Mémoire déposé à Élections Québec

Consultation
« Le vote par Internet, vous en pensez quoi? »
Octobre 2019

Mémoire rédigé par
Clément Gagnon

3 novembre 2019

1. Résumé

Ce mémoire présente une analyse des risques du vote par Internet, des constats sur plusieurs points d'intérêt ainsi qu'une recommandation sur la marche à suivre.

2. Courte biographie de l'auteur du mémoire

Ce mémoire est une implication citoyenne *pro bono*. Je suis un consultant en sécurité de l'information numérique. Je possède plusieurs certifications dans les domaines de la sécurité de l'information, les audits et la gestion des risques.

En 2005 et 2006, j'ai été impliqué dans l'analyse du vote électronique lors des élections municipales.

- Mémoire sur le vote électronique déposé à la Commission sur l'avant-projet de loi sur la Loi électorale, 9 janvier 2006;
- Article dans le journal Le Soleil, 19 novembre 2005, « Le vote électronique à Québec, un système excessivement préoccupant »;
- Mention comme observateur dans le rapport du DGE, « Élections municipales de novembre 2005, Rapport d'évaluation des nouveaux mécanismes de votation », octobre 2006

Clément Gagnon
[redacted]
Québec, Québec

Courriel : [redacted]
Cell. [redacted]

3. Introduction

Ce mémoire présente une analyse sommaire des risques du vote par Internet. Ce mémoire adresse également la question de l'utilisation de la blockchain ou la chaîne de blocs. Cette dernière fait l'objet d'un engouement et même d'une frénésie qui parfois dépasse la raison.

Ce document est organisé de la façon suivante :

- Établissement du contexte;
- Définition des termes et des concepts importants;
- Identification des menaces et des risques;
- Traitement des risques;
- Constats;
- Recommandation.

4. Contexte

La consultation publique d'Élections Québec place deux balises. La première concerne la définition du vote par Internet et la seconde affirme que le vote par Internet ne remplace pas le vote papier traditionnel.

Il est inutile de rappeler que la transformation numérique de notre société a complètement bouleversé les échanges sociaux, économiques et politiques. En 50 ans, grâce à Internet, la transformation numérique suit une courbe algorithmique. L'accélération des changements est étourdissante.

Au cours de ces dernières années, nous avons également constaté, des événements perturbateurs et parfois malveillants viennent perturber la vie sociale, économique et politique par des moyens numériques. Il suffit de mentionner les cyberattaques envers les infrastructures critiques, les influences de puissances étrangères et hostiles sur les activités politiques de la nation et les attaques de toutes sortes provenant de groupes criminels organisés et compétents.

En marge de cette transformation, le processus démocratique du vote au Québec et Canada a été très peu influencé par le numérique. Il y a des initiatives à petite échelle pour l'utilisation de moyens numériques dans les municipalités et organismes, mais une utilisation de grande envergure à la grandeur d'une province ou du pays n'a pas encore eu lieu. Dans le reste du continent américain, notamment aux États-Unis, plusieurs états

utilisent le vote électronique et certains utilisent le vote par Internet. De nombreux vulnérabilités et problèmes ont été constatés[1].

Le pays souvent cité en exemple comme nation numérique est l'Estonie. Ce pays utilise le vote par Internet. Malgré sa maturité numérique, le système de vote estonien est vulnérable[2] sur plusieurs aspects. Ces vulnérabilités ont été découvertes par des audits de sécurité indépendants.

[1] https://www.npr.org/2019/09/04/755066523/cyber-experts-warn-of-vulnerabilities-facing-2020-election-machines

[2] https://estoniaevoting.org/faq/

5. Définitions

Dépersonnalisation du vote

La dépersonnalisation consiste à dissocier le citoyen qui a voté du vote qu'il a fait. Lors du vote traditionnel, cette dissociation est facile accomplir et à vérifier contrairement au vote électronique ou par Internet. La conception de la solution de vote doit éviter les designs déficients, les bogues et les moyens collatéraux qui permettraient d'associer un vote à un électeur.

