes juridiques européens : responsabilité, transparence, finalité, consentement, minimisation, limitation temporelle, exactitude, information, sécurité, respect des droits de la personne concernée ;
- il requiert un changement des pratiques de gouvernance des organisations en exigeant l'intégration de la protection des renseignements personnels en amont — dans leurs politiques et leurs façons de faire — afin qu'elles soient en mesure de rendre compte, à tout moment, de la conformité de leurs traitements ;
- il oblige les organisations à obtenir un consentement par un acte affirmatif — clair et distinct — de la part de l'individu concerné par l'usage de ses renseignements personnels pour chacune des finalités auxquelles ces organisations destinent les données qu'elles recueillent, traitent et exploitent ;
- il réaffirme et renforce les droits des personnes (accès, information, rectification, opposition) et introduit pour la première fois le droit à la portabilité et, de manière formelle, le droit à l'oubli, lequel contraint les responsables du traitement à effacer les renseignements personnels si la personne concernée le demande ;
- il impose aux responsables du traitement des données de tenir un registre permettant de retracer les opérations et à rendre publique toute atteinte à la vie privée dans un délai maximum de 72 heures après en avoir pris connaissance ;
- il confirme les prérogatives des autorités nationales de contrôle de données et renforce leurs compétences en leur donnant un pouvoir d'enquête et des moyens dissuasifs de contrainte, notamment par des amendes graduées pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel mondial d'une entreprise.

---

132. Cette réglementation s'applique également aux organisations basées hors de l'Union européenne : si une organisation offre un produit ou un service dans l'Union européenne ou utilise les données de citoyens européens, les règles du RGPD s'appliquent à cette organisation, quel que soit l'endroit depuis lequel elle opère.

133. « La neutralité technologique est un néologisme souvent invoqué pour tenter de concilier la révolution technologique avec l'évolution souvent lente du droit. » Selon ce principe, une règle est neutre sur le plan technologique lorsqu'elle est destinée à couvrir toutes les situations, indépendamment de la technologie utilisée. Voir Vincent Gautrais, *Neutralité technologique : rédaction et interprétation des lois face aux technologies*, Thémis, mai 2012. [https://www.gautrais.com/publications/neutralite-technologique/].

Une vraie culture de la protection des renseignements personnels est mise en place à toutes les étapes de la collecte et du traitement de données et elle concerne tout le monde, tant ceux qui consentent à leur divulgation que ceux qui les utilisent à des fins commerciales, professionnelles ou électorales. Le traitement des données doit forcément répondre à un but ou à un besoin défini. Il est impossible de collecter des renseignements personnels sans raison particulière.

Le RGPD couvre l'intégralité des moyens permettant l'identification directe ou indirecte d'une personne[134]. La collecte et le traitement de catégories particulières de renseignements personnels — comme l'origine raciale ou ethnique, les convictions religieuses, l'orientation sexuelle et les opinions politiques — sont interdits, sauf à certaines conditions, avec des mesures de protection appropriées[135]. Nous apporterons un éclairage sur cette problématique dans les pages suivantes, lesquelles évoquent les activités électorales au regard de ce nouveau cadre réglementaire.

Le RGPD laisse encore une marge de manœuvre aux États membres, qui peuvent préciser l'application de certaines règles ou conditions d'application. Plusieurs dispositions de ce règlement prévoient que les États membres pourront maintenir ou adopter des règles spécifiques sur certains sujets. Néanmoins, dans tous les cas, les renseignements personnels sont soumis aux exigences énoncées dans le RGPD.

Des élections libres et la liberté d'expression, notamment la liberté du débat politique, constituent l'assise de tout régime démocratique. En campagne électorale, il est important que les opinions et les informations circulent librement dans la société et l'univers numérique.

Il est d'usage que les partis politiques et les candidates et candidats aient recours aux renseignements personnels à des fins électorales en vue de communiquer avec les citoyennes et citoyens. Leur objectif est de mener une communication politique au moyen de messages adressés aux électeurs dans le but de débattre des enjeux, de présenter un programme politique et de les inciter à voter en leur faveur.

134. L'article 4.1 du RGPD définit les données à caractère personnel comme « toute information se rapportant à une personne physique identifiée ou identifiable [ ] ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ».

135. L'article 9 du RPGD précise les catégories particulières de données à caractère personnel dont le traitement est interdit, sauf à certaines conditions, avec des mesures de protection appropriées : « Le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique sont interdits ».

Activités électorales[136]

Le traitement[137] des renseignements personnels à des fins électorales relève du RGPD, qui définit une série de droits et de devoirs à respecter lors de l'utilisation de listes d'électeurs. Les activités électorales des partis politiques sont aussi assujetties à des modalités particulières énoncées dans les lois électorales de chaque pays européen.

En aucun cas, il n'est prévu un amoindrissement des exigences de protection des renseignements personnels des électrices et des électeurs, que ce soit pour les partis politiques, les candidates et candidats ou pour les autorités publiques compétentes en matière électorale.

Du fait des différences dans l'organisation des systèmes politiques nationaux européens, plusieurs autorités de protection des données européennes ont élaboré des règles ou des lignes directrices sur le traitement des données à des fins politiques, lesquelles donnent une interprétation supplémentaire qui fait autorité sur les dispositions juridiques relatives à la protection des données et au respect de la vie privée énoncées dans le RGPD[138].

Les partis politiques et les candidates et candidats à une élection sont tenus de mettre en œuvre des procédures appropriées de gouvernance pour respecter leurs obligations de protection des données. Ils doivent être en mesure de démontrer à tout moment leur conformité au RGPD, en particulier au regard de la gestion et de la protection des renseignements personnels obtenus par les listes électorales remises par les autorités compétentes responsables de l'organisation des élections.

---

136. Ce texte est inspiré de : Commission de la protection de la vie privée (Belgique), *Traitement de données à caractère personnel à des fins d'envois personnalisés de propagande électorale et respect de la vie privée des citoyens : principes fondamentaux*, mai 2018 [https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Note_elections_RGPD.pdf] ;

    Commission nationale pour la protection des données (Luxembourg), *Prospection électorale et protection des données*, 21 août 2018 [https://cnpd.public.lu/fr/actualites/national/2018/08/communication-administres.html] ;

    Contrôleur européen de la protection des données, *Avis du CEPD sur la manipulation en ligne et les données à caractère personnel (n° 3/2018),* mars 2018 [https://edps.europa.eu/sites/edp/files/publication/18-03-19_opinion_online_manipulation_fr.pdf].

137. Aux fins du RGPD, on entend par *traitement*, à l'article 4.2 : « toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction ».

138. « Considérant que dans plusieurs juridictions, la législation de la protection des données est déjà applicable à la communication politique […] toute activité de communication politique – y compris celles qui ne se rapportent pas aux campagnes électorales – qui implique le traitement de données personnelles devrait respecter les libertés et les droits fondamentaux des personnes concernées, y inclus le droit à la protection des données personnelles, et devrait être conforme aux principes de protection des données reconnus. » Voir 27e Conférence des commissaires à la protection des données et à la vie privée, *Résolution sur l'utilisation de données personnelles pour la communication politique,* 16 septembre 2005. [https://edps.europa.eu/sites/edp/files/publication/05-09-16_resolution_political_communication_fr.pdf].

Listes électorales

En fonction de l'origine des données utilisées — par exemple, données en provenance de listes électorales ou données recueillies directement auprès des électeurs —, le traitement sera aussi soumis à une autre législation plus spécifique.

Selon les législations électorales des pays européens, les listes électorales peuvent être communiquées, en partie ou dans leur intégralité, à tout électeur, candidat, parti politique ou groupement politique, et ce, afin de permettre l'expression de la vie politique, à condition que cette personne ou cette entité s'engage à ne pas en faire un usage commercial.

L'établissement et la communication de listes électorales par une autorité nationale compétente constituent un traitement de renseignements personnels au sens du RGPD et doivent faire l'objet d'une gouvernance rigoureuse.

Une électrice ou un électeur peut raisonnablement s'attendre à ce que les données figurant sur les listes électorales puissent être utilisées comme source de données légitime pour la communication politique à l'approche des élections, conformément à la législation électorale applicable. Un parti politique, une candidate ou un candidat peut ainsi traiter des renseignements personnels à des fins électorales, même sans avoir obtenu le consentement de la personne concernée. Le traitement est considéré comme nécessaire à la réalisation d'intérêts légitimes au regard de l'exercice de la citoyenneté.

Conformément au principe de finalité du RGPD, les listes des électrices et des électeurs ne peuvent être utilisées qu'à des fins électorales, ce qui est d'ailleurs précisé explicitement par la législation électorale. Toute autre utilisation — par exemple à des fins commerciales ou pour une nouvelle élection — est interdite.

L'application des principes de finalité et de qualité (exactitude des renseignements personnels) implique que les listes d'électeurs produites pour une élection particulière sont uniquement utilisées dans le cadre de cette élection et sont supprimées une fois l'élection validée. En fonction de la législation électorale applicable dans chaque pays européen, ces listes peuvent être conservées pour une très courte période, voire quelques jours, après la date de l'élection.

Consentement explicite

Le traitement, à des fins électorales, de renseignements personnels ne provenant pas de listes d'électrices et d'électeurs est autorisé à condition que le responsable du traitement — un parti politique, une candidate ou un candidat — obtienne le consentement avéré de la personne concernée. Ce consentement doit être donné librement et porter sur un traitement spécifique.

Le consentement doit également reposer sur des raisons précises et la personne concernée doit accepter que ses renseignements personnels soient traités pour cette seule finalité. Le consentement doit être donné par un acte positif clair, par lequel la personne concernée manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement des renseignements personnels la concernant, au moyen d'une déclaration écrite, y compris par voie numérique, ou d'une déclaration orale.

Un consentement donné peut toujours être retiré par la personne concernée. Avant de donner son consentement, la personne concernée est informée de cette possibilité. Le retrait du consentement doit être aussi simple que le consentement initial.

Le mode de transmission du message électoral joue un rôle dans la détermination des conditions légales complémentaires à respecter dans le cadre du traitement. Certaines opérations de communication politique sont destinées à l'ensemble de la population — tracts ou programmes déposés dans les boîtes aux lettres, messages diffusés dans les médias de masse —, mais ce type de communication politique n'est pas régi par le RGPD. En revanche, l'envoi de courriels ciblés ou de textos nominatifs n'est admissible que si la personne concernée donne au préalable son consentement en vue d'un tel traitement de ses renseignements personnels.

Cibler un citoyen pour lui proposer un contenu numérique singulier qui devrait lui plaire revient à l'enfermer dans des choix déterminés à sa place par un traitement automatisé fondé sur des algorithmes. En effet, un environnement numérique individualisé tend communément à exposer l'électrice ou l'électeur à un seul type d'opinion et à limiter ses points de vue, d'où un risque accru de polarisation politique et idéologique. Grâce au RGPD, une électrice ou un électeur a la capacité d'éviter de recevoir des communications politiques sur les réseaux sociaux et des publicités numériques personnalisées insérées sur les sites qu'il consulte sur Internet.

Membres et sympathisants d'un parti politique

Un parti politique a le droit de traiter les renseignements personnels de ses membres et sympathisants. Il peut donc utiliser à des fins électorales sa propre liste de membres actuels et anciens, et ce, même sans le consentement explicite des personnes concernées. Ce traitement peut en effet être considéré comme faisant partie des attentes normales de ces personnes, compte tenu de leur affiliation.

Néanmoins, le simple fait que des renseignements personnels soient inscrits dans un fichier[139] tenu par un parti politique rend le traitement délicat, puisqu'il est susceptible de révéler l'opinion politique, réelle ou supposée, des électrices et des électeurs concernés. Lorsqu'une personne consent à donner un renseignement personnel à un parti politique, elle ne renonce pas à la confidentialité inhérente à ce type d'information et s'attend à un usage bien circonscrit et à une protection rigoureuse, comme le prévoit le RGPD.

139. L'article 4.6 du RGPD définit la notion de fichier, qui évoque aussi une base de données, comme « tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ».

Autres données

Conformément à ce règlement européen, le profilage[140] excessif des citoyennes et citoyens est disproportionné par rapport à la finalité électorale. Les partis politiques, les candidates et les candidats à une élection peuvent être tentés d'avoir recours à des renseignements personnels recueillis dans le cadre d'autres traitements, dont la finalité initiale n'avait rien à voir avec une élection. Ils ne peuvent pas réutiliser ces données et les croiser avec les listes électorales dans un but de communication politique. Un tel traitement est incompatible avec les finalités pour lesquelles ces données ont été initialement et légitimement récoltées, ce qui est sanctionnable en vertu du RGPD.

Les partis politiques, les candidates et les candidats enfreignent le principe de finalité lorsqu'ils recueillent des données divulguées librement dans l'univers numérique et qu'ils les utilisent à des fins de communication politique. En vertu du RGPD, ces données, rendues publiques par les personnes elles-mêmes ou par leurs proches, l'ont été dans un but bien déterminé, lequel n'a souvent aucun rapport avec la communication politique. C'est le cas, par exemple, lorsqu'une personne expose sa vie privée sur les réseaux sociaux et laisse des traces numériques — commentaires, contenus partagés, profils, recherches, etc. — à la suite de ses activités sur Internet.

Sur ce point, les pétitions de citoyennes et citoyens révèlent aussi des opinions et des prises de position à sensibilité politique. Certes, il y a des risques de profilage politique liés au fait de rendre visibles publiquement les renseignements personnels des signataires, alors qu'aucun fondement légal n'impose de diffuser l'identité des pétitionnaires. En aucun cas, une personne qui participe à une consultation citoyenne et qui signe une pétition ne donne, de la sorte, son accord pour une démarche complémentaire de communication politique. Par principe, la collecte de ces renseignements personnels et leur traitement ultérieur sont interdits si deux conditions ne sont pas remplies : le consentement explicite de la personne concernée et un intérêt public justifié. En l'occurrence, les partis politiques et les candidats à une élection ne peuvent utiliser les renseignements personnels des signataires d'une pétition de citoyens à des fins électorales.

De même, les candidates et les candidats ne peuvent utiliser des données de personnes qu'ils ont obtenues dans le cadre de l'exercice d'un mandat de députée ou de député pour leur écrire à des fins électorales. Une telle utilisation de renseignements personnels est non seulement interdite, en raison du principe de limitation des finalités, mais elle rompt l'égalité entre les candidats. La législation vise à traiter tous les candidats sur un pied d'égalité, en leur donnant accès aux mêmes données, à savoir celles figurant sur les listes des électrices et des électeurs.

140. L'article 4.1 du RGPD définit le profilage comme « toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique ».

Données sensibles

Selon le RGPD, les renseignements personnels qui révèlent des opinions politiques, l'origine raciale ou ethnique, les convictions religieuses ou l'appartenance syndicale constituent une catégorie de données particulière. Le traitement de ces données est généralement interdit, à moins que la personne concernée y ait consenti explicitement et librement et qu'il porte sur un traitement spécifique parfaitement balisé.

Pour les activités électorales, ce type de données peut revêtir un motif d'intérêt public et un intérêt légitime[141]. La collecte et le traitement de ce type de données doivent faire l'objet de précautions renforcées de la part des partis politiques et des candidates et candidats à une élection.

Les données sensibles ne peuvent être transmises à une autre entité à vocation politique ou sociétale sans le consentement de la personne concernée. Ainsi, même en cas de proximité idéologique avec un parti politique déterminé, il est interdit de communiquer les données liées à une affiliation syndicale à des fins de communication politique, à moins que l'organisme qui veut procéder au traitement n'ait obtenu le consentement explicite de la personne concernée.

Droit à l'information

L'application des principes énoncés dans le RGPD et, en particulier, l'information de la personne concernée au sujet de la finalité et de ses droits, y compris son droit de s'opposer au traitement et de retirer son consentement, doit être assurée. En vertu du RGPD, le parti politique, la candidate ou le candidat est, en principe, tenu d'informer les électrices et les électeurs de la collecte et du traitement de leurs données[142].

La personne concernée doit en effet savoir que ses renseignements personnels sont ou seront traités, par qui (par exemple, un parti politique ou un candidat déterminé), pour quelles raisons (par exemple, pour des finalités électorales) et sur la base de quel fondement légal (par exemple, le consentement de la personne concernée ou la législation électorale). Elle doit aussi recevoir d'autres informations afin que le traitement de ses données lui soit transparent, comme la période pendant laquelle les renseignements personnels seront conservés, l'origine des données (par exemple, les listes des électeurs) ainsi que des informations relatives à ses droits (par exemple, le droit de retirer un consentement accordé précédemment ou le droit d'opposition à la communication politique).

---

141. Le considérant 56 du RGPD le permet à certaines conditions : « lorsque, dans le cadre d'activités liées à des élections, le fonctionnement du système démocratique dans un État membre requiert que les partis politiques collectent des données à caractère personnel relatives aux opinions politiques des personnes, le traitement de telles données peut être autorisé pour des motifs d'intérêt public, à condition que des garanties appropriées soient prévues ».

142. L'article 12 du RGPD précise que l'on doit fournir à la personne concernée des informations « d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples ».

Droit d'accès

Une personne a le droit de consulter les données qui ont été collectées à son sujet de manière à pouvoir s'informer sur leur traitement et à en contrôler la légitimité. Dans le cadre d'une demande d'accès[143], la personne responsable du traitement doit communiquer à la personne concernée toute l'information requise sur l'exploitation de ses renseignements personnels.

Toute personne qui envoie un message politique peut donc devoir fournir à la personne concernée un accès à ses propres données et certaines explications sur les renseignements personnels qui ont été utilisés.

Droit d'opposition

Même s'il est légitime que des renseignements personnels soient traités à des fins de communication politique en période électorale, la citoyenne ou le citoyen concerné a le droit de s'opposer à tout moment à cette exploitation, y compris au profilage de sa personne. Dans ce cas, un parti politique ou un candidat à une élection doit respecter le choix du citoyen et cesser immédiatement le traitement de ses renseignements personnels.

Les électrices et les électeurs sont aussi en mesure de formuler des plaintes — à l'autorité nationale de contrôle de données ou à l'autorité nationale compétente en matière électorale — à propos de la manière dont les partis exploitent leurs renseignements personnels.

Désignation d'un délégué à la protection des données

Les partis politiques sont tenus de désigner une personne déléguée à la protection des données. Cette personne doit s'assurer que les traitements des renseignements personnels s'inscrivent bien dans le respect strict des obligations du RGPD et de la législation électorale. Aussi, elle veille à ce que le personnel et les bénévoles du parti politique soient dûment habilités à avoir accès aux renseignements personnels des électrices et des électeurs que le parti politique détient et exploite. Enfin, elle agit en qualité de répondante auprès de l'autorité nationale de contrôle des données et de l'autorité nationale compétente en matière électorale.

Sécurité

Les renseignements personnels ne peuvent être consultés que par les personnes habilitées à y accéder en raison de leurs fonctions et responsabilités au sein d'un parti politique.

Les partis politiques, les candidates et les candidats doivent veiller à ce que l'accès aux données, leur confidentialité et les possibilités de les traiter demeurent l'apanage des personnes qui en ont effectivement besoin pour accomplir les tâches qui leur

143. Conformément à l'article 15 du RGPD, toute personne peut demander si des données la concernant sont traitées et obtenir des informations sur leur traitement (incluant l'établissement d'un profilage) et sur la durée de leur conservation. Elle peut aussi obtenir une copie de ces données et toute information disponible sur leur origine.

sont confiées, à savoir la préparation et l'exécution de la communication électorale. Ils doivent prendre des mesures appropriées à cet effet, comme, par exemple, la définition de profils d'habilitation, la protection par mot de passe et le verrouillage physique du lieu de conservation du fichier ou du lieu où le traitement automatisé peut être consulté.

Les partis politiques, les candidates et les candidats doivent tenir une documentation interne complète — un registre de conformité permettant notamment d'établir la liste des accès individuels aux fichiers des renseignements personnels — sur les différents traitements de données et s'assurer qu'ils respectent bien les obligations légales du RGPD et celles des législations électorales nationales.

Sous-traitance

Dans le cadre de sa campagne électorale, un parti politique, une candidate ou un candidat peut confier l'exécution de certaines tâches à un sous-traitant[144]. Afin de garantir que le traitement réalisé par le sous-traitant pour le compte du responsable réponde aux prescriptions du RGPD, la personne responsable du traitement ne peut faire appel qu'à des sous-traitants présentant des garanties suffisantes, notamment en matière de connaissances spécialisées, de fiabilité et de ressources, pour la mise en œuvre de mesures techniques et organisationnelles qui satisferont pleinement aux exigences du RGPD, y compris en matière de sécurité du traitement.

Le RGPD et l'encadrement canadien et québécois

Le RGPD se fonde sur des principes de protection des renseignements personnels comparables à ceux de l'encadrement canadien et québécois pour le secteur privé. D'une façon générale, en Europe, les renseignements personnels sont exploités avec transparence afin que la personne concernée sache quels sont les renseignements personnels collectés et traités. On recueille uniquement le nombre minimal de renseignements personnels nécessaires à une activité ponctuelle, clairement énoncée et légitime. Les données sont tenues exactes et actualisées au besoin. La durée de conservation est restreinte. La sécurité et la confidentialité sont assurées. La personne responsable des données est en mesure de démontrer que ces principes sont respectés. En Europe, les modalités de gouvernance des renseignements personnels sont précises et exigeantes, à toutes les étapes de leur exploitation.

Au Canada et au Québec, seuls les organismes publics et les entreprises privées sont assujettis aux législations de protection des renseignements personnels. Les partis politiques doivent plutôt se conformer à des législations spécifiques qui n'ont pas les mêmes exigences en cette matière. En Europe, toutes les organisations — quelle que soit leur nature — doivent observer le RGPD.

144. L'article 4.8 du RGPD définit le sous-traitant comme « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement ».

Les citoyennes et citoyens européens ont la possibilité d'exercer une maîtrise accrue de leurs données au moyen de divers droits : accès, rectification, opposition, effacement, limitation de traitement et portabilité des données[145]. Par exemple, le RGPD reconnaît formellement un droit à l'oubli, à savoir la possibilité de faire déréférencer un contenu par un moteur de recherche ou d'effacer des renseignements personnels à certaines conditions (retrait de consentement, finalités caduques, motifs de traitement illégitime)[146]. Ce type de droit à l'oubli n'existe pas au Canada ni au Québec.

6.4.1 France

Régime d'encadrement

Pour se conformer au cadre juridique européen érigé par le RGPD, le gouvernement français a décidé d'adapter la *Loi relative à l'informatique, aux fichiers et aux libertés*, en vigueur depuis 1978, plutôt que de l'abroger.

En conséquence, la *Loi relative à la protection des données personnelles* a été promulguée le 20 juin 2018[147]. Ce nouveau texte a pour but d'instaurer le cadre juridique français au sein duquel le RGPD s'insère pleinement et de mettre en œuvre les modalités pratiques et techniques de son application[148]. Ainsi, les partis politiques et les candidates et candidats à une élection continuent d'avoir l'obligation d'observer un cadre réglementaire exigeant en matière de protection des renseignements personnels.

Le *Code électoral*[149] énonce les dispositions législatives et réglementaires relatives aux élections politiques, à savoir l'élection des députés, des sénateurs, des conseillers régionaux, des conseillers départementaux et des conseillers municipaux. Il définit, pour chaque type d'élection, les modes d'inscription sur les listes électorales, le découpage des circonscriptions, les conditions pour être élu et les règles de déroulement du scrutin uninominal à deux tours.

145. Grâce au droit à la portabilité des données, une personne a la possibilité de demander à un organisme de récupérer les données la concernant dans un format normalisé, couramment utilisé et lisible par différents dispositifs numériques. Ainsi, ces données – renseignements personnels et traces numériques – peuvent être conservées par la personne concernée ou transmises facilement d'un système à un autre en vue d'une réutilisation à d'autres fins ayant fait l'objet d'un consentement distinct.

146. RPGD, art. 17, Droit à l'effacement (« droit à l'oubli »).

147. *Loi nº 2018-493 du 20 juin 2018 relative à la protection des données personnelles*. [https://www.legifrance.gouv.fr/eli/loi/2018/6/20/JUSC1732261L/jo/texte].

148. *Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*. [https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460].

149. *Code électoral*. [https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070239&dateTexte=20181018].

Renseignements fournis par l'administration électorale

En France, les listes électorales sont élaborées de manière permanente dans chaque commune[150] par une commission administrative composée du maire ou de la personne qui le représente, de la personne déléguée à l'administration désignée par le préfet et de la personne déléguée désignée par le président du tribunal de grande instance. Ces listes font l'objet d'une révision et d'une mise à jour annuelle[151].

On distingue la liste électorale proprement dite, qui concerne les électrices et les électeurs de nationalité française ; et la liste complémentaire, qui regroupe les citoyennes et citoyens ressortissant d'un État membre de l'Union européenne, pour les scrutins français qui leur sont ouverts, soit les élections européennes et les élections municipales.

La liste électorale[152] contient les renseignements personnels suivants sur les électrices et les électeurs :

- Prénoms ;
- Nom ;
- Adresse ;
- Date de naissance ;
- Lieu de naissance.

Les listes électorales sont réunies en un registre et conservées dans les archives de la commune. Tout électeur, tout candidat ou tout parti ou groupement politique peut en obtenir une copie[153]. Cette liste est publique afin de permettre à chaque électrice et électeur d'en prendre connaissance et, le cas échéant, de contester l'inscription de personnes qui n'auraient pas qualité pour y figurer.

Le 1er janvier 2019, la législation française a créé un répertoire électoral unique et permanent tenu par l'Institut national de la statistique et des études économiques (INSEE)[154]. Les maires transmettent désormais l'ensemble des informations à l'INSEE, qui met à jour le fichier numérique et s'assure de la régularité de la liste électorale.

Les listes électorales constituent, par la volonté même du législateur, un fichier public dont il est possible d'obtenir la communication et la copie. Les éventuelles difficultés pour obtenir communication et copie des listes électorales relèvent de la compétence

150. « La commune est la collectivité administrative de « base » ou de proximité. […] Les communes bénéficient de la compétence générale pour gérer toute affaire d'intérêt communal sur un territoire. Les communes connaissent une organisation administrative unique, quelle que soit leur taille. Elles sont gérées par un conseil municipal et par le maire et ont notamment la responsabilité de la gestion de l'état civil et de l'organisation des élections. » [http://www.vie-publique.fr/decouverte-institutions/institutions/collectivites-territoriales/categories-collectivites-territoriales/qu-est-ce-qu-commune.html].

151. *Code électoral*, art. L17.

152. *Ibid.*, art. L18 et L19.

153. *Ibid.*, art. L28.

