Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE L'EUROPE ET DES
AFFAIRES ÉTRANGÈRES

DIRECTION GENERALE DE L'ADMINISTRATION
ET DE LA MODERNISATION

DIRECTION DES RESSOURCES HUMAINES

Sous-direction de la Formation et des Concours

Bureau des concours et examens professionnels
RH4B

CONCOURS INTERNE ET EXTERNE POUR L'ACCES A L'EMPLOI D'ATTACHE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION AU TITRE DE L'ANNEE 2019

EPREUVES ECRITES D'ADMISSIBILITE – 20 ET 21 FEVRIER 2019

NOTE DE SYNTHESE

Note de synthèse, établie à partir d'un dossier à caractère scientifique et technique de quarante pages maximum permettant de vérifier les qualités d'expression, d'analyse et de synthèse du candidat dans les domaines scientifiques et techniques, ainsi que son aptitude à dégager des conclusions et à formuler des propositions.

Durée : 3 heures
Coefficient : 2
Toute note inférieure à 6 sur 20 est éliminatoire.

SUJET

«A l'aide des documents contenus dans le dossier ci-joint, vous rédigerez une synthèse fonctionnelle et technique sur la sécurisation du vote par correspondance électronique par Internet utilisé pour les Français à l'étranger : enjeux et difficultés. »

Ce dossier comporte 40 pages + un sommaire (page de garde non comprise).

Documents proposés :

- *https://www.legifrance.gouv.fr*
  Code électoral, articles R172 et R176-3
- *https://www.legifrance.gouv.fr*
  Décret n° 2014-290 du 4 mars 2014. Article 1 et article 14
- *https://www.cairn.info/revue-le-genre-humain-2011-2-page-41.htm*
  « Le genre humain » n°51 (2011/2)
  Vote papier, vote mécanique, vote électronique (C. Enguehard)
- *https://www.cairn.info/revue-le-genre-humain-2011-2-page-63.htm*
  Revue « Le genre humain » n°51 (2011/2)
  Réflexions sur les attaques possibles contre un système de vote électronique (E. Filiol)
- *https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000023174487*
  CNIL – Délibération n°2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique
- *https://www.cnil.fr/sites/default/files/typo/document/Note_vote_internet_VD.pdf*
  Note de la CNIL – 28/05/2006
  Le vote par internet aux élections politiques, les éléments du débat
- *https://en-marche.fr/emmanuel-macron/le-programme/vie-politique-et-vie-publique*
  La République En Marche, programme d'Emmanuel Macron
- *http://www.senat.fr/notice-rapport/2018/r18-073-notice.html*
  Rapport d'information n°73 de la session ordinaire du Sénat 2018-2019 – 24/10/2018
  Réconcilier le vote et les nouvelles technologies (Jacky Deromedi et Yves Détraigne)
- *http://pagesperso.ls2n.fr/~enguehard-c/note_technique_internet_2014.pdf*
  Publication LINA - UMR CNRS 6241 – 11/07/2014
  Note technique sur le vote par internet (Chantal Enguehard)
- *https://www.alain-bensoussan.com/avocats/vote-electronique-garanties-minimales*
  Cabinet d'avocats Alain Bensoussan – 18/10/2017
  Le vote électronique requiert des garanties minimales (Emmanuel Walle)
- *https://www.nextinpact.com/news/102944-le-numero-l-anssi-defavorable-au-vote-electronique.htm*
  NextImpact.com – 18/01/2017
  Le numéro un de l'ANSSI défavorable au vote électronique (Xavier Berne)
- *https://www.lemonde.fr/pixels/article/2017/03/09/pourquoi-le-vote-electronique-des-francais-de-l-etranger-pour-les-legislatives-a-t-il-ete-annule_5092022_4408996.html*
  Lemonde.fr – 09/03/2017
  Pourquoi le vote électronique des Français de l'étranger pour les législatives a-t-il été annulé ? (Damien Leloup et Martin Untersinger)
- *https://www.nextinpact.com/news/103636-avant-suppression-vote-electronique-dysfonctionnements-pointes-lors-tests.htm*
  NextImpact.com – 11/03/2017
  Retour sur la suppression du vote électronique pour les élections législatives 2017 (Marc Rees)
- *https://www.maddyness.com/2017/06/20/tribune-vote-electronique-blockchain/*
  Maddyness.com – 20/06/2017
  Vote électronique, vers la fin des réticences grâce à la blockchain ? (Alexandre David)
- *https://www.crypto-france.com/ville-japonaise-vote-electronique-blockchain/*
  Crypto-france.com – 02/09/2018

