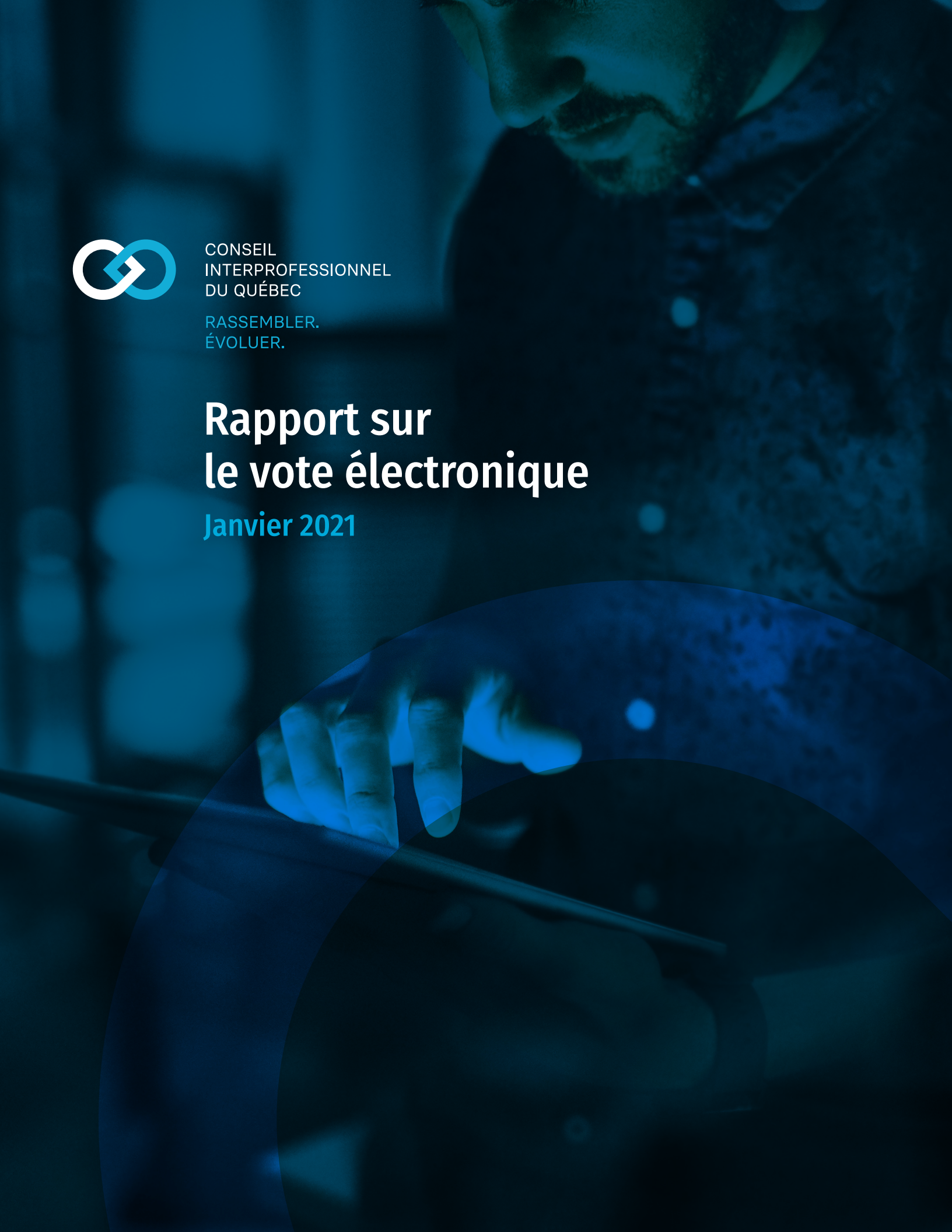


CONSEIL
INTERPROFESSIONNEL
DU QUÉBEC

RASSEMBLER.
ÉVOLUER.

Rapport sur le vote électronique

Janvier 2021

Dépôt légal– Bibliothèque et Archives nationales du Québec, 2021
Dépôt légal – Bibliothèque et Archives du Canada, 2021
ISBN : 978-2-920350-53-3

Table des matières

Présentation du Conseil interprofessionnel du Québec

Le Conseil interprofessionnel du Québec (CIQ) est le regroupement des 46 ordres professionnels du Québec. Il a pour mission d'être la voix collective des ordres professionnels sur des dossiers d'intérêt public. En vertu du *Code des professions*, il agit également à titre d'organisme-conseil auprès du gouvernement du Québec et plus spécifiquement auprès du ou de la ministre responsable de l'application des lois professionnelles.

À ce titre, il peut notamment :

> « [...] fournir au public, à la demande du ou de la ministre ou de l'un ou de plusieurs ordres, de l'information concernant le système professionnel, les professionnels et professionnelles ainsi que les devoirs et les pouvoirs des ordres[1] [et]
>
> [...] effectuer des recherches et formuler des avis sur toute question relative à la protection du public que doivent assurer les ordres[2]. »

Au Québec, le système professionnel compte 46 ordres professionnels. Les ordres ont la responsabilité de réglementer 55 professions, soit plus de 400 000 professionnels. Ceux-ci sont encadrés par le *Code des professions*, la loi-cadre du système professionnel québécois. Également, 25 lois professionnelles et près de 800 règlements encadrent le fonctionnement des ordres.

Pour s'acquitter de sa mission, le CIQ procure aussi aux ordres professionnels des occasions de partager des pratiques innovantes et de développer des outils communs permettant d'améliorer leur efficacité. Il offre également des activités de formation, tout en agissant comme agent mobilisateur sur les dossiers qui concernent et affectent le système professionnel.

Le CIQ est formé des ordres professionnels; chacun des ordres y est représenté par son président ou par un autre membre désigné par le conseil d'administration. L'assemblée des membres est la plus haute instance du CIQ.

Finalement, le CIQ diffuse de l'information sur le système professionnel et sa valeur ajoutée pour la population du Québec, tant auprès des médias que du grand public. Il met à la disposition du public divers documents et études concernant les professions réglementées ou tout autre sujet relatif à la protection du public.

---

1 *Code des professions*, RLRQ, c. C-26, art. 19 al. 2 par. 4.

2 *Ibidem*, art. 19 al. 2 par. 8.

Avant-propos

En janvier 2019, le Conseil interprofessionnel du Québec a mis sur pied le Groupe de travail sur le vote électronique en lui conférant le mandat de produire un rapport visant à orienter les ordres professionnels et les instances gouvernementales quant au cadre législatif et réglementaire afférent au vote électronique.

Composé de personnes ayant une expertise en droit professionnel, en droit des technologies de l'information et en cybersécurité, le groupe de travail était coordonné par Me Julie de Gongre, directrice des affaires juridiques du CIQ.

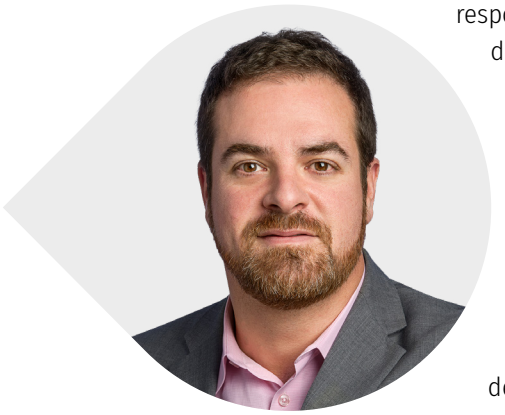
Me Christiane Brizard, C.OCPAQ

Avocate, associée-conseil, Langlois avocats, S.E.N.C.R.L.

Me Brizard est associée au bureau de Langlois avocats à Montréal. Elle exerce principalement dans le domaine de la gouvernance, de l'éthique et du droit professionnel. Elle a agi pendant plusieurs années à titre de secrétaire, vice-présidente aux affaires juridiques et conseillère stratégique auprès de l'Ordre des comptables agréés du Québec et de l'Ordre des comptables professionnels agréés du Québec. À ce titre, elle a conseillé la haute direction sur des enjeux éthiques, juridiques, systémiques et de gouvernance. Elle possède une connaissance approfondie du système professionnel et de l'encadrement des acteurs des marchés financiers et a participé à plusieurs commissions parlementaires. Elle a été un acteur clé dans la réalisation de l'unification des professions comptables.

Me Dominic Jaar, Ad. E.

Associé et leader régional, conseil en management, KPMG au Canada



L'équipe que dirige Me Jaar répond aux besoins informationnels des professionnels responsables des affaires juridiques, de la conformité, des risques et des TI dans des sociétés ouvertes et fermées. Il s'intéresse aux enquêtes technologiques et offre des services qui englobent l'administration de la preuve électronique, la récupération de preuves, la gestion des documents et de l'information, l'analyse de données et les cyberenquêtes. Avant de se joindre à KPMG, Me Jaar était directeur général du Centre canadien de technologie judiciaire et président de la société Conseils Ledjit. Il a été avocat plaidant et praticien du domaine de la protection des renseignements personnels chez Bell Canada et avocat plaidant dans un cabinet d'avocats national. Me Jaar enseigne l'investigation informatique, la preuve électronique, la méthodologie des enquêtes et la protection des renseignements personnels dans diverses universités nord-américaines et dans le cadre de congrès internationaux.

M. Jean-Philippe Racine

Président fondateur du Groupe CyberSwat, une entreprise spécialisée en cybersécurité

Fort de 19 années d'expérience dans le secteur des TI et de nombreuses certifications et formations, M. Racine possède plus de 15 ans d'expérience en cybersécurité. Ayant commencé sa carrière du côté technique de la sécurité informatique, il a rapidement évolué dans les volets tactiques et stratégiques de la sécurité. Entrepreneur depuis 2009, M. Racine sait vulgariser les concepts et les enjeux de sécurité à une clientèle d'affaires tout en restant au fait des derniers développements technologiques du marché.
M. Racine détient une maîtrise en administration, option gouvernance, audit et sécurité des TI. Il s'est également spécialisé en obtenant plusieurs certifications, dont celles de CISA, de CISSP ainsi que le CCSK de la Cloud Security Alliance.

Me Pierre Trudel

Professeur titulaire au Centre de recherche en droit public de la Faculté de droit de l'Université de Montréal

Me Pierre Trudel est professeur titulaire au Centre de recherche en droit public (CRDP) de la Faculté de droit de l'Université de Montréal. Il a été professeur invité aux Universités Laval (Québec), Paris II (Panthéon-Assas) et Namur (Belgique). De 1986 à 1988, il a été directeur de la recherche du Groupe de travail fédéral sur la politique de radiodiffusion. De 1990 à 1995, il a été directeur du Centre de recherche en droit public de l'Université de Montréal. De 2003 à 2015, il a été le premier titulaire de la Chaire L.R. Wilson sur le droit des technologies de l'information et du commerce électronique. En mai 2018, il a été nommé par le ministère de l'Industrie et le ministère du Patrimoine membre du groupe d'experts sur la révision des lois sur les télécommunications et de la radiodiffusion. Il enseigne en droit de l'information et en droit du cyberespace. Il est l'auteur de plusieurs livres et articles en droit des médias et en droit des technologies de l'information. Il travaille présentement à des projets de recherche sur les droits fondamentaux de l'information, la protection de la vie privée, l'évaluation des enjeux et risques juridiques, les objets connectés, la e-santé, le droit de l'audiovisuel, le commerce électronique et les méthodologies d'élaboration des règles de conduite dans les environnements en réseaux. Il est chroniqueur régulier au journal *Le Devoir*. Le site www.pierretrudel.info rend compte au jour le jour de ses activités professionnelles.

Le groupe de travail s'est réuni à quelques reprises en 2019 et 2020 afin d'échanger sur le cadre législatif et réglementaire afférent au vote électronique et pour finaliser le présent rapport.

1. Rappel historique

Dès 2011, le CIQ recommandait à l'Office des professions du Québec de permettre à un ordre professionnel d'utiliser le vote électronique sur une base facultative afin d'élire les membres de son conseil d'administration. Le Conseil avait alors précisé que les principes légitimant un résultat électoral devaient être respectés, et ce, à toutes les étapes du scrutin.

En 2014, le *Code des professions*, la loi-cadre du système professionnel québécois, a ainsi été modifié afin de prévoir que le conseil d'administration d'un ordre professionnel puisse choisir de tenir une élection du président et des autres administrateurs par un moyen technologique, lequel doive assurer la sécurité, le secret et l'intégrité du vote. Le *Code* prévoit également que pour tenir une telle élection par moyen technologique le conseil d'administration doive en fixer les modalités dans un règlement. Il prévoit aussi que ce dernier puisse adapter les dispositions [relatives au vote sur support papier] du *Code* pour permettre la mise en œuvre de cette élection. Il faut savoir qu'un tel règlement doit être transmis pour examen à l'Office des professions du Québec qui peut l'approuver avec ou sans modifications. À ce jour, certains ordres ont ainsi fixé de telles modalités[3].

L'introduction au *Code* de l'élection par un moyen technologique visait notamment à faciliter les communications entre les ordres et leurs membres[4].