Chaîne de blocs ou blockchain

Selon Wikipedia, « une chaîne de blocs est une base de données distribuée qui gère une liste d'enregistrements protégés contre la falsification ou la modification par des nœuds de stockage ; c'est donc un registre distribué et sécurisé de toutes les transactions effectuées depuis le démarrage du système réparti ».

D'un point de vie technique, la chaine de blocs est « une base de données distribuée dont les informations envoyées par les utilisateurs et les liens internes à la base sont vérifiés et groupés à intervalles de temps réguliers en blocs, formant ainsi une chaîne. L'ensemble est sécurisé par cryptographie ».

Menaces

La menace est la combinaison d'un agent provoquant un événement ou une attaque qui peut, potentiellement, concrétiser un risque.

Risque

Selon ISO 31000 *Risk management – Guidelines, Second edition 2018-02*, le risque est l'effet de l'incertitude sur l'atteinte des objectifs. Dans le domaine de la sécurité de l'information, nous pouvons résumer grossièrement que le risque est le succès d'une attaque sur un actif en exploitant une vulnérabilité.

Traitement du risque

La finalité de la gestion du risque est son traitement afin de mitiger le risque. Il existe quatre options du traitement du risque :

- Le refus ou l'évitement : le risque considéré est trop élevé, l'activité amenant le risque doit être supprimée.
- Le transfert : le risque sera partagé avec une autre entité (un assureur, un sous-traitant) capable de le gérer.
- La réduction : le risque doit être diminué. Il s'agit d'en réduire l'impact et/ou la potentialité de manière que le risque soit acceptable.
- Conservation du risque : le risque est maintenu tel quel.

Vote par Internet

Le vote par Internet permet à l'électeur de voter, peu importe l'endroit avec un dispositif lui appartenant et qui est connecté à Internet.

Vote électronique

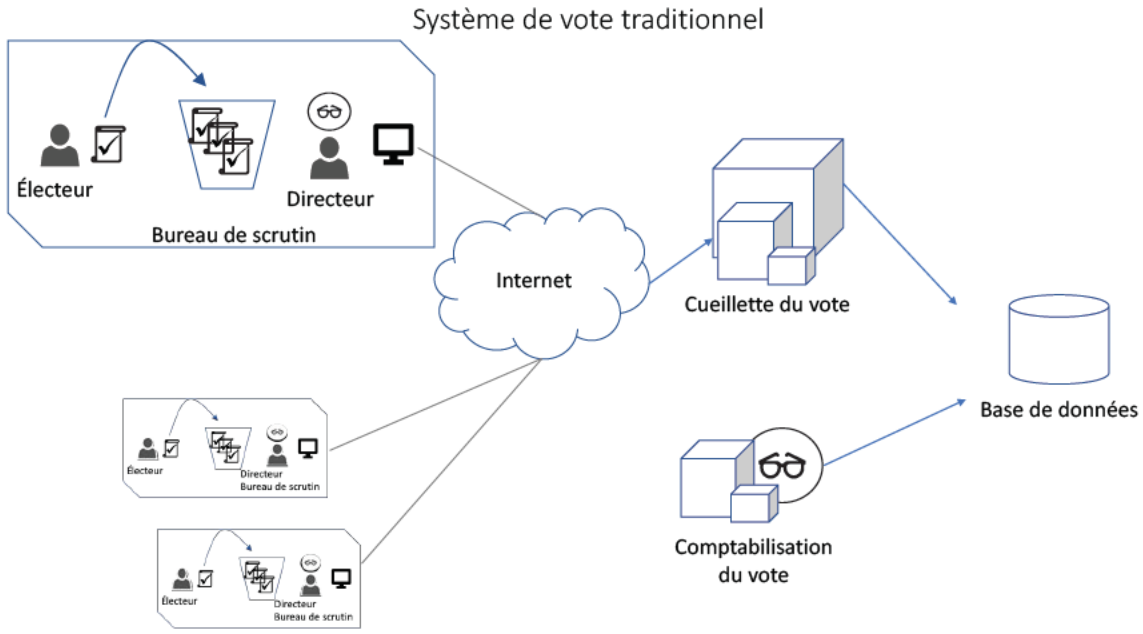
Le vote électronique est l'utilisation d'un dispositif électronique et parfois de nature informatique pour faciliter l'acte de voter et la comptabilisation du vote. Le citoyen doit se présenter dans un lieu physique pour voter ou utiliser un moyen de communication comme le téléphone.