Une ville japonaise déploie un système de vote électronique sécurisé par la technologie blockchain

- *https://www.ledevoir.com*
  Le vote par Internet, une technologie mûre
- *https://inria.fr*
  Vote électronique : le logiciel Belenios s'ouvre au grand public
- *https://www.pseudo-sciences.org*
  Le vote électronique est-il transparent, sûr, fiable ?

https://www.legifrance.gouv.fr
Code électoral – Partie réglementaire – Livre III – Section 5 : opérations de vote

Section 1 : Liste électorale
Article R172

Sont électeurs les Français établis hors de France inscrits sur les listes électorales consulaires établies, révisées et contrôlées dans les conditions prévues au chapitre Ier du décret n° 2005-1613 du 22 décembre 2005 portant application de la loi organique n° 76-97 du 31 janvier 1976 relative aux listes électorales consulaires et au vote des Français établis hors de France pour l'élection du Président de la République

Sous-section 4 : Vote par correspondance électronique
Article R176-3

I. – Pour l'élection de députés par les Français établis hors de France, les électeurs mentionnés à l'article R. 172 peuvent voter par correspondance électronique. A cette fin, il est créé un traitement automatisé de données à caractère personnel, placé sous la responsabilité du ministre de l'intérieur et du ministre des affaires étrangères.
Ce traitement automatisé garantit la séparation, dans des fichiers distincts, des données relatives aux électeurs, d'une part, et aux votes, d'autre part.
Les droits d'accès et de rectification prévus aux articles 39 et 40 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'exercent auprès du ministre des affaires étrangères. Le droit d'opposition prévu à l'article 38 de la même loi ne s'applique pas à ce traitement automatisé.

II. – Préalablement à sa mise en place, ou à toute modification substantielle de sa conception, le système de vote électronique fait l'objet d'une expertise indépendante destinée à vérifier le respect des garanties prévues par la présente sous-section.
Si, au vu de cette expertise ou des circonstances de l'élection, il apparaît que les matériels et les logiciels ne permettent pas de garantir le secret du vote et la sincérité du scrutin au sens de l'article L. 330-13, le ministre des affaires étrangères peut, par arrêté pris après avis de l'Agence nationale de la sécurité des systèmes d'information, décider de ne pas mettre en œuvre le système de vote électronique.

III. – Un arrêté conjoint du ministre de l'intérieur et du ministre des affaires étrangères précise les caractéristiques du traitement prévu au I.
Il fixe notamment :
1° Les catégories de données à caractère personnel enregistrées dans le traitement ;
2° Les modalités de l'expertise indépendante prévue au II ;

3° Les garanties entourant le recours éventuel à un prestataire technique chargé, dans le respect des obligations de sécurité résultant de la présente sous-section, de la maîtrise d'œuvre du traitement automatisé ainsi que les modalités de son intervention ;
4° Les modalités de transmission de l'identifiant et de l'authentifiant prévues à l'article R. 176-3-7 ainsi que les modalités de récupération en cas de perte par l'électeur de son identifiant ou de son authentifiant ;
5° Les conditions de mise en œuvre d'un dispositif de secours en cas de défaillance.

https://www.legifrance.gouv.fr
Décret n° 2014-290 du 4 mars 2014 portant dispositions électorales relatives à la représentation des Français établis hors de France – Titre Ier – Chapitre Ier

Section 1 : Listes électorales
Article 1

Sont électeurs les Français établis hors de France inscrits sur les listes électorales consulaires établies, révisées et contrôlées dans les conditions prévues au chapitre Ier du décret n° 2005-1613 du 22 décembre 2005 susvisé.