2. Une responsabilité des ordres professionnels

En 2017, l'Office des professions du Québec a produit un document intitulé *Élection au conseil d'administration des ordres professionnels : aspects légaux et pratiques d'un scrutin tenu par un moyen technologique*. Ce document énonce avec justesse qu'en vertu des dispositions du *Code des professions*, « le secrétaire de l'ordre agit comme secrétaire d'élection[5] ». Toutefois, dans un courriel transmis en 2018 dans le cadre d'un échange entre le directeur général du CIQ et la directrice de la veille et des orientations de l'Office des professions du Québec sur le positionnement de l'Office, cette dernière apportait la précision suivante à l'égard de ce document :

> « Rappelons que ce document fait l'énumération de toutes les exigences nécessaires à l'utilisation du vote électronique lors d'élection des membres du conseil d'administration d'un ordre professionnel. Parmi ces conditions, on y trouve la nécessité de faire l'embauche d'un expert indépendant qui sera chargé d'assurer la sécurité, l'intégrité et le secret du vote par un moyen technologique. »

(notre soulignement)

Il importe de rappeler que le **secrétaire de l'ordre demeure l'ultime responsable du processus** et qu'il doit s'assurer que les principes légitimant un résultat électoral soient respectés, et ce, à toutes les étapes du scrutin. Cela évidemment n'empêche pas la participation d'autres acteurs et experts au processus dès lors que leur rôle s'inscrit en soutien des tâches incombant au secrétaire de l'ordre.

3 Une liste de certains règlements afférents est reproduite à l'annexe IV.

4 En effet, lors de l'étude détaillée du projet de loi nº 17, *Loi modifiant la Loi sur le Barreau, la Loi sur le notariat et le Code des professions*, qui a introduit ce droit au Code, la ministre de la Justice précisait : « Nous, ici, là, ce qu'on souhaite faire, là, c'est tout simplement de permettre au Barreau d'utiliser la voie électronique pour rejoindre ses membres parce que de plus en plus de membres du Barreau sont branchés, et donc ça facilite les communications entre notre ordre professionnel et les membres, tout simplement » (extrait du *Journal des débats de la Commission des institutions* de l'Assemblée nationale du Québec, mardi 18 novembre 2014, vol. 44, nº 17), accessible à l'adresse : http://www.assnat.qc.ca/fr/travaux-parlementaires/commissions/ci-41-1/journal-debats/CI-141118.html (consulté le 23 janvier 2021).

5 Office des professions du Québec, « *Élection au conseil d'administration des ordres professionnels : aspects légaux et pratiques d'un scrutin tenu par un moyen technologique* », Québec, juillet 2017, 51 pages.

Toutefois, si le secrétaire ne possède pas les connaissances et les habiletés requises quant au moyen technologique envisagé, il devra s'adjoindre un expert afin de prendre des décisions éclairées et de pallier le manque de certaines compétences technologiques. Un expert pourra également s'avérer nécessaire pour auditer le moyen technologique ou certaines étapes du processus.

3. Les équivalences à assurer pour le vote électronique

Le document de l'Office des professions du Québec (2017) prévoit que les mesures de sécurité à mettre en place pour l'utilisation du vote au moyen d'Internet dans le cadre d'une élection au sein d'un ordre professionnel « **doivent correspondre à celles du vote par correspondance sans qu'il ne soit nécessaire de les surpasser**[6] ». Ainsi, les exigences afférentes au vote électronique doivent être proportionnées par rapport aux exigences que l'on retrouve au *Code des professions* quant au vote sur support papier.

À cet égard, le **principe de l'équivalence fonctionnelle**[7] constitue le fil conducteur qui doit guider la transposition des exigences reconnues afin d'assurer l'intégrité du vote. Les exigences afférentes au vote sur support papier prévues notamment au *Code des professions*, comportent en effet des garanties qu'il importe d'adapter au vote électronique. C'est à l'aide de ce principe que le secrétaire de l'ordre devra se guider, afin d'identifier les mesures à mettre en place en vue d'une élection par un moyen technologique.

De plus, il faut s'assurer que les modalités envisagées pour la tenue de l'élection **ne viennent pas restreindre ou rendre inopérant le droit expressément reconnu par le législateur**[8] de tenir une élection par moyen technologique et de permettre aux professionnels d'élire le président et les autres administrateurs selon un processus favorisant l'expression de leur vote. Un tel droit doit aussi s'exercer en harmonie avec la spécificité des ordres et en tenant compte des moyens à leur disposition.

Dans le cadre de l'état d'urgence sanitaire, plusieurs ordres auraient souhaité tenir l'élection du président et des autres administrateurs par un moyen technologique. Toutefois, faute de modalités prévues par règlement, ils en sont incapables[9]. Ainsi, plusieurs ordres ne peuvent pas actuellement procéder à l'élection du président et des autres administrateurs par un moyen technologique[10].

---

6 *Ibidem*, p. 5. Le document fait aussi état d'un tableau des articles pertinents du *Code* « auxquels ont été ajoutés des commentaires et suggestions pour permettre leur adaptation à un vote électronique » (voir l'annexe I).

7 Celle-ci peut être définie comme étant une « Approche selon laquelle des exigences que l'on retrouve dans certaines lois telles que l'écrit, la signature ou l'original, puissent être appliquées à un support technologique dans la mesure où ces exigences remplissent les mêmes fonctions que l'équivalent papier », une définition tirée de l'ouvrage intitulé « Afin d'y voir clair - Guide relatif à la gestion des documents électroniques » produit par M[e] Vincent Gautrais et publié en novembre 2005 par la Fondation du Barreau du Québec, accessible à l'adresse : https://www.fondationdubarreau.qc.ca/wp-content/uploads/2016/10/Guidetech_allege_FR.pdf (consulté le 23 janvier 2021). Comme indiqué sur le site Internet LCCJTI.ca (à l'adresse suivante : https://www.lccjti.ca/definitions/equivalence-fonctionnelle/), l'équivalence fonctionnelle est en fait « une méthode interprétative qui permet de combler les silences et flous inhérents de la Loi ».

8 À cet effet, voir notamment le mémoire de Philippe Mercorio intitulé « Le vote par Internet à distance est-il conforme aux exigences du droit électoral québécois et canadien ? », présenté en janvier 2007 à la Faculté des études supérieures de l'Université de Montréal, accessible à l'adresse : https://papyrus.bib.umontreal.ca/jspui/handle/1866/2456 (consulté le 23 janvier 2021). À la page 146, l'auteur suggère de trouver « le moyen de faire les adaptations nécessaires au niveau des textes de lois afin d'empêcher qu'un changement de contexte technologique n'enlève un droit consenti par le législateur ».

9 Mentionnons que l'Office des professions transmettait le 29 mai 2020 une note aux ordres précisant que « L'Arrêté 2020-029 de la ministre de la Santé et des Services sociaux » prévoit des dispositions particulières qui peuvent trouver application dans le cas où le président de l'ordre est élu au suffrage des administrateurs, mais que « ces dispositions ne peuvent s'appliquer pour une élection au suffrage universel des membres de l'ordre » et que « ces dispositions ne peuvent suppléer l'absence de règles concernant le vote par un moyen technologique dans le règlement sur l'organisation ».

10 Or, considérant la capacité de traitement réglementaire actuelle du système professionnel, on peut envisager que ces ordres ne pourront pas bénéficier de telles modalités au cours de l'état d'urgence sanitaire.

4. La responsabilité des ordres

Le document de l'Office des professions du Québec (2017) prévoit que « **l'ordre demeure le seul responsable de s'assurer du respect des lois et des règlements applicables en la matière**[11] ». Le *Code des professions* prévoit par ailleurs que le conseil d'administration de l'ordre est chargé de la surveillance générale de l'ordre ainsi que de l'encadrement et de la supervision de la conduite des affaires de ce dernier. Il prévoit qu'il est également chargé de veiller à l'application des dispositions du *Code*, de la loi ou des lettres patentes constituant l'ordre et des règlements adoptés conformément au code ou à ladite loi.

Toutefois, ce même document prévoit **plusieurs éléments d'ordre opérationnel qui « devront être soumis » à l'Office pour approbation** : « déterminer un budget, choisir un prestataire de services selon un mandat précis, prévoir le contenu du contrat de services à signer, choisir les acteurs qui interviendront dans le processus puis élaborer les modifications nécessaires à son règlement sur les élections ».

Force est de constater que **les règlements qui ont été approuvés par l'Office des professions prévoient également de telles considérations d'ordre opérationnel** qui vont au-delà des modalités permettant la tenue d'une élection par moyen technologique. Une analyse de ces règlements révèle de plus que les normes que l'on y retrouve présentent de grandes similitudes et qu'au fil du temps trois types de rédaction semblent avoir été approuvés à quelques différences près (voir l'annexe IV).

Or, il est important que **les normes fixées par règlement soient empreintes d'une certaine pérennité et d'un caractère de permanence**. Les considérations d'ordre opérationnel sont évolutives par essence et habituellement liées au moyen technologique envisagé.

Les obligations législatives et réglementaires imposées aux ordres pour la tenue d'une élection par un moyen technologique pourraient prévoir des objectifs précis, mais elles devraient laisser aux ordres une certaine liberté de choix quant aux moyens à prendre en vue de les atteindre. D'autant que les ordres sont tenus de respecter les exigences prévues au *Code des professions* et à la *Loi concernant le cadre juridique des technologies de l'information* (voir l'annexe I).

5. Favoriser l'exercice du vote

L'élection est une composante fondamentale de ce qui donne vie aux valeurs et aux principes démocratiques[12]. Les procédures afférentes à l'élection doivent favoriser et permettre l'exercice du droit de vote :

> « Il est important de ne pas oublier que le but et l'objectif des procédures d'élection, selon une jurisprudence qui est devenue constante, est de favoriser et de permettre l'exercice du vote et la manifestation du choix démocratique de l'électeur. Le droit de vote est même maintenant un droit protégé par les chartes[13]. »
>
> (notre soulignement)

11 Office des professions du Québec, *op. cit.*, p. 2.

12 À cet effet, voir notamment le rapport de la Global Commission on Elections, Democracy & Security de la Kofi Annan Foundation, *Deepening Democracy : a Strategy for Improving the Integrity of Elections Worldwide*, septembre 2012, p. 13, accessible à l'adresse : https://www.idea.int/sites/default/files/publications/deepening-democracy.pdf (consulté le 23 janvier 2021).

13 Extrait du jugement *Lambert c. Gagliardi*, 2008 QCCS 5168, 30 octobre 2008, par. 29.

Dans un tel esprit, l'introduction du vote électronique peut contribuer à accroître la participation à l'élection en améliorant l'accessibilité au processus[14]. Toutefois, **tout processus électoral peut faire l'objet d'irrégularités pouvant entacher le vote et, en définitive, la confiance envers le processus**.

Le groupe de travail a rapidement conclu que même si le processus électoral d'un ordre respecte l'ensemble des modalités fixées par règlement approuvé par l'Office, voire l'ensemble des considérations d'ordre opérationnel énoncées au document de 2017 de l'organisme, ce processus, comme tout autre processus électoral, peut faire l'objet de telles irrégularités.

Par ailleurs, le vote électronique exige la plupart du temps à recourir à la technologie d'une entreprise externe. Comme le souligne avec justesse Jérôme Couture, chercheur au Centre d'analyse des politiques publiques de l'Université Laval, il s'agit d'une « forme de privatisation du processus électoral qui n'est pas sans risque[15] ».

Une étude récente d'Élections Québec[16] fait état d'autres enjeux liés au vote par Internet, qu'il importe de considérer :

> « [...] le vote par Internet soulève certains enjeux [...]. D'abord, le fait que le vote s'exerce à distance pose un risque pour la liberté et pour le secret du vote. Cela rend aussi la vérification de l'identité des électrices et des électeurs plus difficile. De plus, la dématérialisation et la centralisation des votes représentent des enjeux pour l'intégrité du processus électoral et des résultats. Le vote par Internet entraîne également une perte de transparence : les autres modalités de vote peuvent être observées et comprises plus facilement[17]. »

Ainsi, bien que le *Code des professions* (art. 62.1 *in fine*) énonce que le moyen technologique doit assurer la sécurité, le secret et l'intégrité du vote, le groupe de travail est d'avis, à l'instar des travaux réalisés en 2011 par le CIQ, que **le secrétaire doit s'assurer que les principes légitimant un résultat électoral soient respectés, et ce, à toutes les étapes du scrutin**.

Or, comme l'explique Philippe Mercorio dans son mémoire de 2007[18], les principes légitimant un résultat électoral[19] varient selon les sources documentaires que l'on consulte. Malgré tout, un patrimoine commun peut être toutefois constitué[20].

---

14 Dans le rapport *Établir un cadre juridique pour le vote électronique au Canada* produit pour Élections Canada, les auteurs, Brian Schwartz, Ph.D, professeur à la Faculté de droit de l'Université du Manitoba, et Dan Grice, J.D, Université du Manitoba précisent à la page 12 « [...] que l'incitation à adopter le vote par Internet ou d'autres technologies électorales (appelés collectivement vote électronique) cadre parfaitement avec les tentatives d'accroître l'accessibilité des élections ». Mentionnons également que dans l'étude d'Élections Québec de juin 2020 intitulée « Vote par Internet – Étude en contexte québécois », on précise avoir réalisé un sondage téléphonique afin d'évaluer notamment l'acceptabilité sociale du vote par Internet au sein de la population québécoise en général. On souligne notamment que « Les répondantes et répondants favorables au vote par Internet ont majoritairement justifié leur position à l'aide de raisons liées à l'accessibilité[441] : réduction des déplacements, facilité du vote et réduction des files d'attente. ».
SCHWARTZ, Brian, et GRINCE, Dan, *Établir un cadre juridique pour le vote électronique au Canada*, Élections Canada, septembre 2013, 92 pages, accessible à l'adresse : https://www.elections.ca/content.aspx?section=res&dir=rec/tech/elfec&document=index&lang=f. (consulté le 23 janvier 2021).
Élections Québec, « Vote par Internet – Étude en contexte québécois », Québec, Directeur général des élections du Québec, juin 2020, 225 pages, p. 126, accessible à l'adresse : https://www.electionsquebec.qc.ca/francais/chercheurs/vote-par-internet.php (consulté le 23 janvier 2021).