6. Le vote traditionnel et le vote électronique.

Le vote traditionnel repose essentiellement sur un support papier. Après une identification sommaire, l'électeur marque le bulletin de vote. Les bulletins sont comptés au bureau de scrutin ou dans un bureau régional. Les résultats sont transmis électroniquement ou de vive voix à un bureau central ou au directeur des élections pour être comptabilisés.

Le vote électronique peut intervenir sur certains points de ce processus pour faciliter le traitement du vote. Le bulletin de vote peut être remplacé par un écran, un papier perforé, le comptage des votes peut être mécanique ou électronique, etc.

Le vote électronique fut utilisé lors des élections municipales de 2005. Le système de vote électronique utilisé par la ville de Québec a connu des ratés importants. Cependant, d'autres municipalités ont connu du succès.



7. Le vote par Internet

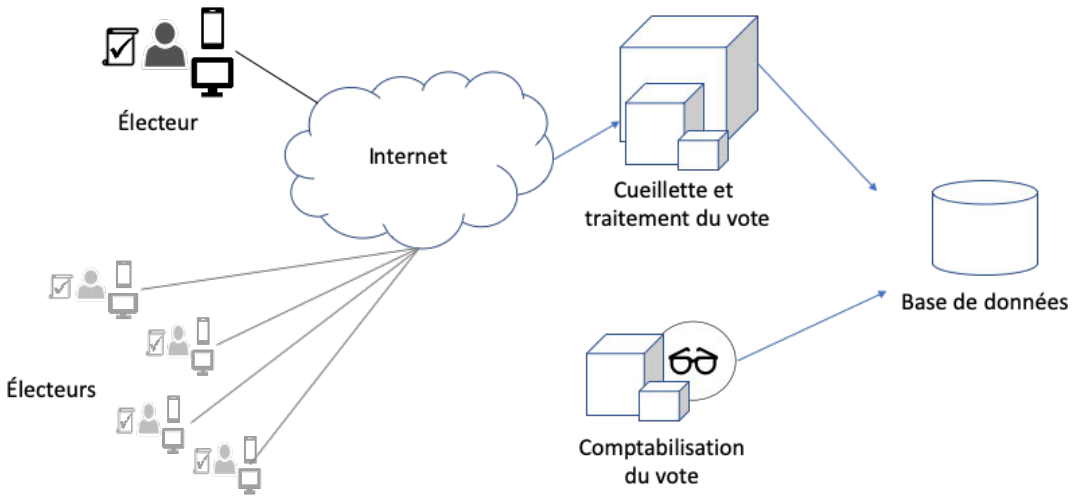
Le vote par Internet est complexe et compliqué. Plusieurs plateformes doivent être prises en compte : téléphone intelligent provenant de plusieurs manufacturiers, ordinateurs, plusieurs types de navigateurs Internet.

Internet est un réseau sans contrôle, l'exposition aux menaces est constante. Contrairement au vote électronique qui est un réseau « fermé », le vote par Internet se déroule dans un réseau qui fait l'objet de menaces de toutes sortes provenant de partout sur la planète.