Section 4 – Sous-section 4 : Vote par correspondance électronique
Article 14

Les électeurs mentionnés à l'article 1er peuvent voter par correspondance électronique pour l'élection des conseillers consulaires et des délégués consulaires. A cette fin, est autorisée la mise en œuvre du traitement automatisé de données à caractère personnel prévu à l'article R. 176-3 du code électoral.
Sous réserve des dispositions de la présente sous-section, les articles R. 176-3, R. 176-3-1, R. 176-3-3 à R. 176-3-10, R. 177-5 et R. 179-1 du même code sont applicables.

Article 15

Lorsqu'il est mis en œuvre dans le cadre de l'élection des conseillers consulaires et des délégués consulaires, le traitement automatisé mentionné à l'article précédent est placé sous la responsabilité du ministre des affaires étrangères.
Les arrêtés prévus aux articles R. 176-3 et R. 176-3-1 du code électoral sont pris par le ministre des affaires étrangères.

https://www.cairn.info/revue-le-genre-humain-2011-2-page-41.htm
Revue « Le genre humain » n°51 (2011/2)
Vote papier, vote mécanique, vote électronique (C. Enguehard)

L’introduction de médias techniques au sein du processus de vote a pris de multiples formes, depuis les machines mécaniques à levier jusqu’au plus récent vote par Internet. Nous dresserons une typologie de ces différents systèmes, en particulier des systèmes de vote électroniques. L’examen des contraintes caractérisant la tenue d’élections démocratiques permettra de distinguer les difficultés rencontrées dans la représentation des objets du vote. Nous analyserons le concept de vote vérifiable, forgé pour répondre à ces difficultés, et en présenterons les limites.

Enfin, nous observerons quelques documents d'origine nationale ou supranationale : tentative d'encadrement technique, recommandations, manuel d'observation.
Le Code électoral décrit les procédures à suivre pendant une journée de vote. Il en identifie les acteurs, les objets (urne, isoloir, enveloppes, bulletins, liste des émargements) et les êtres humains (membres du bureau de vote, électeurs, délégués, scrutateurs, etc.). Ce code détaille scrupuleusement leurs rôles, en particulier en ce qui concerne l'étape délicate du dépouillement.
L'introduction de dispositifs de vote automatique a profondément modifié l'organisation des scrutins : l'expression des suffrages par les électeurs est réalisée *via* des médias techniques qui effectuent également le décompte des suffrages à la fin de la journée. D'importantes fonctionnalités (réception, vérification de la représentation interne des votes, dépouillement, etc.) sont alors exclusivement réalisées par des entités conçues et maîtrisées par des acteurs extérieurs au bureau de vote (entreprises de fabrication et de maintenance, instituts de certification) au détriment de la capacité de contrôle et de décision des membres du bureau de vote.
Il apparaît que cette modification du processus électoral n'a pas été accompagnée des études nécessaires pour en identifier les nouveaux acteurs, pour préciser leurs rôles et leurs relations avec les membres du bureau de vote, le corps électoral, les organes de contrôle, enfin pour modifier en conséquence le Code électoral.

Processus de vote

1°) Rappel historique
[...]

2°) L'environnement du vote
[...]

Environnement contrôlé
L'environnement est dit « contrôlé » lorsque le processus de vote se déroule dans un lieu identifié, en présence de personnes ayant l'autorité pour y faire régner l'ordre et veiller au respect des principes qui régissent une élection démocratique :

- unicité : chaque électeur ne peut voter qu'une seule fois par scrutin ;
- confidentialité : les électeurs expriment leur vote à l'abri du regard d'autrui et sont protégés des pressions ;
- anonymat : il est impossible de relier un bulletin de vote à l'électeur qui l'a choisi (par conséquent, les bulletins permettant l'identification des électeurs qui les ont choisis sont déclarés nuls) ;
- transparence : toutes les étapes du processus de vote peuvent être contrôlées par les scrutateurs ;
- sincérité : le décompte des bulletins permet de proclamer le gagnant choisi par l'ensemble des suffrages qui ont été exprimés.