15 JOURNET, Paul, « Le vote contagieux », sur le site de *La Presse*, 11 mai 2020, accessible à l'adresse : https://www.lapresse.ca/debats/editoriaux/2020-05-11/le-vote-contagieux (consulté le 23 janvier 2021).

16 Élections Québec, *op. cit.*, p. 201.

17 *Ibidem.*

18 Mercorio, *op. cit.*, p. 4.

19 Rappelons que c'est sur la base de ces principes que le CIQ avait recommandé en 2011 à l'Office des professions du Québec de permettre à un ordre professionnel d'utiliser le vote électronique, sur une base facultative, afin d'élire les membres de son conseil d'administration. Le CIQ avait alors précisé que ces principes devaient être respectés, et ce, à toutes les étapes du scrutin.

20 Notamment à l'aide des principes que l'on retrouve au *Code de bonne conduite en matière électorale* de la Commission de Venise, soit le suffrage universel, égal, libre, secret et périodique. Commission européenne pour la démocratie par le droit (Commission de Venise), *Code de bonne conduite en matière électorale : Lignes directrices et rapport explicatif*, Venise, 51e et 52e sessions, 5-6 juillet 2002 et 18-19 octobre 2002, Strasbourg, Conseil de l'Europe, 31 pages, CDL-AD(2002) 23rev2-cor, accessible à l'adresse : https://www.venice.coe.int/webforms/documents/default.aspx?pdf=CDL-AD(2002)023rev2-cor-f&lang=fr (consulté le 23 janvier 2021).

Le groupe de travail a ainsi identifié sept principes dont le secrétaire de l'ordre devra tenir compte à toutes les étapes du scrutin. Trois de ces principes sont déjà prévus au *Code des professions* : la **sécurité**, le **secret** et l'**intégrité** du vote. Les quatre autres ont déjà été transmis à l'Office des professions par le Conseil dans le cadre des travaux réalisés en 2011, soit le vote **universel**, **égal** et **libre** et la **transparence**. Afin d'aider les ordres à cet égard, le groupe de travail a explicité chacun de ces principes à l'annexe I.

À la lumière du principe de l'équivalence fonctionnelle, du mémoire de Philippe Mercorio (2007)[21] et des normes et standards généralement reconnus (voir l'annexe III), le Groupe de travail sur le vote électronique du CIQ a identifié **sept étapes clés** du processus électoral :

1. L'organisation de l'élection
2. L'inscription des électeurs
3. La transmission des bulletins de vote
4. Le vote
5. La clôture du vote
6. Le dépouillement du vote
7. La destruction de l'information

Le groupe de travail décrit brièvement chacune d'elles à l'annexe II qui fait également état de certaines pistes de réflexion pouvant guider les parties prenantes.

21 Mercorio, *op. cit.*, p. 4.

Conclusion

C'est à l'égard des principes fondamentaux légitimant un résultat électoral (annexe I), des principales étapes du scrutin (annexe II) et des normes et standards généralement reconnus (annexe III) que l'ensemble des parties prenantes devraient tourner leur attention.

Les exigences afférentes au vote sur support papier, que l'on retrouve notamment au *Code des professions*, comportent des garanties qu'il importe d'adapter au vote électronique. Le principe de l'équivalence fonctionnelle est le fil conducteur qui doit guider la transposition de ces exigences.

Tous les éléments afférents au processus électoral doivent tenir compte des principes fondamentaux légitimant un résultat électoral. Dès l'organisation de l'élection, pierre d'assise du processus, le secrétaire de l'ordre doit ainsi se poser des questions et prendre des décisions, notamment quant au choix de s'adjoindre un expert pour pallier le manque de certaines compétences technologiques ou encore pour auditer le moyen technologique ou certaines étapes du processus. Il est recommandé qu'une analyse de risques soit réalisée afin d'identifier les mesures à mettre en place. Il sera également nécessaire de réaliser de telles analyses et des validations en ce qui concerne la sécurité du moyen technologique retenu, et ce, tout au long du processus.

Quant au choix du moyen technologique, celui-ci devrait idéalement faire l'objet d'une certification reconnue. Par ailleurs, tout système électoral devrait comprendre un mécanisme d'audit afin d'assurer son intégrité et la confiance des électeurs. Ce mécanisme peut prendre différentes formes, tel que précisé à l'annexe II[22]. Toutefois, avant le début de l'élection, le secrétaire devrait au minimum s'assurer de l'authenticité, de la fiabilité et du bon fonctionnement du système de vote électronique, en faisant appel à un expert s'il ne détient pas les compétences technologiques requises.

Il est aussi primordial que le secrétaire s'assure que le système puisse fournir des preuves permettant d'établir notamment que le vote est authentique, qu'il a correctement été inclus dans les résultats de l'élection et que seuls les votes des membres en règle ont été pris en compte. Le secrétaire devra également s'assurer de la conservation des documents et des données relatives au vote pendant un délai raisonnable tenant compte d'une contestation possible de l'élection. Il devra ensuite prendre des mesures en vue d'assurer la destruction de façon sécuritaire de l'information et des documents.

Le rôle de l'expert doit s'inscrire en soutien des tâches incombant au secrétaire de l'ordre, puisque ce dernier demeure l'ultime responsable du processus. Par ailleurs, le conseil d'administration, chargé de la surveillance générale de l'ordre, devra veiller à ce que le secrétaire mette en place les mesures requises en vue de mitiger les risques identifiés, tel que le fait de s'adjoindre un expert lorsque l'on ne possède pas les connaissances et les habiletés nécessaires quant au moyen technologique envisagé. Au terme du processus, il pourrait être pertinent que le secrétaire fasse une reddition de compte au conseil d'administration et aux membres de l'ordre quant au déroulement du scrutin.

On optera pour le choix d'un expert indépendant lorsqu'il y a un risque quant à l'impartialité ou à l'intégrité des décisions ou quant à la perception que l'on pourrait en avoir. Un tel choix s'avérera également impératif en cas de contestation de l'élection.

Au terme de ses travaux, le groupe de travail formule la recommandation suivante :

22 Le chapitre 3 de l'étude d'Élections Québec (*op. cit.*, p. 3) l'illustre également. On y examine des expériences canadiennes et internationales de vote par Internet.

Recommandation

Revoir, alléger et recentrer les obligations législatives et réglementaires imposées aux ordres pour la tenue d'une élection du président et des autres administrateurs par un moyen technologique, dans la perspective de permettre à tous les ordres de tenir une telle élection, et ce, dans le respect de l'ensemble des principes légitimant un résultat électoral.

Les normes à envisager devraient être empreintes d'une certaine pérennité, d'un caractère de permanence et être axées sur le respect de ces principes. Bien que lesdites normes pourraient prévoir des objectifs précis, elles devraient laisser aux ordres une certaine liberté de choix quant aux moyens à prendre en vue de les atteindre. Elles devraient aussi être exemptes de considérations d'ordre opérationnel, celles-ci étant évolutives par essence et habituellement liées à un moyen envisagé.

Annexe I : Les principes fondamentaux légitimant un résultat électoral

Comme l'explique Philippe Mercorio[23], les principes susceptibles de garantir la légitimité d'un résultat électoral[24] varient selon les sources documentaires que l'on consulte, mais il y a des principes constants[25].

On peut en effet identifier sept principes énonçant les impératifs devant présider au déroulement du processus électoral. Il s'agit des trois principes prévus au *Code des professions* (la **sécurité**, le **secret** et l'**intégrité** du vote), auquel il convient d'ajouter le principe du vote **universel**, **égal** et **libre** et le principe de **transparence**.

La présente annexe explicite comment devrait s'appliquer chacun de ces principes.

1. La sécurité du vote

Il s'agit du premier principe prévu au *Code des professions* (art. 62.1 *in fine*) pour l'élection par moyen technologique. On peut définir celui-ci comme étant la mise en place de mesures « pour protéger l'intégrité du processus[26] ».

Par ailleurs, dans l'étude *Établir un cadre juridique pour le vote électronique au Canada*, Schwartz et Grince (2013) précisent : « Pour que la mise en œuvre du vote électronique réussisse, on doit définir avec précision les rôles et les responsabilités pour s'assurer que le système est sécuritaire et pour convaincre le public que toute négligence ou tout méfait commis au niveau de l'organisme électoral ne peut pas nuire à l'exactitude des votes ou à l'anonymat des électeurs[27] ».

En outre, l'Office des professions (2017) précise que, « [lorsqu'il] est question de voter au moyen d'Internet, la sécurité de l'information constitue la pierre angulaire de tout système, puisque c'est elle qui permettra d'assurer le secret, l'intégrité et la disponibilité de l'information[28] ».

L'Office y précise également que des mesures appropriées doivent être mises en place, notamment pour :

> « [...] empêcher un accès non autorisé au système de votation, ou encore le contournement d'une mesure de contrôle (par exemple, une tentative de voter plus d'une fois), et pour éviter une attaque en déni de services qui rendrait le système non fonctionnel pendant une certaine période » et qu'un « processus doit également être prévu pour la remise en fonction rapide du système s'il cesse de fonctionner pour quelque raison que ce soit[29]. »

23 Mercorio, *op. cit.*, p. 4.

24 Rappelons que c'est sur la base de ces principes que le CIQ avait recommandé en 2011 à l'Office des professions du Québec de permettre à un ordre professionnel d'utiliser le vote électronique, sur une base facultative, afin d'élire les membres de son conseil d'administration. Le CIQ avait alors précisé que ces principes devaient être respectés, et ce, à toutes les étapes du scrutin.

25 Notamment à l'aide des principes que l'on retrouve au *Code de bonne conduite en matière électorale* de la Commission de Venise, soit le suffrage universel, égal, libre, secret et périodique.

26 KPMG/Sussex Circle, *La technologie et le processus de vote,* Élections Canada, 1998, p. 15.

27 Schwartz et Grince, *op. cit.*, p. 56.

28 Office des professions du Québec, *op. cit.*, p. 6.

29 *Ibidem.*

Enfin, quant à la conception et à la mise en place du système de votation, le document énonce notamment que les « prescriptions de l'article 26 de la LCCJTI [*Loi concernant le cadre juridique des technologies de l'information*, LRQ, c-1.1] doivent être scrupuleusement respectées[30] ». Cet article prévoit notamment que :

> « Quiconque confie un document technologique à un prestataire de services pour qu'il en assure la garde est, au préalable, tenu d'informer le prestataire quant à la protection que requiert le document en ce qui a trait à la confidentialité de l'information et quant aux personnes qui sont habilitées à en prendre connaissance[31]. »

2. Le secret du vote

Second principe prévu au *Code des professions* (art. 62.1 *in fine*) pour l'élection par moyen technologique, le secret du vote est également prévu au *Code de bonne conduite en matière électorale* de la Commission de Venise[32]. Il signifie notamment que le suffrage doit être exercé individuellement[33].

Dans le document *Élection au conseil d'administration des ordres professionnels : aspects légaux et pratiques d'un scrutin tenu par un moyen technologique,* l'Office des professions du Québec précise que le secret du vote « constitue une valeur fondamentale de notre système démocratique[34] ».

Le *Code des professions* prévoit depuis 1973 un système visant à préserver le secret du vote par la poste. Ainsi, au moins quinze jours avant la date fixée pour la clôture du scrutin, le secrétaire de l'ordre transmet à chacun des membres deux types d'enveloppes : l'une qui est adressée au secrétaire et l'autre qui doit être insérée dans la première et qui vise à contenir le bulletin de vote, sans permettre d'identifier le membre.

Comme le précise l'Office des professions du Québec (2017), ce système :

> « [...] permet à un membre de transmettre son choix au secrétaire de l'ordre dans une enveloppe anonyme, non identifiée. De la même manière, le vote au moyen d'Internet doit pouvoir être fait en toute confidentialité, c'est-à-dire sans qu'il ne soit jamais possible de lier une personne à l'expression de son vote. [...] Des mesures de sécurité adéquates devront être mises en place afin de protéger la transmission de l'information[35]. »

Quant à la confidentialité, mentionnons par ailleurs que l'article 34 de la *Loi concernant le cadre juridique des technologies de l'information* (LCCJTI) prévoit que : « [lorsque] la loi déclare confidentiels des renseignements que comporte un document, leur confidentialité doit être protégée par un moyen approprié au mode de transmission, y compris sur des réseaux de communication ».

30 *Ibidem.*

31 *Loi concernant le cadre juridique des technologies de l'information*, LRQ (2001), c. C – 1.1., art. 26, accessible à l'adresse : http ://www.legisquebec.gouv.qc.ca/fr/showdoc/cs/C-1.1 (consulté le 24 janvier 2021).

32 Conseil de l'Europe, Commission de Venise, *op. cit.*

33 À la page 26 de son mémoire, Mercorio (*op. cit.*, p. 26) précise : « Le vote doit aussi être secret, ce qui implique qu'il doit être exercé individuellement ».

34 Office des professions du Québec, *op. cit.*, p. 7.

35 *Ibidem.*

3. L'intégrité du vote

Il s'agit du troisième principe prévu au *Code des professions* (art. 62.1 *in fine*) pour l'élection par moyen technologique. Le jugement *Lambert* c. *Gagliardi* rappelle l'importance de ce principe en ces termes : « La protection de l'intégrité du scrutin et de l'intégrité du système demeure une valeur primordiale[36] ».