154. *Loi* nº *2016-1048 du 1er août 2016 rénovant les modalités d'inscription sur les listes électorales,* art. 2. [https://www.legifrance.gouv.fr/affichCode.do ;jsessionid=408B89F377F89D5C0EE092FAD7E721DE.tplgfr33s_2 ?idSectionTA=LEGISCTA000006164052&cidTexte=LEGITEXT000006070239&dateTexte=20190101].

exclusive de la Commission d'accès aux documents administratifs (CADA)[155]. Dans ce contexte, les citoyens saisissent la CADA pour régler un différend avec une autorité publique qui refuse de leur transmettre la liste électorale – par exemple, lors d'un refus pour une allégation de finalité commerciale[156] ; lors d'un refus pour organiser une réunion familiale[157] ; ou lors d'un refus de communiquer la liste sur support numérique[158]. Dans ces trois cas, la CADA a donné raison aux citoyens, qui ont pu obtenir un exemplaire des listes électorales.

Les principales obligations à respecter[159]

Selon les termes du *Code électoral*, un parti politique, une candidate ou un candidat peut utiliser les listes électorales sans que les électrices, les électeurs et les maires sollicités puissent le refuser. Ils peuvent effectuer des tris à partir des informations électorales afin d'adresser une communication politique à une catégorie particulière de personnes votantes, en fonction de leur âge ou de leur bureau de vote, par exemple. En cas d'envoi simultané, la personne responsable du traitement doit veiller à ne pas divulguer à l'ensemble des destinataires les coordonnées des intéressés.

Par contre, les tris effectués ne doivent pas faire ressortir l'origine ethnique ou l'opinion politique des personnes, réelle ou supposée. De fait, un parti politique, une candidate ou un candidat ne peut pas, par exemple, adresser un message personnalisé à l'occasion d'une fête religieuse ou inciter une citoyenne ou un citoyen à soutenir une candidature issue d'une communauté particulière. Dans le même ordre d'idées, il est interdit d'effectuer des tris sur la base de la consonance des noms ou du lieu de naissance des personnes inscrites sur les listes électorales.

Le RGPD précise que la durée de conservation des renseignements personnels est dictée par la finalité de chaque traitement. En France, les listes d'électrices et d'électeurs et les fichiers numériques de communication politique constitués pour les besoins d'une campagne électorale particulière doivent être détruits par les candidates, les candidats et les partis politiques à l'issue de l'élection.

---

155. La Commission d'accès aux documents administratifs est une autorité administrative indépendante chargée de veiller à la liberté d'accès aux documents administratifs et aux archives publiques ainsi qu'à la réutilisation des informations publiques.

156. Commission d'accès aux documents administratifs, *Communication des listes électorales du département (Avis 20180832)*, 15 septembre 2018. [https://cada.data.gouv.fr/20180832/].

157. Commission d'accès aux documents administratifs, *Communication des listes électorales en vue de l'organisation d'une cousinade (Avis 20180364),* 17 mai 2018. [https://cada.data.gouv.fr/20180364/].

158. Commission d'accès aux documents administratifs, *Copie sur support numérique, et non simple consultation, des listes électorales (Avis 20131138)*, 4 juillet 2013. [https://cada.data.gouv.fr/20131138/].

159. Ce texte est inspiré de : Commission nationale informatique et libertés et Conseil supérieur de l'audiovisuel, *Campagnes électorales : tout savoir sur les règles CSA et CNIL* [https://www.cnil.fr/sites/default/files/atoms/files/guide_cnil_et_csa.pdf] ;

Commission nationale informatique et libertés, *Communication politique : obligations légales et bonnes pratiques* [https://www.cnil.fr/sites/default/files/typo/document/CNIL_Politique.pdf] ; Commission nationale informatique et libertés, *Délibération n° 2012-020 du 26 janvier 2012 portant recommandation relative à la mise en œuvre, par les partis ou groupements à caractère politique, élus ou candidats à des fonctions électives, de fichiers dans le cadre de leurs activités politiques* [https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000025364626&fastReqId=1082859898&fastPos=1].

Les partis politiques et les candidats peuvent utiliser des fichiers déjà constitués par des entités privées (par exemple, un annuaire mis à la disposition des citoyennes et des citoyens). Dans ce cas, ils doivent informer les citoyens de l'origine des données utilisées. En outre, ils doivent obtenir expressément le consentement de la personne concernée dès la première prise de contact, et ce, avant de lui envoyer toute communication à des fins politiques. À tout moment, cette personne peut exercer ses droits stipulés dans le RGPD, notamment pour s'opposer à la collecte des informations ou à la réception de nouveaux messages à finalité politique.

La collecte de données issues des réseaux sociaux n'est pas légale en l'absence d'information et de consentement de la personne concernée. Le caractère public des données disponibles sur les réseaux sociaux ne leur fait pas perdre le statut de renseignements personnels : si leur simple consultation est toujours possible, le traitement de ces données — extraction, enregistrement, utilisation, enrichissement, etc. — est soumis à l'ensemble des conditions prévues par le RGPD, en particulier un consentement explicite par un acte affirmatif. Sur ce point, l'information générale que les réseaux sociaux soumettent à leurs usagers quant à la possibilité d'une utilisation ultérieure des données à d'autres fins, qui figure généralement dans leur politique de confidentialité, ne peut suffire à considérer ces personnes comme informées et consentantes.

En cas d'envoi de courriels, la présence d'un lien de désabonnement facilite l'exercice du droit d'opposition de la personne concernée. Ce lien doit être opérationnel, clair, visible et aisément accessible. Il en va de même de tout dispositif semblable en cas d'envoi de SMS.

Pour leurs communications politiques, les partis politiques, les candidates et les candidats peuvent utiliser les fichiers constitués par leurs soins (par exemple, un fichier de gestion des membres d'un parti ou des soutiens avérés d'un candidat). L'exploitation de ces fichiers doit respecter les principes généraux de protection des données et les droits des personnes concernées. À l'opposé, toute utilisation de fichiers publics à des fins de communication politique est susceptible de constituer un détournement de finalité passible de sanctions.

En vertu du RGPD, toute personne ayant accompli, auprès d'un parti, une démarche positive en vue d'établir des rapports soutenus directement liés à son action politique — abonnement à une lettre de diffusion, soutien financier récurrent, participation aux activités ou aux réunions du parti, demande d'adhésion, etc. — devient de ce fait un contact régulier de ce parti. À moins qu'elle n'effectue une démarche contraire, ses renseignements personnels peuvent donc être inscrits dans un fichier de contacts courants et son consentement est tenu pour acquis. L'exception au principe d'interdiction de traiter des informations sensibles, qui s'applique aux fichiers des membres et des contacts courants des partis politiques, doit être interprétée de manière responsable.

Lorsqu'il s'agit uniquement d'une démarche ponctuelle (une demande d'information sur une proposition politique, par exemple) n'exprimant pas une volonté affirmée d'établir un lien fondé sur un intérêt partagé, la personne concernée ne peut être considérée comme membre ou contact courant du parti. Elle constitue plutôt un contact occasionnel du parti politique ; ses coordonnées peuvent être utilisées une

seule fois afin de l'inviter à entretenir des relations plus soutenues ou à devenir membre du parti. Une telle sollicitation ne doit pas être réitérée si la personne concernée n'y donne pas suite ; dans ce cas, les renseignements personnels collectés doivent être supprimés dans un délai raisonnable.

Les contenus numériques sur Internet conçus par un parti politique, une candidate ou un candidat permettent souvent à un individu, à l'aide d'outils de partage, de commenter, noter, apprécier, recommander un contenu ou y réagir (c'est le cas du bouton « Like/J'aime » de Facebook ou d'une formule du type « X recommande la page de [parti politique] »). Ces outils tissent un lien entre le profil d'un individu et un contenu numérique. Lorsqu'un individu active un dispositif de partage, son identité numérique devient visible pour le parti politique.

En sa qualité de responsable du traitement et de la mise en place d'un outil de partage, le parti politique, la candidate ou le candidat doit recueillir le consentement de l'individu avant de révéler publiquement, dans l'espace numérique, certains de ses renseignements personnels, son opinion politique (réelle ou supposée) et toute autre donnée sensible. Le fait qu'un individu active l'outil numérique de partage ne suffit pas pour obtenir son consentement : le parti ou le candidat doit l'informer clairement et précisément de la portée de son action et du caractère public de sa contribution pour que ce consentement soit libre et éclairé.

Les signataires de pétitions ne peuvent être automatiquement considérés comme des contacts courants ou des sympathisants de la candidate, du candidat ou du parti qui en est l'initiateur. La participation à une consultation citoyenne ne peut être liée à une démarche complémentaire de suivi et d'engagement politique, à moins que la pétition ait pour objet de soutenir directement et manifestement l'action politique d'un parti. Dans cette hypothèse, les personnes concernées sont considérées comme des contacts occasionnels du parti ; leurs renseignements personnels, qu'ils ont volontairement communiqués, peuvent être utilisés une seule fois afin de les inviter à donner leur consentement pour entretenir des relations plus soutenues ou pour devenir membres du parti.

En sa qualité de responsable du traitement, la candidate, le candidat ou le parti politique veille à la sécurité des données qu'il exploite. Il s'assure de prendre rigoureusement toutes les mesures nécessaires pour en garantir la confidentialité et éviter toute divulgation d'information. Aussi, les données contenues dans les fichiers ne peuvent être consultées que par les personnes habilitées à y accéder en raison de leurs fonctions.

Rôle et pouvoirs de l'autorité de surveillance

La Commission nationale de l'informatique et des libertés (CNIL) est une autorité administrative indépendante créée en 1978. Sa mission est de veiller à ce que le développement des nouvelles technologies ne porte pas atteinte à l'identité humaine, à la vie privée et aux libertés individuelles ou publiques.

C'est à ce titre que la CNIL peut intervenir en matière de communication politique, dès lors que des opérations de communication nécessitent la constitution ou l'utilisation de renseignements personnels.

La CNIL informe les personnes de leurs droits et les partis politiques de leurs obligations, tels que définis par le RGPD. Elle joue aussi un rôle d'alerte, d'anticipation et de conseil. Enfin, la CNIL est dotée d'un pouvoir de contrôle sur place et de sanctions, lesquelles sont graduées selon la gravité des manquements.

6.4.2 Belgique

Régime d'encadrement

Le RGPD protège la vie privée des citoyens belges lors du traitement de leurs renseignements personnels. Il impose aux partis politiques et aux candidates et candidats à une élection qui traitent ces données dans un but de communication électorale[160] de respecter des principes généraux et les droits des citoyennes et des citoyens concernés.

La *Constitution belge* fixe les éléments fondamentaux du système électoral. Elle est complétée par un ensemble de lois et d'arrêtés généraux ou particuliers concernant les élections communales, provinciales, régionales, communautaires, fédérales et européennes.

Le *Code électoral*[161] précise les diverses modalités inhérentes aux opérations électorales, notamment la qualité d'électeur, les listes d'électeurs, l'éligibilité des candidatures, les réclamations et recours, les bureaux de vote, les modes de vote, le dépouillement du scrutin, la désignation des élus, les sanctions, etc.

Renseignements fournis par l'administration électorale

En Belgique, la liste des électrices et des électeurs est arrêtée par le collège des bourgmestres et échevins de chaque commune. Elle répertorie l'identité de tous les citoyens appelés à voter en indiquant leurs renseignements personnels ci-après :

- Prénoms ;
- Nom ;
- Adresse de la résidence principale ;
- Date de naissance ;
- Sexe.

Selon le type d'élection — communale, provinciale, régionale, communautaire, fédérale, européenne —, la liste d'électeurs d'une commune est transmise au gouvernement compétent, lequel vérifie qu'aucune personne n'est mentionnée sur plus d'une liste en contrôlant le numéro de registre national des électeurs[162]. Une fois la liste validée, elle

160. Ce texte s'inspire de la note *Traitement de données à caractère personnel à des fins d'envois personnalisés de propagande électorale et respect de la vie privée des citoyens : principes fondamentaux*. [https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Note_elections_RGPD.pdf].

161. *Code électoral*. [http://www.ejustice.just.fgov.be/eli/loi/2018/04/19/2018011790/justel].

162. En Belgique, le numéro du registre national est un identifiant unique et personnel composé de onze chiffres. Le registre national désigne le système de traitement d'informations qui assure l'enregistrement, la mémorisation et la communication d'informations relatives à l'identification des citoyens. Pour toutes les personnes résidant légalement en Belgique, ainsi que pour les Belges immatriculés auprès de consulats, cette base de données répertorie notamment le lieu et la date de naissance ainsi que les historiques de l'état civil, des résidences principales, de la nationalité, des professions déclarées, des permis de conduire et de la qualité d'électeur (http://www.ibz.rrn.fgov.be/fr/registre-national/).

est affichée publiquement jusqu'au 12e jour précédant l'élection. Pendant cette période, chaque personne peut examiner si son nom est inscrit et si les mentions la concernant sont exactes.

La loi électorale autorise la transmission de la liste des électeurs aux partis politiques qui présentent des candidates et des candidats dans la circonscription électorale et aux candidats à une élection qui en font la demande par lettre recommandée adressée au bourgmestre. Le numéro de registre national des électrices et des électeurs n'est jamais inscrit sur les listes transmises.

Les données qui figurent sur les listes d'électeurs ne peuvent être utilisées qu'à des fins électorales. Ainsi, les listes obtenues pour une élection déterminée ne peuvent être utilisées que dans le cadre de cette élection et ne peuvent être communiquées à des tiers. Toute autre utilisation (par exemple, à des fins commerciales ou après la date de l'élection) est interdite.

Les principales obligations à respecter

Afin d'influencer favorablement les résultats électoraux le jour du scrutin, les partis, les candidates et les candidats utilisent avant tout les renseignements personnels des électrices et des électeurs pour communiquer avec eux. Pour maximiser l'efficacité de leurs communications électorales, les partis et les candidats puisent aussi des données sur les électeurs dans des sources diverses afin de mieux établir leur profil.

La communication avec les électrices et les électeurs s'effectue de différentes manières : par courrier, par le porte-à-porte, par téléphone, sur les réseaux sociaux ou par courriel, par exemple. En fonction de l'origine des données et de la manière dont elles sont exploitées, le traitement est soumis à des législations spécifiques qui s'ajoutent au RGPD.

La législation électorale belge autorise les partis, les candidates et les candidats à se livrer à de la communication électorale personnalisée au moyen des données provenant des listes des électrices et des électeurs. Les partis et candidats ont ainsi un intérêt légitime et le droit de procéder à des traitements sans que le consentement de la personne concernée soit requis. Ainsi, un citoyen dont les données figurent sur les listes d'électeurs peut raisonnablement s'attendre à ce qu'on exploite ses renseignements personnels à des fins électorales.

Dans leur premier message de communication électorale, les partis politiques sont tenus de préciser au citoyen, de manière claire et séparée de toute autre information, qu'il peut exercer son droit à s'opposer au traitement des données le concernant. L'électrice ou l'électeur doit également être informé de l'identité et des coordonnées de la personne responsable du traitement désignée par les partis politiques, des finalités électorales de l'exploitation des renseignements personnels et de l'origine de toutes les données collectées. L'électeur a aussi la possibilité de s'opposer à l'utilisation de ses renseignements personnels à des fins de communications politiques. Une personne qui a exercé son droit d'opposition ne peut plus être jointe par les partis politiques.

Un parti politique est autorisé à transmettre les listes à un sous-traitant (par exemple, le responsable de l'exécution d'un publipostage politique ou d'une opération numérique). Dans ce cas, le sous-traitant est tenu de présenter des garanties suffisantes en matière de connaissances spécialisées, de fiabilité avérée et de ressources nécessaires pour la mise en œuvre de mesures techniques et organisationnelles qui satisfont pleinement aux exigences du RGPD.

Le recours à des moyens de communication numérique à des fins électorales requiert une attention particulière de la part des partis, des candidates et des candidats. En Belgique, l'envoi de messages numériques par courriel ou par texto est considéré comme particulièrement intrusif, de sorte que les libertés et les droits fondamentaux des électrices et des électeurs pèsent, en principe, plus lourd dans la balance que les intérêts légitimes des partis politiques.

Les partis politiques, les candidates et les candidats doivent obtenir le consentement préalable de la personne concernée, lors d'une première communication, avant d'exploiter ses renseignements personnels — adresse de courriel, numéro de téléphone, identifiant de réseaux sociaux, etc. — provenant d'une autre source que les listes d'électeurs. Sans ce consentement, le traitement de ces renseignements à des fins électorales est considéré comme incompatible avec la finalité pour laquelle ces données ont été obtenues à l'origine.

En raison d'une relation préexistante, il s'avère raisonnable qu'un parti politique utilise les dispositifs numériques pour effectuer des communications politiques auprès de ses membres et sympathisants. Cependant, lors de la collecte de leurs coordonnées numériques, les membres et les sympathisants doivent être clairement et distinctement informés de l'utilisation possible de ces données à des fins de communication politique et avoir l'occasion de s'opposer à une telle utilisation. Si la personne concernée ne s'est pas opposée à cette utilisation dans un premier temps, on doit lui proposer de le faire dans chaque nouveau message numérique constituant une communication politique.

Les données à caractère personnel dites sensibles — par exemple, origine raciale ou ethnique, convictions religieuses ou philosophiques, appartenance syndicale, opinion politique — ne peuvent faire l'objet d'un traitement à des fins électorales par les partis politiques, les candidates et les candidats. Il est, par exemple, strictement interdit d'utiliser ces données pour identifier les membres d'une communauté culturelle afin de leur adresser une communication électorale personnalisée.

En règle générale, la précision des diverses données collectées tend à décroître au fil du temps. Comme le RGPD interdit de traiter des renseignements personnels erronés, les données inexactes ou incomplètes doivent être rectifiées ou complétées aussi rapidement que possible. Sinon, les partis politiques sont contraints de supprimer les données inexactes ou incomplètes en période électorale. En tout état de cause, toutes les données doivent être radiées des fichiers à l'expiration du délai fixé — autrement dit, à l'issue de l'élection pour laquelle ces données ont été obtenues.

Rôle et pouvoirs de l'autorité de surveillance

En Belgique, l'Autorité de protection des données (APD) est un organe de contrôle indépendant chargé de veiller au respect des principes fondamentaux de la protection des données à caractère personnel. L'APD est une entité fédérale disposant de la personnalité juridique. Depuis le 25 mai 2018, l'Autorité de protection des données est le successeur de la Commission de la protection de la vie privée.

Dans l'exercice de sa mission, l'APD veille au respect des principes fondamentaux de la protection des renseignements personnels. Elle surveille le traitement des données à caractère personnel et s'assure d'informer les personnes, les partis politiques ainsi que les autres instances concernées de leurs droits et obligations à cet égard. L'APD traite des réclamations, procède à des contrôles et peut également imposer des sanctions lorsque le RGPD n'est pas respecté.

Pour sa part, la Direction des élections du Service public fédéral intérieur de Belgique est responsable de l'organisation des élections et de l'application du droit électoral, mais n'est pas habilitée à contrôler la gouvernance des renseignements personnels par les partis politiques.

6.4.3 Luxembourg

Régime d'encadrement

Comme tous les pays membres de l'Union européenne, le Luxembourg est assujetti, depuis le 25 mai 2018, au RGPD. Les partis politiques ainsi que les candidates et les candidats à une élection sont ainsi tenus de respecter les exigences de ce règlement, en particulier les conditions d'utilisation des données issues des listes électorales[163].

Les élections législatives et communales sont déterminées, dans les grandes lignes, par la constitution et, dans le détail, par la loi électorale[164]. Les élections européennes sont uniquement régies par la loi électorale.

Renseignements fournis par l'administration électorale

Le collège des bourgmestres et des échevins de chaque commune est responsable de l'établissement et de la révision des listes d'électeurs, qui sont permanentes. Chaque année, durant dix jours, les listes actualisées sont affichées au secrétariat de la commune pour inspection par le public afin que les citoyennes et les citoyens puissent en valider le contenu et, au besoin, effectuer une demande de modification, d'inscription ou de suppression[165].

163. Commission nationale pour la protection des données (Luxembourg), *Prospection électorale et protection des données*, 21 août 2018. [https://cnpd.public.lu/fr/actualites/national/2018/08/communication-administres.html].

164. Luxembourg, *Recueil de la législation relative aux élections législatives, communales et européennes*, 21 juin 2018. [http://data.legilux.public.lu/file/eli-etat-leg-recueil-elections-20180625-fr-pdf.pdf].

165. Luxembourg, *Avis de dépôt des listes électorales à l'inspection du public*, 11 juillet 2018. [https://elections.public.lu/fr/actualites/2018/avis-depot.html].

Au Luxembourg, le vote est obligatoire pour toutes les électrices et tous les électeurs inscrits sur les listes électorales. Au cours du mois suivant la proclamation du résultat du scrutin, le procureur d'État dresse, par commune, le relevé des électrices et des électeurs qui n'ont pas pris part au vote et dont les raisons n'ont pas été admises. Depuis plusieurs années, il n'y a cependant aucune sanction pour les non-votants[166].

La loi électorale prévoit que « [t]out citoyen peut […] demander par écrit une copie des listes [électorales] actualisées […]. Les données des citoyens contenues dans les listes ne peuvent pas être utilisées à des fins autres qu'électorales[167] ».

Les données[168] contenues dans ces listes comprennent les informations suivantes sur les électrices et les électeurs :

- Prénoms et nom ;
- Domicile (adresse) ;
- Lieu et date de naissance ;
- Nom et prénoms du conjoint (le cas échéant) ;
- Nationalité (le cas échéant, pour les élections communales et européennes).

Les principales obligations à respecter[169]

L'établissement des listes des électrices et des électeurs constitue un traitement de données à caractère personnel. Cette opération est mise en œuvre par le collège des bourgmestres et échevins, qui est le responsable du traitement, conformément aux dispositions du RGPD.

La finalité du traitement est déterminée par la loi électorale, qui précise que les données des listes d'électeurs ne peuvent être utilisées qu'à des fins électorales.

Ces données permettent de constater la qualité d'électeur des personnes physiques satisfaisant les conditions de la loi électorale. Elles peuvent également être utilisées par des partis politiques pour des fins de communication politique pendant les périodes électorales.

Les partis politiques ont l'obligation de respecter les principes généraux en matière de protection des données énoncés dans le RGPD. Aussi, ils veillent à sécuriser de façon adéquate les données traitées, à vérifier leur exactitude ainsi qu'à établir une documentation adéquate — un registre — des traitements effectués.

Il convient de rappeler que la constitution du Luxembourg réserve aux partis politiques un rôle particulier dans le contexte électoral en reconnaissant qu'ils « concourent à la formation de la volonté populaire et à l'expression du suffrage universel[170] ». Ainsi, les partis politiques ainsi que les candidates et les candidats à une élection peuvent

166. David Marques, « Abstention : il n'y a plus de poursuites depuis 1964 », *Le Quotidien*, 23 novembre 2017. [http://www.lequotidien.lu/politique-et-societe/abstention-il-ny-a-plus-de-poursuites-depuis-1964/].

167. Luxembourg, *Recueil de la législation relative aux élections*, art. 20, p. 10.

168. *Ibid.*, art. 13-14, p. 9.

169. Ce texte est inspiré de : Commission nationale pour la protection des données (Luxembourg), *Prospection électorale et protection des données*.

170. *Constitution du Grand-Duché de Luxembourg*, art. 32bis. [http://legilux.public.lu/eli/etat/leg/recueil/constitution/20171020].

transmettre les programmes politiques aux électrices et aux électeurs sans obtenir leur consentement au préalable, et ce, dans les limites de la finalité électorale posée par la loi électorale.

En outre, si les candidates, les candidats et leurs partis politiques ont un souci légitime d'approcher les électrices et les électeurs et de leur exposer leurs programmes dans le cadre de leur campagne électorale, ils ne peuvent utiliser, à cette fin, des fichiers qu'ils se seraient procurés en dehors de toute base légale ou réglementaire auprès d'organismes publics. Sur ce point, le RGPD précise que la finalité d'un traitement de données est un principe essentiel dans le domaine de la protection des données : les renseignements personnels doivent être collectés uniquement pour des finalités déterminées, explicites et légitimes.

En l'occurrence, les données à caractère personnel des listes électorales doivent être utilisées licitement et ne doivent pas être traitées ultérieurement, de manière incompatible avec leur finalité électorale. Par exemple, elles ne peuvent pas faire l'objet d'une quelconque utilisation — notamment commerciale — incompatible avec la finalité électorale. Pour respecter le principe de limitation temporelle, les partis politiques sont invités à prévoir la durée de conservation des données des listes d'électeurs en fonction de la finalité recherchée ; ils devraient donc s'en départir quelques jours après l'élection.

Les associations à but non lucratif ne peuvent communiquer à des tiers la liste de leurs membres sans leur consentement. La prospection politique par téléphone, par courriel ou par tout autre moyen de communication numérique ne peut se faire qu'avec l'accord sans équivoque des personnes contactées.

Lorsqu'ils utilisent des données personnelles qui n'ont pas été collectées directement auprès des personnes concernées, les partis politiques ont l'obligation, de façon à respecter le principe d'information découlant du RGPD, de fournir, au plus tard au moment de la première communication, les informations suivantes aux personnes concernées :

- l'identité et les coordonnées de la personne responsable du traitement des données (le parti politique ou la section locale ou régionale du parti politique) ;
- l'origine des données traitées (les listes électorales, sur la base de la loi électorale) ;
- la finalité du traitement de données (la prospection politique, dans le cadre de l'élection) ;
- la durée de conservation des données (elles doivent être effacées dans un délai raisonnable après les élections) ;
- les droits des citoyennes et citoyens en matière de protection des données (leur droit d'accès aux données, leur droit de rectification et d'effacement des données, leur droit de s'opposer au traitement de leurs données à des fins de prospection électorale) ;
- les moyens disponibles pour exercer ces droits (adresse postale, lien vers un site Internet et adresse électronique).

Les partis politiques sont tenus d'éviter un profilage des citoyennes et citoyens qui serait disproportionné par rapport à la finalité électorale. Ils doivent notamment éviter de rapprocher le contenu des listes électorales avec des données des électrices et des électeurs provenant d'autres fichiers. Ils peuvent effectuer des opérations de tri et de sélection sur les listes, en fonction de l'âge ou de l'adresse des électeurs, par exemple, mais pas sur la base de leurs origines réelles ou supposées (notamment par la consonance des noms ou le lieu de naissance), conformément au RGPD. Toute discrimination des personnes, notamment sur la base de distinctions fondées sur l'origine, le genre ou l'appartenance ou la non-appartenance, vraie ou supposée, à une ethnie, une nation, une race ou une religion déterminée, peut faire l'objet d'une infraction.

Rôle et pouvoirs de l'autorité de surveillance

La Commission nationale pour la protection des données (CNPD) est l'autorité de régulation de la protection des renseignements personnels qui est responsable de veiller à l'application des dispositions du RGPD.