Environnement non contrôlé
L'environnement est dit « non contrôlé » lorsque le processus de vote se déroule hors d'un lieu contrôlé et échappe à la surveillance des autorités compétentes. Il s'agit du vote par correspondance (vote à distance). Dans la majorité des cas, le principe de confidentialité n'est plus respecté, et la transparence est amoindrie, car les suffrages voyagent dans un canal de transmission qui échappe à la surveillance des scrutateurs.

3°) Les acteurs du vote moderne

[...]

Environnement contrôlé
Divers objets sont indispensables au processus de vote lorsqu'il se déroule au sein d'un lieu de vote identifié et sous contrôle : bulletins de vote, urne, isoloirs, enveloppes, registre des émargements, procès-verbaux des bureaux de vote, stylos, exemplaire du Code électoral lorsqu'il s'agit de vote politique, etc. Évidemment, le processus fait intervenir les électeurs, mais aussi les membres du bureau ; des scrutateurs peuvent également être présents ainsi que des représentants des organisateurs du vote (préfecture, Conseil d'État par exemple).
Tous les objets intervenant dans le processus électoral sont inertes. Les transformations qu'ils subissent sont le fait d'acteurs humains et restent sous leur contrôle : les bulletins de vote enregistrent les votes ; l'isoloir et les enveloppes protègent la confidentialité des électeurs ; l'urne conserve les bulletins. Les membres du bureau de vote (président, assesseurs) veillent au respect de la procédure ; ils contrôlent le droit à voter, font signer le registre des émargements, surveillent l'unicité du vote (une seule enveloppe par électeur) et l'intégrité de l'urne, ils interdisent les éventuelles pressions par l'usage obligatoire de l'isoloir et le respect des procédures. Le président du bureau de vote assure la police du lieu.

En environnement non contrôlé
Les électeurs expriment leur suffrage depuis n'importe quel lieu. Il est nécessaire qu'ils disposent d'un canal de transmission afin de faire parvenir leurs suffrages au bureau de vote qui les stocke, théoriquement de manière sécurisée. Cet envoi est réalisé selon un système de deux enveloppes afin de permettre la mise à jour du registre des émargements sans violer l'anonymat des votes.
L'expression du vote hors d'un environnement contrôlé expose l'électeur à d'éventuelles pressions, et la transmission des bulletins par courrier postal échappe à tout contrôle de la part des scrutateurs ou du bureau de vote. De par son caractère asynchrone et sa mise en œuvre en environnement non contrôlé, le vote par correspondance est donc caractérisé par une faible capacité à observer les éventuelles atteintes aux principes régissant une élection démocratique.

[…]

Nouveaux acteurs

[…]

3°) Expression du vote
L'expression du vote est le moment où l'électeur effectue son choix et l'exprime grâce au dispositif dont il dispose.
Dans la configuration du vote moderne, les électeurs expriment leur vote en choisissant eux-mêmes un bulletin parmi ceux qui leur sont proposés. Cette étape se déroule sous le contrôle personnel de chaque électeur. L'obligation de passer par un isoloir et d'utiliser une enveloppe participe au respect de la confidentialité et protège l'électeur contre les éventuelles pressions. Les membres du bureau de vote (président, assesseurs) veillent au respect de la procédure et de l'unicité du vote (une seule enveloppe par électeur).
De nombreux dispositifs de vote automatique prennent en charge l'expression des choix émis par les électeurs. Les électeurs ne votent plus en choisissant eux-mêmes un bulletin parmi ceux qui leur sont proposés, mais en effectuant ce choix *via* un média technique : appui sur un bouton, clic de souris, saisie d'un code sur un téléphone, etc. Deux cas doivent être distingués selon le caractère matérialisé ou dématérialisé des choix des électeurs :