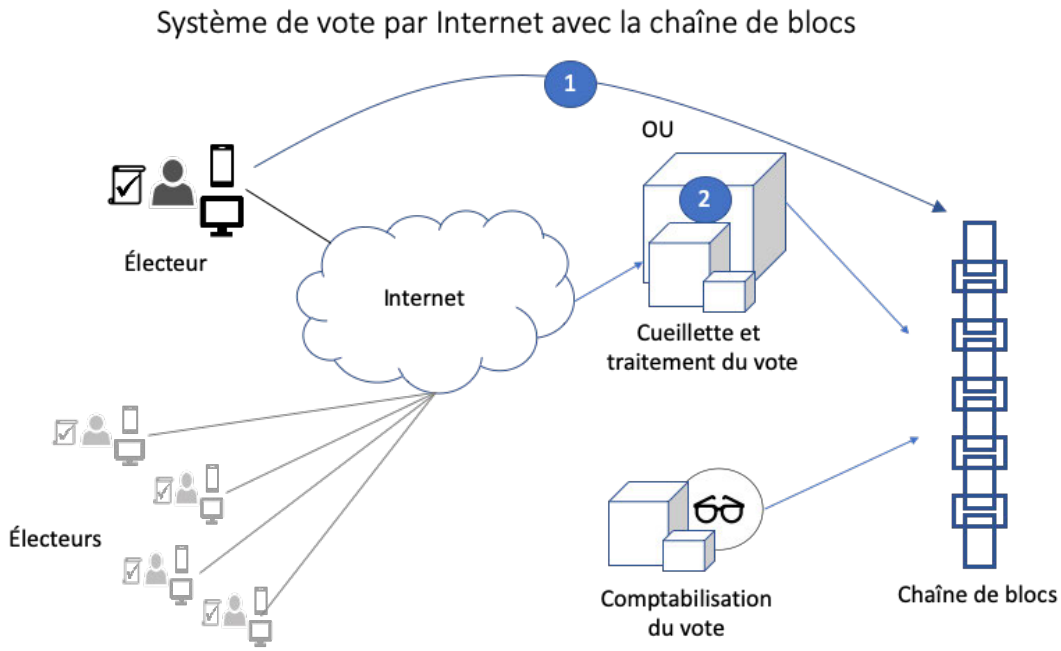
Le système de vote par Internet suit un processus séquentiel analogue au vote traditionnel. Le vote est fait par l'électeur mais il est collecté directement par un système de cueillette et sa comptabilisation est pratiquement instantanée. Les informations sont conservées dans une base de données.

Un des enjeux importants du vote par Internet est l'identification et la validation de l'identité de l'électeur. Il faut s'assurer que l'électeur est bien celui qu'il prétend être avec un niveau de confiance suffisant. Présentement, nous ne disposons pas de moyen de réaliser cette identification et cette validation. Pour réaliser cette étape, il faut un processus qui est l'équivalent de la liste des électeurs avec un processus d'inscription et de distribution d'identifiant et de droit d'accès.

Système de vote par Internet sans la chaîne de blocs



Ces dernières années, la blockchain ou la chaîne de blocs fait beaucoup parler d'elle. Elle est présentée comme la solution à beaucoup de problèmes notamment ceux qui affectent le vote électronique.



La chaine de blocs est construite pour inscrire et traiter des transactions d'une manière irrévocable et immuable dans un système distribué soit un accès ouvert (sans contrôle) ou fermée (avec un contrôle d'accès). La chaîne de blocs n'offre pas de moyens d'identification et d'authentification qui lui sont intrinsèques. Des systèmes périphériques sont nécessaires pour gérer et opérer la gestion des identités.

La chaine de blocs est lente (5 à 6 transactions par seconde). Elle nécessite une grande puissance de calcul. Cette puissance est distribuée sur plusieurs nœuds en constante communication.

En fait, elle est utile dans certaines situations particulières : les cryptomonnaies, des besoins de traçabilité de biens, les transactions de biens financiers, etc.