L'Office des professions du Québec (2017) énonce ce qui suit, citant notamment l'article 5 de la LCCJTI :

> « L'intégrité du vote requiert que chaque vote soit comptabilisé tel qu'exprimé par le membre habile à voter, de sorte que les candidats élus lors de l'élection le soient légitimement. [...] Un bulletin de vote sur support technologique est juridiquement équivalent à un bulletin sur support papier, mais uniquement dans la mesure où l'intégrité du document est assurée[37]. »

Ce même document de l'Office (2017) précise de plus qu'il faut s'assurer de l'intégrité du bulletin de vote et du système de votation, spécifiant notamment « l'intégrité de la liste des candidats et de la liste des membres habiles à voter au moment où ils exercent leur droit de vote et, surtout, l'intégrité des résultats du scrutin[38] ».

À l'égard de l'intégrité, mentionnons que les articles 6, 7 et 19 de la LCCJTI prévoient respectivement que :

> « 6. L'intégrité du document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue.
>
> L'intégrité du document doit être maintenue au cours de son cycle de vie, soit depuis sa création, en passant par son transfert, sa consultation et sa transmission, jusqu'à sa conservation, y compris son archivage ou sa destruction.
>
> Dans l'appréciation de l'intégrité, il est tenu compte, notamment des mesures de sécurité prises pour protéger le document au cours de son cycle de vie.
>
> 7. Il n'y a pas lieu de prouver que le support du document ou que les procédés, systèmes ou technologies utilisés pour communiquer au moyen d'un document permettent d'assurer son intégrité, à moins que celui qui conteste l'admission du document n'établisse, par prépondérance de preuve, qu'il y a eu atteinte à l'intégrité du document.
>
> [...]
>
> 19. Toute personne doit, pendant la période où elle est tenue de conserver un document, assurer le maintien de son intégrité et voir à la disponibilité du matériel qui permet de le rendre accessible et intelligible et de l'utiliser aux fins auxquelles il est destiné. »

36 *Lambert* c. *Gagliardi*, *op. cit.*, par. 31.

37 Office des professions du Québec, *op. cit.*, p. 7 et suivantes.

38 *Ibidem*, p. 8.

Enfin, le document de l'Office des professions du Québec (2017) conclut que « le fait qu'un document n'ait pas été altéré doit donc être vérifiable a posteriori », en précisant :

> « Il existe plusieurs façons de démontrer cette intégrité : documenter le fonctionnement du système, y compris l'ensemble des mesures de sécurité déployées pour le protéger; conserver des traces des actions dans le système (registres des accès, journaux de transactions, etc.); utiliser des procédés physiques ou technologiques permettant de sceller l'information (ex. : inscription sur des supports non réinscriptibles, utilisation de procédés cryptographiques ou utilisation, lors du dépouillement, d'une enveloppe papier scellée portant la signature du secrétaire); faire appel à des experts indépendants qui pourront vérifier le système avant le scrutin et surveiller le déroulement du vote et du dépouillement. Le témoignage de ces experts pourrait être crucial en cas de contestation pour démontrer l'intégrité des résultats du vote[39]. »

Le groupe de travail est toutefois d'avis, se basant sur la notion de l'équivalence fonctionnelle, que les exigences afférentes à l'intégrité du vote électronique doivent être proportionnées par rapport aux exigences que l'on retrouve au *Code des professions* quant au vote sur support papier.

4. Le vote universel

Tiré du *Code de bonne conduite en matière électorale* de la Commission de Venise[40], ce principe est composé du droit à l'information, du droit de vote et du droit de se porter candidat.

Précisons que le droit de voter est consacré par la *Charte des droits et libertés de la personne*. L'article 22 de la Charte prévoit en effet que : « Toute personne légalement habilitée et qualifiée a droit de se porter candidat lors d'une élection et a droit d'y voter[41] ». Cette disposition est applicable à une élection d'un ordre professionnel[42].

Ainsi, le suffrage est considéré universel lorsqu'il permet à l'ensemble des membres de l'ordre professionnel habiles à voter d'exercer leur droit de vote.

5. Le vote égal

Le suffrage doit viser la pleine et entière participation de l'électeur au mode de votation[43]. Il s'agit également d'un principe tiré du *Code de bonne conduite en matière électorale* de la Commission de Venise[44].

À cet égard, le Groupe de travail sur le vote électronique du CIQ est d'avis que le suffrage doit permettre à toute personne de voter sans discrimination, et ce, malgré les obstacles liés aux technologies.

---

39 *Ibidem,* p. 8 et 9.

40 Conseil de l'Europe, Commission de Venise, *op. cit.*

41 *Charte des droits et libertés de la personne*, RLRQ, c. C-12, art 22, accessible à l'adresse : http://legisquebec.gouv.qc.ca/fr/ShowDoc/cs/C-12 (consulté le 24 janvier 2021).

42 Dans *Lambert* c. *Gagliardi* (*op. cit.*, par. 30) on précise : « [...] cette disposition s'applique lors d'une élection. L'application n'en est donc pas restreinte aux élections provinciales. Très certainement, cette disposition s'applique aux élections municipales et scolaires et, également, aux élections au bureau des corporations professionnelles ».

43 À cet effet, Mercorio (*op. cit.*, p. 54) précise : « Il semble donc que le vote par Internet à distance rencontre le principe d'égalité du suffrage, toute inégalité d'un électeur liée à une caractéristique immuable, tel un handicap physique, obligerait le législateur à prévoir des mesures permettant la pleine et entière participation de cet électeur à ce mode de vote ».

44 Conseil de l'Europe, Commission de Venise, *op. cit.*, p. 6.

Il faut par ailleurs considérer le principe de liberté de choix quant au support ou à la technologie qu'une personne entend utiliser. Ce principe est introduit par l'article 2 de la LCCJTI et est évoqué à l'article 29 de cette loi[45] :

> « 29. Nul ne peut exiger de quelqu'un qu'il se procure un support ou une technologie spécifique pour transmettre ou recevoir un document, à moins que cela ne soit expressément prévu par la loi ou par une convention. »

Enfin, il faut aussi s'assurer que chacun ne puisse voter qu'une seule fois.

6. Le vote libre

Le vote ne doit être admis que s'il est « sûr et fiable[46] ». Comme mentionné précédemment, l'élection doit favoriser et permettre la manifestation du choix démocratique de l'électeur[47].

7. La transparence du vote

Comme précisé par Mercorio (2007), étant donné que le vote électronique est porteur d'un certain nombre de risques sur le plan de la sécurité, il importe « d'obtenir l'adhésion de l'électorat [au] projet[48]. À cette fin, l'auteur propose de mettre en place une « chaîne transparente de contrôles [...] du début à la fin du processus électoral, afin de détecter et circonscrire, dans les limites jugées acceptables, les risques identifiés[49] ».

Par ailleurs, Schwartz et Grince (2013) précisent que la transparence du système technologique est l'un des principaux enjeux auquel il faut porter attention « pour que le système électoral inspire confiance au public[50] » et que celle-ci est aussi importante pour assurer l'intégrité des mesures sous-jacentes. Les auteurs estiment notamment à cet égard qu'un système de vote électronique doit impérativement comporter des dispositions assurant que « chaque aspect du système retenu [puisse] être examiné et surveillé en vue de détecter soit des erreurs, soit des manipulations[51] ». Le groupe de travail est d'avis que le système doit non seulement pouvoir être examiné et surveillé à cette fin, mais qu'on doive également prévoir des dispositifs permettant de vérifier, en temps réel, qui a accédé à celui-ci au cours du scrutin.

45 Pour en savoir plus, on peut consulter le site Internet LCCJTI.ca à l'adresse suivante : https://www.lccjti.ca/articles/article-2/

46 Conseil de l'Europe, Commission de Venise, *op. cit.*, p. 8.

47 *Lambert* c. *Gagliardi*, *op. cit.*, par. 29.

48 Mercorio, *op. cit.*, p. 75.

49 *Ibidem.*

50 Schwartz et Grince, *op. cit.*, p. 48.

51 *Ibidem*, p. 49.

Annexe II : Principales étapes du scrutin

À la lumière du principe de l'équivalence fonctionnelle, du mémoire de Philippe Mercorio (2007)[52] et des normes et standards généralement reconnus (voir l'annexe III), le Groupe de travail sur le vote électronique du CIQ a identifié **sept étapes clés** du processus électoral :

1. L'organisation de l'élection
2. L'inscription des électeurs
3. La transmission des bulletins de vote
4. Le vote
5. La clôture du vote
6. Le dépouillement du vote
7. La destruction de l'information

Le groupe de travail est d'avis que le secrétaire doit s'assurer que les principes légitimant un résultat électoral soient respectés, et ce, à chacune de ces étapes.

La présente annexe décrit brièvement chacune de ces étapes.

1. L'organisation de l'élection

L'organisation de l'élection est la pierre d'assise du processus. C'est à cette étape que l'on doit se poser des questions et prendre des décisions quant aux éléments suivants :

- Le choix du moyen technologique, les risques afférents et, s'il y a lieu, la propriété de l'équipement[53];
- Le choix de s'adjoindre un expert pour pallier le manque de certaines compétences technologiques ou pour auditer le moyen technologique ou certaines étapes du processus, aux critères requis à cet égard[54] et au mandat envisagé;
- La conservation de l'information et la protection des données[55];
- La transposition sur écran des bulletins de vote et, s'il y a lieu, à la sécurité du site Internet qui sera utilisé[56];
- L'assistance aux personnes présentant des limites physiques ou intellectuelles;
- La préservation du secret du vote;
- L'évaluation des événements imprévisibles pouvant avoir un impact sur le vote et aux mécanismes à mettre en place à cet égard;
- La validation des résultats;
- Le mécanisme d'audit;
- Les tâches confiées aux scrutateurs ou aux témoins ainsi que la désignation et la formation de ces derniers;
- L'examen du matériel nécessaire au vote et à son administration.

52 Mercorio, *op. cit.*, p. 4.

53 Par exemple, détenir les licences nécessaires pour l'utilisation de l'équipement.

54 Par exemple, posséder l'expérience ou détenir une formation pertinente ou des certifications reconnues, telles : Information Security Auditor (CISA) de ISACA ou ISO/CEI 27001 Lead Auditor de PECB.

55 Rappelons que l'article 34 de la LCCJTI (*op.cit.*) prévoit que : « Lorsque la loi déclare confidentiels des renseignements que comporte un document, leur confidentialité doit être protégée par un moyen approprié au mode de transmission, y compris sur des réseaux de communication ».

56 Par exemple, par l'ajout d'un certificat de sécurité attestant de l'authenticité du site Web.

Mentionnons quant au choix du moyen technologique qu'idéalement, celui-ci devrait faire l'objet d'une certification reconnue telle que ISO/IEC27001 :2013, ISO/IEC27018 :2019 ou SOC 2 Type 2. La certification devrait être valide et s'appliquer à l'ensemble du système de vote électronique et à tous les endroits où se retrouveront les systèmes informatiques et l'information ayant trait au moyen technologique utilisé. Dans le cas contraire, une analyse de risques devrait être réalisée par une méthode reconnue, par exemple ISO/IEC27005 :2018, afin d'identifier les mesures de sécurité à mettre en place afin d'en arriver à un risque de niveau acceptable.

Précisons également qu'il sera toujours nécessaire de réaliser des analyses de risques et des validations en ce qui concerne la sécurité du moyen technologique retenu, notamment quant au volet des processus d'affaires et des configurations du système, et ce, indépendamment de la certification dont ce dernier fait l'objet.

Quant aux mécanismes à mettre en place à l'égard de l'évaluation des événements imprévisibles pouvant avoir un impact sur le vote, pensons notamment à des mécanismes permettant d'informer promptement le secrétaire de l'ordre en cas d'incidents susceptibles de menacer l'intégrité du système ou encore à des mécanismes de sauvegarde et de récupération de données du système en cas de plantage informatique, d'erreur humaine ou d'attaque ayant pour conséquence d'altérer ou de supprimer des données (ex. : rançongiciel). L'ordre pourrait de plus souhaiter mettre en place des mécanismes administratifs dans l'éventualité où un tel événement aurait des impacts sur une élection en cours.

Pour Mercorio (2007), « [il] semble manifeste que tout système électoral informatisé devra comprendre un mécanisme d'audit afin d'assurer son intégrité et la confiance des électeurs[57] ».

Dans l'étude d'Élections Québec de juin 2020, on précise :

> « De plus, l'encadrement devrait prévoir des obligations relatives à la certification de la plateforme par une autorité compétente, de même qu'un audit externe, pour attester du bon déroulement du processus et de la fiabilité de la plateforme[58]. »
>
> (notre soulignement)

Quant à la forme et à l'étendue de ce mécanisme d'audit, à l'instar de Mercorio (2007), le groupe de travail est d'avis que la LCCJTI[59] nous en donne un indice :

> « La *Loi concernant le cadre juridique des technologies de l'information* nous donne un indice à ce niveau en déclarant qu'un audit doit comporter : « l'examen et l'évaluation des méthodes d'accès, d'entretien ou de sauvegarde du support, des mesures de sécurité physiques, logiques ou opérationnelles, des registres de sécurité et des correctifs apportés en cas de défaillance d'un élément pouvant affecter l'intégrité d'un document[60]. »
>
> (notre soulignement)

57 Mercorio, *op. cit.*, p. 155.

58 Élections Québec, *op. cit.*, p. 164.

59 LJCCTI, *op. cit.*, art. 64 par. 5.

60 Mercorio, *op. cit.*, p. 155.

Traitant de la Recommandation Rec(2004)11 du Comité des Ministres du Conseil de l'Europe portant sur le vote électronique[61], Mercorio (2007) précise que « ce mécanisme d'audit se doit d'être complet, en ce qu'il couvrira toutes les phases du processus électoral et sera présent à différents niveaux du système de vote : de l'enregistrement, au contrôle, à la vérification[62] ».

