Directeur général des élections du Canada

Enjeux découlant des communications téléphoniques inappropriées reçues par des électeurs

---

Document de discussion

Table des matières

Introduction

- Le présent document de discussion vise à encourager la discussion sur les enjeux découlant des allégations d'appels inappropriés reçus par des électeurs les jours précédant le jour de l'élection ainsi que le jour de l'élection, soit le 2 mai 2012.

- Le document donne un bref aperçu des allégations et des plaintes reçues, ainsi que des mesures prises pour traiter ces plaintes. Il définit le cadre opérationnel et juridique d'une élection générale et indique les autres règles qui s'appliquent en dehors du contexte strict de la *Loi électorale du Canada* (LEC). Il fait état de plusieurs défis auxquels les enquêteurs ont dû faire face et examine les changements législatifs et régulatoires possibles qui pourraient aider à prévenir ce genre de conduite ou faciliter l'application de la loi. À ce stade, les changements ne sont énumérés dans ce document qu'à des fins de discussion. Il reste beaucoup de travail à faire avant que le directeur général des élections (DGE) soit en mesure de présenter des recommandations à ce sujet au Parlement. Les commentaires et suggestions reçus permettront de présenter des recommandations équilibrées et mieux informées au Parlement.

- Bien que les technologies de communication puissent ouvrir la porte à des abus, leurs avantages pour le processus démocratique ne devraient pas être ignorés.

- Les valeurs et les principes qui sous-tendent cette discussion sont : le droit fondamental de tous les électeurs de voter dans une élection fédérale, le droit et la nécessité pour les partis politiques et les candidats de communiquer avec les électeurs, le droit à la vie privée des électeurs et l'obligation pour tous les intervenants de préserver l'intégrité du processus électoral.

- On doit trouver les moyens d'éviter que des pratiques comme celles décrites dans ce document ne se répètent. Ces pratiques minent le processus électoral au détriment de tous ses participants. Dans ce contexte, cependant, il faut garder à l'esprit que les mesures législatives ne peuvent à elles seules prévenir une conduite inappropriée. Tous les participants au processus électoral se doivent d'agir de façon à respecter et promouvoir les valeurs démocratiques et la primauté du droit.

1. Allégations de communications inappropriées avec les électeurs lors de l'élection générale du 2 mai 2011

Cette partie du document résume les événements qui se sont produits lors de l'élection générale du 2 mai 2011, et décrit les démarches subséquentes d'Élections Canada pour enquêter sur ces événements.

- **Appels et plaintes initiaux (dans Guelph et ailleurs)**
  - Les journées précédant le jour du scrutin, le jour de l'élection, et les journées suivantes, des électeurs se sont plaints d'avoir reçu des appels automatisés, prétendument d'Élections Canada, les avisant à tort du changement de leur lieu de scrutin (principalement dans Guelph, mais également dans d'autres circonscriptions).
  - D'autres plaintes d'électeurs ont fait état d'appels répétés, agaçants, voire agressifs, tantôt automatisés, tantôt de vive voix; d'autres appels auraient été reçus tard le soir, des jours de fête religieuse, ou avec des numéros accompagnés d'un indicatif régional américain. Ces communications auraient été faites de la part de candidats qui, souvent, ont ensuite nié en être à l'origine.
  - Dans quelques cas, des centres d'appels professionnels ont reconnu par la suite que certains électeurs avaient reçu de l'information erronée sur l'adresse de leur lieu de scrutin, information fondée sur des données inexactes ou périmées.

- **Enquête sur les plaintes dans Guelph**[1]
  - De nombreuses plaintes à propos d'appels téléphoniques ont été reçues vers 10 h le 2 mai 2011. La voix à l'appareil a été décrite comme une voix féminine enregistrée prétendant appeler de la part d'Élections Canada. Le message était que puisqu'on s'attendait à une augmentation de la participation électorale, l'adresse du lieu de scrutin de l'électeur avait été changée. Rien dans ce message n'était vrai : l'appelante ne représentait pas Élections Canada, et aucun lieu de scrutin n'avait changé d'adresse.
  - Le numéro d'où provenait ce message, selon l'afficheur des destinataires, était le même : il s'agissait du numéro d'un téléphone cellulaire facturé à l'utilisation et activé le 30 avril 2011. Le nom de l'abonné dans les dossiers de Bell Canada était Pierre Poutine, habitant la rue Séparatiste, à Joliette, au Québec. Ni ce nom ni cette rue n'existent à Joliette.
  - Le téléphone de Pierre Poutine a servi à appeler uniquement deux numéros de téléphone, tous deux assignés à une entreprise de communication d'Edmonton, qui a également fourni des services à une campagne dans Guelph.
  - L'individu à l'origine des appels a été accepté comme client par l'entreprise de communication. Les dossiers de l'entreprise indiquent que 7 676 appels portant le numéro d'appel attribué à l'individu ont été effectués à des numéros de téléphone de Guelph le 2 mai 2011, entre 10 h 03 et 10 h 15 HAE.

[1] Les énoncés suivants sont fondés sur l'information rendue disponible au public grâce aux dossiers de la cour pendant l'enquête du commissaire aux élections fédérales. L'enquête se poursuivait toujours au moment de rédiger ce document.

- Les numéros de téléphone sur cette liste concordent avec ceux d'une liste de personnes qui n'appuient pas un certain parti politique et la liste a été obtenue de la base de données de ce parti.
- L'individu a utilisé un faux nom et une fausse adresse dans ses communications avec l'entreprise (Pierre Jones, au 54, rue Lajoie, à Joliette). Cette adresse n'existe pas.
- Il a utilisé PayPal pour payer les services de l'entreprise, et a fourni à PayPal les mêmes faux nom et adresse. Les paiements (d'un montant total de 162,10 $) ont été faits au moyen de trois cartes Visa prépayées, achetées à deux magasins Shoppers Drug Mart, à Guelph. Tous ont été faits depuis un ordinateur avec la même adresse IP[2], par un serveur mandaté, conçu à dessein pour dissimuler l'emplacement de l'ordinateur. L'individu a de même utilisé le serveur mandaté pour communiquer avec l'entreprise de communication à certaines occasions.
- À d'autres occasions, l'individu a communiqué avec l'entreprise de communication à partir d'une adresse IP associée à un bureau de campagne. Le personnel de ce bureau de campagne a utilisé la même adresse IP pour ses communications légitimes avec cette même entreprise de communication, ainsi que pour l'accès à la base de données d'un parti politique.
- Les appels aux électeurs ont été envoyés par l'entreprise de communication au moyen de services de téléphonie sur protocole Internet (VoIP).
- Les appels VoIP se font par ordinateur et sont transmis, par Internet, aux téléphones des destinataires. Cette technologie permet au fournisseur du service de configurer le programme de façon à ce que n'importe quel numéro souhaité par le client apparaisse sur l'afficheur des destinataires. Ce numéro affiché n'a donc rien à voir avec l'origine réelle de l'appel fait par le fournisseur.

- **Découverte par les médias en février 2012 de documents judiciaires sur l'enquête et afflux subséquent de plaintes et de réactions**
  - Plus de 40 000 communications ont été reçues de la part d'électeurs après que ces renseignements ont été rendus publics dans les pages de l'*Ottawa Citizen*, le 23 février 2012 et les jours suivants.
  - La plupart de ces communications exprimaient l'indignation des électeurs à l'idée qu'on tente d'affaiblir le processus électoral par des appels mensongers ou trompeurs.

- **Comparution du directeur général des élections devant le Comité permanent de la procédure et des affaires de la Chambre**
  - Dans le contexte de la couverture médiatique et du débat public qu'ont suscités ces articles, le DGE a demandé à comparaître devant le Comité permanent de la procédure et des affaires de la Chambre afin d'expliquer des aspects importants des processus d'administration et d'enquête d'Élections Canada. Cette comparution a eu lieu le 29 mars 2012.

[2] L'adresse de protocole Internet (IP) est une adresse numérique affectée à tout ordinateur qui utilise le protocole Internet pour communiquer sur Internet. On peut déterminer l'adresse physique d'un ordinateur connecté à Internet à partir de l'adresse IP, si on consulte la base de données du fournisseur d'accès Internet.

- Ce jour-là, le DGE a déclaré que près de 800 plaintes avaient été reçues au sujet de cas précis d'appels inappropriés ou frauduleux[3].
- Le DGE s'est engagé à déposer au plus tard le 31 mars 2013 un rapport qui examinerait les défis posés par de tels appels et recommanderait des améliorations au cadre législatif.

- **Situation actuelle**
  - Le commissaire aux élections fédérales a déclaré qu'au 16 août 2012, il avait reçu 1 394 plaintes au sujet d'appels de cette sorte. Ces plaintes émanaient d'électeurs de 234 circonscriptions, dont Guelph.

[3] Ce nombre reflète les cas d'allégations d'appels inappropriés signalés par les électeurs, et non pas les manifestations d'indignation ou les appels à l'action.

2. Contexte juridique

Cette partie du document traite des règles qui s'appliquent – ou ne s'appliquent pas selon le cas – aux appels inappropriés faits durant la dernière élection générale. On décrit les dispositions pertinentes de la *Loi électorale du Canada*; on note que les principales lois fédérales en matière de vie privée ne s'appliquent pas aux partis politiques et on explique que certaines dispositions des *Règles sur les télécommunications non sollicitées* du CRTC en matière de télémarketing et d'appels automatisés sont par contre applicables aux entités politiques. Finalement, on mentionne certaines dispositions du *Code criminel.*

- **Communications avec les électeurs par les entités politiques aux termes de la *Loi électorale du Canada***
  - Les communications avec les électeurs par les entités politiques sont essentielles au processus démocratique. Le but principal de toute campagne électorale est de convaincre les électeurs de voter, et de voter pour un candidat particulier. Plusieurs moyens peuvent être employés à cette fin, mais pour beaucoup, le contact direct entre le candidat (ou son équipe) et l'électeur fait partie d'une stratégie importante, si ce n'est la plus importante.
  - Afin de faciliter ces communications, le Parlement a inclus dans la LEC plusieurs dispositions exigeant la transmission aux partis, aux candidats ou aux députés de renseignements sur les électeurs dans des listes électorales (art. 93, 104.1, 107, 109 et 45).
  - Ces listes contiennent les nom, adresse (postale et municipale) et numéro d'identificateur de chaque électeur. Elles ne contiennent pas leurs numéros de téléphone.
  - Quatre de ces listes sont remises aux candidats et aux partis pendant la période électorale (listes préliminaires, listes préliminaires à jour, les listes révisées et les listes officielles). Les listes définitives, produites après l'élection pour chaque circonscription, sont fournies aux partis enregistrés qui y ont soutenu un candidat, ainsi qu'aux députés. Les députés reçoivent aussi chaque année la liste des électeurs de leur circonscription, tout comme les partis politiques qui en font la demande, du moment qu'ils ont soutenu un candidat dans cette circonscription à la dernière élection.
  - La Loi n'impose aucune obligation aux destinataires des listes quant à la protection et au contrôle de l'accès aux renseignements personnels qu'elles contiennent. Élections Canada leur fournit des lignes directrices comprenant des pratiques exemplaires en matière de protection des renseignements personnels contenus dans les listes. Ces lignes directrices ne sont cependant pas exécutoires.
  - Élections Canada détient peu de renseignements sur la façon dont ces renseignements personnels sont gérés par les partis politiques et ne sait pas s'il existe des mesures afin de contrôler ou de limiter leur utilisation.