- dématérialisation des bulletins de vote : l'usage de dispositifs dématérialisant les bulletins fait disparaître les bulletins de vote matérialisés, les enveloppes ainsi que les urnes. Le dispositif de vote interprète les actions réalisées par un électeur pour produire une représentation interne au dispositif. Cette représentation interne est connue des concepteurs du dispositif, mais inconnue de l'électeur et des membres du bureau de vote ; elle échappe donc à leur contrôle. L'électeur ne peut savoir si l'enregistrement interne est conforme au choix qu'il a exprimé ;
- matérialisation des bulletins de vote : certains dispositifs de vote cohabitent avec l'usage de bulletins de vote. Deux configurations doivent être distinguées selon que l'expression du vote par les électeurs est directe ou indirecte. L'expression du vote est dite directe lorsque l'électeur produit directement son bulletin de vote, par exemple en cochant des cases ou en collant des étiquettes sur sa carte de vote (vote par correspondance hybride). L'incarnation du choix de l'électeur sur son bulletin de vote est alors sous son seul contrôle, l'électeur est la seule source d'erreur.

L'expression du vote est dite indirecte lorsque l'électeur doit utiliser un média pour produire son bulletin de vote. Ce sont les cas faisant intervenir des machines avec cartes perforées (États-Unis) ou des ordinateurs de vote avec trace papier (États-Unis, Venezuela). Le bulletin est alors exprimé *via* un intermédiaire mécanique (poinçon) ou électronique (ordinateurs de vote avec trace papier) susceptible d'éviter des erreurs à l'électeur (par exemple, cocher davantage de cases que ce qui est autorisé) ; mais cet intermédiaire est aussi une source potentielle d'erreur. Il est parfois prévu que l'électeur ait la possibilité de vérifier la justesse du bulletin ainsi produit. La procédure de vote se complexifie alors, car l'électeur peut dénoncer son bulletin comme non conforme à son choix – mais il ne doit pas trahir le secret du vote et n'est donc pas en mesure d'apporter la preuve du dysfonctionnement qu'il révèle. Dans ce cas, les procédures légales autorisent l'électeur à produire un nouveau bulletin de vote remplaçant le précédent ; cependant, en l'absence de possibilité de constat du dysfonctionnement par le bureau de vote, le dispositif de vote n'est pas déclaré en erreur et reste en usage. Il faut noter que cette étape de vérification du bulletin est toujours facultative, l'électeur pouvant s'y soustraire ou être peu performant. Des études d'accessibilité ont montré que la plupart des électeurs négligent cette vérification.

https://www.cairn.info/revue-le-genre-humain-2011-2-page-63.htm
Revue « Le genre humain » n°51 (2011/2)
Réflexions sur les attaques possibles contre un système de vote électronique (Eric Filiol)

Les attaques possibles contre les systèmes de vote électronique ont été répertoriées et, pour certaines d'entre elles, testées (dans le cas du vote par Internet). Techniquement, ces attaques sont assez faciles à porter et, contrairement aux idées reçues, il n'est pas nécessaire de les mener à grande échelle pour altérer un vote.
Nous montrerons que les risques techniques liés à l'utilisation de tels systèmes surpassent de loin les quelques avantages – souvent illusoires – que l'on espère pour ces derniers. Ces risques existeront toujours. Leur nature réelle et l'ampleur des attaques possibles sont perçues de manière erronée.
Nous étudierons essentiellement le cas des systèmes de vote *via* Internet (dénommés contexte principal ou cas I, aujourd'hui utilisés pour les élections professionnelles ou locales) : ils sont architecturés autour d'un ou de plusieurs serveurs (assimilables aux urnes classiques) et de postes clients (assimilables aux bulletins papier). Ce poste client est un environnement informatique classique avec un système d'exploitation propriétaire. Toutefois, dans un souci d'exhaustivité, nous envisagerons également le cas (contexte secondaire ou cas II) des « machines à voter » de type automate dédié (par exemple, celles de la marque Nedap). Le

plus souvent, ces systèmes dédiés reposent néanmoins sur de l'électronique et des environnements classiques (ainsi le processeur Motorola 68000).