Ajoutons que la *Recommandation CM/Rec (2017)5* prévoit :

> « Le système de vote électronique pourra faire l'objet d'un audit. Le système d'audit sera ouvert et complet, et signalera effectivement les menaces et les problèmes potentiels[63] ».

Dans l'annexe II de cette recommandation, le terme (ou contrôle) est ainsi défini : « évaluation indépendante, avant ou après une élection, d'une personne, organisation, système, processus, entité, projet ou produit, qui inclut des analyses quantitatives et qualitatives[64] ».

Ainsi, le mécanisme d'audit peut prendre différentes formes[65]. Toutefois, avant le début de l'élection, le secrétaire devrait au minimum s'assurer de l'authenticité, de la fiabilité et du bon fonctionnement du système de vote électronique, en faisant appel à un expert s'il ne détient pas les compétences technologiques requises.

2. L'inscription des électeurs

À cette étape, le secrétaire doit s'assurer que les données qui apparaissent au tableau de l'ordre soient « figées » au moment du déclenchement du processus électoral.

Il doit établir la liste des candidats et des membres habiles à voter, en vérifiant que l'électeur figure au tableau de l'ordre en fonction du domicile professionnel déclaré.

Une procédure stricte et des moyens cryptographiques appropriés devront être mis en place pour conserver l'intégrité des listes, et ce, tout au long de leur cycle de vie. Celles-ci ne devront être accessibles qu'aux personnes autorisées.

Un identifiant approuvé (ex. : numéro de membre et code d'identifiant numérique personnel) devra permettre de valider l'identité de l'électeur. Réciproquement, l'identifiant approuvé devra aussi permettre au membre habileté à voter de s'identifier (identification) et de démontrer qu'il est bien la personne qu'il prétend être (authentification).

3. La transmission des bulletins de vote

Avant la période de votation, il est impératif que les électeurs reçoivent de l'information, afin d'identifier le site électoral où il sera possible de voter et de connaître le moyen pour s'y connecter (ex. : envoi d'une adresse URL en format sécurisé).

L'utilisation d'un protocole de communication sécuritaire et respectant les bonnes pratiques de l'industrie devra être en place entre l'électeur et le site Internet afin d'éviter qu'une personne ait la capacité de rediriger l'électeur vers un autre site Internet à son insu.

À cette étape, en plus des documents prévus à l'article 69 du *Code des professions*, le secrétaire transmet notamment à chacun des membres ayant droit de vote un avis d'élection contenant l'information nécessaire à l'exercice du droit de vote et une description de la procédure à suivre pour le déroulement du vote.

---

61 La *Recommandation Rec(2004)11* prévoit des normes juridiques, opérationnelles et techniques relatives au vote électronique. Elle prévoit notamment des dispositions sur l'audit dont le système de vote électronique peut faire l'objet (art. 100 et suivants). CONSEIL DE L'EUROPE, Comité des Ministres (2004), *Recommandation Rec(2004)11 du Comité des Ministres aux États membres sur les normes juridiques, opérationnelles et techniques relatives au vote électronique* (adoptée par le Comité des Ministres le 30 septembre 2004, lors de sa 898e réunion), accessible à l'adresse https://www.coe.int/t/dgap/goodgovernance/activities/key-texts/recommendations/00rec(2004)11_rec_adopted_FR.asp (consulté le 24 janvier 2021).

62 Mercorio, *op. cit.*, p. 155.

63 CONSEIL DE L'EUROPE, Comité des Ministres (2017), *Recommandation CM/Rec(2017)5 du Comité des Ministres aux États membres sur les normes relatives au vote électronique* (adoptée par le Comité des Ministres le 14 juin 2017, lors de la 1289e réunion des Délégués des Ministres), par. 39, accessible à l'adresse : https://rm.coe.int/0900001680726f6a (consulté le 24 janvier 2021).

64 *Ibidem*, p.6.

65 Le chapitre 3 de l'étude d'Élections Québec (op. cit.) l'illustre également. On y examine des expériences canadiennes et internationales de vote par Internet.

4. Le vote

Dans son mémoire, Mercorio (2007) précise :

> « Toutes les dispositions ayant traits [sic] à des manipulations physiques sur un bulletin de vote devront donc être abrogées ou modifiées, selon que la transition technologique impose un changement de forme ou de fond à l'action visée. [...] Ainsi, quand le législateur déclare que l'électeur reçoit du scrutateur un bulletin de vote, la substance de la disposition sera conservée[66]. »

À cette étape, l'électeur devra fournir une preuve suffisante de son identité (identification) et devra démontrer qu'il est bien la personne qu'il prétend être (authentification).

Le membre devra ensuite s'authentifier en échangeant une information connue uniquement de lui-même et du système de vote électronique (ex. : mot de passe, NIP, etc.). Le niveau d'authentification demandé doit être adapté à l'importance du scrutin et à l'évaluation de risque réalisée par le secrétaire de l'ordre ou la personne mandatée par ce dernier pour ce faire.

Le secrétaire devra s'assurer que le système de vote électronique permette à la personne qui exerce son droit de vote de vérifier que son intention est correctement représentée avant que le vote ne soit enregistré. Le système devra aussi permettre *à cette* personne de recevoir une confirmation à l'effet que le vote a été effectué avec succès et que toute la procédure de vote a été menée à bien. Afin de garantir le secret du vote, cette confirmation ne devra pas contenir d'information sur le choix de l'électeur.

Comme mentionné précédemment, une procédure stricte devra être mise en place, de même que des moyens cryptographiques appropriés pour conserver l'intégrité des listes, et ce, tout au long de leur cycle de vie. Celles-ci ne devront être accessibles qu'aux personnes autorisées. Toutefois, advenant le cas où une modification doive être apportée à cette liste[67], des mécanismes d'approbation et de journalisation devraient être en place pour les éléments suivants :

- Les raisons nécessitant une modification de la liste électorale,
- L'identité de la personne ayant approuvé la modification,
- L'identité de la personne ayant à effectuer la modification,
- La date et l'heure de la modification,
- L'endroit et le dispositif électronique à partir duquel la modification a été effectuée,
- La confirmation que la modification a bel et bien été effectuée avec succès,
- La confirmation du contenu de la modification effectuée.

5. La clôture du vote

Le système de vote électronique devra se mettre à jour à intervalle régulier avec une source de temps fiable (atomique)[68].

À cette étape, le secrétaire de l'ordre devra s'assurer de clore le vote manuellement ou de façon automatisée. Dans les deux cas, une source de temps fiable devra être utilisée.

66 Mercorio, *op. cit.*, pp. 126-127.

67 Par exemple, un membre qui n'aurait plus droit de vote suite à une radiation.

68 À titre indicatif, cette mise à jour se fait généralement par l'utilisation du protocole Network Time Protocol (NTP) ou du Network Time Security (NTS).

Dans le cas d'une clôture du vote manuelle, seule une personne autorisée par le secrétaire de l'ordre et détenant les droits d'accès à la plateforme de vote électronique devrait pouvoir y procéder au moment défini.

Le système de vote électronique devra permettre aux personnes ayant accédé au site et s'étant identifié correctement avant l'heure de clôture du vote de pouvoir compléter le processus de vote. Ainsi, une période de temps raisonnable pourrait être prévue afin de permettre à ces personnes d'exercer leur droit de vote avant la clôture du vote.

6. Le dépouillement du vote

Dans son mémoire, Mercorio (2007) précise :

> « Toutes les tâches mécaniques liées au dépouillement sont prises en charge par le système. [...] Même si, dans la forme, la majorité des exigences légales au dépouillement ne pourraient trouver application dans le cadre d'un système de vote par Internet à distance, le fond ne s'en trouverait pas affecté. [...] Ce qui importe est que la finalité de cette procédure soit atteinte, soit de permettre au véritable résultat du scrutin d'apparaître. [...] En résumé, il pourrait suffire de s'inspirer des expériences estonienne et helvétique pour rencontrer les exigences légales liées au dépouillement[69]. »

Ainsi, le secrétaire devra notamment s'assurer que le système :

- soit en mesure de garantir que le nombre exact de votes a été compilé, en se basant sur le nombre de membres en règle et le nombre de suffrages exprimés et que le tout ait été enregistré dans l'urne électronique (base de données sécurisée);
- n'a pas permis la divulgation du nombre de votes exprimés pour une option de vote avant la fermeture de l'urne électronique[70].

Le processus de vote électronique, en particulier durant cette étape, devrait être organisé de manière à ce que les informations relatives aux électeurs soient conservées sous scellés jusqu'au début du processus de dépouillement et qu'il ne soit pas possible de reconstituer un lien entre le vote non scellé et le membre en règle.

Le secrétaire devrait également s'assurer que le système soit en mesure de fournir des preuves permettant d'établir que :

- Chaque vote est authentique et a été correctement inclus dans les résultats respectifs de l'élection ;
- Seuls les votes des membres en règle ont été pris en compte dans les résultats finaux respectifs.

Ces preuves devront pouvoir être vérifiées par des moyens indépendants du système de vote. Plusieurs moyens sont possibles à cet égard.

Le secrétaire devra également s'assurer que tout observateur, dans la mesure permise par la loi et les règlements, puisse être autorisé à observer et à commenter le processus d'élection, y compris la compilation des résultats.

69 Mercorio, *op. cit.*, p. 137.

70 Cette information ne devrait pouvoir être divulguée qu'après la fermeture de la période de vote et selon un processus établi permettant le dépouillement du vote devant témoins. Bien qu'on retrouve le terme « urne électronique » à l'annexe I du document *Élections au conseil d'administration des ordres professionnels* de l'Office des professions du Québec (2017), on doit comprendre ici que l'on parle en fait d'une base de données sécurisée à laquelle l'accès est restreint et sous l'autorité du secrétaire.

7. La destruction de l'information

Dans l'étude d'Élections Québec de juin 2020, on précise :

> « Après l'échéance de la période officielle de contestation du résultat d'une élection, tous les votes chiffrés devraient, idéalement, être détruits de façon irréversible, incluant toutes les copies de sauvegarde, pour éviter toute possibilité de percer le secret du vote dans le futur[71]. »
>
> (nos soulignements)

Des mesures doivent être prises par le secrétaire en vue d'assurer la destruction de l'information et des documents de façon sécuritaire.

Il est impératif que l'ordre établisse par ailleurs un calendrier de conservation. Le secrétaire devra également s'assurer de la conservation des documents et des données relatives au vote pendant un délai raisonnable tenant compte d'une contestation possible de l'élection (ex. : au moins 120 jours suivant le dépouillement du vote ou, le cas échéant, jusqu'à ce que le jugement en contestation d'élection soit passé en force de chose jugée).

Il devrait aussi obtenir du fournisseur de service ou des experts indépendants, une confirmation à l'effet que l'ensemble des données a été détruit.

71 Élections Québec, *op. cit.*, p. 115.

Annexe III :
Normes et standards généralement reconnus

Le groupe de travail s'est penché sur les normes et standards généralement reconnus en ce qui concerne le vote électronique.

Le groupe s'est d'abord intéressé, à l'instar du Conseil interprofessionnel du Québec en 2011, aux normes adoptées par le Conseil de l'Europe. Il s'est penché dans un premier temps sur la *Recommandation Rec(2004)11* puis sur la *Recommandation CM/Rec(2017)5*.

À l'égard de cette dernière, on précise sur le site Internet du Conseil de l'Europe[72] :

> « Cette nouvelle Recommandation CM/Rec(2017)5, qui suit la précédente recommandation Rec(2004)11, a été développée afin de s'assurer que le vote électronique respecte les principes des élections démocratiques et elle est la seule norme internationale existante sur le vote électronique jusqu'à présent. »

Dans l'étude *Établir un cadre juridique pour le vote électronique au Canada* (2013), les auteurs précisent qu'il s'agit de la seule norme internationale régissant une forme de vote électronique *:*

> L'étude de traités internationaux, dont des documents tels que la Charte démocratique interaméricaine de l'Organisation des États Américains (OEA, 2001), fait ressortir des principes généraux, tels que la tenue régulière d'élections libres et honnêtes, fondées sur un scrutin secret et sur des principes universels. La majorité des traités n'abordent cependant que des principes généraux déjà appliqués dans notre système actuel et ne se concentrent pas sur les questions liées au vote électronique. La seule norme internationale régissant une forme de vote électronique est la recommandation Rec (2004) 11 (CE, 2005) du Conseil de l'Europe, commentée plus loin, mais cette recommandation n'a pas force exécutoire au Canada[73].
>
> (notre soulignement)

72 Conseil de l'Europe, « Le Conseil de l'Europe adopte une nouvelle Recommandation sur les normes relatives au vote électronique » [communiqué de presse], *Salle de presse de l'assistance électorale* (site Internet), Strasbourg (France), 14 juin 2017, accessible à l'adresse : https://www.coe.int/fr/web/electoral-assistance/-/council-of-europe-adopts-new-recommendation-on-standards-for-e-voting (consulté le 24 janvier 2021).