En période électorale, ses actions ont pour but d'inciter les partis politiques, les candidates et les candidats à mettre en place les mesures de gouvernance appropriées pour se conformer aux exigences du RGPD.

La mission de la CNPD consiste à contrôler et à vérifier la légalité de la collecte et de l'utilisation des données, à veiller au respect des libertés et des droits fondamentaux des personnes et à examiner les plaintes. Elle peut effectuer des enquêtes et imposer des sanctions administratives.

6.5 Suisse

Régime d'encadrement

La *Constitution fédérale de la Confédération suisse* fixe le principe selon lequel toute personne a droit au respect de sa vie privée et familiale, de son domicile, de sa correspondance et des relations qu'elle établit par la poste et par les télécommunications, ainsi qu'à la protection contre l'emploi abusif des données qui la concernent[171].

Cette protection est inscrite dans la *Loi fédérale sur la protection des données*[172], en vigueur depuis 1993. L'ordonnance correspondante en règle les détails[173]. D'autres lois contiennent de nombreuses dispositions relatives à la protection de la personnalité dans des domaines particuliers.

171. *Constitution fédérale de la Confédération suisse* du 18 avril 1999, art. 13. [https://www.admin.ch/opc/fr/classified-compilation/19995395/index.html#a13].
172. *Loi fédérale sur la protection des données* du 19 juin 1992. [https://www.admin.ch/opc/fr/classified-compilation/19920153/index.html].
173. *Ordonnance relative à la loi fédérale sur la protection des données* du 14 juin 1993. [https://www.admin.ch/opc/fr/classified-compilation/19930159/index.html].

Les partis politiques — au même titre que les particuliers et que les organes fédéraux — sont soumis à cet encadrement juridique pour la collecte et l'exploitation des renseignements personnels des électrices et des électeurs, comme de toute personne physique et morale.

Depuis 2008, la Suisse a intégré l'espace Schengen de l'Union européenne, sans signer d'accord pour une union douanière. Cet accord d'association avec l'Union européenne permet la libre circulation des personnes aux frontières intérieures communes, mais n'a pas de répercussions sur les activités réglementaires et législatives relatives à la circulation des marchandises et des données. La Suisse n'est donc pas assujettie au *Règlement général sur la protection des données* (RGPD) de l'Union européenne.

Néanmoins, l'échange de données avec l'Union européenne est astreint à un niveau de protection équivalent aux législations suisses et européennes en matière de protection des données[174]. La Suisse a engagé des travaux en vue d'actualiser et de renforcer son encadrement normatif au cours de l'année 2019 et de se rapprocher des exigences du RGPD en protégeant mieux les personnes contre les mauvais usages de leurs renseignements personnels.

Renseignements fournis par l'administration électorale

En Suisse, le peuple élit directement ses représentants, à l'Assemblée fédérale comme dans les parlements et les gouvernements cantonaux. Les modalités et les dates des élections varient selon les cantons. Seul le Conseil fédéral, qui constitue le pouvoir exécutif, n'est pas élu directement par le peuple ; ses sept membres sont élus par les députées et députés de l'Assemblée fédérale, qui représente le pouvoir législatif.

Les électrices et les électeurs domiciliés en Suisse sont automatiquement inscrits dans le registre électoral[175] de la commune de leur domicile dès qu'ils remplissent les conditions requises. Ce registre est tenu à jour et il peut être consulté par toute électrice ou tout électeur[176].

Les inscriptions et les radiations à cette liste sont opérées d'office. Les demandes d'inscription en vue d'une élection ou d'un vote sont acceptées jusqu'au cinquième jour qui précède le jour fixé pour l'élection ou le vote, s'il est établi que les conditions permettant de participer au scrutin seront remplies ce jour-là.

174. Office fédéral de la justice (Suisse), *Esquisse d'acte normatif : rapport du groupe d'accompagnement à la révision de la loi sur la protection des données,* 29 octobre 2014. [https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-f.pdf].

175. En Suisse, le *registre électoral* ou le *registre des électeurs* est la liste des personnes ayant le droit de vote lors d'une élection. La *liste électorale*, elle, présente la liste des candidates et des candidats proposés par un parti politique dans un système électoral de représentation à caractère proportionnel avec scrutin de listes. On doit éviter de confondre ces deux concepts.

176. *Loi fédérale sur les droits politiques* du 17 décembre 1976, art. 4. [https://www.admin.ch/opc/fr/classified-compilation/19760323/index.html].

La commune inscrit au registre électoral[177] les données suivantes pour chaque personne qui jouit de l'exercice des droits politiques :

- nom et prénoms officiels ;
- date de naissance ;
- commune et canton ou pays d'origine ;
- sexe ;
- adresse ;
- date du dépôt des documents de légitimation ;
- paliers électifs (fédéral, cantonal et communal) dans lesquels la personne est autorisée à voter ;
- langue de réception du matériel de vote.

En période électorale, les différents partis politiques peuvent s'adresser aux communes pour obtenir une copie du registre des électrices et des électeurs. Sous certaines conditions, les communes sont libres de communiquer ou même de vendre des informations sur leurs habitants, notamment à des groupements à but politique ou au profit d'associations[178]. Dans le canton de Fribourg, cependant, le registre des électeurs est uniquement accessible pour en vérifier l'exactitude ; les partis politiques ne sont pas autorisés à l'utiliser pour leurs communications électorales.

Les citoyennes et les citoyens peuvent demander de préserver leurs données confidentielles. Toute personne a le droit de s'opposer à ce que les renseignements personnels la concernant soient communiqués par les communes.

Quand les communes refusent de transmettre le registre des électrices et des électeurs, les partis politiques ou les associations ont recours à des sociétés tierces qui recueillent des données sur Internet. Ils peuvent utiliser ces données pour communiquer avec les citoyennes et les citoyens des communes qui ne souhaitent pas donner leur adresse ou tout autre renseignement personnel.

177. *Règlement sur l'exercice des droits politiques* du 10 juillet 2001, art. 2. [http://www.lexfind.ch/dta/4528/3/115.11.pdf].

178. Pauline Vrolixs, « Les communes hésitent peu à donner l'adresse de leurs électeurs aux partis », *Radio Télévision Suisse*, 22 octobre 2015. [https://www.rts.ch/info/suisse/7191163-les-communes-hesitent-peu-a-donner-l-adresse-de-leurs-electeurs-aux-partis.html].

Les principales obligations à respecter

La *Loi sur la protection des données* a été adoptée dans le contexte où le recours aux technologies modernes d'information et de communication, dans presque tous les domaines de la vie courante, et l'intensification massive du traitement et de la diffusion des données ont fortement amplifié les risques d'atteinte à la personnalité[179].

L'évolution technologique constitue un véritable défi pour le législateur suisse, puisqu'elle entraîne une multiplication des traitements de données transfrontaliers, qui sont peu transparents. Lorsque des renseignements personnels sont divulgués, c'est toujours plus difficile d'en conserver le contrôle.

Les trois objectifs principaux de la *Loi* se déclinent comme suit : protéger la vie privée et familiale contre les atteintes ; protéger de façon spécifique les informations concernant l'exercice des droits fondamentaux ; et empêcher qu'un individu ne soit réduit à l'état de simple objet d'information (il doit pouvoir déterminer l'image et les informations que son environnement aura de lui)[180].

La Suisse n'a pas édicté de loi pour réglementer les campagnes consacrées à des élections ou à des votes lors de référendums. Elle accorde en effet une grande importance à la liberté d'expression et d'opinion[181]. Le droit en vigueur s'applique aux réseaux sociaux et à Internet. Bien des actions sont permises durant les campagnes électorales ; par exemple, il n'est pas interdit de divulguer délibérément des informations qui ne sont pas toujours avérées et qui s'apparentent à de la désinformation[182].

Néanmoins, après un scrutin, tous les fichiers de renseignements personnels collectés par les partis politiques doivent être effacés, parce que ces renseignements avaient une finalité déterminée et une durée de conservation limitée. Ces principes sont énoncés dans la *Loi fédérale sur la protection des données*.

Comme la Suisse est le pays où les citoyennes et les citoyens se rendent le plus souvent aux urnes, soit en moyenne quatre fois par année, il est prévu — pour donner suite à la phase d'expérimentation en cours — que les citoyens seront en mesure de voter par un moyen électronique (dans les deux tiers des cantons) en 2019. Le vote électronique

179. En Suisse, on utilise l'expression *atteinte à la personnalité* lors de manquements à certaines dispositions du *Code civil* relatives à la protection de la personnalité, laquelle porte sur l'ensemble des valeurs essentielles, physiques, affectives et sociales, liées à la personne dans toute sa dimension humaine comme le respect de la vie privée, l'honneur, l'intégrité corporelle, la liberté de mouvement, la protection des données personnelles, etc. Voir ARTIAS, « Protection de la personnalité », *Guide social romand* (https://www.guidesocial.ch/recherche/fiche/protection-de-la-personnalite-125).

180. Conseil fédéral suisse, *Rapport du Conseil fédéral sur l'évaluation de la loi fédérale sur la protection des données*, 9 décembre 2011. [https://www.admin.ch/opc/fr/federal-gazette/2012/255.pdf].

181. Confédération Suisse, *Prescriptions régissant les campagnes électorales et les votations.* [https://www.ch.ch/fr/democratie/les-partis-politiques/regles-pour-la-publicite-des-partis-en-suisse/].

182. Des représentants de l'Organisation des Nations unies ont écrit au gouvernement suisse pour le sommer de s'exprimer sur une campagne tendancieuse. Le ministre suisse de l'Intérieur avait répondu qu'il « revient au peuple de juger ces pratiques, et le cas échéant de les sanctionner au travers des processus démocratiques ». Voir Cristina Del Biaggio, « L'UDC, des moutons noirs aux rangers », *Le Monde diplomatique*, 18 octobre 2011. [https://blog.mondediplo.net/2011-10-18-L-UDC-des-moutons-noirs-aux-rangers].

constituera le troisième canal de vote ordinaire, en plus du vote aux urnes et du vote par correspondance[183]. Les électrices et les électeurs choisiront librement leur lieu et leur mode de votation.

Dans cette perspective, la confiance est indispensable pour l'exercice des droits politiques. Les spécialistes de la protection des renseignements personnels ont appelé à une vigilance accrue contre les dangers du vote électronique, montrant du doigt la vulnérabilité d'un dispositif avec des failles ou des dysfonctionnements techniques pouvant porter atteinte à l'intégrité du système de votation et conduire à une exploitation malveillante, ce qui risquerait d'interférer avec le secret du vote ou d'occasionner une collecte non consentie de données et de renseignements personnels[184].

De manière à respecter les droits des citoyennes et des citoyens et à assurer un contrôle démocratique sur les opérations électorales, les autorités suisses ont choisi un système de vote électronique satisfaisant les exigences les plus élevées en matière de sécurité et concrétisant le principe de la vérifiabilité individuelle (chaque électeur peut s'assurer que son vote a bien été transmis à l'urne officielle sans que ses choix aient été modifiés) et universelle (des observateurs peuvent contrôler si les votes ont été enregistrés correctement). En fonction de ces exigences, les systèmes de votation doivent être non propriétaires et multiplateformes et leur code source doit être ouvert.

Des modifications à la loi fédérale sur les droits politiques et à celle sur la protection des données s'avèrent nécessaires, selon les experts, en vue d'y inscrire explicitement ces exigences de sécurité. Ainsi, les électrices et les électeurs suisses seront en mesure de voter électroniquement sans crainte d'un accès non autorisé à leurs renseignements personnels ou d'une manipulation malintentionnée[185].

Le recours à des systèmes de vote électronique en Suisse doit s'inscrire dans le respect des principes fondamentaux que requièrent les opérations électorales, à savoir : le caractère personnel, libre et anonyme de l'expression du suffrage ; le secret du scrutin ; la légitimité des opérations électorales ; la surveillance effective du vote ; et le contrôle *a posteriori* par les instances responsables de l'élection.

Rôle et pouvoirs de l'autorité de surveillance

Le préposé fédéral à la protection des données et à la transparence exerce ses compétences dans deux domaines : celui de la *Loi fédérale sur la protection des données* et celui de la *Loi fédérale sur le principe de la transparence dans l'administration* (communément appelée *loi sur la transparence*).

Le préposé défend la sphère privée en sa qualité de préposé fédéral à la protection des données. Il conseille et renseigne les particuliers, les organes fédéraux et les cantons dans le domaine de la protection des données. Il exerce une surveillance, à des degrés divers, sur les données traitées par les organes fédéraux, les particuliers,

183. Confédération Suisse, *Faire du vote électronique un canal de vote ordinaire : le Conseil fédéral projette d'ouvrir une consultation en automne 2018,* 27 juin 2018. [https://biblio.parlament.ch/e-docs/394980.pdf].

184. *Ibid.*

185. *Ibid.*

les organisations et les partis politiques. À cet effet, le préposé peut procéder à des vérifications et, en cas de violation des dispositions légales, recommander que certaines données soient traitées différemment ou ne le soient plus du tout.

Le préposé fédéral à la protection des données et à la transparence ne peut sanctionner lui-même une violation du droit lié à la protection des renseignements personnels qu'il constaterait par une enquête, ni le non-respect de ses propres décisions contraignantes. Confronté à de telles situations, il doit dénoncer l'affaire au Ministère public de la Confédération afin d'enclencher une procédure pénale.

Chaque canton nomme une préposée cantonale ou un préposé cantonal à la protection des données, qui est l'interlocuteur de l'administration et du public. Afin de favoriser la coopération entre les cantons, les communes et la Confédération ainsi que l'échange continu d'information et une utilisation plus efficiente des ressources, une nouvelle instance de concertation a été créée : le privatim, ou la Conférence des préposé(e)s suisses à la protection des données.

6.6 Royaume-Uni

Régime d'encadrement

Au Royaume-Uni, le *Data Protection Act*[186] a été adopté pour mettre en œuvre le RGPD et remplacer le *UK Data Protection Act*[187]. Les partis politiques britanniques sont assujettis à cette nouvelle loi régissant la protection des renseignements personnels et sont tenus de respecter les mêmes obligations que les partis politiques européens[188].

Cette législation fixe également le cadre de la protection des renseignements personnels en permettant au Royaume-Uni de préparer son avenir à l'extérieur de l'Union européenne. Dans cette perspective, le gouvernement britannique a apporté quelques modifications complémentaires[189] visant à renforcer[190] le pouvoir d'enquête, de contrainte et de poursuite du commissaire à l'information (Information Commissioner's Office), mais aussi à mettre en place des dispositions particulières pour le traitement des données par les corps policiers et par les services de renseignement, afin qu'ils soient en mesure de faire face aux menaces d'atteinte à la sécurité nationale.

En s'alignant sur le RGPD, le Royaume-Uni espère construire un mécanisme amélioré de protection des données qui dépasse le modèle d'adéquation que l'Union européenne impose aux pays tiers, ce qui permettra aux données personnelles de circuler librement entre le Royaume-Uni et l'Union européenne à la suite du Brexit[191].

---

186. *Data Protection Act*, 2018, chap. 12. [https://services.parliament.uk/bills/2017-19/dataprotection.html].
187. *UK Data Protection Act*, 1998, chap. 29. [https://www.legislation.gov.uk/ukpga/1998/29/contents].
188. Information Commissioner's Office, *Elected Representatives and Political Parties*. [https ://ico.org.uk/for-organisations/political/].
189. Information Commissioner's Office, *An Introduction to the Data Protection Bill*. [https://ico.org.uk/media/for-organisations/documents/2258303/ico-introduction-to-the-data-protection-bill.pdf].
190. Information Commissioner's Office, *Preparing for the Law Enforcement Requirements (part 3) of the Data Protection Act 2018: 12 Steps to Take Now*. [https://ico.org.uk/media/for-organisations/documents/2014918/dp-act-12-steps-infographic.pdf].
191. Blogue Droit européen, *Brexit or not Brexit: How Will the GDPR Rules Apply to the UK?*. [https://blogdroiteuropeen.com/2017/03/01/brexit-or-not-brexit-how-will-the-gdpr-rules-apply-to-the-uk-part-1/].

Aussi longtemps que le Royaume-Uni restera membre de l'Union européenne, tous les droits et obligations qui découlent du droit de l'Union européenne resteront en vigueur. Lorsque le Royaume-Uni quittera l'Union européenne, les exigences du RGPD seront déjà intégrées dans la législation nationale du Royaume-Uni et dans le projet de loi sur le retrait de l'Union européenne. Le traité de retrait conclu en novembre 2018 doit être ratifié par le Parlement européen et le Parlement britannique avant d'entrer en vigueur le 29 mars 2019.

Opérations électorales

Diverses lois, dont l'*Electoral Administration Act*[192] et le *Political Parties and Elections Act*[193], précisent l'encadrement pour la tenue des élections et des référendums au Royaume-Uni ainsi que les règles auxquelles sont assujettis les partis politiques.

Depuis sa création en 2000, la commission électorale (Electoral Commission) joue un rôle déterminant dans l'organisation et l'encadrement des élections au Royaume-Uni. Elle est notamment responsable du respect des règles de financement des partis politiques, de l'évaluation des opérations électorales, de la formulation de politiques, de la conduite de recherches, de l'exercice de veille stratégique et de la prospective. Cette commission s'est imposée comme une source d'expertise en droit électoral et elle dispose de pouvoirs de recommandation, d'enquête, de sanction et de poursuite. La responsabilité des opérations électorales relève toutefois des agentes et agents nommés par les autorités locales.

Le commissaire à l'information est habilité à encadrer la gouvernance des partis politiques au regard des renseignements personnels des électrices et des électeurs. En 2018, il a produit un rapport sur l'utilisation des renseignements personnels à des fins politiques, dans lequel il a recommandé au gouvernement d'adopter un encadrement législatif sur l'utilisation des renseignements personnels en période électorale[194]. Le commissaire a également mené une enquête sur le rôle de Cambridge Analytica lors de la campagne du Brexit[195]. Cette procédure a conduit le commissaire à imposer une amende de 500 000 livres à Facebook[196].

Au Royaume-Uni, le registre des électrices et des électeurs répertorie toutes les personnes autorisées à voter. Ce registre se décline en deux versions : une liste électorale complète et une liste électorale ouverte[197].

---

192. *Electoral Administration Act*, 2006, chap. 22. [https://www.legislation.gov.uk/ukpga/2006/22/contents].
193. *Political Parties and Elections Act*, 2009, chap. 12. [https://www.legislation.gov.uk/ukpga/2009/12/contents].
194. Information Commissioner's Office, *Democracy Disrupted? Personal Information and Political Influence*, 2018, p. 44. [https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf].
195. Information Commissioner's Office, *Investigation into the Use of Data Analytics in Political Campaigns – Investigation Update*, 11 juillet 2018. [https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf].
196. Information Commissioner's Office, *The ICO Has Fined Facebook £500,000 for Serious Breaches of Data Protection Law*. [https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf].
197. Information Commissioner's Office, *Electoral Register*. [https://ico.org.uk/your-data-matters/electoral-register/].

La liste électorale complète est communiquée aux partis politiques et aux autorités compétentes pour les opérations électorales ; aux corps policiers et aux services de renseignements pour la prévention de la criminalité ; aux tribunaux pour la convocation d'un jury ; ainsi qu'aux agences de solvabilité financière. C'est la loi qui en limite l'usage et elle interdit d'en détenir un exemplaire pour une autre finalité.

La liste électorale complète contient les renseignements suivants pour toutes les électrices et tous les électeurs :

- Prénoms ;
- Nom ;
- Adresse.

La liste électorale ouverte contient les mêmes renseignements que la liste électorale complète et toute personne souhaitant en avoir un exemplaire peut l'acheter, et ce, peu importe la finalité. Par contre, une électrice ou un électeur peut, lorsqu'il s'inscrit à la liste électorale, demander que ses renseignements ne soient pas inclus dans la liste électorale ouverte.

Les autorités compétentes britanniques, dont le commissaire à l'information, la commission électorale et les associations d'administrateurs d'élections locales, ont recommandé que le registre des électrices et des électeurs soit exclusivement utilisé pour les élections et les référendums[198]. Ils sont d'avis que la vente des renseignements personnels des électrices et des électeurs est une pratique qui peut démotiver une citoyenne ou un citoyen à s'inscrire pour voter[199]. Le gouvernement britannique a rejeté cette proposition et a décidé de maintenir les règles et les pratiques existantes[200].

6.7 Synthèse

Le tableau 4 résume les principaux éléments décrits dans ce chapitre. Il indique, pour chacun des pays étudiés, si les partis politiques sont assujettis à une loi générale en matière de protection des renseignements personnels ; et il décrit les renseignements inscrits sur les listes électorales, les modalités de transmission et de conservation ainsi que les entités qui peuvent accéder aux listes électorales. Les indications sur le Québec sont incluses à des fins de comparaison.

198. House of Commons, Political and Constitutional Reform Committee, *The Government's Proposals on Individual Electoral Registration and Electoral Administration, Written Evidence*, 2011. [https://publications.parliament.uk/pa/cm201012/cmselect/cmpolcon/writev/1463/1463.pdf].

199. House of Commons Library, *Note for the Members of Parliament, Supply and Sale of the Electoral Register*, 12 août 2014. [http://researchbriefings.files.parliament.uk/documents/SN01020/SN01020.pdf].

200. Parliament of the United Kingdon, *Electoral Registration and Administration Bill, Explanatory Notes*, 29 juin 2012. [https://publications.parliament.uk/pa/bills/lbill/2012-2013/0033/en/2013033en.htm].

Tableau 4 – Synthèse de l'encadrement à l'extérieur du Canada

	États-Unis	Australie	Nouvelle-Zélande	France	Belgique	Luxembourg	Suisse	Royaume-Uni	Québec
Partis politiques assujettis à un encadrement normatif sur la protection des renseignements personnels									
			X	X	X	X	X	X	
Type de renseignements inscrits sur les listes électorales									
Nom	X	X	X	X	X	X	X	X	X
Adresse	X	X	X	X	X	X	X	X	X
Date de naissance	X			X	X	X	X		X
Groupe d'âge			X						
Sexe					X		X		X
Lieu de naissance	X			X		X	X		
Origine ethnique	Selon l'État		Si Maori						
Profession			X						
Nom du conjoint						X	X		
Courriel	X								
Allégeance politique	X								
Fréquence de transmission des listes électorales aux partis politiques									
	Période électorale	Période électorale	Période électorale	Annuelle	Période électorale	Annuelle	Période électorale	Annuelle	Trois fois par année
Durée de conservation des listes électorales par les partis politiques									
	Aucune limite	Aucune limite	Aucune limite	Période électorale	Période électorale	Période électorale	Aucune limite	Aucune limite	Aucune limite
Accès aux listes électorales									
Partis politiques et candidats	X	X	X	X	X	X	X	X	X
Députés	X	X	X	X	X	X	X	X	X
Électeurs	X		X	X		X	X	X	
Chercheurs	X		X	X			X	X	X[a]
Organismes sans but lucratif	X						X	X	
Entreprises (usage commercial)	Selon l'État							X	

a. Au Québec, l'article 570 de la *Loi électorale* prévoit que le directeur général des élections peut accorder une autorisation de communiquer des renseignements personnels à des fins d'étude, de recherche ou de statistiques, sous certaines conditions.

EN BREF

L'examen des législations électorales et des systèmes normatifs de protection des renseignements personnels de certains pays montre que les approches réglementaires sont diverses et contrastées. Les modes de gouvernance des autorités électorales et des partis politiques oscillent entre un usage responsable et une utilisation souple des renseignements personnels des électrices et des électeurs.

L'observation de la situation en Nouvelle-Zélande, en France, en Belgique, au Luxembourg, en Suisse et au Royaume-Uni démontre que les partis politiques et les candidates et candidats à une élection — ainsi que toutes les organisations qui collectent et exploitent des données — sont pleinement responsables et doivent encadrer la protection des renseignements personnels et de la vie privée des électrices et des électeurs. En revanche, aux États-Unis et en Australie, les partis politiques ne sont pas tenus de respecter les mêmes principes, réglementations et pratiques que ceux auxquels sont soumises les organisations privées et publiques.

Au sein de l'Union européenne, le *Règlement général sur la protection des données* (RGPD) s'applique à l'ensemble des organisations privées, des administrations publiques, des mouvements associatifs et des partis politiques. Dans le but d'harmoniser les législations nationales européennes et de les faire évoluer pour tenir compte des usages numériques, le RGPD réitère, actualise et opérationnalise les principes de protection existants. Il renforce les obligations des responsables de la collecte et du traitement des données tout en instaurant les modalités de gouvernance appropriées. Il réaffirme les droits des individus en vigueur et en consacre de nouveaux pour leur donner une véritable capacité d'agir. Il accentue les compétences des autorités de régulation et prévoit des sanctions graduelles en cas de manquement aux exigences réglementaires.

En comparant les obligations des partis politiques sous le RGPD et celles qui prévalent au Québec et au Canada, on constate que les renseignements personnels des électrices et des électeurs d'Europe qui sont inscrits sur les listes électorales sont diversifiés et détaillés et que ces listes sont accessibles à davantage de personnes. L'encadrement est tout de même plus rigoureux : les listes doivent être détruites après les élections et l'électeur maîtrise mieux le traitement de ses données.

À des degrés divers, tous ces pays ont amorcé une réflexion sur l'encadrement et la responsabilisation des partis politiques. Dans cette perspective, les listes électorales suscitent des interrogations, notamment quant au type de renseignements personnels qu'elles comportent, à la fréquence de leur transmission aux partis politiques, à la durée de leur conservation et à leur accessibilité aux électrices, aux électeurs et aux organisations qui en demandent un exemplaire.

7 Enjeux et recommandations

Dans les chapitres précédents, nous avons présenté les façons dont les partis politiques utilisent les renseignements personnels sur les électrices et les électeurs ainsi que l'encadrement applicable à ces pratiques au Canada et ailleurs dans le monde. Nous aborderons maintenant les principaux enjeux soulevés par ces pratiques et par l'encadrement actuel au Québec. Nous proposerons également des recommandations afin de répondre à ces enjeux.

7.1 Les enjeux

Les attentes des électrices et des électeurs à l'égard de leur vie privée

L'encadrement des partis politiques en matière de protection des renseignements doit être examiné selon le point de vue des électrices et des électeurs, qui sont les principales personnes concernées par ces renseignements. Si les électeurs pouvaient juger, à une certaine époque, qu'il était approprié d'afficher les listes électorales dans des endroits publics, il semble qu'ils sont aujourd'hui davantage préoccupés par la protection de leur vie privée.