Machine à voter dans le cadre de la réglementation actuelle

[…]

Attaques des systèmes électroniques de vote

D'une manière générale, les attaques envisageables – transparentes pour le votant et le gestionnaire du système – contre un système automatisé de vote sont :

- le changement automatique (à la volée) de votes ;
- le changement aléatoire (à la volée) de votes. Il est équivalent à une attaque de type « déni de service » distribué ou non (DDoS ou DoS ;
- l'annulation de votes (votes non validés) ;
- l'usurpation d'identité (vol de certificats cryptographiques) et le détournement de votes ;
- le fait de rendre publics des votes.

Même si ce n'est pas spécifique au domaine du vote automatisé, il est également nécessaire de prendre en compte les attaques classiques envers la disponibilité du système. En effet, le rendre inopérant au moment crucial (la journée de vote) a pour résultat une annulation de ce dernier. Il est également important d'identifier les attaques non conventionnelles qui exploitent une faille ou une limitation dans l'environnement de ces machines.

Les attaquants ne sont pas ceux que l'on imagine le plus souvent

C'est sans doute à propos de la typologie des attaquants que la vision commune est la plus fausse. L'attaquant type pour le grand public et les candidats est l'adversaire ou le camp politique adverse, dont le but est le détournement de bulletins à son profit. C'est malheureusement une vision à courte vue qui ne prend en compte qu'une « menace » interne et peut-être réduite. La fraude a toujours existé. Ce ne sont pas les systèmes automatisés qui l'empêcheront. Ils la rendront juste plus difficile à détecter. En revanche, cette automatisation va permettre à des attaquants extérieurs d'agir.

Les attaquants sont de deux types :

- internes (nationaux). Cela concerne essentiellement des tentatives de manipulation des élections en faveur d'un parti, et un activisme anti-État (mouvements anarchistes, altermondialistes…) ;
- externes. Il s'agit là d'attaquants extra-nationaux dont le but est de perturber le processus démocratique et de remettre en cause la légitimité du pouvoir et la stabilité du pays. Il peut s'agir aussi d'actes terroristes à l'encontre de pays tiers dans un but économique ou politique (déstabilisation, ingérence…).

Attaques de systèmes de type I

Il est très facile dans ce contexte de modifier les résultats d'une élection et d'attaquer les systèmes de vote. Des travaux récemment publiés montrent techniquement comment réaliser de manière opérationnelle toutes les attaques précédemment répertoriées. Ces attaques consistent en l'utilisation et l'installation de navigateurs (Firefox, Internet Explorer) par des virus de *plug-in* malveillants. Cela permet de contourner *tous* les mécanismes cryptologiques en place.

Ces travaux (code source des attaques à l'appui) démontrent clairement que *tout* système de vote électronique de type I est facile à attaquer grâce à un (simple) code malveillant. Ce

dernier, agissant au niveau le plus bas, sera capable de toujours contourner n'importe quel type de mécanisme cryptologique censé assurer la sécurité du vote.
Ce type de code malveillant peut être déployé de multiples manières. Toutefois, le cas le plus simple et le plus anodin reste l'utilisation d'un simple document bureautique (formats DOC ou PDF) contenant la charge active et envoyé aux votants *via* une opération de *mailing*, avant le vote.
Il est indispensable de rappeler qu'aucun antivirus n'est capable de stopper une telle attaque dans le cas d'un code malveillant inconnu. De plus, comme l'a démontré Fred Cohen en 1986, la détection antivirale est un problème sans solution (problème dit « indécidable »). Cela veut dire que l'on peut toujours contourner un antivirus.
Une attaque contre les serveurs de vote est encore plus efficace et d'une portée opérationnelle plus grande. Les serveurs jouent le rôle des urnes classiques. Une attaque contre ces serveurs est donc plus rentable qu'une attaque contre chacun des bulletins (les postes clients traités dans le paragraphe précédent). D'un point de vue technique, les attaques sont rigoureusement les mêmes (utilisation de codes malveillants).
Enfin, il ne faut pas oublier le cas des « trappes », ou fonctions cachées, dans les logiciels de vote eux-mêmes. Elles peuvent être implantées soit au moment de la programmation, soit au moment de la compilation, ce qui implique que le seul moyen de les détecter est d'effectuer, sur chaque client suspect, une phase de *reverse engineering* et ensuite d'auditer le code produit. Il s'agit d'une procédure longue et coûteuse, si tant est qu'elle soit légalement possible (autorisation de l'éditeur). Il suffit d'introduire de telles trappes dans un nombre limité de machines pour mener une attaque (voir *infra*, « Ampleur nécessaire d'une attaque ») ou pour, tout simplement, porter atteinte dans la confiance placée dans le système de vote lui-même.