73 Schwartz et Grince, *op. cit.*, p. 22.

Mentionnons à cet égard que les auteurs de cette étude précisent également :

> « Il pourrait être utile que les gouvernements démontrent aussi la conformité du système ou, au moins, l'évaluent en fonction de méthodes internationales. [...] On peut également opter pour l'obligation légale de conformité du système à un organisme reconnu en matière de sécurité ou d'intégrité des données. L'article 68 de la Loi concernant le cadre juridique des technologies de l'information du Québec est un exemple de disposition législative rendant obligatoire l'approbation par un organisme international, en citant la Commission électrotechnique internationale (CEI), l'Organisation internationale de normalisation (ISO) ou l'Union internationale des télécommunications (UIT) et le Conseil canadien des normes (ou un organisme accrédité par ce dernier) au titre d'organismes faisant autorité. Dans le même ordre d'idées, le Conseil de l'Europe, dans ses recommandations, cite l'European co-operation for Accreditation (EA), l'International Laboratory Accreditation Cooperation (ILAC) et l'International Accreditation Forum (IAF)[74]. »
>
> (nos soulignements)

Le groupe s'est également intéressé aux normes ISO qui tiennent compte des risques afférents à la sécurité de l'information et visent l'amélioration continue des applications ainsi qu'à d'autres normes et standards. Le groupe s'est particulièrement penché sur les normes et standards présentés dans le tableau suivant.

Norme ou standard	Description
ISO/IEC 27001:2013 Systèmes de management de la sécurité de l'information ISO/IEC 27002:2013 Code de bonne pratique pour le management de la sécurité de l'information	Ces deux standards proviennent de l'Organisation internationale de normalisation (ISO) et sont couramment utilisés dans l'industrie de la sécurité de l'information pour attester de la mise en œuvre et de l'amélioration continue des bonnes pratiques de sécurité de l'information pour l'entreprise, le département ou le système d'information faisant l'objet de la certification ISO.
ISO27005:2018 Gestion des risques liés à la sécurité de l'information	Ce standard provient également d'ISO. Ce standard, qui s'appuie notamment sur ISO/IEC 27001 et ISO/IEC 27002, contient des lignes directrices relatives à la gestion des risques en sécurité de l'information.

74 *Ibidem*, p. 51.

Norme ou standard	Description
ISO/IEC 27018 :2019	Ce standard provient également d'ISO et se spécialise dans la mise en place de bonnes pratiques de protection des renseignements personnels dans un contexte infonuagique. Bien qu'il ne soit pas nécessaire d'utiliser une plateforme infonuagique pour procéder à un vote électronique, la tangente du marché à utiliser de plus en plus des plateformes infonuagiques nous amène à nous y attarder.
ISO/IEC 27034 Application security (partie 1 à 7)	Ce standard provient également d'ISO et se spécialise dans le domaine de la sécurité des applications informatiques. Plus précisément, il fournit des lignes directrices pour un système de gestion de la sécurité logicielle, pendant tout le cycle de vie de l'application, et se base sur les risques et l'amélioration continue. Bien que chacune des parties du standard soit importante, les parties ayant le plus de liens avec la sécurité du vote électronique sont les **parties 5 et 7,** notamment pour ce qui a trait au cycle de vie d'un moyen technologique et de la façon de l'auditer.
Rapports SOC1, SOC2, SOC3	Les rapports de type SOC1, SOC2 et SOC3 ont été définis par l'organisme American Institute of Certified Public Accountants (AICPA). Le rapport SOC1 se rapporte surtout à la surveillance des contrôles informatiques permettant la génération des états financiers. Les rapports SOC2 et SOC3 sont, de leur côté, axés sur la mise en place d'un ensemble de contrôle portant sur la disponibilité, l'intégrité, la confidentialité et le respect de la vie privée. Le rapport donnant le plus haut niveau d'assurance est le SOC2 Type 2. Il permet de donner une assurance raisonnable que les contrôles informatiques étaient en place et efficaces pendant toute la période couverte (ex. : une période de six ou douze mois). Un rapport est alors généré à nouveau pour la période suivante afin d'assurer une couverture en continu.
Open Web Application Security Project (OWASP) Top 10	Ce standard créé par la OWASP Foundation vise la sécurité des applications web. Le top 10 de l'OWASP représente un large consensus sur les risques de sécurité les plus critiques pour les applications web. Bien que les organisations ne puissent pas se certifier « Top 10 OWASP », c'est généralement l'utilisation d'un standard comme celui-là qui permet aux organisations d'attester qu'ils réalisent effectivement des tâches liées à la sécurité du développement web.
NIST Cybersecurity Framework v1.1	Ce cadre volontaire comprend des normes, des lignes directrices et les meilleures pratiques pour gérer les risques liés à la cybersécurité. L'approche prioritaire, souple et économique du cadre de cybersécurité contribue à promouvoir la protection et la résilience des infrastructures critiques et d'autres secteurs importants pour l'économie et la sécurité nationale.

Annexe IV :
Survol de quelques règlements pris notamment en vertu de l'article 63.1 et du paragraphe *b* de l'article 93 du *Code des professions*

Règlement sur les élections du Barreau du Québec, c. B-1, r. 8.1 (ci-après « Barreau »)

Règlement sur l'organisation de l'Ordre des comptables professionnels agréés du Québec et les élections à son Conseil d'administration, c. C-48.1, r. 24.1 (ci-après « CPA »)

Règlement sur l'organisation de l'Ordre des infirmières et infirmiers du Québec et les élections à son Conseil d'administration, c. I-8, r. 16.1 (ci-après « infirmières »)

Règlement sur la représentation et les élections au Conseil d'administration de l'Ordre des ingénieurs du Québec, c. I-9, r. 11.1 (ci-après « ingénieurs »)

Règlement sur l'organisation du Collège des médecins du Québec et les élections à son Conseil d'administration, c. M-9, r. 25.2 (ci-après « médecins »)

Règlement sur l'organisation de l'Ordre des médecins vétérinaires du Québec et les élections à son Conseil d'administration, c. M-8, r. 14.1 (ci-après « médecins vétérinaires »)

Règlement sur les élections et l'organisation de la Chambre des notaires du Québec, c. N-3, r. 6.1 (ci-après « notaires »)

Règlement sur l'organisation de l'Ordre des technologues en imagerie médicale, en radio-oncologie et en électrophysiologie médicale du Québec et les élections à son Conseil d'administration, c. T-5, r. 11.02 (ci-après « TIMROEPM »)

Objet	Articles pertinents	Éléments communs	Disparités
Moyen technologique	Barreau – art. 12 et 13 Infirmières – art. 18	Vote par moyen technologique exclusivement.	
	CPA – art. 20 Ingénieurs – art. 17 et 30 Médecins – art. 24 Médecins vétérinaires – art. 30 Notaires – sous-section 1.1 et 3.1 TIMROEPM – art. 17	Vote par correspondance/ exprimé par voie postale ou vote par moyen technologique.	
Critères pour le choix des experts indépendants	Barreau – art. 15 CPA – art. 31 Infirmières – art. 19 Ingénieurs – art. 32 Médecins – art. 36 Médecins vétérinaires – art. 32 Notaires – art. 20.1 TIMROEPM – art. 30	Expérience dans le domaine de la sécurité des TI ; ne pas être en conflit d'intérêts.	Barreau : informaticien spécialisé dans la sécurité de l'information ; ne pas avoir de lien avec un candidat à l'élection. Infirmières, ingénieurs, médecins, médecins vétérinaires, notaires et TIMROEPM : certification dans le domaine de la sécurité des TI.
Nombre d'experts	Barreau – art. 14	Au moins deux	
	CPA – art. 31 Infirmières – art. 19 Ingénieurs – art. 32 Médecins – art. 36 Médecins vétérinaires – art. 32 Notaires – art. 20.1 TIMROEPM – art. 30	Au moins un	

Objet	Articles pertinents	Éléments communs	Disparités
Mandat des experts indépendants	Barreau – art. 14 (16, 16.1, 23, 26, 27, 28, 28.1) CPA – art. 32 Infirmières – art. 20 (21, 24, 25, 26, 27) Ingénieurs – art. 33 (34, 35, 42, 43) Médecins – art. 37 (38, 39, 40, 45, 47, 49, 50) Médecins vétérinaires – art. 33 (34, 35, 38, 39, 41, 42) Notaires – art. 20.2 (20.3, 20.4, 20.11, 20.12, 20.13) TIMROEPM – art. 31 (32, 33, 35, 37, 39, 41, 43)	S'assure/garantit que les mesures de sécurité mises en place sont adéquates et qu'elles permettent d'assurer le secret, la sécurité et l'intégrité du vote. Supervise le déroulement du vote/du scrutin et les étapes postérieures à celui-ci, dont le dépouillement du vote, la conservation et la destruction de l'information.	Barreau, ingénieurs, médecins, médecins vétérinaires, notaires et TIMROEPM : gère ou surveille la gestion, pendant le scrutin, des accès aux serveurs du système de vote électronique. CPA : s'assure que les paramètres du système de vote électronique correspondent aux règles établies par le secrétaire. CPA, médecins, médecins vétérinaires et TIMROEPM : le système de vote électronique, la liste des candidats et la liste des électeurs font l'objet d'un contrôle par l'expert indépendant afin de permettre de déceler toute modification qui apparaîtrait ultérieurement. Infirmières, médecins, médecins vétérinaires et TIMROEPM : si des irrégularités sont décelées pendant le scrutin, en fait rapport immédiatement au secrétaire et lui fait part de ses conclusions quant à leur incidence sur le résultat du scrutin. Infirmières, médecins vétérinaires et TIMROEPM : s'assure qu'un électeur ne vote qu'une seule fois.

Annexe V :
Articles pertinents du *Code des professions*, c. C -26

62.1. Le Conseil d'administration peut :

1° déléguer à un comité qu'il crée à cette fin le pouvoir de décider de toute demande présentée dans le cadre d'une candidature à l'exercice de la profession ainsi que l'exercice des pouvoirs prévus aux articles 45 à 45.3, 46.0.1, 48 à 52.1 et 55 à 55.3 ; les membres d'un tel comité sont soumis aux normes d'éthique et de déontologie déterminées par l'ordre et prêtent le serment prévu à l'annexe II ; le serment ne peut cependant être interprété comme interdisant l'échange de renseignements ou de documents au sein de l'ordre, pour les fins de protection du public ;

2° établir des règles concernant la conduite de ses affaires, dont le nombre et la périodicité des séances qu'il tient, ainsi que des règles concernant l'administration des biens de l'ordre ;

3° déterminer les modes de communication permettant aux membres du Conseil d'administration ou du comité exécutif, lorsqu'ils ne sont pas présents ou n'assistent pas physiquement à l'endroit où se tient une séance du Conseil d'administration ou du comité exécutif, selon le cas, de s'exprimer en vue d'une prise de décision, les conditions suivant lesquelles ils peuvent s'en prévaloir et, pour l'application du quatrième alinéa de l'article 79, du deuxième alinéa de l'article 84 et du deuxième alinéa de l'article 99, déterminer ce qui constitue un défaut de s'exprimer ou un empêchement, selon le cas ;

4° **choisir de tenir une élection du président et des autres administrateurs par un moyen technologique, lequel doit assurer la sécurité, le secret et l'intégrité du vote**.

63.1. Le Conseil d'administration doit, pour tenir une élection du président et des autres administrateurs par un moyen technologique, en fixer les modalités dans un règlement pris en vertu du paragraphe b de l'article 93. Ce règlement peut adapter les dispositions du présent code pour permettre la mise en œuvre de cette élection.

66.1. Seuls peuvent être candidats les membres de l'ordre qui sont inscrits au tableau et dont le droit d'exercer des activités professionnelles n'est pas limité ou suspendu au moins 45 jours avant la date fixée pour la clôture du scrutin. Le Conseil d'administration peut toutefois fixer, dans un règlement pris en vertu du paragraphe b de l'article 93, un délai plus long d'une durée maximale de 60 jours. Le candidat qui est radié ou dont le droit d'exercer des activités professionnelles est limité ou suspendu avant l'élection ou qui ne respecte pas les règles de conduite qui lui sont applicables établies dans un règlement pris en application du paragraphe a du premier alinéa de l'article 94 perd son éligibilité pour l'élection en cours. Le candidat ne peut être membre du conseil d'administration ou dirigeant d'une personne morale ou de tout autre groupement de personnes ayant pour objet principal la promotion des droits ou la défense des intérêts des membres de l'ordre ou des professionnels en général.

Seuls peuvent être candidats dans une région donnée les membres de l'ordre qui y ont leur domicile professionnel.

67. Les candidats aux postes d'administrateurs sont proposés par un bulletin signé par le candidat et remis au secrétaire de l'ordre au moins trente jours avant la date fixée pour la clôture du scrutin. Le Conseil d'administration peut toutefois fixer, dans un règlement pris en application du paragraphe b de l'article 93, un délai plus long d'une durée maximale de 45 jours. Ce bulletin doit également être signé par cinq membres de l'ordre ou par le nombre de membres que peut déterminer le Conseil d'administration dans ce règlement. Le bulletin doit contenir uniquement les renseignements déterminés par le Conseil d'administration dans ce règlement. Les renseignements contenus dans le bulletin de présentation constituent les seuls messages de communication électorale qu'un candidat peut transmettre aux membres de l'ordre ; le Conseil d'administration peut toutefois, dans ce règlement, encadrer la diffusion d'autres messages.

L'Office établit, en collaboration avec le Conseil interprofessionnel, des lignes directrices visant à encadrer les messages ou les moyens de communication électoraux utilisés par les candidats, notamment au sujet des messages qui ne concernent pas la protection du public ou qui visent à répondre aux messages des autres candidats ou, encore, en ce qui concerne l'utilisation des médias sociaux ou les publipostages.

Le Conseil d'administration s'inspire de ces lignes directrices de l'Office lorsqu'il adopte un règlement conformément au premier alinéa.

Il en est de même pour les candidats au poste de président, si ce dernier est élu au suffrage universel des membres de l'ordre.

Si un seul candidat a été présenté à un poste dans le délai fixé, le secrétaire le déclare immédiatement élu.