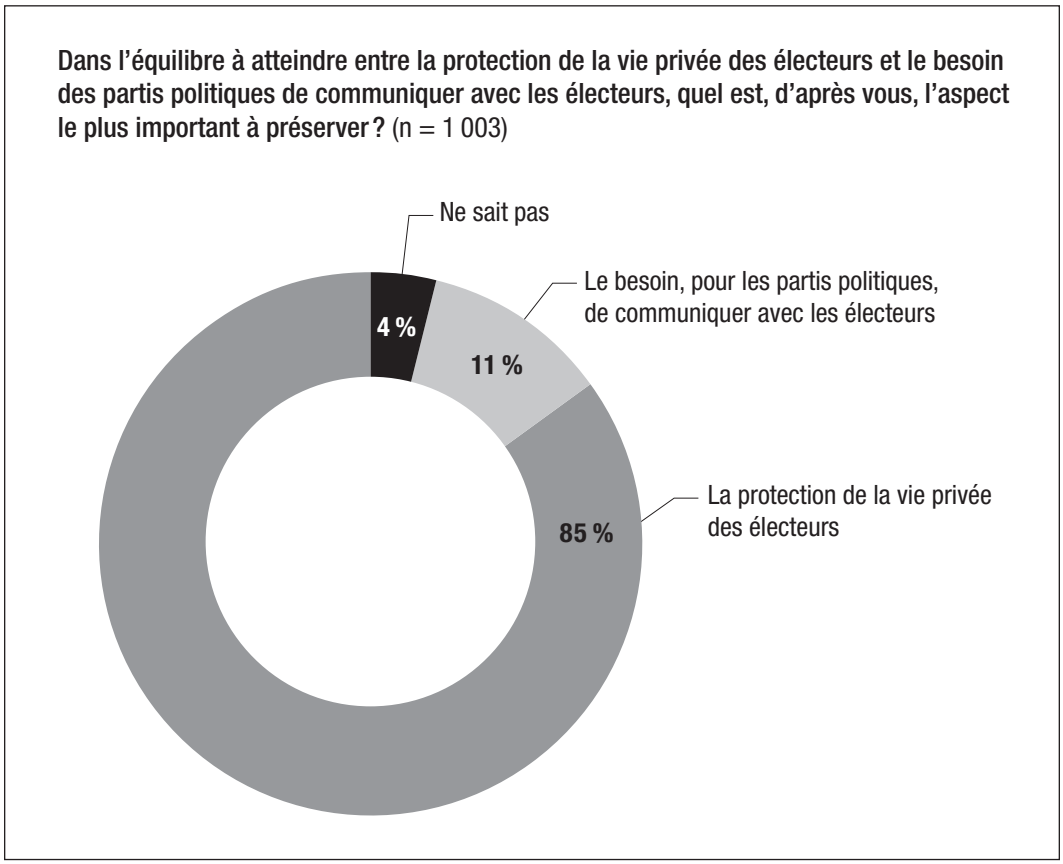
Le directeur général des élections a voulu mesurer la perception des citoyens en matière de communication des partis politiques avec les électrices et les électeurs[201] à l'aide d'un sondage réalisé après les élections générales provinciales du 1er octobre 2018[202].

La figure 1, à la page suivante, nous permet de constater que la grande majorité des répondantes et des répondants (85 %) sont d'avis que la protection de la vie privée des électeurs doit avoir préséance sur le besoin des partis politiques de communiquer avec eux.

201. BIP Recherche, *Évaluation de la satisfaction des citoyens du Québec à la suite des élections générales du 1er octobre 2018*. [https://www.pes.electionsquebec.qc.ca/services/set0005.extranet.formulaire.gestion/ouvrir_fichier.php?d=1999].

202. Ce sondage a été effectué par téléphone, du 2 au 23 octobre 2018, auprès de 1003 personnes ayant la qualité d'électeur au Québec.

Figure 1 – Équilibre entre la protection de la vie privée des électrices et des électeurs et le besoin des partis politiques de communiquer avec eux[203]



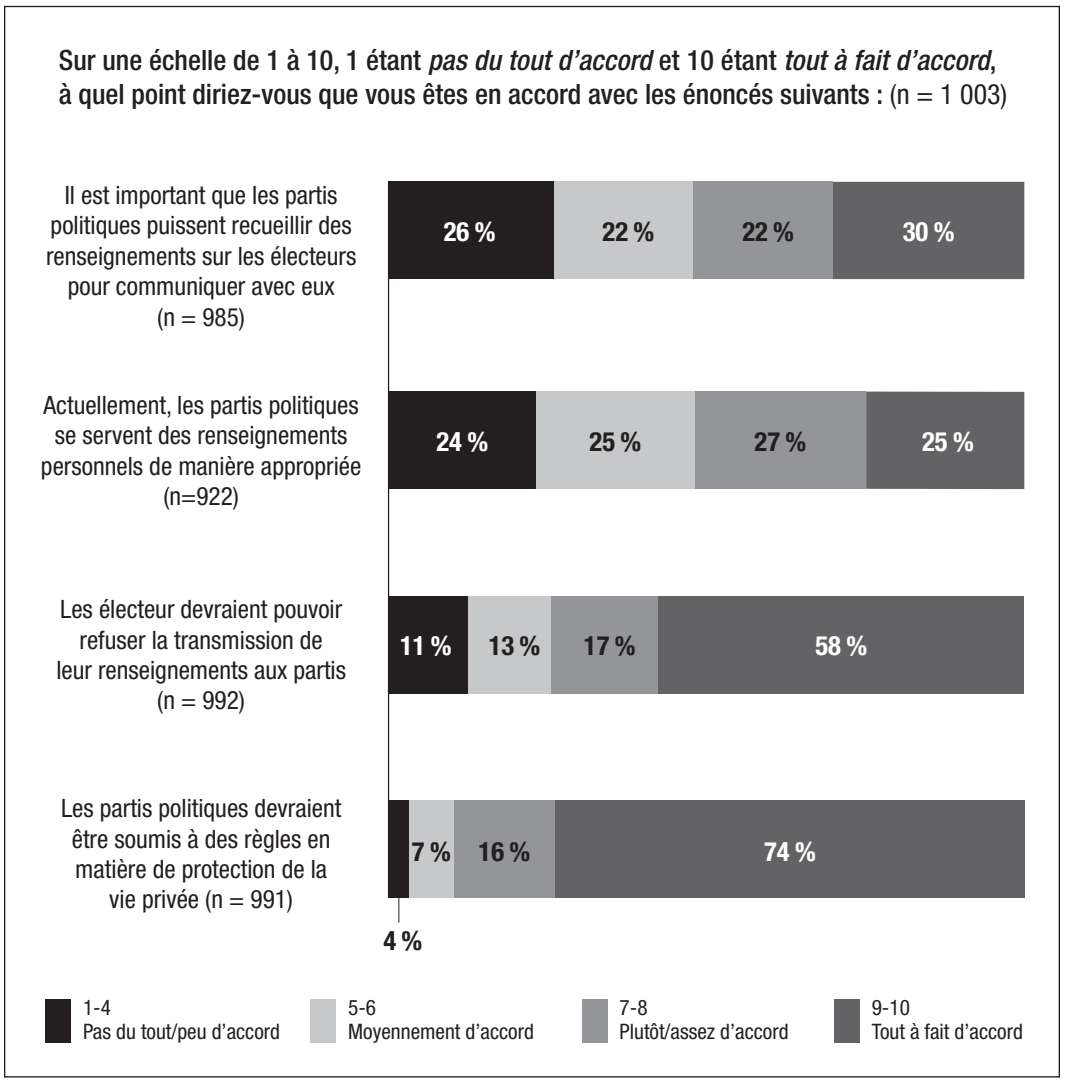
La figure 2 décrit la perception des citoyens quant aux pratiques des partis politiques en matière de protection des renseignements personnels. Pas moins de 52 % des répondantes et des répondants estiment qu'il est important que les partis politiques puissent recueillir des renseignements sur les électrices et les électeurs pour communiquer avec eux. Une proportion semblable croit que les partis politiques se servent des renseignements personnels de manière appropriée.

Les électrices et les électeurs souhaitent garder un certain contrôle de leurs renseignements personnels. En effet, les trois quarts des répondants jugent que les électeurs doivent pouvoir refuser que leurs renseignements personnels soient transmis aux partis politiques.

Ce sondage révèle également que 90 % des répondantes et des répondants souhaitent que les partis politiques soient soumis à des règles en matière de protection de la vie privée.

203. BIP Recherche, *Évaluation de la satisfaction des citoyens du Québec à la suite des élections générales du 1er octobre 2018*, p. 50. [https://www.pes.electionsquebec.qc.ca/services/set0005.extranet.formulaire.gestion/ouvrir_fichier.php?d=1999].

Figure 2 – Communication des partis avec les électrices et les électeurs et protection des renseignements[204]



Cette mesure de la perception de l'électorat se rapproche des constats qui découlaient d'un sondage similaire réalisé pour le compte d'Élections Canada en 2013 :

> « Dans une proportion avoisinant les quatre cinquièmes (78 %), les répondants se disent d'avis que les électeurs rejoints par un parti ou un candidat devraient avoir le droit de se retirer de toutes nouvelles communications de la part de ce parti ou de ce candidat. De plus, la majorité des électeurs interrogés (69 %) ne sont pas d'accord avec le point de vue à l'effet qu'il est important que les partis politiques fédéraux puissent recueillir des renseignements personnels sur les électeurs. Le droit à la vie privée et la protection des renseignements personnels revêtent de l'importance pour les électeurs : près du tiers (32 %) estiment que les partis politiques fédéraux et les candidats ne se servent pas

204. *Ibid.*, p. 49.

> des renseignements personnels de manière appropriée pour communiquer avec les électeurs. Il ne faut donc pas se surprendre que, dans le compromis entre la préservation de la vie privée d'un électeur et le besoin des partis politiques et des candidats de pouvoir communiquer avec les électeurs, près des deux tiers des répondants sont d'avis que la vie privée doit toujours avoir la primauté (53 %) ou encore, qu'elle doit avoir la primauté la plupart du temps (13 %).[205] »

La Table citoyenne « est un espace de réflexions et de discussions mis sur pied en 2017[206] » par le directeur général des élections. Elle est composée de douze électrices et électeurs qui ont le « mandat de […] donner leur opinion, de façon impartiale et non partisane, sur des questions se rapportant au système électoral québécois[207] ». La Table citoyenne s'est également prononcée sur la protection des renseignements personnels détenus par les partis politiques. Lors d'une rencontre tenue en novembre 2018, les membres se sont dits surpris par la situation actuelle au Québec, notamment par « le peu d'encadrement régissant les pratiques des partis politiques et des personnes candidates en matière d'utilisation et de protection des renseignements personnels[208] ».

Les membres ont notamment exprimé un malaise quant à l'existence de bases de données électorales et aux stratégies clientélistes qui découlent du microciblage des électrices et des électeurs par les partis politiques[209].

À la suite des recommandations précédemment formulées par le directeur général des élections, dans ses rapports annuels de gestion, quant à la nature des renseignements transmis aux partis politiques et aux personnes candidates, les membres estiment que « les partis politiques n'ont pas besoin de connaître le sexe des électeurs [et que] [l]a date de naissance est […] une information jugée trop sensible pour être fournie[210]. »

Les droits des personnes à l'égard de leurs renseignements personnels

Les principes reconnus en matière de protection des renseignements personnels accordent certains droits aux personnes à l'égard des renseignements qui les concernent, notamment celui de consentir à la collecte, à l'utilisation et à la communication ainsi que le droit d'être informé des finalités des renseignements et des mesures mises en place pour protéger leur caractère confidentiel. Le droit des personnes concernées d'avoir accès aux renseignements qu'une organisation détient à leur sujet et de contester le non-respect des principes par cette organisation fait également partie des principes reconnus.

---

205. Phoenix Strategic Perspectives, *Sondage auprès des électeurs au sujet des communications avec les électeurs : rapport rédigé pour le compte d'Élections Canada*, mars 2013, p. 7. [http://www.elections.ca/res/cons/sece/sece_f.pdf].
206. Élections Québec, *Table citoyenne*. [https://www.electionsquebec.qc.ca/francais/a-propos-de-nous/table-citoyenne.php].
207. *Ibid.*
208. Élections Québec, *Compte rendu de la rencontre de la Table citoyenne tenue le vendredi 16 novembre 2018*, p. 11. [https://www.electionsquebec.qc.ca/documents/pdf/table_citoyenne/compte_rendu_TC_2018-11-16.pdf].
209. *Ibid.*, p. 12
210. *Ibid.*, p. 14.

Au Québec, une électrice ou un électeur bien informé peut savoir que le directeur général des élections communique les renseignements inscrits à son sujet sur la liste électorale permanente aux partis politiques, aux députées et députés ainsi qu'aux candidates et candidats. Cette personne n'a, toutefois, aucune possibilité de s'opposer à cette transmission autrement qu'en demandant à ne plus être inscrite sur les listes électorales provinciales ou d'être radiée de la liste électorale permanente. Elle devrait alors, si elle souhaite exercer son droit de vote, s'inscrire sur la liste électorale à chaque élection en se présentant devant une commission de révision. Cela n'empêcherait toutefois pas les partis politiques, les candidates et les candidats d'obtenir ses renseignements personnels en période électorale, puisqu'ils reçoivent également la liste électorale produite après la révision.

Cet exemple met en lumière le fait que l'électrice ou l'électeur québécois exerce peu de contrôle sur les renseignements personnels que les partis politiques détiennent à son sujet. En effet, il ne dispose d'aucun moyen pour connaître avec précision quelles sont les données à la disposition d'un parti politique, ce qu'il en fait et à qui il les communique. Contrairement aux organismes publics et aux entreprises privées, les partis politiques n'ont aucune obligation de donner suite aux demandes de personnes (qu'elles soient électrices, candidates, membres du parti ou bénévoles) voulant avoir accès aux renseignements qui les concernent.

Actuellement, une personne peut uniquement s'adresser au directeur général des élections pour contester les pratiques des partis politiques en matière de protection des renseignements personnels, si ces pratiques contreviennent à la *Loi électorale* en matière d'utilisation ou de communication des listes électorales.

Si elle souhaite dénoncer toute autre pratique qui ne lui semble pas conforme à l'égard de la protection des renseignements personnels, cette personne ne dispose d'aucun recours, puisque nul autre organisme de surveillance n'a d'autorité sur un parti politique. En effet, la Commission d'accès à l'information, qui a le mandat de faire enquête sur des plaintes en matière de protection des renseignements personnels, ne peut agir que si la plainte concerne une entité assujettie à l'une des deux lois applicables[211] au Québec, ce qui n'est pas le cas des partis politiques.

Il importe toutefois de souligner que la protection des renseignements personnels est une responsabilité partagée qui ne peut reposer que sur les partis politiques. Bien qu'ils ne puissent s'opposer à l'accès aux renseignements contenus dans les listes électorales, les électrices et les électeurs doivent être vigilants lorsqu'ils communiquent volontairement des renseignements à des partis politiques, notamment au cours d'une conversation téléphonique, lorsqu'ils signent une pétition électronique, à l'occasion d'une rencontre ou lorsqu'ils exposent leurs champs d'intérêt et leurs allégeances politiques sur les médias sociaux. Il est également de la responsabilité des électrices et des électeurs d'éviter de divulguer des renseignements personnels à des partis politiques s'ils ne souhaitent pas que ces derniers les recueillent et les utilisent.

211. La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels dans le secteur privé*.

La gouvernance en matière de protection des renseignements personnels

La présente étude a mis en évidence que peu d'information était rendue publique à l'égard des pratiques des partis politiques en matière de collecte et d'utilisation des renseignements personnels, ainsi que sur les mesures de sécurité qu'ils ont mises en place pour assurer la protection de ces renseignements. Cette absence de transparence est contraire aux principes reconnus en la matière.

Il y a donc lieu de s'interroger sur la possibilité que les partis politiques doivent respecter un cadre de gouvernance qui favoriserait une plus grande transparence, une plus grande responsabilisation et une meilleure imputabilité à l'égard de la protection des renseignements personnels qu'ils détiennent.

Comme nous l'avons exposé au deuxième chapitre, le principe de la responsabilité est au cœur de la protection des renseignements personnels :

> « La responsabilité dans le domaine de la protection de la vie privée est la reconnaissance du devoir de protéger les renseignements personnels. Une organisation responsable doit se doter de politiques et de procédures appropriées pour promouvoir l'application d'un ensemble de bonnes pratiques qui constitue un programme de gestion de la protection de la vie privée. Un tel programme permet aux organisations de respecter, au minimum, les lois applicables sur la protection des renseignements personnels. S'il est bien appliqué, il permet habituellement de renforcer le niveau de confiance des [individus], ce qui donne un avantage concurrentiel et rehausse la réputation des organisations[212]. »

Afin de renforcer la gouvernance des partis politiques à l'égard des renseignements sur les électeurs, l'Ontario et la Colombie-Britannique ont fait le choix de rendre obligatoire l'adoption d'une politique par les partis politiques qui souhaitent obtenir des listes électorales. Ces politiques prévoient notamment la désignation d'un responsable ; le maintien d'un registre des personnes qui accèdent aux renseignements personnels ; des normes pour assurer la conservation, la communication et la destruction sécuritaire des renseignements ; ainsi que le signalement des incidents pouvant porter atteinte à la vie privée. Ces politiques, qui sont régies par des directives émises par le directeur général des élections, doivent également être adoptées par les députés et les candidats qui souhaitent obtenir des listes électorales. Ces politiques ne s'appliquent toutefois qu'aux renseignements personnels issus des listes électorales.

Nous sommes d'avis qu'il est nécessaire que tout encadrement législatif des partis politiques en matière de protection des renseignements personnels doive permettre de rehausser la transparence et la gouvernance des partis politiques à cet égard.

---

212. Commissariat à la protection de la vie privée du Canada, Office of the Information and Privacy Commissioner of Alberta, Office of the Information & Privacy Commissioner for British Columbia, *Un programme de gestion de la protection de la vie privée : la clé de la responsabilité*, 17 avril 2012, p. 1. [https://www.priv.gc.ca/media/2104/gl_acc_201204_f.pdf].

La conservation des renseignements personnels

Dans la recherche de l'équilibre entre le respect de la vie privée des électrices et des électeurs et le besoin des partis politiques de communiquer avec eux, la durée de conservation des renseignements est importante.

Si un parti politique doit conserver des renseignements personnels pour pouvoir communiquer avec les électrices et les électeurs ou organiser ses opérations lors d'une campagne électorale, l'utilité de ces renseignements a manifestement une échéance. Un parti politique n'a pas intérêt, par exemple, à conserver des renseignements sur des électeurs décédés ou radiés des listes électorales. Maintenant que les élections ont lieu à date fixe, tous les quatre ans, combien de temps un parti politique devrait-il conserver des renseignements recueillis au sujet d'un candidat potentiel ou d'une personne qui a exprimé ses positions politiques par l'entremise d'une campagne de porte-à-porte ou d'une pétition ?

Le modèle européen encadré par le *Règlement général sur la protection des données* impose aux partis politiques une durée de conservation limitée en fonction de la finalité de chaque renseignement. En France, par exemple, les partis politiques ont l'obligation de détruire, après la tenue de l'élection, les listes des électrices et des électeurs ainsi que les fichiers constitués pour les besoins d'une campagne. Le règlement impose également aux partis politiques d'informer les électeurs, lorsqu'ils collectent des renseignements à leur sujet, de la durée de conservation de ces renseignements.

Au Canada, seule la loi électorale de la Nouvelle-Écosse oblige les candidates et les candidats à détruire les listes électorales dans les dix jours suivant l'élection. Bien que ce ne soit pas prévu expressément par la loi, les politiques de protection des renseignements personnels que doivent développer les partis politiques en Ontario et en Colombie-Britannique comprennent également des modalités relatives à la conservation des renseignements issus des listes électorales. En Colombie-Britannique, le *Personal Information Protection Act*[213], qui s'applique aux partis politiques, prévoit également que les renseignements personnels doivent être détruits lorsqu'ils ne sont plus nécessaires.

Au Québec, la *Loi électorale* ne prévoit pas de délai de conservation pour les renseignements détenus par les candidates, les candidats et les partis politiques. Un parti politique peut donc compiler l'historique de participation d'un électeur, à l'aide des renseignements fournis par le directeur général des élections, sans jamais devoir épurer sa banque de données. La situation est très différente de celle qui prévaut dans les pays européens, où la loi impose la destruction des listes électorales après les élections.

213. SBC 2003, chap. 63.

Le contrôle des accès et la communication des renseignements personnels

La description du régime d'encadrement actuel révèle que les partis politiques ne sont soumis à aucune mesure permettant de contrôler l'accès aux listes électorales qui leur sont communiquées par le directeur général des élections.

La *Loi électorale* prévoit que les partis politiques ne peuvent utiliser des renseignements sur les électrices et les électeurs ou communiquer de tels renseignements qu'aux fins prévues par la *Loi*. Il revient ainsi à la personne qui reçoit la liste électorale du directeur général des élections de s'assurer de l'utiliser ou de la communiquer en conformité avec la *Loi*, notamment lorsqu'elle communique ces renseignements à d'autres personnes, comme des membres de son parti ou des bénévoles lors d'une campagne électorale.

Le modèle de l'Ontario est intéressant puisque, contrairement aux lois applicables ailleurs au Canada et au Québec, il y est strictement interdit, pour les partis politiques, de communiquer des renseignements issus des listes électorales à toute personne qui ne s'est pas engagée par écrit à respecter les restrictions prévues par la loi. Cette approche permet de dresser la liste des personnes autorisées à accéder aux renseignements sur les électrices et les électeurs, qui doivent d'ailleurs faire l'objet d'un registre tenu par le parti, que ce dernier transmet annuellement au directeur général des élections.

D'après certaines sources, des partis politiques ont développé des banques de données électorales en collaboration avec des prestataires de services, notamment avec des firmes qui offrent des services de développement informatique, d'hébergement de serveurs ou d'analyse de mégadonnées.

Les principes reconnus exposés précédemment prévoient qu'une organisation doit demeurer responsable de la protection des renseignements personnels qu'elle confie à des prestataires de services pour l'exécution d'un mandat ou d'un contrat de service. Cela suppose qu'une organisation prévoit, par des clauses contractuelles, que ce prestataire s'engage à respecter la protection des renseignements personnels qui lui sont confiés. Or, l'encadrement actuel permet aux partis politiques de confier les renseignements qu'ils détiennent sans aucune obligation particulière, dans la mesure où la communication de ces renseignements est effectuée à des fins prévues par la *Loi électorale*.

7.2 Adoption d'un cadre législatif général en matière de protection des renseignements personnels

À l'exception des obligations prévues par la *Loi électorale*, les partis politiques du Québec ne sont régis par aucune loi générale en matière de protection des renseignements personnels. Or, dans un contexte où ils peuvent constituer des bases de données électorales constituées de renseignements sur plus de 6 millions de personnes, il faut remettre en question le statut d'exception des partis politiques, qui n'ont pas les mêmes obligations à respecter que les organismes publics et les entreprises du Québec. D'autant plus que les partis politiques détiennent d'autres renseignements qui ne sont pas encadrés par la *Loi électorale*, comme ceux sur leurs bénévoles, leurs membres et leurs candidates et candidats.

Les exemples de la Colombie-Britannique, des pays de l'Union européenne, du Royaume-Uni et de la Nouvelle-Zélande démontrent qu'il est possible, pour des partis politiques, de suivre les mêmes règles que les autres organisations qui détiennent des renseignements personnels. L'avènement de l'ère numérique et le resserrement des attentes des électrices et des électeurs à l'égard de leur vie privée, notamment à la suite de l'affaire Cambridge Analytica, poussent les gouvernements à revoir l'encadrement de l'utilisation des renseignements personnels à des fins politiques. C'est le cas au Royaume-Uni, où le commissaire à l'information a recommandé au gouvernement d'adopter un encadrement législatif sur l'utilisation des renseignements personnels en période électorale[214].

Les partis politiques pourraient affirmer qu'ils disposent de peu de ressources, qu'ils ont peu d'activités en dehors d'une période électorale ou que tout encadrement supplémentaire serait trop contraignant pour la taille de leur entité. Or, ce serait faire abstraction du fait que la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* s'applique à tous les organismes publics, y compris des municipalités de faible population, qui ont également des ressources limitées. La *Loi sur la protection des renseignements personnels dans le secteur privé*[215] (LPRPSP) s'applique, quant à elle, à toute personne qui exploite une entreprise au Québec, peu importe sa taille.

Il apparait difficile de justifier, aux yeux des électrices et des électeurs, que les renseignements les concernant soient sujets à des garanties de protection moins grandes lorsqu'ils sont détenus par un parti politique.

Dans une résolution conjointe[216], les commissaires à l'information et à la vie privée du Canada ont récemment invité les gouvernements à adopter des lois qui exigeraient que les partis politiques respectent les principes reconnus de protection des renseignements personnels. Le directeur général des élections approuve cette recommandation.

214. Voir note 194.
215. RLRQ, chap. P-39.1.
216. Voir note 101.

L'assujettissement des partis politiques à un encadrement législatif général nous apparait comme une solution permettant d'encadrer les partis politiques aux principes reconnus en matière de protection des renseignements personnels. Cela aurait notamment pour effet de protéger tous les types de renseignements personnels détenus par les partis politiques, incluant les renseignements sur leurs candidates et candidats, leurs bénévoles, leurs membres ainsi que les renseignements sur les électrices et les électeurs qui ne sont pas obtenus du directeur général des élections.

Plus concrètement, un tel encadrement devrait inclure les obligations suivantes :

- Un parti politique devrait désigner une personne responsable de la protection des renseignements personnels ;
- Un parti politique qui recueille des renseignements personnels devrait avoir préalablement déterminé les finalités pour lesquelles il recueille ces renseignements ;
- Avant de recueillir, d'utiliser ou de communiquer des renseignements personnels, un parti politique devrait obtenir le consentement de la personne concernée. Ce consentement devrait être manifeste, libre, éclairé, donné à des fins précises et être valide pour une durée déterminée ;
- Avant de recueillir des renseignements, un parti politique devrait informer la personne concernée des finalités de la collecte, de l'utilisation qui serait faite de ses renseignements personnels, des catégories de personnes qui y auraient accès au sein du parti politique et de l'endroit où ils seraient détenus. Le parti politique devrait également informer les personnes concernées de leurs droits d'accès et de rectification ;
- Un parti politique ne devrait utiliser les renseignements qu'il a recueillis qu'aux seules fins pour lesquelles il a obtenu le consentement des personnes concernées ;
- Un parti politique devrait restreindre la communication des renseignements personnels ;
- Un parti politique devrait veiller à ce que les renseignements personnels qu'il détient soient exacts et tenus à jour au moment où il les utilise ;
- Un parti politique devrait détruire les renseignements personnels lorsque leur utilisation n'est plus nécessaire ;
- Un parti politique devrait prendre les mesures de sécurité adéquates pour assurer la protection des renseignements personnels recueillis, utilisés, communiqués, conservés ou détruits ;
- Un parti politique devrait signaler tout incident impliquant des renseignements personnels, susceptible de porter préjudice aux personnes concernées, auprès d'une autorité de surveillance compétente ;
- Un parti politique devrait permettre l'accès aux renseignements personnels à son personnel, à ses bénévoles et à ses autres mandataires seulement lorsque cela leur est nécessaire. Il devrait également maintenir un registre des personnes autorisées à accéder aux renseignements personnels ;
- Un parti politique devrait conclure une entente garantissant la protection des renseignements personnels avant de communiquer des renseignements à un prestataire de services ;

- Un parti politique devrait répondre avec diligence aux demandes d'accès aux renseignements personnels et aux demandes de rectification qu'il reçoit des personnes concernées ;
- Un parti politique devrait élaborer des politiques et des procédures décrivant les mesures mises en place afin de respecter ses obligations en matière de protection des renseignements personnels et rendre ces documents accessibles sur demande.