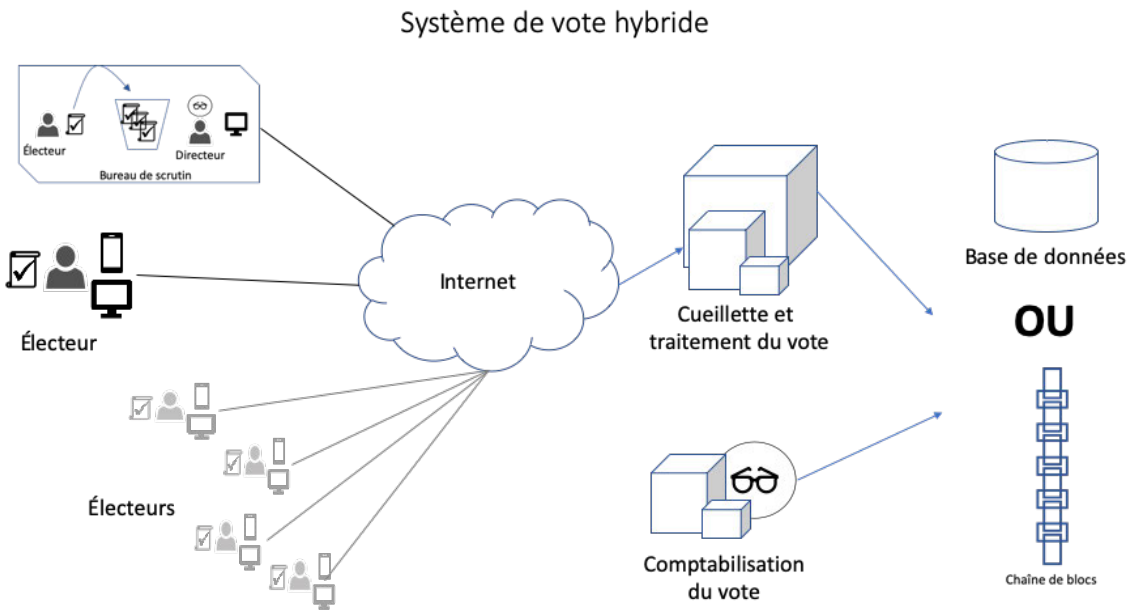
Dans le schéma du vote par Internet avec la chaîne de blocs, deux scénarios se présentent à l'électeur.

Le premier scénario (noté #1 dans le schéma) consiste à ce que l'électeur avec une application spécifique inscrive son vote directement dans la chaîne de bloc. Ce scénario impose que l'application est sécuritaire et qu'elle assure l'authentification et la dépersonnalisation du vote.

Le second scénario (noté #2) est que la chaîne de blocs remplace la base de données. La chaîne de blocs est invisible à l'électeur.

8. Système de vote hybride

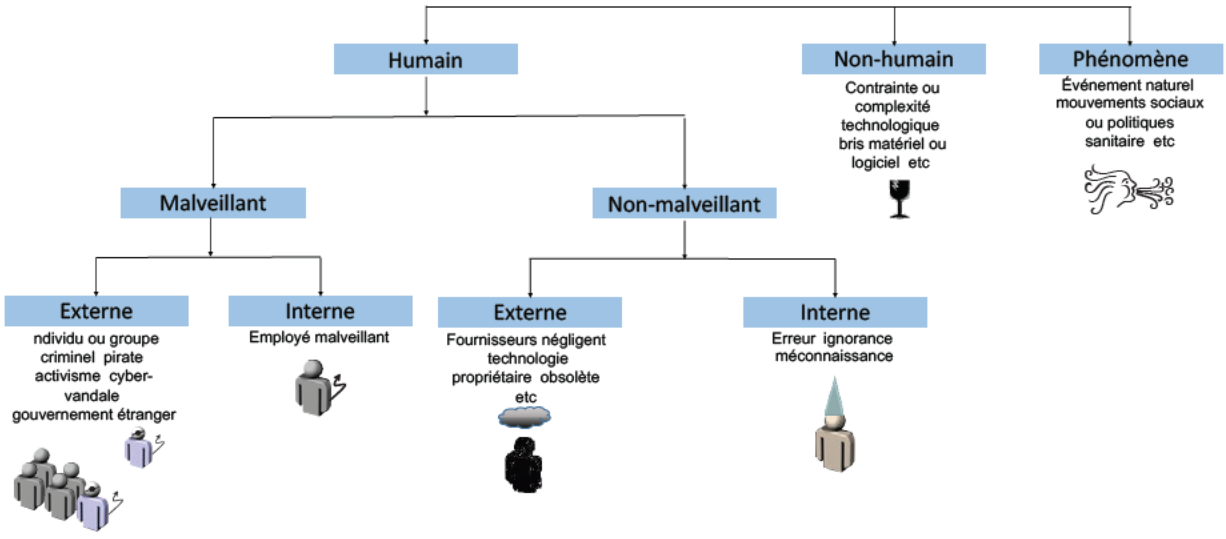
Une des prémisses d'Élection Québec est que le vote par Internet va cohabiter avec le vote traditionnel. Cette situation peut introduire des vulnérabilités. Il serait possible qu'un électeur « malveillant » tente de voter en même temps par Internet et de la façon traditionnelle. Laquelle a préséance ? Comment bloquer la seconde tentative de vote, etc.