68. Seuls peuvent **signer un bulletin de présentation** d'un candidat à un poste d'administrateur dans une région donnée les professionnels qui y ont leur domicile professionnel.

69. Au moins quinze jours avant la date fixée pour la clôture du scrutin, le **secrétaire de l'ordre transmet à chacun des membres** de l'ordre ayant droit de vote les documents suivants, en même temps qu'il les avise de cette date :

a. un bulletin de vote certifié par le secrétaire, indiquant les noms des candidats aux postes d'administrateurs dans la région où chaque membre peut exercer son droit de vote et une enveloppe destinée à recevoir ce bulletin de vote, sur laquelle sont écrits les mots « BULLETIN DE VOTE ADMINISTRATEUR » et le nom de l'ordre ;

b. dans les cas où le président est élu au suffrage universel des membres de l'ordre, un bulletin de vote certifié par le secrétaire indiquant les noms des candidats au poste de président et une enveloppe destinée à recevoir ce bulletin de vote, sur laquelle sont écrits les mots « BULLETIN DE VOTE PRÉSIDENT » et le nom de l'ordre ;

c. une enveloppe adressée au secrétaire de l'ordre et sur laquelle sont écrits le mot « ÉLECTION », le nom du votant, son adresse et la région dans laquelle il peut exercer son droit de vote ;

d. tout autre document que peut prescrire le Conseil d'administration dans un règlement pris en application du paragraphe b de l'article 93.

70. Tous les **bulletins de vote et les enveloppes** destinés à servir à une élection doivent avoir la même forme et être aussi semblables que possible.

Chaque bulletin contient à droite du nom de chaque candidat, un espace réservé à l'exercice du droit de vote.

71. Seules **peuvent voter** les personnes qui étaient membres de l'ordre le 45e jour avant la date fixée pour la clôture du scrutin et le sont demeurées. Le Conseil d'administration peut toutefois fixer, dans un règlement pris en application du paragraphe b de l'article 93, un délai plus long d'une durée maximale de 60 jours.

Elles **expriment leur vote en marquant le bulletin de vote** dans un ou plusieurs des espaces réservés à l'exercice du droit de vote, selon qu'il y a un ou plusieurs candidats à élire.

72. Le votant **transmet son bulletin de vote** ou, si le président est élu au suffrage universel, ses bulletins de vote au secrétaire de l'ordre dans l'enveloppe visée au paragraphe c de l'article 69 et qui lui a été envoyée à cette fin.

73. Le secrétaire de l'ordre dépose dans une **boîte de scrutin scellée**, sans les ouvrir, toutes les enveloppes contenant les bulletins de vote qu'il reçoit avant la clôture du scrutin.

74. Dans les dix jours de la date de la clôture du scrutin, le secrétaire de l'ordre procède au **dépouillement du vote** en présence des scrutateurs désignés par le Conseil d'administration ; ces scrutateurs doivent être au nombre de trois à moins que le Conseil d'administration n'en fixe un nombre supérieur dans un règlement pris en application du paragraphe b de l'article 93.

Tout bulletin de vote marqué dans un ou plusieurs des espaces réservés à l'exercice du droit de vote est reconnu valide.

Toutefois, doit être rejeté un bulletin qui :

1° n'est pas certifié par le secrétaire de l'ordre ;

2° n'a pas été marqué ;

3° a été marqué en faveur de plus de candidats qu'il n'y en a à élire ;

4° a été marqué en faveur d'une personne qui n'est pas candidate ;

5° a été marqué ailleurs que dans l'espace prévu ;

6° porte des inscriptions fantaisistes ou injurieuses ;

7° porte une marque permettant d'identifier l'électeur.

Aucun bulletin ne doit être rejeté pour le seul motif qu'une marque dépasse l'espace réservé à l'exercice du droit de vote ou qu'il n'est pas complètement rempli.

Au cas d'égalité des voix, un tirage au sort détermine lequel des candidats est élu.

Annexe VI :
Articles pertinents de la *Loi concernant le cadre juridique des technologies de l'information*, c. C -1.1

1. La présente loi a pour objet d'assurer :

1° la sécurité juridique des communications effectuées par les personnes, les associations, les sociétés ou l'État au moyen de documents quels qu'en soient les supports ;

2° la cohérence des règles de droit et leur application aux communications effectuées au moyen de documents qui sont sur des supports faisant appel aux technologies de l'information, qu'elles soient électronique, magnétique, optique, sans fil ou autres ou faisant appel à une combinaison de technologies ;

3° l'équivalence fonctionnelle des documents et leur valeur juridique, quels que soient les supports des documents, ainsi que l'interchangeabilité des supports et des technologies qui les portent ;

4° le lien entre une personne, une association, une société ou l'État et un document technologique, par tout moyen qui permet de les relier, dont la signature, ou qui permet de les identifier et, au besoin, de les localiser, dont la certification ;

5° la concertation en vue de l'harmonisation des systèmes, des normes et des standards techniques permettant la communication au moyen de documents technologiques et l'interopérabilité des supports et des technologies de l'information.

2. À moins que la loi n'exige l'emploi exclusif d'un support ou d'une technologie spécifique, chacun peut utiliser le support ou la technologie de son choix, dans la mesure où ce choix respecte les règles de droit, notamment celles prévues au Code civil.

Ainsi, les supports qui portent l'information du document sont interchangeables et, l'exigence d'un écrit n'emporte pas l'obligation d'utiliser un support ou une technologie spécifique.

3. Un document est constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles.

Pour l'application de la présente loi, est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

Un dossier peut être composé d'un ou de plusieurs documents.

Les documents sur des supports faisant appel aux technologies de l'information visées au paragraphe 2° de l'article 1 sont qualifiés dans la présente loi de documents technologiques.

4. Un document technologique, dont l'information est fragmentée et répartie sur un ou plusieurs supports situés en un ou plusieurs emplacements, doit être considéré comme formant un tout, lorsque des éléments logiques structurants permettent d'en relier les fragments, directement ou par référence, et que ces éléments assurent à la fois l'intégrité de chacun des fragments d'information et l'intégrité de la reconstitution du document antérieur à la fragmentation et à la répartition.

Inversement, plusieurs documents technologiques, même réunis en un seul à des fins de transmission ou de conservation, ne perdent pas leur caractère distinct, lorsque des éléments logiques structurants permettent d'assurer à la fois l'intégrité du document qui les réunit et celle de la reconstitution de chacun des documents qui ont été ainsi réunis.

5. La **valeur juridique** d'un document, notamment le fait qu'il puisse produire des effets juridiques et être admis en preuve, n'est ni augmentée ni diminuée pour la seule raison qu'un support ou une technologie spécifique a été choisi.

Le document dont l'intégrité est assurée a la même valeur juridique, qu'il soit sur support papier ou sur un autre support, dans la mesure où, s'il s'agit d'un document technologique, il respecte par ailleurs les mêmes règles de droit.

Le document dont le support ou la technologie ne permettent ni d'affirmer, ni de dénier que l'intégrité en est assurée peut, selon les circonstances, être admis à titre de témoignage ou d'élément matériel de preuve et servir de commencement de preuve, comme prévu à l'article 2865 du Code civil.

Lorsque la loi exige l'emploi d'un document, cette exigence peut être satisfaite par un document technologique dont l'intégrité est assurée.

6. L'intégrité du document est assurée, lorsqu'il est possible de vérifier que l'information n'en est pas altérée et qu'elle est maintenue dans son intégralité, et que le support qui porte cette information lui procure la stabilité et la pérennité voulue.

L'intégrité du document doit être maintenue au cours de son cycle de vie, soit depuis sa création, en passant par son transfert, sa consultation et sa transmission, jusqu'à sa conservation, y compris son archivage ou sa destruction.

Dans l'appréciation de l'intégrité, il est tenu compte, notamment des mesures de sécurité prises pour protéger le document au cours de son cycle de vie.

7. Il n'y a **pas lieu de prouver que le support du document ou que les procédés, systèmes ou technologies utilisés pour communiquer au moyen d'un document permettent d'assurer son intégrité, à moins** que celui qui conteste l'admission du document n'établisse, par prépondérance de preuve, qu'il y a eu atteinte à l'intégrité du document.

9. Des documents sur des supports différents ont la même valeur juridique s'ils comportent la même information, si l'intégrité de chacun d'eux est assurée et s'ils respectent tous deux les règles de droit qui les régissent. L'un peut remplacer l'autre et ils peuvent être utilisés simultanément ou en alternance. De plus, ces documents peuvent être utilisés aux mêmes fins.

En cas de perte, un document peut servir à reconstituer l'autre.

10. Le seul fait que des documents porteurs de la même information, mais sur des supports différents, présentent des différences en ce qui a trait à l'emmagasinage ou à la présentation de l'information ou le seul fait de comporter de façon apparente ou sous-jacente de l'information différente relativement au support ou à la sécurité de chacun des documents n'est pas considéré comme portant atteinte à l'intégrité du document.

De même, ne sont pas considérées comme des atteintes à l'intégrité du document, les différences quant à la pagination du document, au caractère tangible ou intangible des pages, à leur format, à leur présentation recto ou verso, à leur accessibilité en tout ou en partie ou aux possibilités de repérage séquentiel ou thématique de l'information.

11. En cas de divergence entre l'information de documents qui sont sur des supports différents ou faisant appel à des technologies différentes et qui sont censés porter la même information, le document qui prévaut est, à moins d'une preuve contraire, celui dont il est possible de vérifier que l'information n'a pas été altérée et qu'elle a été maintenue dans son intégralité.

12. Un document technologique peut remplir les fonctions d'un original. À cette fin, son intégrité doit être assurée et, lorsque l'une de ces fonctions est d'établir que le document :

1° est la source première d'une reproduction, les composantes du document source doivent être conservées de sorte qu'elles puissent servir de référence ultérieurement ;

2° présente un caractère unique, les composantes du document ou de son support sont structurées au moyen d'un procédé de traitement qui permet d'affirmer le caractère unique du document, notamment par l'inclusion d'une composante exclusive ou distinctive ou par l'exclusion de toute forme de reproduction du document ;

3° est la forme première d'un document relié à une personne, les composantes du document ou de son support sont structurées au moyen d'un procédé de traitement qui permet à la fois d'affirmer le caractère unique du document, d'identifier la personne auquel le document est relié et de maintenir ce lien au cours de tout le cycle de vie du document.

Pour l'application des paragraphes 2° et 3° du premier alinéa, les procédés de traitement doivent s'appuyer sur des normes ou standards techniques approuvés par un organisme reconnu visé à l'article 68.

13. Lorsque l'apposition d'un sceau, d'un cachet, d'un tampon, d'un timbre ou d'un autre instrument a pour fonction :

1° de protéger l'intégrité d'un document ou d'en manifester la fonction d'original, celle-ci peut être remplie à l'égard d'un document technologique, au moyen d'un procédé approprié au support du document ;

2° d'identifier une personne, une association, une société ou l'État, cette fonction peut être remplie à l'égard d'un document technologique, selon les règles prévues à la sous-section 1 de la section II du chapitre III ;

3° d'assurer la confidentialité du document, cette fonction peut être remplie à l'égard d'un document technologique, selon les règles prévues à l'article 34.

14. Au plan de la forme, un ou plusieurs procédés peuvent être utilisés pour remplir les fonctions prévues aux articles 12 et 13 et ils doivent faire appel aux caractéristiques du support qui porte l'information.

15. Pour assurer l'intégrité de la copie d'un document technologique, le procédé employé doit présenter des **garanties suffisamment sérieuses pour établir le fait qu'elle comporte la même information que le document source**.

Il est tenu compte dans l'appréciation de l'intégrité de la copie des circonstances dans lesquelles elle a été faite ainsi que du fait qu'elle a été effectuée de façon systématique et sans lacunes ou conformément à un procédé qui s'appuie sur des normes ou standards techniques approuvés par un organisme reconnu visé à l'article 68.

Cependant, lorsqu'il y a lieu d'établir que le document constitue une copie, celle-ci doit, au plan de la forme, présenter les caractéristiques qui permettent de reconnaître qu'il s'agit d'une copie, soit par l'indication du lieu et de la date où elle a été effectuée ou du fait qu'il s'agit d'une copie, soit par tout autre moyen.

La copie effectuée par une entreprise au sens du Code civil ou par l'État bénéficie d'une présomption d'intégrité en faveur des tiers.

16. Lorsque la copie d'un document doit être certifiée, cette exigence peut être satisfaite à l'égard d'un document technologique au moyen d'un procédé de comparaison permettant de reconnaître que l'information de la copie est identique à celle du document source.

17. L'information d'un document qui doit être conservé pour constituer une preuve, qu'il s'agisse d'un original ou d'une copie, peut faire l'objet d'un transfert vers un support faisant appel à une technologie différente.

Toutefois, sous réserve de l'article 20, pour que le document source puisse être détruit et remplacé par le document qui résulte du transfert tout en conservant sa valeur juridique, le transfert doit être documenté de sorte qu'il puisse être démontré, au besoin, que le document résultant du transfert comporte la même information que le document source et que son intégrité est assurée.

La documentation comporte au moins la mention du format d'origine du document dont l'information fait l'objet du transfert, du procédé de transfert utilisé ainsi que des garanties qu'il est censé offrir, selon les indications fournies avec le produit, quant à la préservation de l'intégrité, tant du document devant être transféré, s'il n'est pas détruit, que du document résultant du transfert.

La documentation, y compris celle relative à tout transfert antérieur, est conservée durant tout le cycle de vie du document résultant du transfert. La documentation peut être jointe, directement ou par référence, soit au document résultant du transfert, soit à ses éléments structurants ou à son support.