Si l'on soumettait les partis politiques aux principes reconnus, les renseignements personnels détenus par les partis bénéficieraient d'un régime de protection équivalent à ceux détenus par les organismes publics et privés au Québec.

Pour ces motifs, nous recommandons :

1. D'assujettir les partis politiques provinciaux autorisés à un encadrement législatif général en matière de protection des renseignements personnels.

Considérant que les partis politiques municipaux reçoivent également des listes électorales en période électorale[217], il apparait justifié que l'encadrement soit le même au palier municipal qu'au palier provincial.

Pour ces motifs, nous recommandons :

2. D'assujettir les partis politiques municipaux autorisés à un encadrement législatif général en matière de protection des renseignements personnels.

Différentes solutions législatives sont susceptibles de répondre aux recommandations précédentes. On pourrait notamment envisager d'assujettir les partis politiques à l'une des lois existantes en matière de protection des renseignements personnels ou encore d'adopter une nouvelle loi propre aux partis politiques.

Il y a lieu de souligner que la LPRPSP, qui n'a pas été modifiée depuis 2006, n'intègre pas les principes de responsabilité et de transparence, ne prévoit aucun mécanisme de signalement des atteintes à la vie privée et n'inclut aucune obligation de destruction des renseignements personnels. Ces lacunes ne sont pas inconnues de la Commission d'accès à l'information : dans son dernier rapport quinquennal, elle recommandait notamment d'y introduire une obligation de responsabilité, de désigner une personne responsable de la protection des renseignements personnels, de signaler les incidents pouvant porter atteinte à la vie privée ainsi que de détruire les renseignements personnels[218].

---

217. La *Loi sur les élections et les référendums dans les municipalités ne prévoit pas la communication de listes électorales en dehors d'une période électorale*.

218. Commission d'accès à l'information, *Rétablir l'équilibre : rapport quinquennal 2016*, p. 76, 108 et 109. [http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf].

L'adoption d'un modèle mixte, fondé sur l'assujettissement des partis politiques à loi générale, combiné à des dispositions complémentaires dans la *Loi électorale*, est également un scénario à évaluer. Il s'agit du modèle en vigueur en Colombie-Britannique.

Dans tous les cas, la présente étude ne vise pas à identifier la solution qui devrait être adoptée par le législateur. Elle vise avant tout à lui permettre d'obtenir un éclairage sur les enjeux liés à la protection des renseignements personnels détenus par les partis et sur les éléments que devrait comprendre un éventuel encadrement législatif.

Les députés et les candidats

Les recommandations précédentes ne visent que les partis politiques, aux paliers provincial et municipal. Il y a toutefois lieu de s'assurer que les députées, les députés, les candidates et les candidats, qui reçoivent également des listes électorales et qui sont susceptibles de recueillir des renseignements personnels, soient assujettis à des règles de protection équivalentes à celles applicables aux partis politiques. Les candidats des partis pourraient être soumis aux obligations applicables à leur parti politique.

Pour ces motifs, nous recommandons :

3. De prévoir des obligations similaires pour les députées, les députés, les candidates et les candidats aux élections provinciales, municipales et scolaires, avec les adaptations nécessaires.

7.3 Révision des lois électorales

Revoir la nature des renseignements sur les électrices et les électeurs communiqués aux partis politiques

La transmission des renseignements personnels sur les électrices et les électeurs par le directeur général des élections soulève certaines questions quant à la nécessité, pour un parti politique, d'obtenir des renseignements sur l'électorat de la part du directeur général des élections.

Les partis politiques obtiennent depuis longtemps les listes électorales, notamment afin de pouvoir s'assurer que toutes les personnes pouvant être inscrites sur la liste électorale puissent exercer leur droit de vote le jour du scrutin. Or, depuis la mise en place de la liste électorale permanente, en 1997, et la fin des recensements[219], il est légitime de se demander quel rôle exercent désormais les partis politiques sur la qualité de la liste électorale, alors que le directeur général des élections est en mesure d'assurer la mise à jour de cette liste en continu.

219. La *Loi électorale* prévoit qu'un recensement peut être ordonné afin d'effectuer une vérification de la liste électorale permanente.

Les partis politiques ont besoin de connaître et d'identifier les électrices et les électeurs afin qu'ils puissent efficacement communiquer avec eux, particulièrement lors d'une campagne électorale. Il apparait plus difficile de justifier la nécessité, pour les partis politiques, de connaître le sexe et la date de naissance des électeurs, d'autant plus que ces renseignements sont désormais jugés plus sensibles qu'ils ne l'étaient auparavant. Il en va de même pour l'adresse temporaire des électeurs exerçant leur droit de vote à l'extérieur du Québec.

L'examen des législations au Canada révèle d'ailleurs que seules les listes électorales transmises au Québec contiennent la date de naissance des électeurs. Ailleurs au Canada, seules les listes électorales du Nouveau-Brunswick contiennent également le sexe des électeurs.

Bien que ces communications soient prévues par la *Loi*, il est opportun de se demander si la communication des listes électorales, une pratique établie depuis plus de 70 ans, respecte les attentes actuelles des électrices et des électeurs à l'égard de leur vie privée. Rappelons que les résultats du sondage présenté précédemment indiquent que les électeurs priorisent la protection de leur vie privée plutôt que le besoin des partis politiques de communiquer avec les électeurs. Le même constat ressort des débats de la Table citoyenne qui ont eu lieu en novembre 2018.

Le directeur général des élections est d'avis que le nom et l'adresse du domicile sont suffisants pour que les partis politiques puissent joindre efficacement les électrices et les électeurs.

Les renseignements inscrits sur les listes des électeurs inscrits au vote en installation d'hébergement ou au vote à domicile, qui sont communiqués en période électorale, soulèvent eux aussi des questions. Ces documents révèlent l'intention d'aller voter de ces électeurs et confirment qu'ils sont incapables de se déplacer pour des raisons de santé. Dans les faits, les partis politiques n'ont pas à inciter ces personnes à aller voter, puisqu'une équipe désignée par le directeur du scrutin se déplacera pour s'assurer qu'elles puissent le faire. L'utilité de ces listes pour les partis politiques est donc bien relative.

Pour ces motifs, nous recommandons :

4. De retirer le sexe et la date de naissance des électrices et des électeurs des listes électorales transmises aux députés, aux candidats et aux partis politiques, et ce, à tous les paliers électoraux.

5. De modifier la *Loi électorale* afin de cesser la transmission de renseignements permettant d'identifier des électrices et des électeurs vulnérables ou de révéler leur adresse temporaire à l'extérieur du Québec.

Dans son rapport annuel 2016-2017, le directeur général des élections recommandait de permettre aux électrices et aux électeurs de refuser la communication de leurs renseignements inscrits sur les listes électorales aux partis politiques, aux députées et députés ainsi qu'aux candidates et candidats. Considérant que nous recommandons d'assujettir les partis politiques à un encadrement législatif général en matière de protection des renseignements personnels, nous ne jugeons plus opportun de renouveler cette recommandation.

Déterminer les fins permettant l'utilisation des renseignements inscrits sur les listes électorales

L'application des sanctions pénales en matière de protection des renseignements issus de la liste électorale permanente découle des obligations prescrites par la loi. Or, la *Loi électorale* ne précise pas les fins pour lesquelles ces renseignements peuvent être utilisés Les dispositions de la *Loi sur les élections et les référendums dans les municipalités*[220] et de la *Loi sur les élections scolaires*[221] concernant l'utilisation des listes électorales sont similaires.

Il est également opportun d'examiner plus attentivement la nécessité, pour les députées et les députés, d'obtenir et d'utiliser des listes électorales dans l'exercice de leurs fonctions.

Dans ce contexte, nous recommandons :

6. De préciser dans les lois électorales les fins pour lesquelles les députés, les candidats et les partis politiques peuvent utiliser ou communiquer les renseignements issus des listes électorales.

220. RLRQ, chap. E-2.2, art. 659.1.

221. RLRQ, chap. E-2.3, art. 282.1.

Revoir les modalités de transmission des listes électorales

Depuis 2006, en dehors d'une période électorale, tous les partis politiques provinciaux autorisés peuvent, trois fois par année, obtenir la liste des électrices et des électeurs inscrits à la liste électorale permanente aux fins de la tenue d'un scrutin provincial. Il y a lieu de s'interroger sur la nécessité, pour un parti politique, d'obtenir la liste électorale aussi souvent en dehors d'une période électorale, alors qu'il est moins susceptible de communiquer avec les électrices et les électeurs, à l'exception de ses membres et de ses contributeurs. Les partis politiques du Québec reçoivent les listes électorales plus fréquemment que les autres partis politiques canadiens.

Tous les partis politiques provinciaux autorisés peuvent demander d'obtenir la liste électorale des 125 circonscriptions, et ce, qu'ils y aient présenté ou non des candidates ou des candidats lors des dernières élections. Lors des élections générales provinciales, tenues le 1er octobre 2018, seuls quatre partis politiques sur dix-huit ont présenté des candidats dans toutes les circonscriptions.

Depuis 1997, une version électronique de la liste électorale est accessible aux députés, aux candidats et aux partis politiques, mais une version papier demeure également accessible, puisque la *Loi électorale* prévoit toujours cette possibilité. Le directeur général des élections est d'avis qu'il serait préférable qu'il détermine les modalités de transmission de cette liste afin de les adapter à la réalité technologique et d'y appliquer les mesures de sécurité nécessaires.

Pour ces motifs, nous recommandons :

7. De transmettre les listes électorales aux partis politiques provinciaux et aux députées et députés une seule fois par année en dehors d'une période électorale.

8. De communiquer les listes électorales aux candidats, aux députés et aux partis politiques uniquement en version électronique, selon les modalités déterminées par le directeur général des élections.

Examen des recommandations du directeur général des élections

Les recommandations proposées dans la présente étude sont susceptibles d'avoir d'importantes répercussions. Elles nécessiteraient notamment des modifications législatives à la *Loi électorale*, à la *Loi sur les élections et les référendums dans les municipalités* ainsi qu'à la *Loi sur les élections scolaires*.

Il nous apparait donc opportun de solliciter la contribution de toutes les parties prenantes à ces modifications, soit la Commission d'accès à l'information, le ministère des Affaires municipales et de l'Habitation (responsable de la *Loi sur les élections et les référendums dans les municipalités*), le ministère de l'Éducation et de l'Enseignement supérieur (responsable de la *Loi sur les élections scolaires*), les partis politiques provinciaux et municipaux, de même que des experts en matière de protection de la vie privée, qui seraient en mesure d'approfondir et d'améliorer ces recommandations.

Nous sommes également d'avis que l'examen de ces recommandations devrait être soumis, pour consultation, aux principales personnes concernées : les électrices et les électeurs du Québec.

Pour ces motifs, nous recommandons :

9. Que l'Assemblée nationale mandate une commission spéciale sur l'encadrement des partis politiques à l'égard de la protection des renseignements personnels afin d'étudier les recommandations du directeur général des élections.

Conclusion

Le Québec a été un précurseur en matière de protection des renseignements personnels au Canada. En effet, il a adopté la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, en 1982, et la *Loi sur la protection des renseignements personnels dans le secteur privé*, en 1993, alors qu'aucune entreprise canadienne à l'extérieur du Québec n'a été régie par un cadre législatif avant l'adoption de la loi fédérale, en 2000.

En matière électorale, au Québec, depuis les modifications législatives pour la mise en place de la liste électorale permanente, en 1995, le cadre électoral en vigueur n'a pas été actualisé en matière de protection des renseignements personnels sur les électrices et les électeurs. Au cours des années 1990 et au début des années 2000, le législateur et le directeur général des élections n'ont pas anticipé l'impact de la transmission régulière de la liste électorale aux partis politiques sur la vie privée des électeurs. Personne n'avait prévu l'omniprésence des technologies numériques et la constitution de bases de données électorales par les partis politiques.

Par la présente étude, le directeur général des élections a souhaité apporter un éclairage sur les règles relatives à la protection des renseignements personnels à des fins électorales. Nous avons ainsi examiné l'encadrement législatif applicable au Québec, au Canada, dans les pays de l'Union européenne et dans d'autres pays dotés d'un système politique similaire à celui du Québec, afin de recenser les meilleures pratiques.

Certaines provinces canadiennes, telles la Saskatchewan, l'Ontario et plus particulièrement la Colombie-Britannique, ont réussi à améliorer la protection des renseignements personnels détenus par les partis politiques en permettant à une autorité de surveillance indépendante d'exercer un plus grand contrôle des activités des partis. L'absence d'encadrement au Québec contraste encore davantage avec le nouveau régime européen mis en œuvre par le *Règlement général sur la protection des données*, qui s'applique à tout type d'organisation, incluant les partis politiques.

Cette étude a également permis de démontrer que les enjeux liés à l'utilisation des renseignements personnels par les partis politiques ne sont pas propres au Québec. En effet, les autorités responsables de la protection de la vie privée, au Canada comme ailleurs, ont invité, au cours des dernières années, les gouvernements à actualiser l'encadrement législatif afin de mieux protéger les renseignements détenus par les partis politiques.

Si les partis politiques se dotent désormais de bases de données électorales, cette tendance nous amène à nous interroger sur les mesures de gouvernance et de sécurité mises en place pour protéger les renseignements qu'ils détiennent. Ce contexte est d'autant plus préoccupant que le Centre de la sécurité des télécommunications du Canada considère, depuis peu, que le risque pour un parti politique de se faire voler ou manipuler sa base de données sur les électrices et les électeurs constitue une cybermenace contre le processus démocratique[222].

---

222. Centre de la sécurité des télécommunications, *Cybermenaces contre le processus démocratique du Canada*, juin 2017, p. 18. [https://cyber.gc.ca/sites/default/files/publications/cse-cyber-threat-assessment-f.pdf].

Depuis 2013, le directeur général des élections recommande de réviser les dispositions de la *Loi électorale* quant à la protection des renseignements sur les électrices et les électeurs. Dans le cadre de cette étude, nous avons voulu approfondir et élargir l'éventail de ces recommandations en considérant tous les renseignements détenus par les partis politiques. En effet, avec les possibilités de croisement de données, les enjeux de protection des renseignements personnels ne peuvent se limiter aux seuls renseignements inscrits sur les listes électorales transmises par le directeur général des élections.

Il ne fait aucun doute que les partis politiques jouent un rôle primordial dans la promotion de la participation à la démocratie et que la communication avec l'électorat est un élément central de cette participation. Toutefois, il importe de trouver un juste équilibre entre les besoins des partis en matière de communication et les attentes des électrices et des électeurs à l'égard de la protection de leur vie privée, afin d'éviter, en bout de piste, que ne soit altérée la confiance qu'ont les individus dans leurs institutions politiques.

ANNEXE 1

Liste des recommandations du directeur général des élections

Le directeur général des élections recommande :

1. D'assujettir les partis politiques provinciaux autorisés à un encadrement législatif général en matière de protection des renseignements personnels.
2. D'assujettir les partis politiques municipaux autorisés à un encadrement législatif général en matière de protection des renseignements personnels.
3. De prévoir des obligations similaires pour les députées, les députés, les candidates et les candidats aux élections provinciales, municipales et scolaires, avec les adaptations nécessaires.

L'encadrement visé aux recommandes précédentes devrait inclure les obligations suivantes :

- Un parti politique devrait désigner une personne responsable de la protection des renseignements personnels ;
- Un parti politique qui recueille des renseignements personnels devrait avoir préalablement déterminé les finalités pour lesquelles il recueille ces renseignements ;
- Avant de recueillir, d'utiliser ou de communiquer des renseignements personnels, un parti politique devrait obtenir le consentement de la personne concernée. Ce consentement devrait être manifeste, libre, éclairé, donné à des fins précises et être valide pour une durée déterminée ;
- Avant de recueillir des renseignements, un parti politique devrait informer la personne concernée des finalités de la collecte, de l'utilisation qui serait faite de ses renseignements personnels, des catégories de personnes qui y auraient accès au sein du parti politique et de l'endroit où ils seraient détenus. Le parti politique devrait également informer les personnes concernées de leurs droits d'accès et de rectification ;
- Un parti politique ne devrait utiliser les renseignements qu'il a recueillis qu'aux seules fins pour lesquelles il a obtenu le consentement des personnes concernées ;
- Un parti politique devrait restreindre la communication des renseignements personnels ;
- Un parti politique devrait veiller à ce que les renseignements personnels qu'il détient soient exacts et tenus à jour au moment où il les utilise ;

- Un parti politique devrait détruire les renseignements personnels lorsque leur utilisation n'est plus nécessaire ;
- Un parti politique devrait prendre les mesures de sécurité adéquates pour assurer la protection des renseignements personnels recueillis, utilisés, communiqués, conservés ou détruits ;
- Un parti politique devrait signaler tout incident impliquant des renseignements personnels, susceptible de porter préjudice aux personnes concernées, auprès d'une autorité de surveillance compétente ;
- Un parti politique devrait permettre l'accès aux renseignements personnels à son personnel, à ses bénévoles et à ses autres mandataires seulement lorsque cela leur est nécessaire. Il devrait également maintenir un registre des personnes autorisées à accéder aux renseignements personnels ;
- Un parti politique devrait conclure une entente garantissant la protection des renseignements personnels avant de communiquer des renseignements à un prestataire de services ;
- Un parti politique devrait répondre avec diligence aux demandes d'accès aux renseignements personnels et aux demandes de rectification qu'il reçoit des personnes concernées ;
- Un parti politique devrait élaborer des politiques et des procédures décrivant les mesures mises en place afin de respecter ses obligations en matière de protection des renseignements personnels et rendre ces documents accessibles sur demande.

Le directeur général des élections recommande également :

4. De retirer le sexe et la date de naissance des électrices et des électeurs des listes électorales transmises aux députés, aux candidats et aux partis politiques, et ce, à tous les paliers électoraux.

5. De modifier la *Loi électorale* afin de cesser la transmission de renseignements permettant d'identifier des électrices et des électeurs vulnérables ou de révéler leur adresse temporaire à l'extérieur du Québec.

6. De préciser dans les lois électorales les fins pour lesquelles les députés, les candidats et les partis politiques peuvent utiliser ou communiquer les renseignements issus des listes électorales.

7. De transmettre les listes électorales aux partis politiques provinciaux et aux députées et députés une seule fois par année en dehors d'une période électorale.

8. De communiquer les listes électorales aux candidats, aux députés et aux partis politiques uniquement en version électronique, selon les modalités déterminées par le directeur général des élections.

9. Que l'Assemblée nationale mandate une commission spéciale sur l'encadrement des partis politiques à l'égard de la protection des renseignements personnels afin d'étudier les recommandations du directeur général des élections.

ANNEXE 2

Affaire Cambridge Analytica

Le 17 mars 2018, le *Guardian*[223] et le *New York Times*[224] ont révélé que Cambridge Analytica, société de conseil en stratégie d'influence, avait illégitimement recueilli des renseignements personnels issus des profils Facebook de plus de cinquante millions d'utilisateurs sans leur consentement. Ce nombre a par la suite été réévalué à quatre-vingt-sept millions[225].

En raison du rôle de Cambridge Analytica durant la campagne présidentielle américaine de 2016 et de la mise à disposition de ses outils spécialisés au service du mouvement Leave.EU[226] lors du référendum sur le Brexit de juin 2016, cette enquête journalistique a eu un retentissement considérable partout dans le monde.

Cambridge Analytica offrait des outils d'exploration et d'analyse des données. Elle proclamait être en mesure d'établir le profil comportemental des électrices et des électeurs à partir de l'étude de leurs renseignements personnels. Par la communication de publicités ciblées sur les réseaux sociaux, elle cherchait à infléchir le suffrage dans le sens attendu. Sur son site Internet, Cambridge Analytica prétendait avoir collecté près de 5 000 données sur chaque électrice et chaque électeur des États-Unis[227].

Rappel des faits

En 2014, Cambridge Analytica était impliquée dans 44 élections de mi-mandat aux États-Unis[228]. En 2015, elle soutenait le sénateur Ted Cruz lors des élections primaires en vue de l'élection présidentielle américaine de 2016.

---

223. Carole Cadwalladr et Emma Graham-Harrison, *op. cit.*

224. M. Rosenberg, N. Confessore et C. Cadwalladr, *op. cit.*

225. O. Solon, « Facebook Says Cambridge Analytica May Have Gained 37M More Users' Data », *The Guardian*, 4 avril 2018. [https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought].

226. https://leave.eu/about/.

227. Paul-Olivier Dehaye, « Cambridge Analytica Demonstrably Non-compliant with Data Protection Law », *PersonalData.IO*, 3 mars 2017. [https://medium.com/personaldata-io/cambridge-analytica-demonstrably-non-compliant-with-data-protection-law-95ec5712b61].

228. Frances Stead Sellers, « Cruz Campaign Paid $750,000 to 'Psychographic Profiling' Company », *The Washington Post*, 19 octobre 2015. [https://www.washingtonpost.com/politics/cruz-campaign-paid-750000-to-psychographic-profiling-company/2015/10/19/6c83e508-743f-11e5-9cbb-790369643cf9_story.html?noredirect=on&utm_term=.b09e391c21c6].

Dès décembre 2015, une première enquête du *Guardian* révélait que Cambridge Analytica avait permis à Ted Cruz d'utiliser les données de millions d'utilisateurs de Facebook, obtenues en grande partie sans leur autorisation[229].

Après la défaite de Ted Cruz à l'investiture républicaine, Cambridge Analytica a collaboré avec l'équipe de Donald Trump. Au moyen d'une communication politique fondée sur des contenus personnalisés et tendancieux, la firme a tenté de convaincre 20 millions d'électrices et d'électeurs supplémentaires de voter pour Donald Trump[230].

Dans un communiqué diffusé le lendemain de l'élection présidentielle américaine, le directeur du groupe SCL, Alexander Nix, se félicitait : « nous sommes ravis du fait que notre approche révolutionnaire des communications numériques a joué un rôle essentiel dans la victoire extraordinaire du président élu Donald Trump[231] ». Selon les propos recueillis par des journalistes britanniques, il a également affirmé que les nombreuses données et les algorithmes de Cambridge Analytica avaient permis de construire un modèle pour prédire la personnalité des adultes aux États-Unis et développer des réponses réflexes. Selon M. Nix, Cambridge Analytica s'était avérée déterminante dans l'identification des adeptes de Donald Trump et dans la persuasion des électrices et des électeurs indécis pour les amener à participer au scrutin[232].

En 2018, un comité parlementaire britannique a convoqué le lanceur d'alerte Christopher Wylie, ex-directeur de recherche de la firme SCL. Celui-ci a alors affirmé que la société Cambridge Analytica avait joué un rôle crucial lors du vote en faveur du Brexit. Par ailleurs, l'entreprise canadienne AggregateIQ, liée à Cambridge Analytica, avait également collaboré à la campagne pour la sortie de l'Union européenne. Ainsi, Leave.EU aurait contourné son plafond de dépenses en déboursant près d'un million de livres pour cibler les citoyennes et les citoyens britanniques, utilisant leurs renseignements personnels sans leur consentement afin de leur transmettre de la désinformation. Selon M. Wylie, sans cette communication personnalisée et partiale destinée à un public réceptif, le camp du Leave.EU n'aurait pas pu gagner le référendum[233].

---

229. Harry Davies, « Ted Cruz Using Firm that Harvested Data on Millions of Unwitting Facebook Users », *The Guardian*, 11 décembre 2015. [https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data].

230. Adam Payne, « A British Firm which Helped Deliver Brexit is Working for Donald Trump's Campaign », *Business Insider*, 22 septembre 2016. [https://www.businessinsider.com/donald-trump-brexit-us-presidential-election-2016-9/].

231. Cambridge Analytica, *Cambridge Analytica Congratulates President-elect Donald Trump and Vice President-elect Mike Pence*, [Vidéo en ligne], 9 novembre 2016. Repéré au [https://web.archive.org/web/20170127180813/https://cambridgeanalytica.org/news/pressrelease/1293].

232. Channel 4 News, *Exposed: Undercover Secrets of Trump's Data Firm*, 20 mars 2018. [https://www.channel4.com/news/exposed-undercover-secrets-of-donald-trump-data-firm-cambridge-analytica].

233. Le Monde avec Reuters, *Le référendum sur le Brexit « aurait été différent », sans Facebook, soutient Christopher Wylie devant des parlementaires britanniques*, 30 mars 2018. [https://www.lemonde.fr/referendum-sur-le-brexit/video/2018/03/30/le-referendum-sur-le-brexit-aurait-ete-different-sans-facebook-soutient-christopher-wylie-devant-des-parlementaires-britanniques_5278876_4872498.html].

La provenance des renseignements personnels

Des chercheurs du Centre psychométrique de l'Université de Cambridge, au Royaume-Uni, ont élaboré une méthodologie pour comprendre le profil psychologique d'une personne uniquement à partir de son activité sur Facebook, notamment en fonction de ses mentions « J'aime/Like ». Cambridge Analytica s'était intéressée à ces travaux et avait approché les chercheurs du Centre pour travailler avec eux. Bien que le Centre ait refusé, en tant qu'institution universitaire, de collaborer avec la société, l'un de ses professeurs-chercheurs, Aleksandr Kogan, avait accepté de participer à ses travaux[234].

En 2014, M. Kogan a développé l'application numérique *This Is Your Digital Life,* qui était présentée comme une recherche universitaire. Il s'agissait d'un test de personnalité comptant 120 questions[235]. Ce test permettait d'établir des profils psychologiques basés sur la méthode O.C.E.A.N. ; ces tests mesuraient le degré d'ouverture, de conscience, d'extraversion, d'amabilité et de névrose d'un individu[236].

Les personnes qui répondaient aux questions recevaient une rémunération variant entre deux et cinq dollars. Pour obtenir la rémunération attendue, chaque individu devait se connecter à son profil Facebook et consentir à donner accès à ses renseignements personnels. Ainsi, l'application recueillait les réponses au test et s'appropriait toutes les données du compte Facebook de la personne concernée, tout en soutirant les données de son cercle d'amis, sans qu'ils le sachent. Plus de 270 000 personnes ont téléchargé cette application[237].