- Il semble que les partis politiques fusionnent les renseignements contenus dans ces listes avec leurs propres renseignements sur les électeurs. Ces bases de données peuvent contenir beaucoup plus de renseignements, dont les numéros de téléphone des électeurs et leur allégeance politique, si elle est connue[4]. Il semble aussi que, dans certains cas, les campagnes locales et le parti auquel elles sont affiliées mettent en commun leur information sur les électeurs dans la base de données du parti, afin que les deux entités aient le plus de renseignements possible sur les électeurs de la circonscription, ce qui facilite les communications avec eux.
- L'évolution des nouvelles technologies et leur utilisation accrue par les participants au processus électoral permettent à ceux-ci de cibler des segments de l'électorat et de communiquer avec les électeurs plus facilement et efficacement. Une gamme de plus en plus grande de mécanismes sont utilisés à cette fin, dont les campagnes téléphoniques (appels en personne ou automatisés) et les débats interactifs au téléphone, autant d'occasions pour les partis et les candidats de diffuser leur message et d'encourager la participation.
- Ces outils ne sont pas coûteux et relativement faciles à utiliser. Ils présentent donc d'importants avantages pour le processus électoral. Cependant, ce sont justement ces qualités – combinées à la capacité de certains de ces outils de dissimuler l'origine réelle de la communication – qui en font des outils de choix pour ceux qui veulent tromper les électeurs.
- Ainsi, aux États-Unis, on observe depuis une décennie des cas de pratiques trompeuses[5] perpétrées au moyen d'appels automatisés ou de sites Web. Par exemple, des électeurs de Kansas City et de Virginie ont reçu en 2006 des appels automatisés les informant mensongèrement du changement d'adresse de leur lieu de scrutin[6].
- En plus de porter atteinte aux droits constitutionnels des électeurs, de telles pratiques minent la confiance des électeurs ainsi que la capacité des partis politiques et des candidats à communiquer efficacement avec les électeurs et stimuler la participation électorale.

[4]Voir Colin J. Bennett et Robin M. Bayley, *Les partis politiques fédéraux du Canada et la protection des renseignements personnels : une analyse comparative*, Commissariat à la protection de la vie privée du Canada, Ottawa, 2012, p. 40 et suiv. www.priv.gc.ca/information/pub/pp_201203_f.asp.

[5]On utilise dans le présent document le terme « pratiques trompeuses » plutôt que celui, courant mais plus restreint (à certains égards), de « suppression du vote ». Le US Department of Justice définit comme suit la « suppression du vote » dans son manuel sur la poursuite des infractions électorales : « Les manœuvres de suppression du vote visent à assurer l'élection du candidat souhaité en empêchant les électeurs réputés être favorables à ses rivaux de se rendre au bureau de vote. Ces manœuvres peuvent prendre la forme suivante : fournir de faux renseignements à la population – ou à un segment particulier du public – sur les critères d'admissibilité au vote, les conséquences du vote sur le statut de citoyen, les dates ou les qualifications relativement au vote des absents, la date du scrutin, les heures du vote, ou le bureau de scrutin où se rendre. Actuellement, aucune loi fédérale d'application criminelle n'interdit expressément les activités de suppression du vote de cette sorte ». Voir Craig C. Donsanto, *Federal Prosecution of Election Offenses*, 7e éd., Dept. of Justice, 2007, p. 61. Élections Canada donne à l'expression « pratique trompeuse » une portée plus large qui englobe aussi la diffusion de faux renseignements sur les rivaux électoraux.

[6] Voir Common Cause, Lawyers' Committee for Civil Rights Under Law and Century Foundation, *Deceptive Practices 2.0: Legal and Policy Responses*, Washington, Common Cause, 2008.

Communications des partis et des candidats avec les électeurs individuels – ce qui est permis, ce qui ne l'est pas

- Aux termes de la LEC (art. 110, al. 111*f*)), la principale restriction à l'utilisation des renseignements personnels inscrits sur les listes électorales est la suivante : il est interdit aux partis, aux candidats et aux députés d'utiliser sciemment ces renseignements à des fins autres que : a) la communication avec des électeurs ou b) une élection ou un référendum fédéral. Pour qu'il y ait infraction, il faut prouver non seulement qu'il y a eu mauvaise utilisation, mais aussi que la personne connaissait la source de l'information, et savait à quoi on l'utilisait[7].
- La publicité électorale – favoriser ou contrecarrer un candidat ou un parti (LEC, art. 319 et suiv.) – est permise. Elle peut prendre plusieurs formes, dont le porte-à-porte ou d'autres formes de communication avec les électeurs.
- Les appels pour « faire sortir le vote » sont également permis.
- Par contre, il est interdit de volontairement empêcher ou s'efforcer d'empêcher un électeur de voter (LEC, al. 281*g*); l'infraction est énoncée à l'al. 491(3)*d*)).
- De même, il est interdit d'inciter une personne à s'abstenir de voter (ou à voter pour ou contre un candidat donné) « par quelque prétexte ou ruse » (LEC, al. 482*b*)).
- Il est interdit de faire ou de publier sciemment une fausse déclaration concernant la réputation ou la conduite personnelle d'un candidat ou d'une personne qui désire se porter candidat avec l'intention d'influencer les résultats de l'élection (LEC, art. 91; l'infraction est énoncée à l'al. 486(3)*c*)).
- Il faut dire, en leur faveur, que ces interdictions ont une grande portée. Les interdictions énoncées aux alinéas 281*g*) et 482*b*) ne sont pas en lien avec une technologie ou un moyen d'obstruction particulier. L'alinéa 482*b*) couvrirait les stratagèmes employés pour décourager les électeurs de voter selon leur préférence (p. ex. en prétendant (faussement) appeler au nom d'un autre candidat) et ceux employés pour supprimer le vote (p. ex. en informant faussement les électeurs que leur lieu de vote a changé).
- Toutefois, il est également important de noter que ces interdictions font l'objet de sanctions pénales et non de pénalités administratives. Par conséquent, les cas de non-conformité sont traités dans le cadre d'une enquête pénale, ce qui limite les outils disponibles pour recueillir l'information et exige des procédures relativement lourdes et longues. Il existe également un déséquilibre important entre la lourdeur et la longueur de ces procédures et les faibles amendes qui peuvent être imposées advenant un verdict de culpabilité, limitant ainsi l'effet dissuasif d'un tel verdict.

[7]La LEC ne régit pas la collecte ou la communication des renseignements personnels par les entités politiques. Le procureur doit prouver que la personne qui a utilisé l'information savait qu'elle provenait d'une liste électorale (par opposition à une autre source), ce qui réduit les chances de succès de la poursuite, et affaiblit la responsabilisation quant à la protection et à l'utilisation des renseignements personnels inscrits sur les listes.

- **Communications avec les électeurs à propos des lieux de scrutin**
  - Chaque circonscription est divisée en parcelles géographiques appelées sections de vote et qui comptent chacune au moins 250 électeurs. On compte habituellement un bureau de scrutin par section de vote, et la règle de base est que chaque bureau de scrutin doit se trouver dans la section de vote correspondante. Cela dit, le directeur du scrutin peut, s'il le juge indiqué, réunir plusieurs bureaux de scrutin en un centre de scrutin. En pratique, la plupart des bureaux de scrutin sont regroupés de cette façon.
  - Avant chaque élection, les directeurs du scrutin sont chargés de trouver un emplacement dans les sections de vote pour les bureaux de scrutin ou pour le centre de scrutin (ce dernier peut réunir au maximum 15 bureaux de scrutin). Si possible, les bureaux doivent se trouver dans un édifice public, à un endroit central, à proximité des électeurs, et devraient répondre à des normes d'accessibilité spécifiques, tant à l'intérieur qu'à l'extérieur de l'édifice[8]. Les directeurs du scrutin peuvent engager des discussions préliminaires avec les propriétaires sur la location des locaux, mais ils ne peuvent pas signer de bail avant la délivrance des brefs à moins d'avoir reçu l'autorisation du DGE, qui n'est habituellement pas accordée avant que l'élection ne soit imminente.
  - Une carte d'information de l'électeur (CIE) est ensuite envoyée à tous les électeurs de la circonscription. L'électeur y trouve l'adresse de son bureau de scrutin, les dates et les heures du vote, et le numéro de téléphone à composer pour obtenir de plus amples renseignements.
  - Au début de chaque élection, Élections Canada demande aux partis politiques et aux candidats de ne pas communiquer d'information aux électeurs sur l'adresse ou l'éventuel changement d'adresse des bureaux de scrutin, afin de ne pas semer la confusion ou de transmettre des renseignements potentiellement erronés.
  - S'il faut changer l'adresse d'un bureau de scrutin – par exemple parce qu'un lieu de scrutin s'avère soudainement non disponible – le directeur du scrutin imprime et envoie une CIE révisée aux électeurs concernés. Si le changement se produit trop tard pour que cette carte puisse être envoyée, les électeurs sont informés du changement par les médias, ou personnellement par un travailleur électoral posté à l'entrée du bureau de scrutin fermé.
  - Élections Canada n'appelle pas les électeurs pour les informer de changements d'adresse de lieux de scrutin : sauf exception, l'organisme ne détient pas le numéro de téléphone des électeurs. [9] Dans les rares cas où les électeurs fournissent, volontairement, leur numéro de téléphone à l'organisme, il n'est consigné ni dans le Registre national des électeurs, ni sur la liste électorale, et n'est pas fourni aux directeurs du scrutin.