9. Les agents du risque

Qui sont les agents qui peuvent perturber un vote démocratique ?

Ils sont nombreux et les motivations sont variées et de différents degrés. Ce schéma présente un portrait générique des agents. Ils peuvent être de nature humaine ou tout simplement un événement, un « act of god ».



10. Les menaces

Dans le monde d'Internet, les menaces sont nombreuses. Voici un palmarès des 15 menaces les plus fréquentes répertoriées par ENISA (European Union Agency for Cybersecurity). Ces menaces peuvent s'appliquer sur un système de vote par Internet et tous autres systèmes connexes qui sont exposés sur Internet.

ENISA Threat Landscape Report 2018
ETL 2018 | 1.0 | External | January 2019

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	➲	1. Malware	➲	→
2. Web Based Attacks	↑	2. Web Based Attacks	↑	→
3. Web Application Attacks	↑	3. Web Application Attacks	➲	→
4. Phishing	↑	4. Phishing	↑	→
5. Spam	↑	5. Denial of Service	↑	↑
6. Denial of Service	↑	6. Spam	➲	↓
7. Ransomware	↑	7. Botnets	↑	↑
8. Botnets	↑	8. Data Breaches	↑	↑
9. Insider threat	➲	9. Insider Threat	↓	→
10. Physical manipulation/ damage/ theft/loss	➲	10. Physical manipulation/ damage/ theft/loss	➲	→
11. Data Breaches	↑	11. Information Leakage	↑	↑
12. Identity Theft	↑	12. Identity Theft	↑	→
13. Information Leakage	↑	13. Cryptojacking	↑	NEW
14. Exploit Kits	↓	14. Ransomware	↓	↓
15. Cyber Espionage	↑	15. Cyber Espionage	↓	→

Legend: Trends: ↓ Declining, ➲ Stable, ↑ Increasing
Ranking: ↑Going up, → Same, ↓ Going down

Table 1- Overview and comparison of the current threat landscape 2018 with the one of 2017