Le chercheur semblait respecter les conditions générales d'utilisation de Facebook, mais la revente de données et leur utilisation par Cambridge Analytica pour d'autres fins étaient interdites. Il faut souligner que la collecte des données des amis des utilisateurs était permise au moment des faits, mais que cette possibilité est désormais proscrite par Facebook. Cambridge Analytica a donc volontairement enfreint les règles, par l'intermédiaire de M. Kogan, pour se constituer une base de données de plusieurs millions de profils individuels provenant des données de Facebook, et ce, sans le consentement des personnes concernées[238].

---

234. Paul Handley, « Comment les données de Facebook ont aidé Trump à se faire élire », *TVA/Agence France-Presse*, 21 mars 2018. [https://www.tvanouvelles.ca/2018/03/21/comment-les-donnees-de-facebook-ont-aide-trump-a-se-faire-elire].
235. Scott Detrow, « What Did Cambridge Analytica Do During the 2016 Election ? », *NPR - National Public Radio (US)*, 20 mars 2018. [https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election].
236. Louise Million, « Le FBI et le département de la Justice enquêtent sur Cambridge Analytica », *Siècle digital*, 22 mai 2018. [https://siecledigital.fr/2018/05/22/fbi-departement-justice-enquetent-cambridge-analytica/].
237. Kévin Deniau, « Cambridge Analytica : tout comprendre sur la plus grande crise de l'histoire de Facebook », *Siècle digital*, 23 mars 2018. [https://siecledigital.fr/2018/03/23/cambridge-analytica-tout-comprendre-sur-la-plus-grande-crise-de-lhistoire-de-facebook/].
238. *Ibid.*

À titre d'exemple, le *Guardian* précisait que seulement 53 personnes en Australie et 10 en Nouvelle-Zélande avaient répondu au test de personnalité *This Is Your Digital Life* et autorisé, du même coup, l'accès à leur profil Facebook[239]. Ces accès avaient permis de recueillir des renseignements personnels d'environ 310 000 individus en Australie et 64 000 en Nouvelle-Zélande, à leur insu.

À la suite des révélations de ces enquêtes journalistiques, le réseau social Facebook a confirmé, au printemps 2018, une fuite massive de données concernant 87 millions de personnes[240], dont 71 millions aux États-Unis et 620 000 au Canada[241]. On a alors révélé que Facebook avait découvert l'appropriation illégale de ces données en 2015, mais qu'elle avait gardé le silence en éliminant l'application et en demandant la destruction immédiate des données qu'elle avait recueillies. Malgré les attestations du chercheur, ces données n'ont pas été supprimées et Cambridge Analytica a continué de les utiliser à des fins électorales[242].

239. Christopher Knaus, « Just 53 Australians Used Facebook App Responsible for Cambridge Analytica Breach », *The Guardian*, 10 avril 2018. [https://www.theguardian.com/technology/2018/apr/10/just-53-australians-used-facebook-app-responsible-for-cambridge-analytica-breach].

240. Issie Lapowsky, « Facebook Exposed 87 Million Users to Cambridge Analytica », *Wired*, 4 avril 2018. [https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/].

241. La Presse Canadienne avec Agence France-Presse, « Cambridge Analytica a accédé aux données de 620 000 Canadiens », *La Presse*, 4 avril 2018. [https://www.lapresse.ca/techno/reseaux-sociaux/201804/04/01-5159831-cambridge-analytica-a-accede-aux-donnees-de-620-000-canadiens.php].

242. Richard Nieva, « Facebook peut-il être blâmé pour l'affaire Cambridge Analytica ? », *ZDNet*, 19 mars 2018. [https://www.zdnet.fr/actualites/facebook-peut-il-etre-blame-pour-l-affaire-cambridge-analytica-39865692.htm].

ANNEXE **3**

Encadrement des partis politiques au Canada et dans les autres provinces

Canada

Régime d'encadrement

Les partis politiques ne sont assujettis à aucune des deux lois générales qui encadrent la protection des renseignements personnels, soit la *Loi sur la protection des renseignements personnels*[243], qui s'applique aux renseignements personnels détenus par des institutions fédérales, et la *Loi sur la protection des renseignements personnels et les documents électroniques*[244], qui s'applique aux organisations qui recueillent, utilisent ou communiquent des renseignements personnels dans le cadre d'activités commerciales ainsi qu'aux entreprises fédérales.

La *Loi électorale du Canada*[245] encadre la protection des renseignements personnels détenus par les partis politiques, mais cet encadrement ne porte que sur l'utilisation des listes électorales transmises par le directeur général des élections.

Plus spécifiquement, la *Loi* permet aux candidates et candidats, aux députées et députés ainsi qu'aux partis politiques d'utiliser les listes électorales pour communiquer avec les électrices et les électeurs, notamment pour solliciter des contributions, pour recruter des membres ou pour faire campagne[246].

Renseignements fournis par l'administration électorale

Chaque députée et député peut recevoir, une fois par année, la liste électorale de sa circonscription. Sur demande, cette liste est également transmise à chaque parti politique y ayant présenté un candidat ou une candidate lors de la dernière élection. La liste électorale est transmise en version électronique et contient les renseignements suivants[247] :

- Nom ;
- Adresse municipale et postale ;
- Numéro identificateur unique.

---

243. L.R.C. (1985), chap. P-21.
244. L.C. 2000, chap. 5.
245. L.C. 2000, chap. 9.
246. *Ibid.*, art. 110.
247. *Ibid.*, art. 45.

En période électorale, les partis politiques et les candidates et candidats reçoivent des listes électorales qui contiennent les mêmes renseignements[248].

Pendant les heures de vote, le représentant ou la représentante du candidat peut examiner la liste électorale et communiquer tout renseignement obtenu à un représentant du candidat qui est situé à l'extérieur du bureau du scrutin[249].

Dans les meilleurs délais à la suite du jour du scrutin, le directeur général des élections transmet la liste électorale de la circonscription à chaque parti politique y ayant présenté une candidate ou un candidat ainsi qu'au député élu[250].

Autres obligations

La *Loi* ne prévoit aucune mesure permettant de s'assurer de la conformité des partis politiques à l'égard de l'utilisation et de la communication des renseignements personnels contenus dans les listes électorales.

Infractions pénales et autres sanctions

L'utilisation des renseignements personnels figurant sur les listes électorales à des fins non autorisées constitue une infraction en vertu de la *Loi*[251].

Quiconque utilise sciemment ces renseignements à une fin non autorisée est passible d'une amende maximale de 10 000 $, d'un emprisonnement maximal d'un an ou des deux peines.[252]

Rôle et pouvoirs de l'autorité de surveillance

Le commissaire aux élections fédérales est chargé de veiller à l'observation et au contrôle d'application de la *Loi*. Le commissaire peut, de sa propre initiative ou en réponse à une plainte, mener une enquête. S'il a des motifs de croire qu'une infraction à la *Loi* a été commise, il peut soumettre l'affaire au directeur des poursuites pénales, qui décide s'il y a lieu d'engager des poursuites visant à sanctionner l'infraction[253].

248. *Ibid.*, art. 93 et 94.
249. *Ibid.*, art. 136.
250. *Ibid.*, art. 109.
251. *Ibid.*, art. 111 et 487.
252. *Ibid.*, art. 500.
253. *Ibid.*, art. 509.2, 510 et 511.

Terre-Neuve-et-Labrador

Régime d'encadrement

Les partis politiques ne sont pas assujettis au *Access to Information and Protection of Privacy Act*[254], qui s'applique aux renseignements personnels détenus par les organismes publics[255].

L'*Elections Act*[256] encadre la protection des renseignements personnels détenus par les partis politiques. Cet encadrement ne porte cependant que sur l'utilisation des renseignements provenant de la liste permanente des électrices et des électeurs.

La loi prévoit que la liste électorale ne peut être utilisée à d'autres fins que celles prévues par la loi électorale[257].

Renseignements fournis par l'administration électorale

Les partis politiques reçoivent la liste électorale chaque année. Cette liste peut être transmise en version papier ou électronique et contient les renseignements suivants :

- Nom ;
- Adresse.

En période électorale, les candidates, les candidats et les partis politiques reçoivent des listes électorales qui contiennent les mêmes renseignements[258].

Les candidates et candidats peuvent recevoir la liste des électrices et des électeurs qui ont voté par anticipation. Sur demande, les candidats peuvent obtenir la liste des électeurs inscrits aux votes spéciaux, mais cette liste ne comprend que le nom et l'adresse principale de l'électeur[259].

Autres obligations

La loi ne prévoit aucune mesure permettant de s'assurer de la conformité des partis politiques à l'égard de l'utilisation des renseignements contenus dans les listes électorales.

Infractions pénales et autres sanctions

La loi ne prévoit aucune infraction à l'égard de l'utilisation non conforme des listes électorales.

254. SNL2015, chap. A-1.2.
255. Aucune loi provinciale n'encadre les entreprises à Terre-Neuve-et-Labrador ; c'est la loi fédérale qui s'applique.
256. SNL1992, chap. E-3.1.
257. *Ibid.*, art. 55.
258. *Ibid.*
259. *Ibid.*, art. 86.8 et 133.

Rôle et pouvoirs de l'autorité de surveillance

Le directeur général des élections est chargé de l'application de la loi. Il ne dispose d'aucun pouvoir lui permettant de s'assurer de la conformité des obligations prévues à la loi[260].

Nouvelle-Écosse

Régime d'encadrement

Les partis politiques ne sont pas assujettis au *Freedom of Information and Protection of Privacy Act*[261], qui s'applique aux renseignements personnels détenus par les organismes publics[262].

L'*Elections Act*[263] encadre la protection des renseignements personnels détenus par les partis politiques. Cet encadrement ne porte cependant que sur l'utilisation des renseignements provenant du registre des électrices et des électeurs.

Plus spécifiquement, les partis politiques ne peuvent utiliser les renseignements contenus dans les listes électorales que pour des fins électorales[264].

Renseignements fournis par l'administration électorale

Les partis politiques reçoivent la liste des électrices et des électeurs inscrits au registre chaque année. Les députées et députés peuvent recevoir la liste de leur circonscription. La liste contient les renseignements suivants[265] :

- Nom ;
- Adresse résidentielle et postale ;
- Numéro identificateur unique ;
- Indication précisant si l'électeur a voté aux élections précédentes (depuis 2009) ;
- Catégorie d'âge au 1er janvier[266].

En période électorale, les candidates et candidats reçoivent des listes électorales qui contiennent les mêmes renseignements, à l'exception de la catégorie d'âge. Pendant la période électorale, les listes contiennent également une indication précisant si l'électrice ou l'électeur a voté aux élections précédentes[267].

260. *Ibid.*, art. 5.
261. SNS 1993, chap. 5.
262. Aucune loi provinciale n'encadre les entreprises en Nouvelle-Écosse ; c'est la loi fédérale qui s'applique.
263. SNS 2011, chap. 5.
264. *Ibid.*, art. 44.
265. *Ibid.*, art. 44.
266. Les catégories d'âge sont 18-24 ans, 25-34 ans, 35-44 ans, 45-54 ans, 55-64 ans, 65-74 ans et 75 ans et plus.
267. SNS 2011, chap. 5, art. 52.

Autres obligations

Les candidates et les candidats doivent détruire toute copie des listes électorales qu'ils ont reçues, incluant celles qu'ils ont communiquées à des tiers agissant en leur nom, et attester de leur destruction au directeur général des élections au plus tard dix jours suivant le jour du scrutin[268].

La loi ne prévoit aucune autre mesure de contrôle permettant de s'assurer de la conformité des partis politiques à l'égard de l'utilisation des renseignements contenus dans les listes électorales.

Infractions pénales et autres sanctions

La loi prévoit une infraction pour toute personne qui utilise, autorise ou permet que soient utilisés des renseignements contenus dans les listes électorales à des fins non électorales. La personne déclarée coupable de cette infraction est passible d'une amende maximale de 10 000 $, d'un emprisonnement maximal d'un an ou de ces deux peines[269].

La loi ne prévoit aucune infraction particulière pour une candidate ou un candidat qui manque à son obligation de détruire les listes électorales.

Rôle et pouvoirs de l'autorité de surveillance

Le directeur général des élections est chargé de veiller à l'observation et au contrôle de l'application de la loi électorale. Il peut, de sa propre initiative ou à la demande d'une personne, mener une enquête. S'il a des motifs de croire qu'une infraction à la loi a été commise, il peut soumettre l'affaire au directeur des poursuites pénales, qui décide s'il y a lieu d'engager des poursuites visant à sanctionner l'infraction[270].

Il peut également conclure une entente de conformité avec toute personne qu'il considère avoir enfreint la loi. Cette entente peut imposer des conditions particulières pour que la personne se conforme à la loi, mais ne constitue pas une déclaration de culpabilité[271].

Pour dépister les utilisations non autorisées de la liste électorale, le directeur général des élections peut y insérer des renseignements concernant des électeurs fictifs[272].

268. *Ibid.*, art. 62.
269. *Ibid.*, art. 333 et 348.
270. *Ibid.*, art. 285, 287 et 292.
271. *Ibid.*, art. 294.
272. *Ibid.*,. art. 62.

Île-du-Prince-Édouard

Régime d'encadrement

Les partis politiques ne sont pas assujettis au *Freedom of Information and Protection of Privacy Act*[273], qui s'applique aux renseignements personnels détenus par les organismes publics[274].

L'*Election Act*[275] encadre la protection des renseignements personnels détenus par les partis politiques. Cet encadrement ne porte cependant que sur l'utilisation des renseignements provenant de la liste permanente des électeurs.

Plus spécifiquement, la loi prévoit que la liste électorale ne peut être utilisée à d'autres fins que celles prévues par la loi électorale[276].

Renseignements fournis par l'administration électorale

Les partis politiques reçoivent la liste électorale en période électorale. Cette liste contient les renseignements suivants[277] :

- Nom ;
- Adresse.

Autres obligations

La loi ne prévoit aucune mesure permettant de s'assurer de la conformité des partis politiques à l'égard de l'utilisation des renseignements contenus dans les listes électorales.

Infractions pénales et autres sanctions

La loi prévoit une infraction pour toute personne qui utilise la liste électorale, en tout ou en partie, à une fin qui n'est pas prévue par la loi. Celle-ci prévoit qu'un parti politique et ses membres ainsi qu'une députée ou un député peuvent l'utiliser afin de communiquer avec les électrices et les électeurs, notamment pour faire campagne et pour solliciter des contributions[278].

La personne déclarée coupable de cette infraction est passible d'une amende maximale de 2 000 $, d'un emprisonnement maximal de deux ans ou de ces deux peines[279].

---

273. RSPEI 1988, chap. F-15-01.
274. Aucune loi provinciale n'encadre les entreprises à l'Île-du-Prince-Édouard ; c'est la loi fédérale qui s'applique.
275. RSPEI 1988, chap. E-1.1.
276. *Ibid.*, art. 129.1.
277. *Ibid.*, art. 62.
278. *Ibid.*, art. 129.1.
279. *Ibid.*, art. 137.

Cette infraction constitue également une manœuvre frauduleuse au sens de la loi, ce qui a pour conséquence que la personne déclarée coupable ne peut être inscrite comme électrice ni être élue comme députée pendant une période de cinq ans[280].

Rôle et pouvoirs de l'autorité de surveillance

Le directeur général des élections est chargé de l'application de la loi. Il ne dispose d'aucun pouvoir lui permettant de s'assurer de la conformité des obligations prévues à la loi[281].

Nouveau-Brunswick

Régime d'encadrement

Les partis politiques ne sont pas assujettis à la *Loi sur le droit à l'information et la protection de la vie privée*[282], qui s'applique aux renseignements personnels détenus par les organismes publics[283].

La *Loi électorale*[284] encadre la protection des renseignements personnels détenus par les partis politiques. Cet encadrement ne porte cependant que sur l'utilisation des renseignements provenant du registre des électrices et des électeurs.

Plus spécifiquement, la loi prévoit que les partis politiques ne peuvent utiliser ces renseignements à d'autres fins que pour communiquer avec les électrices et les électeurs, notamment afin de solliciter des contributions et de recruter des membres[285].

Renseignements fournis par l'administration électorale

Les députées et députés reçoivent chaque année la liste des électrices et des électeurs de leur circonscription qui sont inscrits au registre des électeurs. Sur demande, chaque parti politique peut également la recevoir. La liste, transmise en version électronique, contient les renseignements suivants[286] :

- Nom ;
- Sexe ;
- Adresse résidentielle et postale.

En période électorale, les candidates et candidats reçoivent des listes électorales qui contiennent les mêmes renseignements[287].

---

280. *Ibid.*, art. 141-142.
281. *Ibid.*, art. 3.
282. SNB 2009, chap. R-10.6.
283. Aucune loi provinciale n'encadre les entreprises au Nouveau-Brunswick ; c'est la loi fédérale qui s'applique.
284. RSNB 1973, chap. E-3.
285. *Ibid.*, art. 42 et 42.1.
286. *Ibid.*, art. 20.5.
287. *Ibid.*, art. 20(3) et 41.

Autres obligations

La *Loi* ne prévoit aucune mesure permettant de s'assurer de la conformité des partis politiques à l'égard de l'utilisation des renseignements contenus dans les listes électorales.

Infractions pénales et autres sanctions

La *Loi* prévoit une infraction pour quiconque utilise une liste électorale ou le registre des électrices et des électeurs ou qui en tire des extraits à une autre fin que celles expressément prévues par la *Loi*. La personne déclarée coupable de cette infraction est passible d'une amende maximale de 7 620 $[288].

Cette infraction constitue également une manœuvre frauduleuse au sens de la *Loi*, ce qui a pour conséquence que la personne déclarée coupable ne peut être inscrite comme électrice ou être élue comme députée pendant une période de cinq ans[289].

Rôle et pouvoirs de l'autorité de surveillance

Le directeur général des élections doit diriger et surveiller l'application de la *Loi*. Il ne dispose d'aucun pouvoir d'enquête lui permettant de s'assurer de la conformité des obligations prévues à la *Loi*[290].

288. *Ibid.*, art. 112.1.
289. *Ibid.*, art. 118.
290. *Ibid.*, art. 5(4).

Ontario

Régime d'encadrement

Les partis politiques ne sont pas assujettis à la *Loi sur l'accès à l'information et la protection de la vie privée*[291], qui s'applique aux renseignements personnels détenus par les organismes publics[292].

La *Loi électorale*[293] encadre la protection des renseignements personnels détenus par les partis politiques. Cet encadrement ne porte cependant que sur l'utilisation et la communication des renseignements provenant du registre permanent des électrices et des électeurs ou d'une liste électorale produite à partir de ce registre.

Plus spécifiquement, la *Loi* prévoit que les personnes qui obtiennent ces renseignements conformément à la *Loi* ne peuvent les utiliser qu'à des fins électorales et ne doivent pas les utiliser à des fins commerciales. Par ailleurs, la *Loi* interdit de communiquer ces renseignements à toute personne qui ne s'est pas engagée par écrit à respecter ces restrictions[294].

La *Loi* prévoit que le directeur général des élections peut fournir des lignes directrices qui contiennent des exigences supplémentaires concernant l'utilisation et la communication des renseignements sur les électrices et les électeurs[295].

Renseignements fournis par l'administration électorale

Chaque députée et député peut recevoir, une fois par année, la liste électorale de sa circonscription. Sur demande, cette liste est également transmise à chaque parti politique. La liste est transmise en version électronique et contient les renseignements suivants[296] :

- Nom ;
- Adresse permanente et postale ;
- Numéro identificateur unique.

Après l'élection, les partis politiques reçoivent la liste de ces renseignements, incluant une indication précisant si l'électrice ou l'électeur a voté[297].

---

291. RSO 1990, chap. F.31.
292. Aucune loi provinciale n'encadre les entreprises en Ontario ; c'est la loi fédérale qui s'applique.
293. RSO 1990, chap. E.6.
294. *Ibid.*, art. 17.4.
295. *Ibid.*, art. 17.5.
296. *Ibid.*, art. 4.8 et 17.3.
297. *Ibid.*, art. 47.

En période électorale, les candidates, les candidats et les partis politiques reçoivent des listes électorales qui contiennent les mêmes renseignements. Ils peuvent également obtenir la liste des personnes qui ont voté après chaque jour du scrutin[298].

Les partis politiques reçoivent une copie du registre des électrices et des électeurs absents qui résident temporairement à l'extérieur de l'Ontario. La copie qu'ils reçoivent ne contient pas l'adresse postale de l'électeur à l'extérieur de l'Ontario[299].

Autres obligations

Les partis politiques doivent élaborer et mettre en œuvre une politique pour s'assurer que leurs candidats, leurs députés, leurs employés et tout autre mandataire respectent les restrictions relatives à l'utilisation des renseignements sur les électrices et les électeurs et cette politique doit respecter les lignes directrices émises par le directeur général des élections. Les députés indépendants et les candidats indépendants sont également tenus de satisfaire à cette obligation[300].

Les partis politiques, les députés indépendants et les candidats indépendants doivent transmettre leurs politiques au directeur général des élections s'ils souhaitent obtenir des renseignements provenant du registre permanent des électrices et des électeurs.

Selon les exigences prévues aux lignes directrices, les partis politiques doivent, avant de communiquer des renseignements sur les électrices et les électeurs à toute personne qu'ils autorisent à y accéder, s'assurer qu'elle signe un engagement à respecter la confidentialité de ces renseignements. Les partis doivent tenir un registre de toutes ces communications, qui comprend notamment une indication précisant si les renseignements ont été retournés ou détruits.

Ce registre doit être déposé auprès du directeur général des élections après chaque transmission annuelle de la liste des électrices et des électeurs de même qu'après chaque scrutin.

Les partis politiques sont tenus de détruire les renseignements sur les électrices et les électeurs lorsque leur utilisation n'est plus autorisée et de déposer des certificats de destruction auprès du directeur général des élections. Les partis ne sont toutefois pas tenus de supprimer les renseignements intégrés à leurs bases de données électorales. Seuls les documents fournis par le directeur général des élections et les copies supplémentaires doivent être détruits.

298. *Ibid.*, art. 19 et 45.

299. *Ibid.*, art. 45.3 et 45.13.

300. *Ibid.*, art. 17.6.

Infractions pénales et autres sanctions

La *Loi* ne prévoit aucune infraction particulière pour une personne qui utiliserait ou communiquerait des renseignements sur les électrices et les électeurs en contravention à la *Loi*. Cependant, la *Loi* prévoit une infraction générale pour tout manquement qui ne fait pas l'objet d'une infraction particulière. Dans ce cas, une personne est passible d'une amende d'au plus 5000 $[301].

Rôle et pouvoirs de l'autorité de surveillance

Le directeur général des élections est chargé de surveiller l'application de la *Loi*. Il peut mener des enquêtes et des examens. Il doit signaler au procureur général toute contravention apparente à la *Loi*[302].

Il peut rendre publique toute politique reçue d'un parti politique ainsi que toute incompatibilité entre cette politique, les lignes directrices et les pratiques réelles du parti quant à l'utilisation des renseignements sur les électrices et les électeurs[303].

À la demande d'une électrice ou d'un électeur, il peut supprimer tout renseignement des listes électorales transmises aux partis politiques, s'il a des raisons de croire que, si ce renseignement était communiqué, il mettrait la vie, la santé ou la sécurité de cette personne en danger[304].

301. *Ibid.*, art. 97.
302. *Ibid.*, art. 4.0.1 et 4.0.2.
303. *Ibid.*, art. 17.6.
304. *Ibid.*, art. 4.7.

Manitoba

Régime d'encadrement

Les partis politiques ne sont pas assujettis à la *Loi sur l'accès à l'information et la protection de la vie privée*[305], qui s'applique aux renseignements personnels détenus par les organismes publics[306].

La *Loi électorale*[307] encadre la protection des renseignements personnels détenus par les partis politiques. Cet encadrement ne porte cependant que sur l'utilisation des renseignements provenant du registre des électrices et des électeurs.

Plus spécifiquement, les partis politiques ne peuvent utiliser les renseignements contenus dans les listes électorales que pour communiquer avec les électrices et les électeurs. Les députées et députés peuvent les utiliser dans l'exercice de leurs fonctions[308].

Renseignements fournis par l'administration électorale

Chaque année[309], les partis politiques reçoivent la liste des électrices et des électeurs inscrits au registre. Sur demande, chaque députée et député peut recevoir la liste de sa circonscription. La liste est transmise en version électronique et contient les renseignements suivants[310] :

- Nom ;
- Adresse résidentielle et postale ;
- Numéro de téléphone ;
- Numéro identificateur unique.

En période électorale, les candidates et candidats reçoivent des listes électorales qui contiennent les mêmes renseignements[311].

Autres obligations

Les personnes ou les partis politiques qui ont reçu une copie d'une liste électorale sont tenus de prendre les mesures raisonnables afin de protéger la liste et les renseignements qu'elle contient contre la perte ou contre une utilisation non autorisée. Ils sont également tenus de signaler toute perte au directeur général des élections[312].

---

305. CCSM, chap. F175.
306. Aucune loi provinciale n'encadre les entreprises au Manitoba ; c'est la loi fédérale qui s'applique.
307. CPLM, chap. E30.
308. *Ibid.*, art. 63.9(3).
309. Les modifications législatives permettant la création du registre ont été adoptées en 2017. La transmission annuelle des listes débutera en 2019.
310. *Ibid.*, art. 63.8(1)(2).
311. *Ibid.*, art. 75(1).
312. *Ibid.*, art. 63.9(1)(2)

Infractions pénales et autres sanctions

La *Loi* prévoit une infraction pour quiconque utilise la totalité ou une partie de la liste électorale dans un but non autorisé[313].

La personne déclarée coupable de cette infraction est passible d'une amende maximale de 10 000 $, d'un emprisonnement maximal d'un an ou de ces deux peines[314].

Rôle et pouvoirs de l'autorité de surveillance

Le directeur général des élections nomme une ou un commissaire aux élections, qui est chargé du contrôle de l'application de la *Loi*. Le commissaire peut, de sa propre initiative ou à la demande d'une personne, faire enquête sur toute question qui pourrait constituer une contravention à la *Loi*. Il peut intenter des poursuites pour infraction à la *Loi* s'il a des motifs raisonnables de croire qu'une telle infraction a été commise et s'il estime que l'intérêt public le justifie[315].

Pour dépister les utilisations non autorisées de la liste électorale, le directeur général des élections peut y insérer des renseignements concernant des électrices ou des électeurs fictifs[316].

Saskatchewan

Régime d'encadrement

Les partis politiques ne sont pas assujettis à la loi *The Freedom of Information and Protection of Privacy Act*[317] ni à la loi *The Local Authority Freedom of Information and Protection of Privacy Act*[318], qui encadrent la protection des renseignements personnels détenus par les organismes publics et les organismes municipaux[319].