[8] Le 2 mai 2011, jour de l'élection, on dénombrait 64 477 bureaux de scrutin situés dans 15 260 lieux de scrutin. De plus, 1 669 bureaux de scrutin itinérants avaient été installés dans 4 865 établissements.

[9] Par exemple, les électeurs qui demandent un bulletin de vote spécial peuvent fournir leur numéro de téléphone pour qu'Élections Canada puisse communiquer avec eux si les documents télécopiés sont illisibles.

- **La *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques***

  – Les principes généraux régissant la collecte, l'utilisation, la communication et la conservation des renseignements personnels sont exposés dans la *Loi sur la protection des renseignements personnels* (LPRP) et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), et ils reflètent des normes reconnues mondialement[10].

  – Cependant, ni la LPRP ni, de façon générale, la LPRPDE ne s'appliquent aux entités politiques. La LPRP ne s'applique qu'aux institutions fédérales, c'est-à-dire, généralement, aux ministères et aux organismes du gouvernement fédéral. Quant à la LPRPDE, elle se limite aux renseignements personnels recueillis, utilisés ou communiqués dans le cadre d'activités commerciales[11].

  – L'absence d'un cadre juridique pour la gestion et la protection des renseignements personnels par les partis politiques et les candidats est cruciale, puisque le recours à des moyens comme celui des appels automatisés pour tromper des segments ciblés de la population serait impossible sans avoir connaissance des données sur la composition de l'électorat compilées et consultées par les partis politiques.

- **Règles du Conseil de la radiodiffusion et des télécommunications canadiennes sur les télécommunications non sollicitées[12]**

  Autorité législative

  – Selon l'article 41 de la *Loi sur les télécommunications* : « Le Conseil peut, par ordonnance, interdire ou réglementer, dans la mesure qu'il juge nécessaire — compte tenu de la liberté d'expression — pour prévenir tous inconvénients anormaux, l'utilisation par qui que ce soit des installations de télécommunication de l'entreprise canadienne en vue de la fourniture de télécommunications non sollicitées ».

[10] Ces principes sont énoncés dans l'annexe 1 de la LPRPDE et ont été reproduits dans l'annexe du présent document.
[11] Le rapport de Bennett et Bailey, note 4 *supra*, mentionne que la *Personal Information Protection Act* de la Colombie-Britannique « inclut, dans la définition d'organisation, les personnes, les associations non constituées en personne morale, les organisations syndicales, les fiducies et les organisations sans but lucratif » et ne s'applique pas uniquement aux activités commerciales. Selon une décision récente, les partis politiques provinciaux sont assujettis à cette loi, qui pourrait également s'étendre aux activités des partis politiques fédéraux dans cette province. Voir http://www.priv.gc.ca/information/pub/pp_201203_f.pdf, p. 32.
[12] Dans cette section, Élections Canada tente de résumer les règles du CRTC. Les règles elles-mêmes se trouvent sur le site Web du CRTC, à http://crtc.gc.ca/fra/reglest-trules.htm. Une fiche de renseignements d'une page intitulée « Renseignements importants à l'intention des candidats, des partis et des organismes politiques concernant les règles sur le télémarketing » se trouve également à http://crtc.gc.ca/fra/info_sht/t1041.htm. Pour de plus amples renseignements sur les Règles sur les télécommunications non sollicitées, veuillez communiquer avec le CRTC.

- Bien que les règles adoptées par le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) soient complètes à plusieurs égards, il est important de garder en tête qu'elles ne s'appliquent pas aux communications par Internet et par courriel[13].

Règles sur la Liste nationale de numéros de télécommunication exclus

- La Liste nationale de numéros de télécommunication exclus (LNNTE) permet aux consommateurs d'enregistrer un numéro de téléphone pour ne plus recevoir d'appels de télémarketing à ce numéro. Aux termes des alinéas 41.7(1)*c*) à *e*) de la *Loi sur les télécommunications*, les règles sur la LNNTE ne s'appliquent pas aux télécommunications faites par les entités politiques régies par la LEC, soit les partis enregistrés, les candidats, les candidats à l'investiture, les candidats à la direction et les associations de circonscription, ou celles faites en leur nom.
- Cela dit, il est important de noter que le paragraphe 41.7(4) oblige les personnes et les organisations exemptées, telles que les partis politiques et les candidats, à maintenir leur propre liste d'exclusion interne. Les partis politiques et candidats doivent donc s'assurer qu'aucune communication n'est effectuée en leur nom à toute personne qui aurait demandé à être inscrite sur leur liste d'exclusion. Notons toutefois que cette disposition ne s'applique pas à une personne qui fait une télécommunication à la seule fin de recueillir de l'information pour un sondage auprès du public.

Règles de télémarketing

- Les Règles de télémarketing s'appliquent, que la télécommunication à des fins de télémarketing soit visée ou non par les Règles sur la LNNTE. Elles s'appliquent donc aux entités politiques.
- Cependant, « télémarketing » désigne l'utilisation d'installations de télécommunication pour effectuer des télécommunications non sollicitées à des fins de sollicitation, et « sollicitation » s'entend de la vente ou de la promotion d'un produit ou d'un service ou la sollicitation d'argent ou d'une valeur pécuniaire.
- Par conséquent, les Règles de télémarketing s'appliquent aux entités politiques lorsque celles-ci sollicitent des dons, mais elles seraient probablement jugées non applicables lorsque l'entité sollicite le vote de l'électeur, puisque l'appel ne constitue pas une activité commerciale. De même, ces règles seraient probablement non applicables aux appels visant à « faire sortir le vote », ou à aviser les électeurs du changement d'adresse de leur bureau de scrutin.
- Les Règles de télémarketing comprennent les obligations suivantes :
  - Le télévendeur doit s'inscrire au préalable, qu'il fasse les télécommunications pour son propre compte ou pour celui d'un client.
  - Le télévendeur doit tenir une liste d'exclusion interne, qu'il fasse les télécommunications pour son propre compte ou pour celui d'un client.

[13] En décembre 2010, le Parlement a adopté une loi visant à contrer les pourriels (voir L.C. 2010, ch. 23). Lorsque la législation entrera en vigueur, le mandat du CRTC sera élargi et inclura les messages électroniques de nature commerciale.

- Le télévendeur, ou le client de celui-ci selon le cas, doit ajouter à sa liste d'exclusion interne les nom et numéro de téléphone du consommateur qui en fait la demande dans les 31 jours suivant la réception de la demande[14].
- Au début de la télécommunication par téléphone aux fins de télémarketing, le télévendeur doit donner le nom réel ou fictif de la personne qui fait la télécommunication, le nom du télévendeur et le nom du client.
- Sur demande pendant la télécommunication par téléphone aux fins de télémarketing, le télévendeur doit donner un numéro de téléphone que le consommateur peut composer pour s'adresser à un employé ou à un autre représentant du télévendeur et du client.
- Une télécommunication à des fins de télémarketing ne peut être effectuée qu'aux heures suivantes : de 9 h à 21 h 30 la semaine et de 10 h à 18 h la fin de semaine[15].
- Le télévendeur doit afficher le numéro de télécommunication qu'il utilise ou un autre numéro auquel le consommateur peut le joindre.

Les Règles sur les composeurs-messagers automatiques

– Ces règles s'appliquent, que la télécommunication à des fins de télémarketing soit visée ou non par les Règles sur la LNNTE. Elles s'appliquent donc aux entités politiques.

– « Composeur-messager automatique » (CMA) désigne « un appareil de composition automatique capable de mémoriser ou de produire les numéros de télécommunication à composer et qui peut être utilisé seul ou avec un autre appareil pour transmettre un message enregistré ou synthétisé au numéro de télécommunication composé ». Ce sont ces appareils qui servent à faire les appels automatisés.

– Une personne qui utilise un CMA pour effectuer des appels non sollicités ayant un autre objectif que la sollicitation doit néanmoins se conformer à certaines conditions, dont les plus pertinentes – pour les besoins du présent document – sont les suivantes :

- la télécommunication ne peut être effectuée qu'aux heures suivantes : de 9 h à 21 h 30 la semaine et de 10 h à 18 h la fin de semaine[16];
- la télécommunication doit commencer par un message donnant clairement le nom de la personne pour le compte de laquelle la télécommunication est faite ainsi qu'une adresse postale et un numéro de télécommunication local ou sans frais permettant de joindre un représentant de cette personne. Si le message transmis dépasse 60 secondes, le message d'identification doit être répété à la fin de la télécommunication;

[14]Cette question est abordée dans le document du CRTC intitulé « Renseignements importants à l'intention des candidats, des partis et des organismes politiques concernant les règles sur le télémarketing ». On peut y lire que « toute demande de la part d'un électeur désirant ajouter son nom et son numéro de téléphone à la liste d'exclusion interne d'un parti ou d'un candidat, ou encore d'une personne qui fait des appels en leur nom, doit être satisfaite au moment de l'appel. Les partis ont 31 jours pour mettre à jour leur liste d'exclusion interne ». Voir http://crtc.gc.ca/fra/info_sht/t1041.htm.

[15] Ces heures sont sujettes à la législation provinciale qui régit ce type d'activités.

[16] Ces heures sont sujettes à la législation provinciale qui régit ce type d'activités.

- la télécommunication doit afficher le numéro de l'appelant ou un autre numéro permettant de joindre l'appelant.