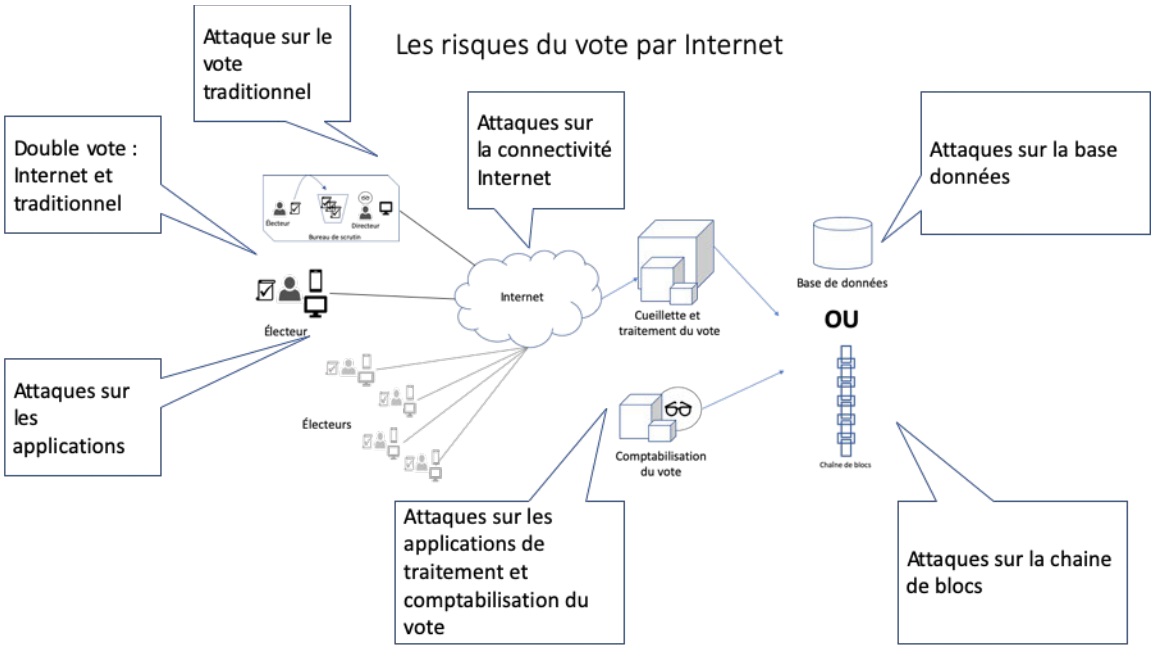
Source : https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

11. Menaces et attaques ayant pour objet le vote par Internet

Le vote par Internet comporte de grands risques, notamment en ce qui concerne le piratage (peu importe la source), la fiabilité technique, l'intégrité et la dépersonnalisation du vote et surtout le maintien de la confiance des citoyens envers le système électoral.

Les menaces identifiées dans la section précédente s'ajoutent à celles qui sont propres au vote traditionnel.

De plus, ces menaces peuvent s'exercer sur plusieurs composants qui constituent le vote par Internet. Signalons qu'un composant comme la chaîne de blocs ajoute une couche de complexité et de menaces encore mal connue.



12. Traitement des risques

Que devons faire face aux risques du vote par Internet ?

Plusieurs éléments doivent pris en compte et ceci va bien au-delà de l'objet de ce mémoire.

L'intégrité et l'anonymat du vote sont des fondamentaux à la vie démocratique. La perte d'intégrité aura pour conséquence une perte de confiance du citoyen. Cette perte de confiance pourrait conduire au chaos social. L'absence d'anonymat du vote pourrait conduire à du népotisme et des représailles de toutes sortes.

Dans les options du traitement du risque, le transfert et la conservation du risque ne sont pas acceptables. Le risque ne peut être transféré à qui ce soit. Le niveau de risque est très élevé, sa conservation ou acceptation n'est pas envisageable.

Il reste le refus et la réduction. Le refus est la solution la plus facile, elle représente le statu quo.

La réduction demandera des efforts et des mesures de contrôle importantes. Une des conditions préalables à la réduction est la mise sur œuvre d'une identité numérique dont l'utilisation sera transversale à la relation du citoyen avec l'appareil gouvernemental.

13. Constats et recommandation

Constat : Le vote par Internet n'aura pas un impact significatif sur la participation citoyenne au vote.

L'idée que le vote par Internet puisse avoir un impact sur la participation citoyenne à une élection est malheureusement erronée. L'utilisation de cette technologie a un faible impact. Le rapport « Scrutins en ligne : la voie de l'avenir pour les élections fédérales » publié par le ministère des Institutions démocratiques du gouvernement du Canada énonce ceci :

> *« Les données probantes qui servent à déterminer si le vote en ligne influence ou non la participation des électeurs varient : certaines études universitaires concluent que le vote en ligne n'a aucun effet, tandis que d'autres relèvent qu'il entraîne de faibles augmentations de l'ordre de moins de 3 % (Gerlach et Gasser, 2009; Trechsel et Vassil, 2010; Vassil et Weber, 2011) ou encore des changements plus importants pouvant être de l'ordre de 10 % (Solop, 2001; Spada et al., 2016). À l'échelle municipale au Canada, les chercheurs qui ont étudié l'adoption du vote en ligne au fil du temps concluent que le vote par Internet fait augmenter la participation électorale de 3 %, ce qui correspond à l'augmentation entraînée par les autres méthodes de vote « conviviales » … »*
>
> Extrait du rapport « Scrutins en ligne : la voie de l'avenir pour les élections fédérales », janvier 2017