The Election Act[320] encadre la protection des renseignements personnels détenus par les partis politiques. Cet encadrement ne porte cependant que sur l'utilisation des renseignements provenant du registre des électrices et des électeurs.

Plus spécifiquement, la loi permet aux candidates, aux candidats et aux partis politiques d'utiliser les listes électorales pour communiquer avec les électrices et les électeurs, notamment pour solliciter des contributions et pour recruter des membres. Les députées et députés peuvent les utiliser dans l'exercice de leurs fonctions[321].

313. *Ibid.*, art. 183(6).
314. *Ibid.*, art. 185(1).
315. *Ibid.*, art. 186(1)(3) et 187(1).
316. *Ibid.*, art. 63.9(5).
317. SS 1990-91, chap. F-22.01.
318. SS 1990-91, chap. L-27.1.
319. Aucune loi provinciale n'encadre les entreprises en Saskatchewan ; c'est la loi fédérale qui s'applique.
320. SS 1996, chap. E-6.01.
321. *Ibid.*, art. 18.8.

Renseignements fournis par l'administration électorale

En période électorale, chaque candidate et chaque candidat reçoit la liste électorale de sa circonscription en version papier et électronique. Les partis politiques peuvent recevoir la liste électorale des circonscriptions dans lesquelles ils présentent un candidat. La version électronique de la liste contient les renseignements suivants[322] :

- Nom ;
- Adresse ;
- Année de naissance, lorsque deux électeurs portent le même nom à la même adresse.

Après l'élection, les partis politiques qui ont conclu une entente de confidentialité avec le directeur général des élections peuvent recevoir la liste électorale qui contient l'année de naissance de l'ensemble des électrices et électeurs.

Autres obligations

En période électorale, les candidates, les candidats et les partis politiques qui souhaitent obtenir la liste électorale doivent signer un engagement à la confidentialité. Les partis politiques qui souhaitent obtenir la liste comprenant l'année de naissance doivent conclure une entente qui prévoit que le parti met en place les meilleures pratiques en matière de sécurité et de protection de la vie privée[323].

Infractions pénales et autres sanctions

La loi ne prévoit aucune infraction particulière pour une personne qui utiliserait ou communiquerait des renseignements sur les électrices et les électeurs en contravention à la loi. Cependant, la loi prévoit une infraction générale pour tout manquement qui ne fait pas l'objet d'une infraction particulière. Dans ce cas, une personne est passible d'une amende d'au plus 5000 $, d'un emprisonnement maximal de deux ans ou des deux peines[324].

Rôle et pouvoirs de l'autorité de surveillance

Le directeur général des élections est chargé de surveiller l'application de la loi. Il peut mener des enquêtes et des examens. Il a le pouvoir de retirer des renseignements du registre des électeurs ou des listes électorales afin d'assurer la sécurité et la vie privée des électrices et des électeurs. Il doit également prendre les mesures raisonnables pour prévenir toute utilisation non autorisée des listes électorales[325].

---

322. Le contenu des listes électorales et ses modalités de transmission sont déterminés par le bulletin d'interprétation ESKIB-2015/01 émis par le directeur général des élections le 28 décembre 2015 (https://cdn.elections.sk.ca/upload/eskib-2015-01-voterslistprivacy_v10_final.pdf).
323. Ces exigences sont également déterminées par le bulletin d'interprétation ESKIB-2015/01.
324. SS 1996, chap. E-6.01, art. 216.
325. *Ibid.*, art. 18.6, 18.7 et 280.

Alberta

Régime d'encadrement

Les partis politiques ne sont assujettis à aucune des deux lois générales qui encadrent la protection des renseignements personnels, soit le *Freedom of Information and Protection of Privacy Act*[326], qui s'applique aux renseignements personnels détenus par les organismes publics, et le *Personal Information Protection Act*[327], qui s'applique aux renseignements détenus par des organismes du secteur privé.

L'*Election Act*[328] encadre la protection des renseignements personnels détenus par les partis politiques. Cet encadrement ne porte cependant que sur l'utilisation des renseignements provenant du registre des électrices et des électeurs.

Plus spécifiquement, la loi prévoit qu'un parti politique ne peut utiliser la liste électorale que pour communiquer avec les électrices et les électeurs, notamment afin de solliciter des contributions ou de recruter des membres. Les députées et les députés peuvent l'utiliser dans l'exercice de leurs fonctions. Les candidates et candidats peuvent l'utiliser pour communiquer avec les électeurs pendant la période électorale et afin de solliciter des contributions, lorsqu'ils y sont autorisés[329].

Renseignements fournis par l'administration électorale

Deux ans après une élection générale, à la suite de l'établissement d'une nouvelle carte électorale[330] et à la suite d'un décret ordonnant la tenue d'une élection, les partis politiques et les députés indépendants reçoivent la liste électorale de toutes les circonscriptions en version papier ou électronique. La liste contient les renseignements suivants[331] :

- Nom ;
- Adresse ;
- Numéro de téléphone ;
- Numéro identificateur unique.

Les candidats indépendants reçoivent la liste électorale de leur circonscription en période électorale[332].

Les candidates et candidats peuvent recevoir la liste des électrices et des électeurs qui ont voté par anticipation. Sur demande, les candidats peuvent obtenir la liste des électeurs inscrits aux votes spéciaux ; cette liste ne comprend que leur nom et leur adresse principale[333].

---

326. RSA 2000, chap. F-25.
327. RSA 2003, chap. P-6.5.
328. RSA 2000, chap. E-1.
329. *Ibid.*, art. 20.
330. Seulement les listes électorales des circonscriptions dont le territoire est modifié par la nouvelle carte électorale.
331. RSA 2000, chap. E-1, art. 17 et 18.
332. *Ibid.*, art. 63.
333. *Ibid.*, art. 98 et 117.

Les partis politiques et chaque députée et député reçoivent la liste électorale après une élection générale[334].

Autres obligations

Toute personne ou tout parti politique qui reçoit la liste électorale conformément à loi doit s'assurer de prendre les mesures raisonnables afin de protéger la liste électorale et les renseignements qu'elle contient d'une perte ou d'une utilisation non autorisée. Il doit notamment signaler toute perte auprès du directeur général des élections[335].

Infractions pénales et autres sanctions

La loi prévoit une infraction pour toute personne qui utilise la liste électorale à une fin non autorisée par la loi. La personne déclarée coupable de cette infraction est passible d'une amende maximale de 100 000 $, d'un emprisonnement maximal d'un an ou de ces deux peines[336].

Rôle et pouvoirs de l'autorité de surveillance

Le commissaire aux élections est chargé du contrôle de l'application de la loi. Il peut, de sa propre initiative ou à la demande d'une personne ou du directeur général des élections, faire enquête sur toute question qui pourrait constituer une contravention à la loi[337].

Le commissaire peut, s'il est d'avis qu'une personne a enfreint la loi, transmettre un avis de sanction pécuniaire ou une lettre de réprimande. Une personne qui paie une sanction ne peut faire l'objet d'une poursuite pénale liée à la même infraction[338].

Il peut également conclure une entente de conformité avec toute personne qu'il considère avoir enfreint la loi. Cette entente peut imposer des conditions particulières pour que cette personne se conforme à la loi, mais ne constitue pas une déclaration de culpabilité[339].

Il peut également soumettre l'affaire au directeur des poursuites pénales, qui décide s'il y a lieu d'engager des poursuites visant à la sanctionner[340].

Pour dépister les utilisations non autorisées de la liste électorale, le directeur général des élections peut y insérer des renseignements concernant des électrices ou des électeurs fictifs[341].

334. *Ibid.*, art. 19.
335. *Ibid.*, art. 19.1.
336. *Ibid.*, art. 163.
337. *Ibid.*, art. 153.09.
338. *Ibid.*, art. 153.1.
339. *Ibid.*, art. 153.4.
340. *Ibid.*, art. 154(1).
341. *Ibid.*, art. 18(7).

Colombie-Britannique

Régime d'encadrement

Les partis politiques sont assujettis au *Personal Information Protection Act*[342] (PIPA), qui s'applique à toute organisation qui détient des renseignements personnels, incluant toute personne, association non incorporée, syndicat, fiducie ou organisation à but non lucratif, sauf exception[343].

Étant donné les obligations qui découlent du PIPA[344] :

- Les partis politiques sont responsables de la protection de tous les renseignements personnels qu'ils détiennent. Ils doivent notamment désigner une personne responsable de la protection des renseignements personnels, qui doit s'assurer que les pratiques du parti respectent les obligations prévues par la loi.
- Les partis politiques ne peuvent recueillir, utiliser ou communiquer des renseignements personnels sans le consentement des personnes concernées, à moins que la loi ne les autorise.
- Lorsqu'ils recueillent des renseignements, les partis doivent préciser à quelles fins seront utilisés ces renseignements. Ils doivent également limiter la collecte de renseignements à ceux qui sont nécessaires à ces fins.
- Les partis politiques ne doivent utiliser les renseignements personnels qu'aux seules fins pour lesquelles ils ont obtenu le consentement des personnes concernées, à moins que la loi ne les autorise. Ils doivent également restreindre la communication de ces renseignements à ces fins.
- Si une personne leur en fait la demande, les partis politiques doivent lui donner accès à tout renseignement qu'ils détiennent à son sujet.
- Les partis politiques doivent prendre les mesures appropriées pour s'assurer que les renseignements personnels qu'ils détiennent demeurent exacts et à jour. Ils doivent également mettre en place des mesures de sécurité afin de prévenir les risques de collecte, d'utilisation, de communication ou de destruction non autorisée de ces renseignements.
- Les partis politiques doivent détruire tout renseignement personnel lorsqu'il ne leur est plus nécessaire.
- Les partis politiques doivent élaborer des politiques leur permettant de respecter ces obligations ainsi qu'une procédure pour gérer toute plainte à ce sujet. Ces politiques et cette procédure doivent être accessibles sur demande.

342. SBC 2003, chap. 63.

343. Depuis 2011, le commissaire à la vie privée et à l'information de la Colombie-Britannique est d'avis que les partis politiques provinciaux sont des organisations au sens de la loi.

344. SBC 2003, chap. 63, art. 4 à 24.

L'*Election Act*[345] encadre également la protection des renseignements personnels détenus par les partis politiques. Cet encadrement ne porte cependant que sur l'utilisation des renseignements provenant du registre des électrices et des électeurs.

Plus spécifiquement, la loi prévoit qu'un parti politique ne peut utiliser la liste électorale qu'à des fins prévues par la loi électorale[346].

L'*Electoral Purposes for Access to and Use of Personal Information Regulation*[347] précise qu'un parti politique, un candidat et un député peut utiliser ces renseignements afin de communiquer avec les électrices et les électeurs, notamment pour solliciter des appuis en campagne électorale, des contributions ou pour recruter des membres.

Renseignements fournis par l'administration électorale

Les députées et députés ainsi que les partis politiques reçoivent la liste électorale deux fois par année. La liste est transmise en version électronique et contient les renseignements suivants :

- Nom ;
- Adresse.

La liste transmise aux partis politiques contient également une indication précisant si l'électrice ou l'électeur a voté lors de la dernière élection générale ou partielle, le cas échéant[348].

En période électorale, les candidates et candidats peuvent recevoir la liste électorale de leur circonscription, qui contient les mêmes renseignements que celle transmise aux partis politiques[349].

Autres obligations

Un parti politique, un candidat ou un député qui souhaite obtenir la liste électorale doit soumettre une politique en matière de protection de la vie privée qui est jugée acceptable par le directeur général des élections. Une politique jugée acceptable doit notamment comprendre des dispositions concernant les mesures de sécurité, la destruction des renseignements, la tenue d'un registre des personnes ayant accès aux renseignements et le signalement des atteintes à la vie privée. La politique doit reconnaître le droit au directeur général des élections d'effectuer des vérifications de conformité[350].

345. RSBC 1996, chap. 106.
346. *Ibid.*, art. 275.
347. BC Reg 205/2015.
348. RSBC 1996, chap. 106, art. 51.
349. *Ibid.*, art. 48.
350. *Ibid.*, art. 275.

Infractions pénales et autres sanctions

La loi électorale prévoit une infraction pour toute personne qui utilise la liste électorale à une fin non autorisée par la loi. La personne déclarée coupable de cette infraction est passible d'une amende maximale de 20 000 $, d'un emprisonnement maximal de deux ans ou de ces deux peines[351].

Rôle et pouvoirs de l'autorité de surveillance

Le commissaire à la vie privée et à l'information est responsable de veiller à l'application du PIPA. Il peut procéder à des vérifications pour s'assurer de son application. Il peut également, de sa propre initiative ou à la demande d'une personne, faire enquête sur tout manquement à cette loi. À la suite d'une enquête, le commissaire peut émettre une ordonnance visant à rectifier tout manquement à loi, pouvant aller jusqu'à la destruction de renseignements qui ont été recueillis en contravention à la loi[352].

Le directeur général des élections est responsable de veiller à l'application de la loi électorale. Il peut procéder à des vérifications pour s'assurer de son application. Il peut également, de sa propre initiative ou à la demande d'une personne, faire enquête sur toute infraction. S'il a des motifs de croire qu'une infraction à la loi a été commise, il peut soumettre l'affaire au directeur des poursuites pénales, qui décide s'il y a lieu d'engager des poursuites visant à sanctionner l'infraction[353].

Pour dépister les utilisations non autorisées de la liste électorale, le directeur général des élections peut y insérer des renseignements concernant des électeurs fictifs. Le directeur général des élections peut également retirer certains renseignements au sujet d'une électrice ou d'un électeur afin d'assurer sa sécurité ou sa vie privée.[354].

351. *Ibid.*, art. 267.
352. SBC 2003, chap. 63, art. 48 et 52.
353. RSBC 1996, chap. 106, art. 276.
354. *Ibid.*, art. 51.

Bibliographie

27e Conférence des commissaires à la protection des données et à la vie privée. *Résolution sur l'utilisation de données personnelles pour la communication politique*, 16 septembre 2005. [https://edps.europa.eu/sites/edp/files/publication/05-09-16_resolution_political_communication_fr.pdf].

Ace Electoral Knowledge Network. « Élections et technologie », *ACE Project*. [http://aceproject.org/ace-fr/topics/et/default].

Alberta. *Freedom of Information and Protection of Privacy Act*, RSA 2000, chap. F-25. [http://www.qp.alberta.ca/documents/Acts/F25.pdf].

Alberta. *Personal Information Protection Act*, RSA 2003, chap. P-6.5. [http://www.qp.alberta.ca/documents/Acts/P06P5.pdf].

Alberta. *Election Act*, RSA 2000, chap. E-1. [http://www.qp.alberta.ca/documents/Acts/E01.pdf].

ARTIAS. « Protection de la personnalité », *Guide social romand*. [https://www.guidesocial.ch/recherche/fiche/protection-de-la-personnalite-125].

Assemblée nationale du Québec*. Code civil du Québec*, RLRQ, chap. CCQ-1991. [http://legisquebec.gouv.qc.ca/fr/showdoc/cs/CCQ-1991].

Assemblée nationale du Québec. *Journal des débats*, vol. 35, nº 85, 8 avril 1997.

Assemblée nationale du Québec. *Journal des débats de la Commission des institutions*, vol. 35, nº 135, 9 juin 1998.

Assemblée nationale du Québec. *Loi électorale*, RLRQ, chap. E-3.3. [http://legisquebec.gouv.qc.ca/fr/ShowDoc/cs/E-3.3].

Assemblée nationale du Québec. *Loi sur les élections et les référendums dans les municipalités*, RLRQ, chap. E-2.2. [http://legisquebec.gouv.qc.ca/fr/ShowDoc/cs/E-2.2].

Assemblée nationale du Québec. *Loi sur les élections scolaires*, RLRQ, chap. E-2.3. [http://legisquebec.gouv.qc.ca/fr/ShowDoc/cs/E-2.3].

Assemblée nationale du Québec*. Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ, chap. A-2.1. [http://legisquebec.gouv.qc.ca/fr/ShowDoc/cs/A-2.1].

Assemblée nationale du Québec. *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ, chap. A-2.1. [http://www.legisquebec.gouv.qc.ca/fr/showdoc/cs/P-39.1].

Assemblée nationale du Québec. *Loi sur la sécurité privée*, RLRQ, chap. S-3.5. [http://www.legisquebec.gouv.qc.ca/fr/ShowDoc/cs/S-3.5].

Audureau, William. « Ce qu'il faut savoir sur Cambridge Analytica », *Le Monde*, 22 mars 2018. [https://www.lemonde.fr/pixels/article/2018/03/22/ce-qu-il-faut-savoir-sur-cambridge-analytica-la-societe-au-c-ur-du-scandale-facebook_5274804_4408996.html].

Australian Electoral Commision. *About the Commonwealth Electoral Roll*. [https://www.aec.gov.au/Enrolling_to_vote/About_Electoral_Roll/].

Australian Law Reform Commission. *For Your Information: Australian Privacy Law and Practice (ALRC Report 108*), vol. 2, mai 2008. [https://www.alrc.gov.au/publications/41.%20Political%20Exemption/introduction].

Australie. *Commonwealth Electoral Act 1918*, art. 83 et 90B. [https://www.legislation.gov.au/Details/C2018C00259].

Autorité de protection des données de Belgique. *Traitement de données à caractère personnel à des fins d'envois personnalisés de propagande électorale et respect de la vie privée des citoyens : principes fondamentaux*. [https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Note_elections_RGPD.pdf].

Barnes, Susan B. « A Privacy Paradox: Social Networking in the United States », *First Monday*, vol. 11, nº 9, 4 septembre 2006. [https://firstmonday.org/ojs/index.php/fm/article/view/1394/1312].

Bartlett J., Smith J. et Acton R. « The Future of Political Campaigning », *Demos*, juillet 2018, [https://demosuk.wpengine.com/wp-content/uploads/2018/07/The-Future-of-Political-Campaigning.pdf].

Belgique. *Code électoral*. [http://www.ejustice.just.fgov.be/eli/loi/2018/04/19/2018011790/justel].

Bennett, Colin J., et Robin M. Bayley. *Les partis politiques fédéraux du Canada et la protection des renseignements personnels : une analyse comparative, Rapport préparé pour le Commissariat à la vie privée du Canada*, 28 mars 2012. [https://www.priv.gc.ca/media/1757/pp_201203_f.pdf.].

Bennett, Colin J. *Voter Surveillance, Micro-Targeting and Democratic Politics: Knowing How People Vote Before They Do*, 11 avril 2014. [https://ssrn.com/abstract=2605183].

Bennett, Colin J. « Voter Databases, Micro-Targeting, and Data Protection Law: Can Political Parties Campaign in Europe as They Do in North America ? », *International Data Privacy Law*, vol. 6, nº 4, novembre 2016, p. 261-275. [https://academic.oup.com/idpl/article-abstract/6/4/261/2567747 ?redirectedFrom=fulltext].

Bennett, Colin. « A Data-Driven Election Can Be Ethical », *The Globe and Mail*, 13 août 2018. [https://www.theglobeandmail.com/opinion/article-a-data-driven-election-can-be-ethical/].

BIP Recherche. *Évaluation de la satisfaction des citoyens du Québec à la suite des élections générales du 1er octobre 2018*. [https://www.electionsquebec.qc.ca/francais/actualite-detail.php?id=6283].

Blais, Annabelle, et Alexandre Robillard. « L'arme secrète à 1 M$ de la CAQ », *TVA Nouvelles*, 4 octobre 2017. [https://www.tvanouvelles.ca/2017/10/04/larme-secrete-a-1-m-de-la-caq].

Blogue Droit européen. *Brexit or Not Brexit: How Will the GDPR Rules Apply to the UK ?* [https://blogdroiteuropeen.com/2017/03/01/brexit-or-not-brexit-how-will-the-gdpr-rules-apply-to-the-uk-part-1/].

Bloomberg. *Company Overview of Cambridge Analytica LLC*. [https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=4348771008].

Brunfaut, Simon. « Antoinette Rouvroy : «À mon sens, Zuckerberg est dépassé» », *L'Écho*, 23 mars 2018. [https://www.lecho.be/opinions/general/antoinette-rouvroy-a-mon-sens-zuckerberg-est-depasse/9995228.html].

Cadwalladr, Carole, et Emma Graham-Harrison. « Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach », *The Guardian*, 17 mars 2018. [https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election].

Cambridge Analytica. « Cambridge Analytica Congratulates President-elect Donald Trump and Vice President-elect Mike Pence », *PRNewswire*, 9 novembre 2016. [https://web.archive.org/web/20170127180813/https://cambridgeanalytica.org/news/pressrelease/1293].

Canada. *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5. [https://laws-lois.justice.gc.ca/fra/lois/p-8.6/TexteComplet.html].

Canada. *Loi sur la protection des renseignements personnels*, L.R.C. (1985), ch. P-21. [https://laws-lois.justice.gc.ca/fra/lois/p-21/].

Canada. *Loi électorale du Canada*, L.C. 2000, ch. 9. [https://laws-lois.justice.gc.ca/fra/lois/E-2.01/].

Cannon, Lawrence. *Mémoire au Conseil des ministres sur l'assujettissement du secteur privé à une loi sur la protection des renseignements personnels*, 9 novembre 1992.

Cardon, Dominique. *À quoi rêvent les algorithmes : nos vies à l'heure des big data*, Seuil, 2015.

Castonguay, Alec. « Les partis politiques vous espionnent », *L'Actualité*, 14 septembre 2015. [https://lactualite.com/societe/2015/09/14/les-partis-politiques-vous-espionnent].

Centre de la sécurité des télécommunications. *Cybermenaces contre le processus démocratique du Canada,* juin 2017. [https://cyber.gc.ca/sites/default/files/publications/cse-cyber-threat-assessment-f.pdf].

Channel 4 News. « Exposed: Undercover Secrets of Trump's Data Firm », 20 mars 2018. [https://www.channel4.com/news/exposed-undercover-secrets-of-donald-trump-data-firm-cambridge-analytica].

Châtillon, Georges. *Les données personnelles : enjeux juridiques et perspectives*, 28 février 2004. [https://www.pantheonsorbonne.fr/diplomes/master-droit-du-numerique/bibliotheque-numerique-du-droit-de-ladministration-electronique/droit/protection-des-donnees/les-donnees-personnelles-enjeux-juridiques-et-perspectives-rapport-de-georges-chatillon/].

Colombie-Britannique. *Personal Information Protection Act*, SBC 2003, chap. 63. [http://www.bclaws.ca/civix/document/id/complete/statreg/03063_01].

Colombie-Britannique. *Election Act,* RSBC 1996, chap. 106. [http://www.bclaws.ca/civix/document/id/complete/statreg/96106_00].

Colombie-Britannique. *Electoral Purposes for Access to and Use of Personal Information Regulation*, BC Reg 205/2015. [http://www.bclaws.ca/civix/document/id/lc/bcgaz2/v58n21_205-2015].

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. *Témoignages*, 1re session, 42e législature, 17 avril 2018, 0850. [http://www.noscommunes.ca/DocumentViewer/fr/42-1/ETHI/reunion-99/temoignages].

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. *Témoignages*, 1re session, 42e législature, 10 mai 2018, 0900. [http://www.noscommunes.ca/DocumentViewer/fr/42-1/ETHI/reunion-106/temoignages].

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. *Démocratie menacée : risques et solutions à l'ère de la désinformation et du monopole des données*, décembre 2018. [http://www.noscommunes.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-f.pdf].

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique. *Témoignages*, 1re session, 42e législature, 1er novembre 2018, 1215. [http://www.noscommunes.ca/DocumentViewer/fr/42-1/ETHI/reunion-124/temoignages].

Commissaire à l'information et à la protection de la vie privée de l'Ontario. *Trente années au service de l'accès à l'information et de la protection de la vie privée : rapport annuel 2017*, juin 2018. [https://www.ipc.on.ca/wp-content/uploads/2018/06/ar-2017-f-web.pdf].

Commissariat à la protection de la vie privée du Canada, Office of the Information and Privacy Commissioner of Alberta et Office of the Information and Privacy Commissioner for British Columbia. *Programme de gestion de la protection de la vie privée : la clé de la responsabilité*, 17 avril 2012. [https://www.priv.gc.ca/media/2104/gl_acc_201204_f.pdf.].

Commissariat à la protection de la vie privée du Canada (2018, 20 mars). *Le commissaire à la protection de la vie privée lance une enquête sur Facebook*. Repéré au https://www.priv.gc.ca/fr/nouvelles-du-commissariat/nouvelles-et-annonces/2018/nr-c_180320/.

Commission d'accès à l'information. *Protection des renseignements personnels*. [http://www.cai.gouv.qc.ca/entreprises/protection-des-renseignements-personnels-1].

Commission d'accès à l'information. *Mémoire relatif au document de réflexion proposant des amendements à la Loi électorale présenté à la Commission des institutions*, février 1996.

Commission d'accès à l'information. *Rétablir l'équilibre : rapport quinquennal 2016*. [http://www.cai.gouv.qc.ca/documents/CAI_RQ_2016.pdf].

Commission d'accès à l'information. *Les gardiens du droit d'accès à l'information et du droit à la vie privée réclament que les partis politiques soient assujettis à la réglementation et à la surveillance en matière de protection de la vie privée*, 17 septembre 2018. [http://www.cai.gouv.qc.ca/les-gardiens-du-droit-dacces-a-linformation-et-du-droit-a-la-vie-privee-reclament-que-les-partis-politiques-soient-assujettis-a-la-reglementation-et-a-la-surveillance-en-matiere-de-p/].

Commission d'accès à l'information. *Assurer la confiance et la confidentialité dans le processus électoral du Canada : résolution des commissaires fédéraux, provinciaux et territoriaux à l'information et à la protection de la vie privée*, 13 septembre 2018. [http://www.cai.gouv.qc.ca/documents/FPT-Resolution-on-privacy-and-political-parties-FRA-Final.pdf].

Commission d'accès aux documents administratifs. *Copie sur support numérique, et non simple consultation, des listes électorales (Avis 20131138),* 4 juillet 2013. [https://cada.data.gouv.fr/20131138/].

Commission d'accès aux documents administratifs. *Communication des listes électorales en vue de l'organisation d'une cousinade (Avis 20180364)*, 17 mai 2018. [https://cada.data.gouv.fr/20180364/].

Commission d'accès aux documents administratifs. *Communication des listes électorales du département (Avis 20180832)*, 15 septembre 2018. [https://cada.data.gouv.fr/20180832/].

Commission de la protection de la vie privée (Belgique). *Traitement de données à caractère personnel à des fins d'envois personnalisés de propagande électorale et respect de la vie privée des citoyens : principes fondamentaux*, mai 2018. [https://www.autoriteprotectiondonnees.be/sites/privacycommission/files/documents/Note_elections_RGPD.pdf].

Commission nationale pour la protection des données (Luxembourg). *Prospection électorale et protection des données,* 21 août 2018. [https://cnpd.public.lu/fr/actualites/national/2018/08/communication-administres.html].