Application des dispositions régissant les télécommunications non sollicitées par le Conseil de la radiodiffusion et des télécommunications canadiennes

- L'application des dispositions sur les télécommunications non sollicitées se fait principalement par l'imposition de pénalités administratives pécuniaires (voir les articles 72.01 à 72.15 de la *Loi sur les télécommunications)*. Comme de telles pénalités ne relèvent pas du droit pénal (et qu'ainsi elles ne sont pas assorties des droits et protections accordés aux personnes soupçonnées ou accusées d'avoir commis une infraction criminelle), elles peuvent être imposées beaucoup plus rapidement et efficacement par l'organisme.
- En vertu de ses pouvoirs d'enquête (art. 72.05 et 72.06 de la Loi), le CRTC peut désigner les agents autorisés à dresser un procès-verbal de violation. Ces personnes peuvent procéder à la visite de tout lieu où se trouvent, à leur avis fondé sur des motifs raisonnables, des objets, des documents ou des renseignements concertant l'application des règles, et examiner ceux-ci. Elles peuvent aussi faire usage directement ou indirectement, de tout système informatique se trouvant dans le lieu pour vérifier les données qu'il contient ou auxquelles il donne accès, les reproduire ou en exiger la reproduction, etc.

- **Dispositions du *Code criminel* sur les communications frauduleuses**

  Les dispositions actuelles du *Code criminel* peuvent être d'une utilité limitée pour traiter les communications inappropriées avec les électeurs.

  *Appels téléphoniques harcelants et trompeurs (*par*. 372(1), (3))*

  - Est coupable d'une infraction quiconque, « avec l'intention de nuire à quelqu'un ou de l'alarmer », transmet par téléphone des renseignements qu'il sait être faux (par. 372(1)). Il n'est cependant pas certain que les tribunaux jugent qu'un appel trompeur cherchant à nuire aux chances de succès d'un candidat dans une élection (et non à la personne elle-même) constitue une infraction aux termes de ce paragraphe;
  - Est également coupable d'une infraction quiconque « fait ou fait en sorte qu'il […] soit fait des appels téléphoniques répétés » « avec l'intention de harasser quelqu'un » (par. 372(3)).

  Fraude à l'identité (art. 403)

  - Il y a infraction lorsque quiconque, frauduleusement, se fait passer pour une autre personne, vivante ou morte, avec l'une de quatre intentions prévues, dont celle « de causer un désavantage […] à une autre personne ». La jurisprudence confirme que l'identité usurpée doit être celle d'une vraie personne. L'infraction ne s'appliquerait donc pas à l'appel ou à l'appelant se prétendant représenter « Élections Canada », ou se faisant passer pour une personne fictive comme « Pierre Poutine »[17].

[17]Le message automatisé envoyé aux électeurs de Guelph contenait (en anglais) le texte suivant : « Ceci est un message automatisé d'Élections Canada ».

Méfaits (art. 430, 430(1.1))

- L’article 430 énumère les activités liées aux « biens » (définis dans le Code) qui constituent des « méfaits ». L’article 430(1.1) précise ainsi que c’est commettre une infraction que de détruire ou altérer des données, ou de gêner leur emploi; le terme « données » est défini à l’art. 342.1 (« représentations d’informations [pouvant] être utilisées dans un ordinateur »). Ces dispositions ne semblent pas s’appliquer aux appels eux-mêmes.

3. Difficultés rencontrées par les enquêteurs

Cette partie du document décrit certains des obstacles auxquels ont été confrontés les enquêteurs d'Élections Canada dans leur recherche de la source des appels inappropriés faits durant la dernière élection générale.

- **Absence de contrats écrits pour les services de télémarketing ou autres services de communication avec les électeurs**

  Les enquêtes d'Élections Canada semblent indiquer que les principaux partis ont leur propre bassin d'entreprises de télémarketing, et qu'ils partagent leurs contacts avec les campagnes des candidats. Bien qu'il existe des factures, il n'y a habituellement pas de contrats écrits entre les campagnes et les entreprises de télémarketing détaillant quels services seront fournis, quand et à quel coût.

- **Limites actuelles à l'obligation de rendre compte à Élections Canada**

  Les renseignements contenus dans les rapports produits par les partis politiques sont actuellement trop limités pour qu'on puisse en tirer de l'information pertinente. En effet, ces rapports ne comprennent que le détail des contributions reçues. Les dépenses électorales des partis y sont regroupées en catégories générales, et peu de détails sont fournis sur la façon dont elles ont été engagées. Aux termes de la loi actuelle, les partis politiques fédéraux ne sont pas tenus de fournir de pièces à l'appui de leurs dépenses.

  Si les rapports des candidats et les documents y afférents sont plus complets, et pourraient révéler qu'une entreprise de télémarketing a été engagée pour la diffusion de messages automatisés ou en personne aux électeurs, la raison de l'utilisation faite de ces services, ou le texte des messages communiqués aux électeurs en sont absents, puisque la LEC ne l'exige pas[18].

  De plus, si le rapport n'indique pas que la campagne a engagé une entreprise de télémarketing ou de télécommunication pour communiquer avec les électeurs, ou si la dépense n'a pas été engagée à des fins de publicité (p. ex. appels pour « faire sortir le vote ») et qu'elle est consignée dans le rapport, moins détaillé, de l'association de circonscription, Élections Canada ne saura pas que la dépense a servi à cet usage, à moins qu'il n'en soit informé autrement : plainte, dénonciation, etc.

  Enfin, les rapports peuvent être produits trop tard pour que l'information qui s'y trouve sur les ententes avec les fournisseurs de service soit vraiment utile à l'enquête.

- **La technologie au service de l'anonymat**

  La technologie actuelle permet aux individus qui souhaitent contourner les règles d'éviter la détection de plusieurs façons. Ainsi, même lorsqu'il existe des dispositions législatives ou réglementaires applicables, comme les Règles du CRTC sur les télécommunications non sollicitées, ces dispositions peuvent être contournées dans la pratique à l'aide de moyens technologiques assurant l'anonymat. La solution à ce problème réside peut-être plus dans les progrès technologiques que dans la création de nouvelles règles.

[18] La loi permet au DGE de demander des documents supplémentaires à l'appui d'une dépense. Généralement, le contenu d'une publicité n'est pas pertinent à cette fin.

Services de téléphonie sur protocole Internet

- La technologie VoIP permet de cacher l'origine d'un appel et de forcer l'affichage d'un faux numéro sur l'afficheur du destinataire. C'est ce que l'on appelle les appels mystérieux (ou, en anglais, « spoofing »). Ceci restreint la possibilité de remonter jusqu'à l'appelant la piste d'un appel fait en utilisant cette technologie .
- La technologie a tellement évolué qu'il est possible d'installer un centre d'appel par VoIP pratiquement n'importe où, même dans un domicile privé, à l'aide d'un ordinateur récent, de quelques serveurs et de listes d'appels.
- Cela dit, dans le cas de la circonscription de Guelph, le système utilisé a été celui d'une entreprise de communications connue qui a conservé ses propres dossiers d'appels et coopéré avec les enquêteurs.

Serveurs mandataires

- L'anonymat peut aussi être facilité par les serveurs mandataires servant d'intermédiaire pour les ordinateurs et les serveurs qui communiquent par Internet. Les serveurs mandataires garantissent l'anonymat en effaçant automatiquement les traces de l'origine des communications.
- Dans l'enquête sur le dossier de Guelph, des documents déposés en cour par le commissaire aux élections fédérales indiquent que des serveurs mandataires ont servi à communiquer avec l'entreprise de communication sous une fausse identité.

Téléphones cellulaires jetables

- Les téléphones cellulaires jetables peuvent servir à dissimuler l'origine d'une communication. Certaines applications pour iPhone permettent également de créer des numéros de téléphone temporaires qui peuvent être utilisés pour faire des appels ou envoyer des messages texte sans laisser de trace.
- Dans cette même enquête, des documents déposés en cour par le commissaire spécifient qu'un téléphone cellulaire jetable a servi à communiquer avec une entreprise de communication sous une fausse identité.

- **Absence de normes sur la rétention des données dans le secteur des télécommunications**

Il n'existe pas de normes dans le secteur des télécommunications, sur les données qui doivent être conservées, et sur la durée de leur rétention. Certaines entreprises ne conservent des données sur leurs télécommunications que si elles sont facturées. D'autres conservent tous les renseignements sur les communications faites par leurs utilisateurs (p. ex. date de l'appel, durée, numéro de téléphone du destinataire). Certaines conservent l'information seulement quelques jours, d'autres pendant trois mois. La durée de la période de rétention des données influe directement sur la capacité des enquêteurs de faire leur travail.

Le *Code criminel* permet aux enquêteurs d'obtenir d'un juge une ordonnance de communication afin d'obliger des particuliers ou des entités à fournir ou à produire certains documents en leur possession. Moins drastiques que les mandats de perquisition, ces ordonnances peuvent être demandées lorsque les circonstances s'y prêtent. Aux termes du paragraphe 487.012(3), l'ordonnance ne sera accordée que si le

dénonciateur (dans le cas d'Élections Canada, l'enquêteur) démontre qu'il a des motifs raisonnables de croire qu'une infraction a été ou est présumée avoir été commise.

La rédaction de la dénonciation en vue de convaincre le juge d'accorder l'ordonnance de communication, la délivrance de l'ordonnance et la production des documents par leur détenteur peuvent prendre des semaines, voire des mois, compte tenu du déroulement de l'enquête et de la complexité du dossier. La chaîne des événements et des communications peut être très difficile sinon impossible à recréer lorsque l'entreprise ne conserve ses données de télécommunication que pendant une très courte période.

- **Critères d'obtention d'une ordonnance de communication**

  Comme mentionné ci-dessus, l'ordonnance de communication ne peut être délivrée que si l'enquêteur prouve qu'il a des motifs raisonnables de croire qu'une infraction a été commise ou est présumée avoir été commise. Il doit également avoir des motifs raisonnables de croire que les documents ou données demandés fourniront une preuve que l'infraction a été commise et que ces documents ou données sont en la possession ou à la disposition de la personne de qui ils sont demandés. Si la plainte n'est fondée que sur la mémoire du témoin, ou sur des doutes après le fait, ces motifs pourraient ne pas suffire pour justifier la délivrance d'une ordonnance de communication de documents à une entreprise de télécommunication.

- **Nature publique de la dénonciation**

  Lorsqu'un juge accorde une ordonnance de communication, un document lui est remis par la suite décrivant l'information obtenue. À ce stade, la dénonciation (c'est-à-dire le document dans lequel l'enquêteur explique pourquoi il a besoin des renseignements demandés, et pourquoi il croit que ces renseignements sont en la possession de la personne à qui ils sont demandés) devient accessible au public.