Certes, ce type de mode de votation comporte des avantages : accessibilité, être disponible en tout temps et la rapidité de calcul des résultats.
Mais il ne faut pas négliger l'ensemble des moyens en mettre en place pour réaliser le vote par Internet. Le premier élément fondamental est de déterminer l'identité de l'électeur afin qu'il exerce son droit et de dissocier son vote de son identité. Le vote par Internet doit reposer sur une identité numérique du citoyen qui soit fiable, de confiance et exploitable.

Certaines des recommandations du rapport d'évaluation des nouveaux mécanismes de votation publié en 2005 par le DGEQ sont encore d'actualité.

La solution au problème de la participation citoyenne se trouve ailleurs, dans l'éducation et la culture à la vie politique.

Constat : La blockchain ou chaîne de blocs ne résout pas tous les problèmes

Les aficionados de la blockchain pour le vote par Internet affirment que les avantages de son utilisation sont :

- Les électeurs peuvent vérifier que leur vote a été exprimé comme prévu et détecter toute altération.

- Le gouvernement et les tiers indépendants peuvent confirmer les résultats du vote stockés dans la blockchain pour une meilleure transparence des élections.
- Avec les bases de données décentralisées de la chaîne de blocs, dans lesquelles les données de vote sont réparties sur de nombreux serveurs, il est plus difficile de détruire ou d'altérer les résultats en piratant un seul système central.

« Les outils Blockchain pourraient servir d'infrastructure de base pour la sélection, le suivi et le dépouillement des votes - éliminant potentiellement la nécessité de recomptages en éliminant la fraude électorale et le jeu déloyal », indique un rapport publié en août par le cabinet d'analyses technologiques CB Insights.

L'idée d'utiliser la chaîne de blocs comme une urne immuable et irrévocable peut sembler prometteuse mais la technologie de la chaîne de blocs ne résout en rien les problèmes de sécurité fondamentaux liés aux élections qui sont exposés à la section 11 de ce document.

En fait, la chaîne de blocs introduit des vulnérabilités. En guise d'exemple, un logiciel malveillant peut être installé sur le dispositif d'un électeur afin de modifier son vote avant même qu'il n'atteigne la chaîne de blocs. L'irrévocabilité de la chaîne de blocs n'offre pas l'intégrité prévue et l'électeur peut ne jamais être au fait de la modification.

L'utilisation tous azimuts de la chaîne de blocs relève de la fantaisie. La complexité, la latence des transactions, les implications légales, la surcapacité de traitement et en énergie qui sont requises pour une transaction font en sorte que cette « technologie » présente un intérêt que pour des cas très particuliers.

Constat : La cohabitation du vote traditionnel et du vote Internet engendre des enjeux d'intégrité du vote.

Ce système de vote hybride imposera une plateforme commune de gestion du vote. Le vote traditionnel devra incorporer des composants du vote par Internet.

Constat : L'absence d'une identité numérique citoyenne rend le vote Internet très difficile à gérer.

Cette absence d'une gestion de l'identité numérique du citoyen est un handicap majeur à l'utilisation du vote par Internet. Il faut adresser cette lacune avant de penser au vote par Internet.

Recommandation

Si la volonté politique ou des attentes citoyennes imposent le vote par Internet, il faudra mettre en place une identité numérique pour le citoyen. Ceci est un projet d'une grande envergure avec sa large part de risques et de défis technologiques.

Sans cette pierre d'assise, il est recommandé d'éviter le vote par Internet. Le cycle de quatre ans du vote démocratique et les efforts de maintien d'une infrastructure de vote Internet imposent des efforts importants en plus menaces sans cesse grandissantes.