Commission nationale informatique et libertés. *Délibération nº 2012-020 du 26 janvier 2012 portant recommandation relative à la mise en œuvre, par les partis ou groupements à caractère politique, élus ou candidats à des fonctions électives, de fichiers dans le cadre de leurs activités politiques*. [https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000025364626&fastReqId=1082859898&fastPos=1].

Commission nationale informatique et libertés. *Communication politique : obligations légales et bonnes pratiques*. [https://www.cnil.fr/sites/default/files/typo/document/CNIL_Politique.pdf].

Commission nationale informatique et libertés et Conseil supérieur de l'audiovisuel. *Campagnes électorales : tout savoir sur les règles CSA et CNIL*. [https://www.cnil.fr/sites/default/files/atoms/files/guide_cnil_et_csa.pdf].

Confédération Suisse. *Prescriptions régissant les campagnes électorales et les votations*. [https://www.ch.ch/fr/democratie/les-partis-politiques/regles-pour-la-publicite-des-partis-en-suisse/].

Confédération Suisse. *Faire du vote électronique un canal de vote ordinaire : le Conseil fédéral projette d'ouvrir une consultation en automne 2018*, 27 juin 2018. [https://biblio.parlament.ch/e-docs/394980.pdf].

Conseil fédéral suisse. *Rapport du Conseil fédéral sur l'évaluation de la loi fédérale sur la protection des données*, 9 décembre 2011. [https://www.admin.ch/opc/fr/federal-gazette/2012/255.pdf].

Contrôleur européen de la protection des données. *Avis du CEPD sur la manipulation en ligne et les données à caractère personnel (nº 3/2018)*, mars 2018. [https://edps.europa.eu/sites/edp/files/publication/18-03-19_opinion_online_manipulation_fr.pdf].

Cornellier, Manon. « Et les partis politiques, eux ? », *Le Devoir*, 29 mars 2018. [https://www.ledevoir.com/opinion/editoriaux/523937/reseaux-sociaux-et-vie-privee-et-les-partis-politiques-eux].

Croteau, Martin. « Scandale Facebook : des pouvoirs d'enquête accrus pour le DGEQ », *La Presse*, 7 avril 2018. [https://www.lapresse.ca/actualites/201804/06/01-5160187-scandale-facebook-des-pouvoirs-denquete-accrus-pour-le-dgeq.php].

Croteau, Martin. « Ce que les partis savent sur vous », *La Presse+*, 20 août 2018. [http://mi.lapresse.ca/screens/8a829cee-9623-4a4c-93cf-3146a9c5f4cc__7C___0.html].

Davies, Harry. « Ted Cruz Using Firm that Harvested Data on Millions of Unwitting Facebook Users », *The Guardian*, 11 décembre 2015. [https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data].

Davison, Janet. « Robocalling and the Art of Finding Voters », *CBC News*, 29 février 2012. [http://www.cbc.ca/news/politics/story/2012/02/29/f-voter-identification.html].

Del Biaggio, Cristina. « L'UDC, des moutons noirs aux rangers », *Le Monde diplomatique*, 18 octobre 2011. [https://blog.mondediplo.net/2011-10-18-L-UDC-des-moutons-noirs-aux-rangers].

Dehaye, Paul-Olivier. « Cambridge Analytica Demonstrably Non-compliant with Data Protection Law », *PersonalData.IO*, 3 mars 2017. [https://medium.com/personaldata-io/cambridge-analytica-demonstrably-non-compliant-with-data-protection-law-95ec5712b61].

Deniau, Kévin. « Cambridge Analytica : tout comprendre sur la plus grande crise de l'histoire de Facebook », *Siècle digital*, 23 mars 2018. [https://siecledigital.fr/2018/03/23/cambridge-analytica-tout-comprendre-sur-la-plus-grande-crise-de-lhistoire-de-facebook/].

Detrow, Scott. « What Did Cambridge Analytica Do During The 2016 Election ? », *NPR - National Public Radio (US)*, 20 mars 2018. [https://www.npr.org/2018/03/20/595338116/what-did-cambridge-analytica-do-during-the-2016-election].

Directeur général des élections. *Documents de réflexion : amendements à la Loi électorale*, 12 décembre 1995.

Directeur général des élections. *Rapport annuel de gestion 2012-2013*. [https://www.electionsquebec.qc.ca/documents/pdf/rapport-annuel-dge-2012-2013.pdf].

Directeur général des élections. *Rapport annuel de gestion 2014-2015*. [https://www.electionsquebec.qc.ca/documents/pdf/DGE-6326_15-09.pdf].

Directeur général des élections. *Rapport annuel de gestion 2015-2016*. [https://www.electionsquebec.qc.ca/documents/pdf/RAG_2015-16.pdf].

Directeur général des élections. *Rapport annuel de gestion 2016-2017*. [https://www.electionsquebec.qc.ca/documents/pdf/RAG_2016-17.pdf].

Directeur général des élections. *Rapport annuel de gestion 2017-2018*. [https://www.electionsquebec.qc.ca/documents/pdf/RAG_2017-18.pdf].

Élections Canada*. Prévenir les communications trompeuses avec les électeurs : recommandations du directeur général des élections du Canada à la suite de la 41e élection générale*, 2013. [http://www.elections.ca/res/rep/off/comm/comm_f.pdf].

Élections Québec. *Compte rendu de la rencontre de la Table citoyenne tenue le vendredi 16 novembre 2018*. [https://www.electionsquebec.qc.ca/documents/pdf/table_citoyenne/compte_rendu_TC_2018-11-16.pdf[.

Elections Saskatchewan. *Interpretation Bulletin ESKIB-2015/01*, 28 décembre 2015. [https://cdn.elections.sk.ca/upload/eskib-2015-01-voterslistprivacy_v10_final.pdf].

États-Unis. *The Privacy Act of 1974*, 5 U. S. C. chap. 5, § 552a. – *Records Maintained on Individuals*. [https://www.law.cornell.edu/uscode/text/5/552a].

États-Unis. *The Privacy Act of 1988*. [https://www.legislation.gov.au/Series/C2004A03712].

États-Unis. *Help America Vote Act of 2002* – 116 Stat. 1666. [http://legislink.org/us/stat-116-1666].

Federal Trade Commission. *Privacy & Data Security – Update: 2017*, 2017. [https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf].

Fournier, Antonin-Xavier. « Les angles morts de la campagne électorale », *La Tribune*, 24 août 2018. [https://www.latribune.ca/chroniques/les-angles-morts-de-la-campagne-electorale-93c6d316967f11e981a7cea315ffdb4f].

France. *Code électoral*. [https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070239&dateTexte=20181018].

France. *Loi no 2018-493 du 20 juin 2018 relative à la protection des données personnelles*. [https://www.legifrance.gouv.fr/eli/loi/2018/6/20/JUSC1732261L/jo/texte].

France. *Loi nº 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés*. [https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460].

France. *Loi nº 2016-1048 du 1er août 2016 rénovant les modalités d'inscription sur les listes électorales, art. 2*. [https://www.legifrance.gouv.fr/affichCode.do ;jsessionid=408B89F-377F89D5C0EE092FAD7E721DE.tplgfr33s_2 ?idSectionTA=LEGISCTA000006164052 &cidTexte=LEGITEXT000006070239&dateTexte=20190101].

Gautrais, Vincent. *Neutralité technologique : rédaction et interprétation des lois face aux technologies*, Thémis, mai 2012. [https://www.gautrais.com/publications/neutralite-technologique/].

Godbout, Marc. « Les partis politiques recourent de plus en plus au profilage des électeurs », *Radio-Canada*, 30 septembre 2015. [https://ici.radio-canada.ca/nouvelle/737249/profilage-bases-donnees-partis-politiques-big-data].

Guthrie Weissman. Cale. « How Amazon Helped Cambridge Analytica Harvest Americans' Facebook Data », *Fast Company*, 27 mars 2018. [https://www.fastcompany.com/40548348/how-amazon-helped-cambridge-analytica-harvest-americans-facebook-data].

Guyader, Antonin. « Les enjeux du grand bouleversement », *Pouvoirs*, 2018/1, nº 164, Seuil.

Handley, Paul. « Comment les données de Facebook ont aidé Trump à se faire élire », *TVA/Agence France-Presse*, 21 mars 2018. [https://www.tvanouvelles.ca/2018/03/21/comment-les-donnees-de-facebook-ont-aide-trump-a-se-faire-elire].

Havenstein, Heather. « My.BarackObama.com Social Network Stays Online After Election », *Computerworld*, 10 novembre 2008. [https://www.computerworld.com/article/2534052/web-apps/my-barackobama-com-social-network-stays-online-after-election.html].

Hourdeaux, Jérôme. « Facebook s'embourbe dans le scandale Cambridge Analytica », *Mediapart*, 21 mars 2018. [https://www.mediapart.fr/journal/international/210318/facebook-s-embourbe-dans-le-scandale-cambridge-analytica].

House of Commons Library. *Note for the Members of Parliament, Supply and Sale of the Electoral Register*, 12 août 2014. [http://researchbriefings.files.parliament.uk/documents/SN01020/SN01020.pdf].

House of Commons, Political and Constitutional Reform Committee. *The Government's Proposals on Individual Electoral Registration and Electoral Administration, Written Evidence*, 2011. [https://publications.parliament.uk/pa/cm201012/cmselect/cmpolcon/writev/1463/1463.pdf].

Île-du-Prince-Édouard. *Freedom of Information and Protection of Privacy Act*, RSPEI 1988, chap. F-15.01. [https://www.canlii.org/en/pe/laws/stat/rspei-1988-c-f-15.01/latest/rspei-1988-c-f-15.01.html].

Île-du-Prince-Édouard. *Election Act*, RSPEI 1988, chap. E-1.1. [https://www.canlii.org/en/pe/laws/stat/rspei-1988-c-e-1.1/latest/rspei-1988-c-e-1.1.html].

Information Commissioner's Office. *An Introduction to the Data Protection Bill*. [https://ico.org.uk/media/for-organisations/documents/2258303/ico-introduction-to-the-data-protection-bill.pdf].

Information Commissioner's Office. *Democracy Disrupted ? Personal Information and Political Influence*, 2018, p. 44. [https://ico.org.uk/media/2259369/democracy-disrupted-110718.pdf].

Information Commissioner's Office. *Elected Representatives and Political Parties*. [https://ico.org.uk/for-organisations/political/].

Information Commissioner's Office. *Electoral Register*. [https://ico.org.uk/your-data-matters/electoral-register/].

Information Commissioner's Office. *Investigation Into the Use of Data Analytics in Political Campaigns – Investigation Update*, 11 juillet 2018. [https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf].

Information Commissioner's Office. *Preparing for the Law Enforcement Requirements (Part 3) of the Data Protection Act 2018: 12 Steps to Take Now*. [https://ico.org.uk/media/for-organisations/documents/2014918/dp-act-12-steps-infographic.pdf].

Information Commissioner's Office. *The ICO has Fined Facebook £500,000 for Serious Breaches of Data Protection Law*. [https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf].

Institut de recherche en politiques publiques (IRPP). *Enjeux découlant des communications inappropriées reçues par les électeurs : rapport de table ronde*, mars 2013. [https://on-irpp.org/2IyxY9e].

JDN – Journal du Net. *Nombre d'utilisateurs de Facebook dans le monde*, 2 novembre 2018. [https://www.journaldunet.com/ebusiness/le-net/1125265-nombre-d-utilisateurs-de-facebook-dans-le-monde/].

Joncas, Hugo. « Partis politiques : ils vous ont tous fichés », *Journal de Montréal*, 28 juillet 2018. [https://www.journaldemontreal.com/2018/07/28/partis-politiques-ils-vous-ont-tous-fiches].

Katz, James E., Michael Barris et Anshul Jain. *The Social Media President – Barack Obama and the Politics of Digital Engagement*, Palgrave Macmillan, 2013.

Knaus, Christopher. « Just 53 Australians Used Facebook App Responsible for Cambridge Analytica Breach », *The Guardian*, 10 avril 2018. [https://www.theguardian.com/technology/2018/apr/10/just-53-australians-used-facebook-app-responsible-for-cambridge-analytica-breach].

Lacroix, Louis. « Les partis politiques à l'ère des mégadonnées », *L'Actualité*, 23 mars 2018. [https://lactualite.com/politique/2018/03/23/les-partis-politiques-a-lere-des-megadonnees/].

Lapowsky, Issie. « Facebook Exposed 87 Million Users to Cambridge Analytica », *Wired*, 4 avril 2018. [https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/].

La Presse/La Presse Canadienne avec Agence France-Presse. « Cambridge Analytica a accédé aux données de 620 000 Canadiens », 4 avril 2018. [https://www.lapresse.ca/techno/reseaux-sociaux/201804/04/01-5159831-cambridge-analytica-a-accede-aux-donnees-de-620-000-canadiens.php].

Le Monde. « Scandale Facebook : la fermeture de Cambridge Analytica ne la met pas à l'abri des poursuites », 4 mai 2018. [https://www.lemonde.fr/pixels/article/2018/05/04/scandale-facebook-la-fermeture-de-cambridge-analytica-ne-la-met-pas-a-l-abri-des-poursuites_5294229_4408996.html].

Le Monde avec Reuters. *Le référendum sur le Brexit « aurait été différent », sans Facebook, soutient Christopher Wylie devant des parlementaires britanniques*, [vidéo en ligne], 30 mars 2018. Repéré au https://www.lemonde.fr/referendum-sur-le-brexit/video/2018/03/30/le-referendum-sur-le-brexit-aurait-ete-different-sans-facebook-soutient-christopher-wylie-devant-des-parlementaires-britanniques_5278876_4872498.html.

Le Monde – You Tube. *Affaire Facebook-Cambridge Analytica : notre entretien avec le lanceur d'alerte Christopher Wylie*, [vidéo en ligne], 28 mars 2018. Repéré au https://www.youtube.com/watch?v=h2Z7tg6-3ZI.

Luxembourg. *Avis de dépôt des listes électorales à l'inspection du public*, 11 juillet 2018. [https://elections.public.lu/fr/actualites/2018/avis-depot.html].

Luxembourg. *Constitution du Grand-Duché de Luxembourg*, art. 32bis. [http://legilux.public.lu/eli/etat/leg/recueil/constitution/20171020].

Luxembourg. *Recueil de la législation relative aux élections législatives, communales et européennes*, 21 juin 2018. [http://data.legilux.public.lu/file/eli-etat-leg-recueil-elections-20180625-fr-pdf.pdf].

Manitoba. *Loi sur l'accès à l'information et la protection de la vie privée*, CCSM, chap. F175. [https://web2.gov.mb.ca/laws/statutes/ccsm/_pdf.php?cap=f175].

Manitoba. *Loi électorale*, CPLM, chap. E30. [https://web2.gov.mb.ca/laws/statutes/ccsm/_pdf.php?cap=e30].

Marques, David. « Abstention : il n'y a plus de poursuites depuis 1964 », *Le Quotidien*, 23 novembre 2017. [http://www.lequotidien.lu/politique-et-societe/abstention-il-ny-a-plus-de-poursuites-depuis-1964/].

Maxwell, Winston J. *La jurisprudence américaine en matière de liberté d'expression sur Internet*. [https://www.hoganlovells.com/~/media/a8a5a7b6d1094edd84d509f9259840bf.ashx].

Merzeau, Louise. « L'intelligence des traces », *Intellectica*, 2013, 1 (59), pp. 115-136. [http://intellectica.org/fr/l-intelligence-des-traces].

Million, Louise. « Le FBI et le département de la Justice enquêtent sur Cambridge Analytica », *Siècle digital*, 22 mai 2018. [https://siecledigital.fr/2018/05/22/fbi-departement-justice-enquetent-cambridge-analytica/].

Musiani, Francesca. *Internet et vie privée*, Uppr Éditions, 2016.

New Zealand Electoral Commission. *Enrolling to Vote: Application.* [https://www.elections.org.nz/sites/default/files/plain-page/attachments/Enrolment%20Form%20ROE1_MAR13.pdf].

New Zealand Electoral Commission. *Enrol and Vote for the First Time*. [https://www.elections.org.nz/voters/get-ready-enrol-and-vote/enrol-and-vote-first-time].

New Zealand Electoral Commission. *Enrol and Vote as New Zealand Maori – Te Reo*. [https://www.elections.org.nz/voters/get-ready-enrol-and-vote/enrol-and-vote-new-zealand-maori-te-reo].

New Zealand Electoral Commission. *Concerned about Your Personal Safety ?* [https://www.elections.org.nz/voters/get-ready-enrol-and-vote/concerned-about-your-personal-safety].

New Zealand Privacy Commissioner. *Privacy Act & Codes*. [https://www.privacy.org.nz/the-privacy-act-and-codes/privacy-act-and-codes-introduction/].

Nieva, Richard. « Facebook peut-il être blâmé pour l'affaire Cambridge Analytica ? », *ZDNet*, 19 mars 2018. [https://www.zdnet.fr/actualites/facebook-peut-il-etre-blame-pour-l-affaire-cambridge-analytica-39865692.htm].

Nouveau-Brunswick. *Loi sur le droit à l'information et la protection de la vie privée*, SNB 2009, chap. R-10.6. [https://www.canlii.org/en/nb/laws/astat/snb-2009-c-r-10.6/latest/snb-2009-c-r-10.6.html].

Nouveau-Brunswick. *Loi électorale*, RSNB 1973, chap. E-3. [http://laws.gnb.ca/fr/ShowTdm/cs/E-3/].

Nouvelle-Écosse. *Freedom of Information and Protection of Privacy Act*, S.N.S. 1993, chap. 5. [https://novascotia.ca/just/regulations/regs/foiregs.htm].

Nouvelle-Écosse. *Elections Act*, SNS 2011, chap. 5. [https://nslegislature.ca/sites/default/files/legc/statutes/elections.pdf].

Office fédéral de la justice (Suisse). *Esquisse d'acte normatif : rapport du groupe d'accompagnement à la révision de la loi sur la protection des données*, 29 octobre 2014. [https://www.bj.admin.ch/dam/data/bj/staat/gesetzgebung/datenschutzstaerkung/ber-normkonzept-f.pdf].

Office of the Australian Information Commisioner. *Australian Privacy Principles*. [https://www.oaic.gov.au/privacy-law/privacy-act/australian-privacy-principles].

Office of the Information & Privacy Commissioner for British Columbia. *P11-01-MS Summary of the Office of the Information and Privacy Commissioner's Investigation of the BC NDP's Use of Social Media and Passwords to Evaluate Candidates*. [https://www.oipc.bc.ca/mediation-summaries/1399].

Office of the Information & Privacy Commissioner for British Columbia. *A Guide to B.C.'s Personal Information Protection Act for Businesses and Organisations*, octobre 2015. [https://www.oipc.bc.ca/guidance-documents/1438].

Office of the Information and Privacy Commissioner for British Columbia *Investigation Report P19-01. Full Disclosure : Political Parties, Campaign Data, and Voter Consent*, 6 février 2019. [https://www.oipc.bc.ca/investigation-reports/2278].

Ontario. *Loi électorale*, L.R.O. 1990, chap. E.6. [https://www.ontario.ca/fr/lois/loi/90e06].

Ontario. *Loi sur l'accès à l'information et la protection de la vie privée*, L.R.O. 1990, chap. F.31. [https://www.ontario.ca/fr/lois/loi/90f31].

Paré, Isabelle. « Les algorithmes, ces nouveaux acteurs dans l'arène politique », *Le Devoir*, 18 février 2017. [https://www.ledevoir.com/societe/science/492017/les-algorithmes-nouveaux-joueurs-sur-l-echiquier-politique].

Paré, Isabelle. « Algorithmes, le profilage électoral », *Le Devoir*, 29 septembre 2018. [https://www.ledevoir.com/societe/537936/algorithmes-et-politiques-a-la-carte].

Parlement européen (2018, 25 octobre). *Facebook-Cambridge Analytica : les députés demandent des mesures pour protéger la vie privée des citoyens*. Repéré au http://www.europarl.europa.eu/news/fr/press-room/20181018IPR16525/facebook-cambridge-analytica-des-mesures-pour-proteger-la-vie-privee.

Parliament of the United Kingdon. *Electoral Registration and Administration Bill, Explanatory Notes*, 29 juin 2012. [https://publications.parliament.uk/pa/bills/lbill/2012-2013/0033/en/2013033en.htm].

Pastor, Robert A. « États-Unis : une administration électorale décentralisée, anachronique et satisfaite d'elle-même », *ACE Project*. [http://aceproject.org/ace-fr/topics/em/electoral-management-case-studies/the-united-states-decentralized-to-the-point-of].

Payne, Adam. « A British Firm which Helped Deliver Brexit is Working for Donald Trump's Campaign », *Business Insider*, 22 septembre 2016. [https://www.businessinsider.com/donald-trump-brexit-us-presidential-election-2016-9/].

Péladeau, Pierrot. « Les partis politiques espionnent-ils vraiment votre « vie privée » ? », *Blogues, Journal de Montréal*, 21 août 2015. [https://www.journaldemontreal.com/2015/08/21/les-partis-politiques-espionnent-ils-vraiment-votre--vie-privee].

Phoenix Strategic Perspectives. *Sondage auprès des électeurs au sujet des communications avec les électeurs : rapport rédigé pour le compte d'Élections Canada*, mars 2013. [http://www.elections.ca/res/cons/sece/sece_f.pdf].

Richard, Jacky. *Le numérique et les droits fondamentaux*, 2014. [https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/144000541.pdf].

Robitaille, Antoine. « Les partis vous espionnent-ils ? », *Journal de Montréal*, 24 mars 2018. [https://www.journaldequebec.com/2018/03/24/les-partis-vous-espionnent-ils].

Rosenberg, Matthew, Nichols Confessore et Carole Cadwalladr. « How Trump Consultants Exploited the Facebook Data of Millions », *The New York Times*, 17 mars 2018. [https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html].

Royaume-Uni. *Data Protection Act, 2018*, chap. 12. [https://services.parliament.uk/bills/2017-19/dataprotection.html].

Royaume-Uni. *UK Data Protection Act, 1998*, chap. 29. [https://www.legislation.gov.uk/ukpga/1998/29/contents].

Royaume-Uni. *Electoral Administration Act, 2006*, chap. 22. [https://www.legislation.gov.uk/ukpga/2006/22/contents].

Royaume-Uni. *Political Parties and Elections Act, 2009*, chap. 12. [https://www.legislation.gov.uk/ukpga/2009/12/contents].

Saskatchewan. *The Freedom of Information and Protection of Privacy Act*, SS 1990-91, chap. F-22.01. [https://www.canlii.org/en/sk/laws/stat/ss-1990-91-c-f-22.01/latest/ss-1990-91-c-f-22.01.html].

Saskatchewan. *The Election Act*, 1996, SS 1996, chap. E-6.01. [https://www.canlii.org/en/sk/laws/stat/ss-1996-c-e-6.01/latest/ss-1996-c-e-6.01.html].

Solon, O. « Facebook Says Cambridge Analytica May Have Gained 37M More Users' Data », *The Guardian*, 4 avril 2018. [https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought].

Stead Sellers, Frances. « Cruz Campaign Paid $750,000 to 'Psychographic Profiling' Company », *The Washington Post*, 19 octobre 2015. [https://www.washingtonpost.com/politics/cruz-campaign-paid-750000-to-psychographic-profiling-company/2015/10/19/6c83e508-743f-11e5-9cbb-790369643cf9_story.html?noredirect=on&utm_term=.b09e391c21c6].

Suisse. *Constitution fédérale de la Confédération suisse du 18 avril 1999*, art. 13. [https://www.admin.ch/opc/fr/classified-compilation/19995395/index.html#a13].

Suisse. *Loi fédérale sur la protection des données du 19 juin 1992*. [https://www.admin.ch/opc/fr/classified-compilation/19920153/index.html].

Suisse. *Ordonnance relative à la loi fédérale sur la protection des données du 14 juin 1993*. [https://www.admin.ch/opc/fr/classified-compilation/19930159/index.html].

Suisse. *Loi fédérale sur les droits politiques du 17 décembre 1976*, art. 4. [https://www.admin.ch/opc/fr/classified-compilation/19760323/index.html].

Suisse. *Règlement sur l'exercice des droits politiques du 10 juillet 2001*, art. 2. [http://www.lexfind.ch/dta/4528/3/115.11.pdf].

Tajani, Antonio. *Twitter*, 19 mars 2018. [https://twitter.com/EP_President/status/975683240777453569].

Terra Nova. *Moderniser la vie politique : innovations américaines, leçons pour la France, rapport de la mission d'étude de Terra Nova sur les techniques de campagne américaines*, janvier 2009. [http://tnova.fr/system/contents/files/000/000/678/original/terranova-rapportmissionus.pdf?1436779596].

Terre-Neuve-et-Labrador. *Access to Information and Protection of Privacy Act – 2015,* SNL2015, chap. A-1.2. [https://assembly.nl.ca/legislation/sr/statutes/a01-2.htm].

Terre-Neuve-et-Labrador. *Elections Act – 1991*, SNL1992, chap. E-3.1. [https://www.assembly.nl.ca/legislation/sr/statutes/e03-1.htm].

Trudel, Pierre. « Protéger les données personnelles », *Le Devoir*, 6 novembre 2018. [https://www.ledevoir.com/opinion/chroniques/540664/signalement-des-incidents-de-donnees-personnelles].

Trudel, Pierre. « Gouverner par tweets », *Le Devoir*, 13 novembre 2018. [https://www.ledevoir.com/opinion/chroniques/541195/gouverner-par-tweets].

Trudel, Pierre. « Les lois et le numérique », *Le Devoir*, 8 janvier 2019. [https://www.ledevoir.com/opinion/chroniques/544988/les-lois-s-ajustent-au-numerique].

Union européenne. *Charte des droits fondamentaux de l'Union européenne.* [http://www.europarl.europa.eu/charter/pdf/text_fr.pdf].

Union européenne. *Directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, 24 octobre 1995. [https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:31995L0046].

Union européenne. *Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46*. [https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016R0679&from=fr].

Union européenne. *Traité de Lisbonne.* [https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=OJ:C:2007:306:FULL&from=FR].

United States Elections Project. *US Voter List Information*. [http://voterlist.electproject.org/].

Vallet, Élisabeth. « L'heure du jugement : le système électoral américain en question », *Politique américaine*, 2005/2 (nº 2), p. 79-90. [https://www.cairn.info/revue-politique-americaine-2005-2-page-79.htm].

Vrolixs, Pauline. « Les communes hésitent peu à donner l'adresse de leurs électeurs aux partis », *Radio Télévision Suisse*, 22 octobre 2015. [https://www.rts.ch/info/suisse/7191163-les-communes-hesitent-peu-a-donner-l-adresse-de-leurs-electeurs-aux-partis.html].