  C'est la découverte d'une de ces dénonciations par les journalistes du *Ottawa Citizen* qui a entraîné l'afflux de plaintes et de réactions de février 2012. Par contre, la publication du contenu des dénonciations a pu porter préjudice à la réputation des personnes ou entités contactées par les enquêteurs, alors que celles-ci n'étaient nullement accusées dans les dénonciations de visées malfaisantes.

4. Comment mieux promouvoir l’observation et l’application de la loi

Dans cette partie du document, diverses mesures sont considérées pour prévenir les problèmes à l’origine des plaintes reçues concernant l’élection générale de 2011 et favoriser une meilleure observation et application de la loi. Toutefois, il est important de garder en tête que les interdictions juridiques et les exigences en matière de divulgation ont peu d’effet sur les gens déterminés à mener des activités illégales. De ce point de vue, il est essentiel que les mesures retenues aient une valeur dissuasive et qu’elles soient assorties de mécanismes efficaces d’application de la loi.

a. Information du public sur le processus électoral

- Comme il a été mentionné précédemment, Élections Canada est chargé de gérer les bureaux de scrutin et de voir à ce que tout changement soit communiqué aux électeurs.
- En préparation pour la prochaine élection, l’organisme devra considérer des moyens de sensibiliser les électeurs à ses procédures (en particulier, le fait que l’organisme ne communique pas avec les électeurs par téléphone), de les mettre en garde contre les appels trompeurs et de les informer des recours possibles.
- Ceci peut inclure une collaboration avec d’autres organismes, par exemple le CRTC.

b. Interdiction de se faire passer pour un travailleur électoral ou de fournir sciemment de faux renseignements sur le processus électoral

- La *Loi modifiant la Loi électorale en ce qui concerne certaines manœuvres électorales,* L.O. 2011, ch. 17, a créé une nouvelle infraction rendant coupable quiconque, en Ontario ou ailleurs, se fait passer pour un employé ou agent du bureau du directeur général des élections, une personne nommée en application de la *Loi électorale*, un candidat ou une personne autorisée par le candidat à agir en son nom, ou une personne autorisée à agir en son nom par un parti inscrit ou une association de circonscription inscrite.
- Aux termes de cette loi, si le juge qui préside conclut que l’infraction a été commise sciemment, la personne est coupable de manœuvre frauduleuse et est passible d’une amende d’au plus 25 000 $ et d’un emprisonnement d’au plus deux ans moins un jour, ou d’une seule de ces peines.
- Alors que l’infraction prévue par cette loi de l’Ontario s’applique à la personne qui fait les appels, celle énoncée à l’alinéa 482*b*) de la LEC (inciter une personne à s’abstenir de voter) pourrait aussi s’appliquer à l’auteur du stratagème (c.-à-d. à la personne qui a donné instruction de faire les appels).
- Cela dit, on devrait considérer une infraction similaire à celle de l’Ontario, non seulement contre les personnes qui se font passer pour un employé ou un agent d’Élections Canada, mais aussi contre celles qui se présentent faussement comme un candidat ou son représentant, ou comme le représentant d’un parti enregistré ou d’une association de circonscription enregistrée. Dans tous ces cas, il ne serait pas nécessaire de prouver que le contrevenant voulait contrarier l’exercice du droit de vote de quelqu’un, ou inciter des électeurs à ne pas voter pour un candidat donné; il

suffirait, pour qu'il y ait infraction, de prouver que la personne s'est fait passer pour quelqu'un d'autre[19].

- L'infraction devrait être formulée de manière à couvrir aussi les pratiques trompeuses sur Internet, telles que les utilisations abusives des noms de domaine des campagnes et la création de sites Web présentés faussement comme ceux de vraies campagnes.
- Enfin, on pourrait envisager d'interdire l'usurpation de l'identité d'un « tiers » enregistré (ou d'un agent ou employé de ce tiers). Aux États-Unis, il est arrivé que des individus aient diffusé de faux renseignements sur le processus de vote en se présentant mensongèrement comme des représentants d'associations de défense des droits des minorités.

c. Élargissement des Règles sur les communications non sollicitées ou création dans la *Loi électorale du Canada* d'un régime similaire couvrant les « communications avec les électeurs », afin de mieux protéger la vie privée des électeurs

- Les Règles de télémarketing du CRTC et les Règles sur les composeurs-messagers automatiques, mentionnées ci-dessus, s'appliquent aux entités politiques dans le cas des appels automatisés ou en personne faits à des fins de sollicitation. Certaines règles s'appliquent aussi si l'appel automatisé est fait à des fins autres que la sollicitation. Dans ce cas, notamment, l'appelant doit donner le nom de la personne au nom de laquelle il fait l'appel, ainsi que l'adresse postale et le numéro de téléphone de cette personne.
- Il y a par contre quelques limites : le régime du CRTC repose sur l'auto-identification des télévendeurs : si ceux-ci ne s'identifient pas et que l'appel automatisé utilise une technologie assurant l'anonymat pour éviter la détection, les organismes responsables de l'application des lois ont peu de recours à l'heure actuelle.
- Dans ce contexte, les points suivants doivent être abordés.
- Convient-il d'élargir les Règles de télémarketing, ou de mettre sur pied un régime distinct, similaire mais sur mesure, de manière à couvrir les communications avec les électeurs (c.-à-d. tous les appels faits pendant la campagne électorale par des entités politiques, ou en leur nom)? Ces règles, comme celles de télémarketing, imposeraient des obligations telles que l'inscription préalable des télévendeurs ou clients, la tenue par ceux-ci d'une liste d'exclusion interne pour les communications avec les électeurs; la divulgation du nom de l'appelant, du télévendeur et du client au début de la communication et des restrictions sur les heures des appels.
- Les Règles de télémarketing s'appliquent actuellement aussi aux élections provinciales et municipales. Les éventuelles règles sur les communications avec les électeurs s'appliqueraient-elles aussi à ces élections?
- Ces règles devraient-elles s'appliquer uniquement pendant la période électorale, ou continuer de s'appliquer en tout temps?
- L'élargissement des Règles du CRTC sur les télécommunications non sollicitées présente un certain avantage, en ce sens que ce régime existe déjà, et que le CRTC

[19]Cependant, au moins dans le cas d'usurpation de l'identité d'un candidat, l'infraction devra être formulée de façon à exclure la satire politique. Elle pourrait préciser, par exemple, qu'il n'y a usurpation que lorsqu'on risque raisonnablement de croire à la fausse identité de l'imitateur.

a l'expérience de son administration. Le CRTC a aussi le pouvoir d'imposer des pénalités administratives en cas de violation des règles, preuve suffisante à l'appui. Il est bien connu du secteur des télécommunications, ce qui lui donne accès à des renseignements de qualité sur les progrès technologiques.

- Conviendrait-il mieux qu'un régime similaire soit autorisé en vertu de la LEC, et qu'il soit administré et appliqué par le Bureau du directeur général des élections?
- Point important, mais distinct : la LEC devrait-elle être modifiée de manière à permettre aux électeurs d'indiquer lorsqu'ils s'inscrivent ou mettent leurs renseignements à jour dans le Registre national des électeurs qu'ils ne veulent pas recevoir d'appels des entités politiques? Cette préférence, qui serait valide pendant une période précise, mais renouvelable (p. ex. cinq ans), pourrait être ajoutée après le nom sur les listes électorales fournies aux partis et aux candidats. Les entités politiques seraient tenues d'inscrire sur leur liste d'exclusion interne les électeurs qui en font la demande. Cette option permettrait au CRTC ou à Élections Canada de garder un œil sur les plaintes reçues et d'intervenir auprès de l'entité politique.
- Toutefois, cette approche peut avoir des effets pervers : les individus ou les organisations pourraient faire des appels trompeurs à des électeurs ciblés (partisans de leurs adversaires politiques) en espérant que les électeurs demanderaient de ne plus recevoir d'appels, ce qui empêcherait un candidat d'un autre parti de joindre ses partisans, existants ou potentiels (p. ex. pour amasser des fonds ou « faire sortir le vote »).

d. Élargissement aux partis politiques des principes sur la protection des renseignements personnels

- Le commissaire à la protection de la vie privée a récemment fait réaliser une étude sur les partis politiques fédéraux et la protection des renseignements personnels[20.] Dans leur rapport, les chercheurs signalent que les partis politiques recueillent des renseignements sur de nombreuses personnes – bénévoles, employés et donateurs du parti – mais aussi sur les électeurs inscrits, dont ils reçoivent les renseignements personnels non seulement d'Élections Canada, mais de diverses sources.
- Certains risques d'atteinte à la vie privée sont associés aux bases de données ainsi créées. Non seulement les partis traitent de grandes quantités de renseignements personnels, mais ils les partagent avec un grand nombre de bénévoles et d'employés de campagnes locales . Tel qu'il est indiqué dans le rapport :

> Mentionnons le risque que les renseignements personnels tombent entre de mauvaises mains ou soient utilisés à des fins non autorisées. Les renseignements peuvent aussi tomber entre de mauvaises mains à cause de la négligence, de l'absence de mesures de contrôle adéquates, d'échanges impropres ou de mauvaises intentions. Cela peut entraîner des préjudices pour les personnes concernées, comme le vol d'identité, le harcèlement ou le refus de services ou de droits. (p. 26)

- Les auteurs ajoutent : « Au-delà des risques pour les personnes, il faut aussi mentionner les risques sociaux lorsque les personnes ne font plus confiance aux organisations quand elles apprennent que celles-ci utilisent ou communiquent leurs

[20] Colin J. Bennett et Robin M. Bayley, *Les partis politiques fédéraux du Canada et la protection des renseignements personnels : une analyse comparative*, Ottawa, Commissaire à la protection de la vie privée, 2012. www.priv.gc.ca/information/pub/pp_201203_f.asp.

renseignements personnels à des fins dont elles ne sont pas informées et auxquelles elles n'ont pas consenti » (p. 26).