Attaques de systèmes de type II
[…]

Des technologies non prouvées pour des scrutins électroniques vulnérables à des attaques d'ampleur même limitée

D'une manière plus générale, il est important de considérer les technologies mises en œuvre dans tous les systèmes automatisés de vote. Les systèmes de vote électronique (types I et II) reposent sur des mécanismes d'authentification, d'intégrité et de signature électronique, autrement dit sur des « primitives », ou protocoles cryptographiques complexes, tous relevant de la cryptologie dite asymétrique (plus connue sous le terme impropre de « cryptologie à clé publique » et reposant sur la notion de certificat cryptographique. [...]
Dans l'esprit de la plupart des gens, une attaque contre un système automatisé de vote requiert des attaques de grande ampleur. Elle nécessiterait d'altérer à la fois un grand nombre de votes et un grand nombre de machines de vote, et ce, simultanément. En fait, cela est faux si l'on tient compte de la nature même du processus de vote et des modélisations statistiques que l'on peut en faire. Dans le cas de résultats serrés ou de scrutins proportionnels, la modification d'un nombre (très) réduit de votes est statistiquement suffisante. Mener une telle attaque est donc facile d'un point de vue opérationnel. Il suffit de cibler quelques machines !

Conclusion

Que penser finalement de la sécurité des systèmes automatisés de vote, et donc de la confiance que nous pouvons leur accorder ? Il existe un très (trop) grand nombre

d’incertitudes et une absence de garanties techniques (si tant est qu’elles existent). Ces systèmes sont propriétaires et fermés. Leur analyse, en termes de protection de la propriété intellectuelle et du secret industriel, est sinon impossible, du moins extrêmement délicate. Même si homologuer un système était une chose faisable, cela ne garantirait que le procédé et non les instances de ce procédé (chaque machine prise séparément) : il resterait toujours la possibilité alors d’introduire des machines « trappées » parmi les machines utilisées.
Le plus préoccupant est que ces systèmes dépendent de technologies non prouvées et/ou impossibles à sécuriser. De plus, souvent produites par des sociétés étrangères, elles nous confrontent à des problèmes de souveraineté, au moins sur le plan numérique. D’autres pays ont eu le courage de prendre des décisions assez radicales :

- en mai 2008, les Pays-Bas ont voté l’abandon définitif du vote électronique ;
- en 2009, le gouvernement brésilien a organisé un concours d’attaque de machines à voter pour se faire une idée plus précise de la sécurité de ces systèmes. La faible participation – les hackers craignaient qu’il ne s’agisse là d’une opération destinée en réalité à les identifier et à les recenser – n’a pas permis de faire avancer le débat.

L’approche du Brésil est intéressante et probablement la plus rationnelle dans un débat éminemment passionnel. Sans systèmes totalement ouverts et susceptibles d’être audités en permanence, et ce, de manière active, sans restriction aucune, il est illusoire d’espérer susciter la confiance dans de tels systèmes.
Dans un domaine aussi sensible que le vote – droit fondamental souvent acquis récemment et de haute lutte –, c’est précisément le problème de la confiance qui est en jeu : ne pas pouvoir prouver la sécurité de ces systèmes est déjà une excellente raison de douter de ces derniers. Certes, leurs défenseurs arguent souvent du fait que le système manuel n’empêche pas lui non plus les fraudes. Cela est vrai. Mais outre le fait que le vote manuel reste centré sur l’humain, l’acteur même de la vie de la cité, pourquoi préférer une copie imparfaite de l’imperfection alors que nous pouvons nous contenter de l’original ? La question est de savoir si l’on a réellement besoin du vote électronique. Pourquoi remplacer un système excellent (vote traditionnel) qui a jusque-là donné entière satisfaction par un système incertain (vote électronique) ?