18. Lorsque le document source est détruit, aucune règle de preuve ne peut être invoquée contre l'admissibilité d'un document résultant d'un transfert effectué et documenté conformément à l'article 17 et auquel est jointe la documentation qui y est prévue, pour le seul motif que le document n'est pas dans sa forme originale.

19. Toute personne doit, pendant la période où elle est tenue de **conserver un document**, assurer le maintien de son intégrité et voir à la disponibilité du matériel qui permet de le rendre accessible et intelligible et de l'utiliser aux fins auxquelles il est destiné.

20. Les documents dont la loi exige la conservation et qui ont fait l'objet d'un transfert peuvent être détruits et remplacés par les documents résultant du transfert. Toutefois, avant de procéder à la destruction, la personne qui en est chargée :

1° prépare et tient à jour des règles préalables à la destruction des documents ayant fait l'objet d'un transfert, sauf dans le cas d'un particulier ;

2° s'assure de la protection des renseignements confidentiels et personnels que peuvent comporter les documents devant être détruits ;

3° s'assure, dans le cas des documents en la possession de l'État ou d'une personne morale de droit public, que la destruction est faite selon le calendrier de conservation établi conformément à la Loi sur les archives (chapitre A-21.1).

Toutefois, doit être conservé sur son support d'origine le document qui, sur celui-ci, présente une valeur archivistique, historique ou patrimoniale eu égard aux critères élaborés en vertu du paragraphe 1° de l'article 69, même s'il a fait l'objet d'un transfert.

21. Lorsqu'une modification est apportée à un document technologique durant la période où il doit être conservé, la personne qui a l'autorité pour faire la modification doit, pour en préserver l'intégrité, noter les renseignements qui permettent de déterminer qui a fait la demande de modification, quand, par qui et pourquoi la modification a été faite. Celle-ci fait partie intégrante du document, même si elle se trouve sur un document distinct.

22. Le prestataire de services qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau de communication n'est pas responsable des activités accomplies par l'utilisateur du service au moyen des documents remisés par ce dernier ou à la demande de celui-ci.

Cependant, il peut engager sa responsabilité, notamment s'il a de fait connaissance que les documents conservés servent à la réalisation d'une activité à caractère illicite ou s'il a connaissance de circonstances qui la rendent apparente et qu'il n'agit pas promptement pour rendre l'accès aux documents impossible ou pour autrement empêcher la poursuite de cette activité.

De même, le prestataire qui agit à titre d'intermédiaire pour offrir des services de référence à des documents technologiques, dont un index, des hyperliens, des répertoires ou des outils de recherche, n'est pas responsable des activités accomplies au moyen de ces services. Toutefois, il peut engager sa responsabilité, notamment s'il a de fait connaissance que les services qu'il fournit servent à la réalisation d'une activité à caractère illicite et s'il ne cesse promptement de fournir ses services aux personnes qu'il sait être engagées dans cette activité.

23. Tout document auquel une personne a droit d'accès doit être intelligible, soit directement, soit en faisant appel aux technologies de l'information.

Ce droit peut être satisfait par l'accès à une copie du document ou à un document résultant d'un transfert ou à une copie de ce dernier.

Le choix d'un support ou d'une technologie tient compte de la demande de la personne qui a droit d'accès au document, sauf si ce choix soulève des difficultés pratiques sérieuses, notamment en raison des coûts ou de la nécessité d'effectuer un transfert.

24. L'utilisation de fonctions de recherche extensive dans un document technologique qui contient des renseignements personnels et qui, pour une finalité particulière, est rendu public doit être restreinte à cette finalité. Pour ce faire, la personne responsable de l'accès à ce document doit voir à ce que soient mis en place les moyens technologiques appropriés. Elle peut en outre, eu égard aux critères élaborés en vertu du paragraphe 2° de l'article 69, fixer des conditions pour l'utilisation de ces fonctions de recherche.

25. La personne responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder.

26. Quiconque confie un document technologique à un prestataire de services pour qu'il en assure la garde est, au préalable, tenu d'**informer le prestataire quant à la protection que requiert le document** en ce qui a trait à la confidentialité de l'information et quant aux personnes qui sont habilitées à en prendre connaissance.

Le prestataire de services est tenu, durant la période où il a la garde du document, de voir à ce que les moyens technologiques convenus soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance. Il doit de même assurer le respect de toute autre obligation prévue par la loi relativement à la conservation du document.

27. Le prestataire de services qui agit à titre d'intermédiaire pour fournir des services sur un réseau de communication ou qui y conserve ou y transporte des documents technologiques n'est pas tenu d'en surveiller l'information, ni de rechercher des circonstances indiquant que les documents permettent la réalisation d'activités à caractère illicite.

Toutefois, il ne doit prendre aucun moyen pour empêcher la personne responsable de l'accès aux documents d'exercer ses fonctions, notamment en ce qui a trait à la confidentialité, ou pour empêcher les autorités responsables d'exercer leurs fonctions, conformément à la loi, relativement à la sécurité publique ou à la prévention, à la détection, à la preuve ou à la poursuite d'infractions.

28. Un document peut être transmis, envoyé ou expédié par tout mode de transmission approprié à son support, à moins que la loi n'exige l'emploi exclusif d'un mode spécifique de transmission.

Lorsque la loi prévoit l'utilisation des services de la poste ou du courrier, cette exigence peut être satisfaite en faisant appel à la technologie appropriée au support du document devant être transmis. De même, lorsque la loi prévoit l'utilisation de la poste recommandée, cette exigence peut être satisfaite, dans le cas d'un document technologique, au moyen d'un accusé de réception sur le support approprié signé par le destinataire ou par un autre moyen convenu.

Lorsque la loi prévoit l'envoi ou la réception d'un document à une adresse spécifique, celle-ci se compose, dans le cas d'un document technologique, d'un identifiant propre à l'emplacement où le destinataire peut recevoir communication d'un tel document.

29. Nul ne peut exiger de quelqu'un qu'il se procure un support ou une technologie spécifique pour transmettre ou recevoir un document, à moins que cela ne soit expressément prévu par la loi ou par une convention.

De même, nul n'est tenu d'accepter de recevoir un document sur un autre support que le papier ou au moyen d'une technologie dont il ne dispose pas.

Lorsque quelqu'un demande d'obtenir un produit, un service ou de l'information au sujet de l'un d'eux et que celui-ci est disponible sur plusieurs supports, le choix du support lui appartient.

30. Pour que le document technologique reçu ait la même valeur que le document transmis, le mode de transmission choisi doit permettre de préserver l'intégrité des deux documents. La documentation établissant la capacité d'un mode de transmission d'en préserver l'intégrité doit être disponible pour production en preuve, le cas échéant.

Le seul fait que le document ait été fragmenté, compressé ou remisé en cours de transmission pour un temps limité afin de la rendre plus efficace n'emporte pas la conclusion qu'il y a atteinte à l'intégrité du document.

31. Un document technologique est présumé transmis, envoyé ou expédié lorsque le geste qui marque le début de son parcours vers l'adresse active du destinataire est accompli par l'expéditeur ou sur son ordre et que ce parcours ne peut être contremandé ou, s'il peut l'être, n'a pas été contremandé par lui ou sur son ordre.

Le document technologique est présumé reçu ou remis lorsqu'il devient accessible à l'adresse que le destinataire indique à quelqu'un être l'emplacement où il accepte de recevoir de lui un document ou celle qu'il représente publiquement être un emplacement où il accepte de recevoir les documents qui lui sont destinés, dans la mesure où cette adresse est active au moment de l'envoi. Le document reçu est présumé intelligible, à moins d'un avis contraire envoyé à l'expéditeur dès l'ouverture du document.

Lorsque le moment de l'envoi ou de la réception du document doit être établi, il peut l'être par un bordereau d'envoi ou un accusé de réception ou par la production des renseignements conservés avec le document lorsqu'ils garantissent les date, heure, minute, seconde de l'envoi ou de la réception et l'indication de sa provenance et sa destination ou par un autre moyen convenu qui présente de telles garanties.

34. Lorsque la loi déclare confidentiels des renseignements que comporte un document, **leur confidentialité doit être protégée par un moyen approprié** au mode de transmission, y compris sur des réseaux de communication.

La documentation expliquant le mode de transmission convenu, incluant les moyens pris pour assurer la confidentialité du document transmis, doit être disponible pour production en preuve, le cas échéant.

35. La partie qui offre un produit ou un service au moyen d'un document préprogrammé doit, sous peine d'inopposabilité de la communication ou d'annulation de la transaction, faire en sorte que le document fournisse les instructions nécessaires pour que la partie qui utilise un tel document puisse dans les meilleurs délais l'aviser d'une erreur commise ou disposer des moyens pour prévenir ou corriger une erreur. De même, des instructions ou des moyens doivent lui être fournis pour qu'elle soit en mesure d'éviter l'obtention d'un produit ou d'un service dont elle ne veut pas ou qu'elle n'obtiendrait pas sans l'erreur commise ou pour qu'elle soit en mesure de le rendre ou, le cas échéant, de le détruire.

36. Le prestataire de services qui agit à titre d'intermédiaire pour fournir les services d'un réseau de communication exclusivement pour la transmission de documents technologiques sur ce réseau n'est pas responsable des actions accomplies par autrui au moyen des documents qu'il transmet ou qu'il conserve durant le cours normal de la transmission et pendant le temps nécessaire pour en assurer l'efficacité.

Il peut engager sa responsabilité, notamment s'il participe autrement à l'action d'autrui :

1° en étant à l'origine de la transmission du document ;

2° en sélectionnant ou en modifiant l'information du document ;

3° en sélectionnant la personne qui transmet le document, qui le reçoit ou qui y a accès ;

4° en conservant le document plus longtemps que nécessaire pour sa transmission.

37. Le prestataire de services qui agit à titre d'intermédiaire pour conserver sur un réseau de communication les documents technologiques que lui fournit son client et qui ne les conserve qu'à la seule fin d'assurer l'efficacité de leur transmission ultérieure aux personnes qui ont droit d'accès à l'information n'est pas responsable des actions accomplies par autrui par le biais de ces documents.

Il peut engager sa responsabilité, notamment s'il participe autrement à l'action d'autrui :

1° dans les cas visés au deuxième alinéa de l'article 36 ;

2° en ne respectant pas les conditions d'accès au document ;

3° en prenant des mesures pour empêcher la vérification de qui a eu accès au document ;

4° en ne retirant pas promptement du réseau ou en ne rendant pas l'accès au document impossible alors qu'il a de fait connaissance qu'un tel document a été retiré de là où il se trouvait initialement sur le réseau, du fait qu'il n'est pas possible aux personnes qui y ont droit d'y avoir accès ou du fait qu'une autorité compétente en a ordonné le retrait du réseau ou en a interdit l'accès.

38. Le lien entre une personne et un document technologique, ou le lien entre un tel document et une association, une société ou l'État, peut être établi par tout procédé ou par une combinaison de moyens dans la mesure où ceux-ci permettent :

1° de confirmer l'identité de la personne qui effectue la communication ou l'identification de l'association, de la société ou de l'État et, le cas échéant, de sa localisation, ainsi que la confirmation de leur lien avec le document ;

2° d'identifier le document et, au besoin, sa provenance et sa destination à un moment déterminé.

39. Quel que soit le support du document, la **signature** d'une personne peut servir à l'établissement d'un lien entre elle et un document. La signature peut être apposée au document au moyen de tout procédé qui permet de satisfaire aux exigences de l'article 2827 du Code civil.

La signature d'une personne apposée à un document technologique lui est opposable lorsqu'il s'agit d'un document dont l'intégrité est assurée et qu'au moment de la signature et depuis, le lien entre la signature et le document est maintenu.

46. Lorsqu'un document utilisé pour effectuer une communication en réseau doit être conservé pour constituer une preuve, son identifiant doit être conservé avec lui pendant tout le cycle de vie du document par la personne qui est responsable du document.

L'identifiant du document doit être accessible au moyen d'un service de répertoire, dont une des fonctions est de relier un identifiant à sa localisation. Le lien entre un identifiant et un objet peut être garanti par un certificat lequel est lui-même accessible au moyen d'un service de répertoire qui peut être consulté par le public.

L'identifiant se compose d'un nom de référence distinct et non ambigu dans l'ensemble des dénominations locales où il est inscrit, ainsi que des extensions nécessaires pour joindre ce nom à des ensembles de dénominations universels.

Pour permettre d'établir la provenance ou la destination du document à un moment déterminé, les autres objets qui ont servi à effectuer la communication, comme les certificats, les algorithmes et les serveurs d'envoi ou de réception, doivent pouvoir être identifiés et localisés, au moyen des identifiants alors attribués à chacun de ces objets.

64. Le comité pour l'harmonisation des systèmes et des normes a pour mission d'examiner les moyens susceptibles :

[...]

4° de garantir l'intégrité d'un document technologique **par des mesures de sécurité physiques, logiques ou opérationnelles ainsi que par des mesures de gestion documentaire adéquates pour en assurer l'intégrité au cours de tout son cycle de vie** ;

[...]

74. L'indication dans la loi de la possibilité d'utiliser un ou des modes de transmission comme l'envoi ou l'expédition d'un document par lettre, par messager, par câblogramme, par télégramme, par télécopieur, par voie télématique, informatique ou électronique, par voie de télécommunication, de télétransmission ou au moyen de la fibre optique ou d'une autre technologie de l'information n'empêche pas de recourir à un autre mode de transmission approprié au support du document, dans la mesure où la disposition législative n'impose pas un mode exclusif de transmission.

CONSEIL
INTERPROFESSIONNEL
DU QUÉBEC

RASSEMBLER.
ÉVOLUER.