- Ils décrivent aussi divers incidents dans lesquels, ces dernières années, les renseignements personnels de certains électeurs ont été compromis, notamment lors d'une « possible tentative de suppression de voix dans des circonscriptions clés par le recours à des appels automatisés » (p. 28).
- Il est peut-être temps d'exiger et de s'assurer que les entités politiques respectent les principes de protection des renseignements personnels largement acceptés (exposés à l'annexe 1 de la LPRPDE et reproduits à l'annexe du présent document) concernant la collecte, l'utilisation, la communication et la conservation des renseignements; la responsabilité et l'obtention du consentement des personnes dont les renseignements personnels sont recueillis, utilisés ou communiqués; et la mise en place de mesures de sécurité.
- Une façon de réglementer les pratiques des partis tout en réduisant ce qu'on pourrait considérer comme un empiètement de l'État dans leurs affaires internes serait d'exiger des partis qu'ils obtiennent la certification d'un vérificateur de gestion externe. Cette certification attesterait que le parti a des mécanismes en place pour protéger les renseignements personnels des électeurs, et que ces mécanismes respectent les principes de la LPRPDE. Le parti devrait détenir cette certification pour continuer à recevoir les listes électorales d'Élections Canada.
- Cette solution ne serait pas nécessairement une panacée – par exemple, il ne serait peut-être pas pratique de l'appliquer aux candidats – mais elle pourrait jouer un rôle préventif et potentiellement limiter les dommages que pourraient causer les personnes négligentes ou celles qui ne souhaitent pas respecter les règles. La certification préserverait aussi la réputation des partis politiques qui la détiennent, et rassurerait les électeurs préoccupés par l'usage fait de leurs renseignements personnels, surtout à la suite des événements de la dernière élection. Cela est essentiel si l'on veut maintenir la capacité des partis et des candidats à communiquer avec les électeurs.

e. Exigences accrues en matière de communication de renseignements

Les options suivantes concernant les exigences accrues en matière de communication de renseignements peuvent être considérées en vue de faciliter l'enquête lorsqu'on reçoit des plaintes au sujet d'appels inappropriés.

Inscription et vérification de l'identité de tous les clients des entreprises de télécommunication pendant une élection générale.

- Cette recommandation, qui faisait partie de la motion adoptée à l'unanimité par la Chambre des communes, le 12 mars 2012[21], aurait de larges ramifications, puisque tous les clients des entreprises de télécommunication devraient s'inscrire (auprès de l'entreprise ou d'Élections Canada?) et être vérifiés (par l'entreprise ou Élections Canada?), que leurs télécommunications aient un lien (direct ou indirect) ou non avec l'élection. Cependant, si cette exigence était appliquée pendant la période électorale (habituellement de 36 jours), il pourrait être plus facile, après coup, de retrouver la piste des auteurs d'appels illégitimes. Il faudrait toutefois déterminer qui administrerait ce régime.

[21]Chambre des communes, 41e législature, 1re session, *Journaux*, no 94, 12 mars 2012.

Cette proposition a été clarifiée et simplifiée dans le projet de loi C-453 déposé en Chambre le 17 octobre 2012. Selon ce projet de loi d'un député, le parti politique, le candidat, le tiers chargé de faire de la publicité électorale ou l'association de circonscription qui, pendant la période électorale, se sert d'appareils ou de systèmes de téléphonie ou de télécommunications pour communiquer des messages vocaux relatifs à l'élection à des électeurs devrait tenir un registre quant au mode de communication des messages vocaux, l'identité des destinataires, la date et l'heure de chaque message ainsi que le nom de l'entreprise avec laquelle il a conclu un contrat pour la transmission de messages vocaux. Ces renseignements devraient être conservés pendant au moins deux ans par l'entité politique mais seraient fournis sur demande au directeur général des élections ou au commissaire aux élections fédérales dans les quatre mois suivant la réception de la demande[22].

- Une autre approche, qui faciliterait et accélérerait l'enquête relative à des appels inappropriés, consisterait à exiger des partis et des candidats qu'ils communiquent à Élections Canada les nom et coordonnées des personnes ou entités qu'ils engagent pour communiquer avec les électeurs avant ou pendant l'élection, dès que le contrat est signé ou l'entente conclue (plutôt que plusieurs mois après l'élection, dans le cadre de leurs rapports financiers).

Les entreprises de télécommunication qui fournissent des services de communication avec les électeurs pendant une élection générale devraient s'inscrire auprès d'Élections Canada.

- Cette recommandation, également incluse dans la motion adoptée par la Chambre des communes, part du principe que les entreprises de télécommunication (ou de télémarketing, selon le cas) reçoivent de leurs clients non seulement la liste des numéros de téléphone à appeler, mais aussi la caractéristique commune à tous ces numéros, en l'occurrence qu'ils appartiennent tous à des électeurs potentiels. La mise en œuvre de cette recommandation pourrait donc être difficile, mais elle sensibiliserait les entreprises de télécommunication au public visé par les partis et les campagnes. Cela dit, Élections Canada ne régit pas les entreprises de télécommunication.
- Le projet de loi C-453 propose une approche différente reflétant l'obligation de tenue de dossiers qui serait imposée aux entités politiques. Ainsi, l'obligation de tenir les mêmes dossiers s'appliquerait à l'entreprise de téléphonie ou de télécommunications ou la personne ou autre entité qui a conclu un contrat avec un parti enregistré, un candidat, un tiers chargé de faire de la publicité électorale ou une association de circonscription afin de fournir pendant la période électorale des appareils ou des systèmes de téléphonie ou de télécommunications en vue de communiquer des messages vocaux relatifs à l'élection à des électeurs. Ces renseignements devraient être transmis au directeur général des élections dans les quatre mois suivant le jour du scrutin.
- Comme c'est le cas pour les renseignements demandés des entités politiques, l'enquête pourrait procéder de façon plus rapide et plus efficace si ces informations étaient transmises à Élections Canada dès qu'une entente a été conclue. Ceci faciliterait également le retraçage d'appels possiblement inappropriés avant que les

[22] Voir l'art. 328.4 du projet de loi C-453, *Loi modifiant la Loi électorale du Canada (messages vocaux frauduleux en période électorale : prévention et poursuites judiciaires).*

informations ne soient effacées des dossiers de l'entreprise dans le cadre normal de leurs pratiques d'affaires.

f. Augmentation des outils de vérification à la disposition du directeur général des élections

Le nombre d'appels inappropriés pourrait être réduit de manière importante à l'aide de moyens administratifs dissuasifs. Les mécanismes possibles de vérification qui suivent devraient être considérés :

Pouvoir d'exiger que les entités politiques produisent tous les documents nécessaires pour assurer une bonne application de la Loi.

- La motion adoptée à l'unanimité par la Chambre des communes proposait en premier lieu le renforcement des capacités d'enquête d'Élections Canada, c'est-à-dire l'octroi au directeur général des élections du pouvoir de demander aux partis politiques tous les documents nécessaires pour assurer l'observation de la LEC. Cette proposition ressemble à ce que demandait le DGE dans son rapport de recommandations de 2010, soit l'autorisation de demander aux partis enregistrés de fournir, au besoin, les documents et les renseignements qu'il estime nécessaires pour vérifier que le parti et son agent principal se sont conformés aux exigences de la Loi relatives au compte de dépenses électorales.

Donner au directeur général des élections le pouvoir de faire tout examen ou vérification nécessaire à l'exercice de son mandat.

- Selon le modèle adopté par d'autres administrations, la LEC pourrait autoriser le DGE à faire tous les examens ou vérifications qu'il considère comme nécessaires à l'exercice de son mandat. Ce pouvoir serait accordé au DGE à des fins administratives, et non pour mener des enquêtes de nature pénale.

Donner au directeur général des élections le pouvoir de demander des renseignements additionnels aux entités politiques quant à l'utilisation de services de télémarketing

- L'augmentation des exigences de divulgation imposées aux partis et à toutes les entités politiques (associations de circonscription, candidats) sur l'utilisation des services de télémarketing et de communication promotionnelle (p. ex. exiger la divulgation du texte des télécommunications adressées aux électeurs pendant la période électorale) faciliterait la vérification et découragerait les usages illégitimes.

g. Augmentation des outils d'enquête du commissaire aux élections fédérales

Les mécanismes suivants peuvent également être considérés en vue de faciliter la tâche du commissaire dans sa collecte des éléments de preuve lorsqu'il est informé d'allégations d'appels inappropriés faits à des électeurs.

Pouvoir d'exiger des entreprises de télémarketing qu'elles conservent des données au sujet de toutes les communications faites durant une période électorale

- Pour faciliter les enquêtes quant aux appels inappropriés, on pourrait exiger des entreprises offrant des services de télémarketing qu'elles conservent les dossiers de toutes les communications effectuées au Canada pendant une élection (y compris les renseignements sur le client et sur tout paiement effectué, les scripts, et les

appels entrants et sortants). Ces dossiers seraient conservés pendant au moins un an après l'élection, mais seraient communiqués au commissaire une fois l'autorisation judiciaire obtenue au titre d'un mandat de perquisition traditionnel ou d'une ordonnance de communication.

Pouvoir d'exiger des entreprises de télécommunication qu'elles préservent des données informatiques spécifiques jusqu'à l'obtention d'une ordonnance de communication

- Il serait également utile que le commissaire aux élections fédérales (ou ses représentants) soit autorisé à exiger, sur demande, la conservation de données informatiques spécifiques en la possession ou sous le contrôle d'une entreprise de télécommunication, de façon à empêcher ces entreprises de détruire ces renseignements dans le cadre normal de leurs pratiques d'affaires.
- Les enquêteurs ne pourraient faire cette demande que s'ils ont des motifs raisonnables à croire a) qu'une infraction à la Loi a été ou sera perpétrée, b) que les données informatiques visées par la demande sont en la possession ou sous le contrôle de la personne en question, et c) que ces données seront utiles à l'enquête. Cette demande pourrait être faite sans autorisation judiciaire, mais ne serait valide que pendant une courte période (p. ex. 90 jours), jusqu'à ce qu'une ordonnance de communication soit obtenue d'un juge.
- Cependant, ce mécanisme ne sera utile que si le commissaire connaît à l'avance quelques détails sur les fournisseurs de services de télécommunication engagés par les candidats et les partis politiques. Actuellement, cette information n'est pas connue dans le cas des partis, et dans celui des candidats, elle ne devient accessible à Élections Canada qu'une fois que ceux-ci présentent leurs rapports financiers, lesquels sont exigés dans les quatre mois suivant le jour de l'élection. Par conséquent, les candidats et les partis devraient être tenus de communiquer les renseignements sur leurs fournisseurs de services de télécommunication (y compris les numéros de téléphone et de compte Internet) dès qu'une entente est conclue pendant ou avant la période électorale. Tel qu'indiqué plus haut, la même obligation devrait s'appliquer aux services de télémarketing.

Pouvoir du Commissaire d'exiger qu'une personne réponde à ses questions, sous réserve d'une autorisation judiciaire préalable

- Un autre mécanisme, qui existe déjà dans la *Loi sur la concurrence*[23], autoriserait le commissaire à saisir un juge d'une demande *ex parte* afin d'obtenir une ordonnance pour qu'une personne qui détient ou détient vraisemblablement des renseignements pertinents à une enquête puisse être interrogée sous serment par le commissaire ou son représentant concernant toute question pertinente à l'enquête. Cette ordonnance pourrait également obliger la personne à produire des documents.
- Avant d'obtenir une telle ordonnance, le commissaire devrait prouver, en s'appuyant sur une preuve par affidavit, qu'une enquête est en cours et que la personne devant être à interroger détient ou détient vraisemblablement les renseignements recherchés.
- Aucun témoignage présenté par une personne en vertu d'une telle ordonnance ne pourrait être utilisé ou reçu contre cette personne dans le cadre d'une procédure pénale.

[23] Voir l'art. 11 de la *Loi sur la concurrence*, L.R.C., 1985, ch. C-34.

- Dans ce contexte, il y a lieu de noter que le directeur général des élections du Québec dispose, à l'égard de ses propres enquêtes, du pouvoir d'exiger que comparaisse devant lui, sans autorisation judiciaire préalable, toute personne dont le témoignage peut se rapporter au sujet de l'enquête, et contraindre toute personne à déposer devant lui les livres, papiers, documents et écrits qu'il juge comme nécessaires pour découvrir la vérité[24].

[24] L'article 494 de la *Loi électorale* du Québec, LRQ, ch. E-3.3, investit le DGE et toute personne qu'il désigne des pouvoirs et immunités d'un commissaire nommé en vertu de la Loi sur les commissions d'enquêtes (ch. C-37). Ceux-ci incluent le pouvoir décrit ici.

Annexe

Principes énoncés dans la norme nationale du Canada intitulée *Code type sur la protection des renseignements personnels*, CAN/CSA-Q830-96[25]

4.1 Premier principe — Responsabilité

Une organisation est responsable des renseignements personnels dont elle a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés ci-dessous.

4.1.1

Il incombe à la ou aux personnes désignées de s'assurer que l'organisation respecte les principes même si d'autres membres de l'organisation peuvent être chargés de la collecte et du traitement quotidiens des renseignements personnels. D'autres membres de l'organisation peuvent aussi être délégués pour agir au nom de la ou des personnes désignées.

4.1.2

Il doit être possible de connaître sur demande l'identité des personnes que l'organisation a désignées pour s'assurer que les principes sont respectés.

4.1.3

Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie.

4.1.4

Les organisations doivent assurer la mise en œuvre des politiques et des pratiques destinées à donner suite aux principes, y compris :

a) la mise en œuvre des procédures pour protéger les renseignements personnels;

b) la mise en place des procédures pour recevoir les plaintes et les demandes de renseignements et y donner suite;

c) la formation du personnel et la transmission au personnel de l'information relative aux politiques et pratiques de l'organisation; et

d) la rédaction des documents explicatifs concernant leurs politiques et procédures.

4.2 Deuxième principe — Détermination des fins de la collecte des renseignements

Les fins auxquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisation avant la collecte ou au moment de celle-ci.

[25] *Loi sur la protection des renseignements personnels et les documents électroniques*, annexe 1

4.2.1

L’organisation doit documenter les fins auxquelles les renseignements personnels sont recueillis afin de se conformer au principe de la transparence (article 4.8) et au principe de l’accès aux renseignements personnels (article 4.9).

4.2.2

Le fait de préciser les fins de la collecte de renseignements personnels avant celle-ci ou au moment de celle-ci permet à l’organisation de déterminer les renseignements dont elle a besoin pour réaliser les fins mentionnées. Suivant le principe de la limitation en matière de collecte (article 4.4), l’organisation ne doit recueillir que les renseignements nécessaires aux fins mentionnées.

4.2.3

Il faudrait préciser à la personne auprès de laquelle on recueille des renseignements, avant la collecte ou au moment de celle-ci, les fins auxquelles ils sont destinés. Selon la façon dont se fait la collecte, cette précision peut être communiquée de vive voix ou par écrit. Par exemple, on peut indiquer ces fins sur un formulaire de demande de renseignements.

4.2.4

Avant de se servir de renseignements personnels à des fins non précisées antérieurement, les nouvelles fins doivent être précisées avant l’utilisation. À moins que les nouvelles fins auxquelles les renseignements sont destinés ne soient prévues par une loi, il faut obtenir le consentement de la personne concernée avant d’utiliser les renseignements à cette nouvelle fin. Pour obtenir plus de précisions sur le consentement, se reporter au principe du consentement (article 4.3).

4.2.5

Les personnes qui recueillent des renseignements personnels devraient être en mesure d’expliquer à la personne concernée à quelles fins sont destinés ces renseignements.

4.2.6

Ce principe est étroitement lié au principe de la limitation de la collecte (article 4.4) et à celui de la limitation de l’utilisation, de la communication et de la conservation (article 4.5).

4.3 Troisième principe — Consentement

Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir, à moins qu’il ne soit pas approprié de le faire.

Note : Dans certaines circonstances, il est possible de recueillir, d’utiliser et de communiquer des renseignements à l’insu de la personne concernée et sans son consentement. Par exemple, pour des raisons d’ordre juridique ou médical ou pour des raisons de sécurité, il peut être impossible ou peu réaliste d’obtenir le consentement de la personne concernée. Lorsqu’on recueille des renseignements aux fins du contrôle d’application de la loi, de la détection d’une fraude ou de sa prévention, on peut aller à l’encontre du but visé si l’on cherche à obtenir le consentement de la personne concernée. Il peut être impossible ou inopportun de chercher à obtenir le consentement d’un mineur, d’une personne gravement malade ou souffrant d’incapacité mentale. De plus, les organisations qui ne sont pas en relation directe avec la

personne concernée ne sont pas toujours en mesure d'obtenir le consentement prévu. Par exemple, il peut être peu réaliste pour une œuvre de bienfaisance ou une entreprise de marketing direct souhaitant acquérir une liste d'envoi d'une autre organisation de chercher à obtenir le consentement des personnes concernées. On s'attendrait, dans de tels cas, à ce que l'organisation qui fournit la liste obtienne le consentement des personnes concernées avant de communiquer des renseignements personnels.

4.3.1

Il faut obtenir le consentement de la personne concernée avant de recueillir des renseignements personnels à son sujet et d'utiliser ou de communiquer les renseignements recueillis. Généralement, une organisation obtient le consentement des personnes concernées relativement à l'utilisation et à la communication des renseignements personnels au moment de la collecte. Dans certains cas, une organisation peut obtenir le consentement concernant l'utilisation ou la communication des renseignements après avoir recueilli ces renseignements, mais avant de s'en servir, par exemple, quand elle veut les utiliser à des fins non précisées antérieurement.

4.3.2

Suivant ce principe, il faut informer la personne au sujet de laquelle on recueille des renseignements et obtenir son consentement. Les organisations doivent faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés. Pour que le consentement soit valable, les fins doivent être énoncées de façon que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués.

4.3.3

Une organisation ne peut pas, pour le motif qu'elle fournit un bien ou un service, exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées.

4.3.4

La forme du consentement que l'organisation cherche à obtenir peut varier selon les circonstances et la nature des renseignements. Pour déterminer la forme que prendra le consentement, les organisations doivent tenir compte de la sensibilité des renseignements. Si certains renseignements sont presque toujours considérés comme sensibles, par exemple les dossiers médicaux et le revenu, tous les renseignements peuvent devenir sensibles suivant le contexte. Par exemple, les nom et adresse des abonnés d'une revue d'information ne seront généralement pas considérés comme des renseignements sensibles. Toutefois, les nom et adresse des abonnés de certains périodiques spécialisés pourront l'être.

4.3.5

Dans l'obtention du consentement, les attentes raisonnables de la personne sont aussi pertinentes. Par exemple, une personne qui s'abonne à un périodique devrait raisonnablement s'attendre à ce que l'entreprise, en plus de se servir de son nom et de son adresse à des fins de postage et de facturation, communique avec elle pour lui demander si elle désire que son abonnement soit renouvelé. Dans ce cas, l'organisation peut présumer que la demande de la personne constitue un consentement à ces fins précises. D'un autre côté, il n'est pas raisonnable qu'une personne s'attende à ce que les renseignements personnels qu'elle fournit à

un professionnel de la santé soient donnés sans son consentement à une entreprise qui vend des produits de soins de santé. Le consentement ne doit pas être obtenu par un subterfuge.

4.3.6

La façon dont une organisation obtient le consentement peut varier selon les circonstances et la nature des renseignements recueillis. En général, l'organisation devrait chercher à obtenir un consentement explicite si les renseignements sont susceptibles d'être considérés comme sensibles. Lorsque les renseignements sont moins sensibles, un consentement implicite serait normalement jugé suffisant. Le consentement peut également être donné par un représentant autorisé (détenteur d'une procuration, tuteur).

4.3.7

Le consentement peut revêtir différentes formes, par exemple :

a) on peut se servir d'un formulaire de demande de renseignements pour obtenir le consentement, recueillir des renseignements et informer la personne de l'utilisation qui sera faite des renseignements. En remplissant le formulaire et en le signant, la personne donne son consentement à la collecte de renseignements et aux usages précisés;

b) on peut prévoir une case où la personne pourra indiquer en cochant qu'elle refuse que ses nom et adresse soient communiqués à d'autres organisations. Si la personne ne coche pas la case, il sera présumé qu'elle consent à ce que les renseignements soient communiqués à des tiers;

c) le consentement peut être donné de vive voix lorsque les renseignements sont recueillis par téléphone; ou

d) le consentement peut être donné au moment où le produit ou le service est utilisé.

4.3.8

Une personne peut retirer son consentement en tout temps, sous réserve de restrictions prévues par une loi ou un contrat et d'un préavis raisonnable. L'organisation doit informer la personne des conséquences d'un tel retrait.

4.4 Quatrième principe — Limitation de la collecte

L'organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite.

4.4.1

Les organisations ne doivent pas recueillir des renseignements de façon arbitraire. On doit restreindre tant la quantité que la nature des renseignements recueillis à ce qui est nécessaire pour réaliser les fins déterminées. Conformément au principe de la transparence (article 4.8), les organisations doivent préciser la nature des renseignements recueillis comme partie intégrante de leurs politiques et pratiques concernant le traitement des renseignements.

4.4.2

L'exigence selon laquelle les organisations sont tenues de recueillir des renseignements personnels de façon honnête et licite a pour objet de les empêcher de tromper les gens et de les induire en erreur quant aux fins auxquelles les renseignements sont recueillis. Cette

obligation suppose que le consentement à la collecte de renseignements ne doit pas être obtenu par un subterfuge.

4.4.3

Ce principe est étroitement lié au principe de détermination des fins auxquelles la collecte est destinée (article 4.2) et à celui du consentement (article 4.3).

4.5 Cinquième principe — Limitation de l'utilisation, de la communication et de la conservation

Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées.

4.5.1

Les organisations qui se servent de renseignements personnels à des fins nouvelles doivent documenter ces fins (voir article 4.2.1).

4.5.2

Les organisations devraient élaborer des lignes directrices et appliquer des procédures pour la conservation des renseignements personnels. Ces lignes directrices devraient préciser les durées minimales et maximales de conservation. On doit conserver les renseignements personnels servant à prendre une décision au sujet d'une personne suffisamment longtemps pour permettre à la personne concernée d'exercer son droit d'accès à l'information après que la décision a été prise. Une organisation peut être assujettie à des exigences prévues par la loi en ce qui concerne les périodes de conservation.

4.5.3

On devrait détruire, effacer ou dépersonnaliser les renseignements personnels dont on n'a plus besoin aux fins précisées. Les organisations doivent élaborer des lignes directrices et appliquer des procédures régissant la destruction des renseignements personnels.

4.5.4

Ce principe est étroitement lié au principe du consentement (article 4.3), à celui de la détermination des fins auxquelles la collecte est destinée (article 4.2), ainsi qu'à celui de l'accès individuel (article 4 9).

4.6 Sixième principe — Exactitude

Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés.

4.6.1

Le degré d'exactitude et de mise à jour ainsi que le caractère complet des renseignements personnels dépendront de l'usage auquel ils sont destinés, compte tenu des intérêts de la personne. Les renseignements doivent être suffisamment exacts, complets et à jour pour réduire au minimum la possibilité que des renseignements inappropriés soient utilisés pour prendre une décision à son sujet.

4.6.2

Une organisation ne doit pas systématiquement mettre à jour les renseignements personnels à moins que cela ne soit nécessaire pour atteindre les fins auxquelles ils ont été recueillis.

4.6.3

Les renseignements personnels qui servent en permanence, y compris les renseignements qui sont communiqués à des tiers, devraient normalement être exacts et à jour à moins que des limites se rapportant à l'exactitude de ces renseignements ne soient clairement établies.

4.7 Septième principe — Mesures de sécurité

Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

4.7.1

Les mesures de sécurité doivent protéger les renseignements personnels contre la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées. Les organisations doivent protéger les renseignements personnels quelle que soit la forme sous laquelle ils sont conservés.

4.7.2

La nature des mesures de sécurité variera en fonction du degré de sensibilité des renseignements personnels recueillis, de la quantité, de la répartition et du format des renseignements personnels ainsi que des méthodes de conservation. Les renseignements plus sensibles devraient être mieux protégés. La notion de sensibilité est présentée à l'article 4.3.4.

4.7.3

Les méthodes de protection devraient comprendre :

a) des moyens matériels, par exemple le verrouillage des classeurs et la restriction de l'accès aux bureaux;

b) des mesures administratives, par exemple des autorisations sécuritaires et un accès sélectif; et

c) des mesures techniques, par exemple l'usage de mots de passe et du chiffrement.

4.7.4

Les organisations doivent sensibiliser leur personnel à l'importance de protéger le caractère confidentiel des renseignements personnels.

4.7.5

Au moment du retrait ou de la destruction des renseignements personnels, on doit veiller à empêcher les personnes non autorisées d'y avoir accès (article 4.5.3).

4.8 Huitième principe — Transparence

Une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne.

4.8.1

Les organisations doivent faire preuve de transparence au sujet de leurs politiques et pratiques concernant la gestion des renseignements personnels. Une personne doit pouvoir obtenir sans effort déraisonnable de l'information au sujet des politiques et des pratiques d'une organisation. Ces renseignements doivent être fournis sous une forme généralement compréhensible.

4.8.2

Les renseignements fournis doivent comprendre :

a) le nom ou la fonction de même que l'adresse de la personne responsable de la politique et des pratiques de l'organisation et à qui il faut acheminer les plaintes et les demandes de renseignements;

b) la description du moyen d'accès aux renseignements personnels que possède l'organisation;

c) la description du genre de renseignements personnels que possède l'organisation, y compris une explication générale de l'usage auquel ils sont destinés;

d) une copie de toute brochure ou tout document d'information expliquant la politique, les normes ou les codes de l'organisation; et

e) la définition de la nature des renseignements personnels communiqués aux organisations connexes (par exemple, les filiales).

4.8.3

Une organisation peut rendre l'information concernant sa politique et ses pratiques accessibles de diverses façons. La méthode choisie est fonction de la nature des activités de l'organisation et d'autres considérations. Par exemple, une organisation peut offrir des brochures à son établissement, poster des renseignements à ses clients, offrir un accès en ligne ou établir un numéro de téléphone sans frais.

4.9 Neuvième principe — Accès aux renseignements personnels

Une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter. Il sera aussi possible de contester l'exactitude et l'intégralité des renseignements et d'y faire apporter les corrections appropriées.

Note : Dans certains cas, il peut être impossible à une organisation de communiquer tous les renseignements personnels qu'elle possède au sujet d'une personne. Les exceptions aux exigences en matière d'accès aux renseignements personnels devraient être restreintes et précises. On devrait informer la personne, sur demande, des raisons pour lesquelles on lui refuse l'accès aux renseignements. Ces raisons peuvent comprendre le coût exorbitant de la fourniture de l'information, le fait que les renseignements personnels contiennent des détails sur d'autres personnes, l'existence de raisons d'ordre juridique, de raisons de sécurité ou de raisons d'ordre commercial exclusives et le fait que les renseignements sont protégés par le secret professionnel ou dans le cours d'une procédure de nature judiciaire.

4.9.1

Une organisation doit informer la personne qui en fait la demande du fait qu'elle possède des renseignements personnels à son sujet, le cas échéant. Les organisations sont invitées à indiquer la source des renseignements. L'organisation doit permettre à la personne concernée

de consulter ces renseignements. Dans le cas de renseignements médicaux sensibles, l'organisation peut préférer que ces renseignements soient communiqués par un médecin. En outre, l'organisation doit informer la personne concernée de l'usage qu'elle fait ou a fait des renseignements et des tiers à qui ils ont été communiqués.

4.9.2

Une organisation peut exiger que la personne concernée lui fournisse suffisamment de renseignements pour qu'il lui soit possible de la renseigner sur l'existence, l'utilisation et la communication de renseignements personnels. L'information ainsi fournie doit servir à cette seule fin.

4.9.3

L'organisation qui fournit le relevé des tiers à qui elle a communiqué des renseignements personnels au sujet d'une personne devrait être la plus précise possible. S'il lui est impossible de fournir une liste des organisations à qui elle a effectivement communiqué des renseignements au sujet d'une personne, l'organisation doit fournir une liste des organisations à qui elle pourrait avoir communiqué de tels renseignements.

4.9.4

Une organisation qui reçoit une demande de communication de renseignements doit répondre dans un délai raisonnable et ne peut exiger, pour ce faire, que des droits minimes. Les renseignements demandés doivent être fournis sous une forme généralement compréhensible. Par exemple, l'organisation qui se sert d'abréviations ou de codes pour l'enregistrement des renseignements doit fournir les explications nécessaires.

4.9.5

Lorsqu'une personne démontre que des renseignements personnels sont inexacts ou incomplets, l'organisation doit apporter les modifications nécessaires à ces renseignements. Selon la nature des renseignements qui font l'objet de la contestation, l'organisation doit corriger, supprimer ou ajouter des renseignements. S'il y a lieu, l'information modifiée doit être communiquée à des tiers ayant accès à l'information en question.

4.9.6

Lorsqu'une contestation n'est pas réglée à la satisfaction de la personne concernée, l'organisation prend note de l'objet de la contestation. S'il y a lieu, les tierces parties ayant accès à l'information en question doivent être informées du fait que la contestation n'a pas été réglée.

4.10 Dixième principe — Possibilité de porter plainte à l'égard du non-respect des principes

Toute personne doit être en mesure de se plaindre du non-respect des principes énoncés ci-dessus en communiquant avec la ou les personnes responsables de les faire respecter au sein de l'organisation concernée.

4.10.1

La question de la désignation de la personne responsable du respect des principes dans l'organisation fait l'objet de l'article 4.1.1.

4.10.2

Les organisations doivent établir des procédures pour recevoir les plaintes et les demandes de renseignements concernant leurs politiques et pratiques de gestion des renseignements personnels et y donner suite. Les procédures relatives aux plaintes devraient être facilement accessibles et simples à utiliser.

4.10.3

Les organisations doivent informer les personnes qui présentent une demande de renseignements ou déposent une plainte de l’existence des procédures pertinentes. Il peut exister un éventail de ces procédures. Par exemple, certaines autorités réglementaires acceptent les plaintes concernant les pratiques de gestion des renseignements personnels des entreprises relevant de leur compétence.

4.10.4

Une organisation doit faire enquête sur toutes les plaintes. Si une plainte est jugée fondée, l’organisation doit prendre les mesures appropriées, y compris la modification de ses politiques et de ses pratiques au besoin.