https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000023174487
CNIL – Délibération n°2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique

La Commission nationale de l'informatique et des libertés,
[…]
Après avoir entendu Mme Isabelle Falque-Pierrotin, vice-présidente, en son rapport et Mme Elisabeth Rolin, commissaire du Gouvernement, en ses observations,
Formule les observations suivantes :

Alors que le vote électronique commençait seulement à s'implanter en 2003, lors de l'adoption de la première recommandation de la CNIL, la commission constate aujourd'hui que les systèmes de vote électronique sur place ou à distance se sont développés et s'étendent désormais à un nombre croissant d'opérations de vote et de types de vote.
La commission souligne que le recours à de tels systèmes doit s'inscrire dans le respect des principes fondamentaux qui commandent les opérations électorales : le secret du scrutin sauf pour les scrutins publics, le caractère personnel, libre et anonyme du vote, la sincérité des opérations électorales, la surveillance effective du vote et le contrôle a posteriori par le juge de l'élection. Ces systèmes de vote électronique doivent également respecter les prescriptions des textes constitutionnels, législatifs et réglementaires en vigueur.
La commission constate que si l'application principale du vote électronique réside dans les élections professionnelles (comité d'entreprise et représentants du personnel), celui-ci se développe également pour les assemblées générales, conseil de surveillance, élection des représentants de professions réglementées et, depuis 2003, pour des élections à caractère politique. De plus, en 2009, pour la première fois, la possibilité de recourir au vote électronique pour une élection nationale, au suffrage universel direct, a été introduite par l'ordonnance n° 2009-936 du 29 juillet 2009 relative à l'élection de députés par les Français établis hors de France.
Devant l'extension du vote par internet à tous types d'élections, la commission souhaite rappeler que le vote électronique présente des difficultés accrues au regard des principes susmentionnés pour les personnes chargées d'organiser le scrutin et celles chargées d'en vérifier le déroulement, principalement à cause de la technicité importante des solutions mises en œuvre. Au cours des travaux que la commission a menés depuis 2003, elle a, en effet, pu constater que les systèmes de vote existants ne fournissaient pas encore toutes les garanties exigées par les textes légaux. Dès lors et en particulier, compte tenu des éléments précités, la commission est réservée quant à l'utilisation de dispositifs de vote électronique pour des élections politiques.
[…]
Compte tenu de ces observations préalables, la commission émet la recommandation suivante :

I. — Sur les exigences préalables à la mise en œuvre des systèmes de vote électronique
1. L'expertise du système de vote électronique

Tout système de vote électronique doit faire l'objet d'une expertise indépendante.
L'expertise doit couvrir l'intégralité du dispositif installé avant le scrutin (logiciel, serveur, etc.), l'utilisation du système de vote durant le scrutin et les étapes postérieures au vote (dépouillement, archivage, etc.).
L'expertise doit porter sur l'ensemble des mesures décrites dans la présente délibération, et notamment sur :

- le code source du logiciel, y compris dans le cas de l'utilisation d'un logiciel libre ;
- les mécanismes de scellement utilisés aux différentes étapes du scrutin (voir ci-après) ;
- le système informatique sur lequel le vote va se dérouler, et notamment le fait que le scrutin se déroulera sur un système isolé ;
- les échanges réseau ;
- les mécanismes de chiffrement utilisé, notamment pour le chiffrement du bulletin de vote sur le poste de l'électeur.

L'expertise doit être réalisée par un expert indépendant, c'est-à-dire qu'il devra répondre aux critères suivants :

- être un informaticien spécialisé dans la sécurité ;
- ne pas avoir d'intérêt financier dans la société qui a créé la solution de vote à expertiser, ni dans la société responsable de traitement qui a décidé d'utiliser la solution de vote ;
- posséder une expérience dans l'analyse des systèmes de vote, si possible en ayant expertisé les systèmes de vote électronique d'au moins deux prestataires différents ;
- avoir suivi la formation délivrée par la CNIL sur le vote électronique.

Le rapport d'expertise doit être remis au responsable de traitement. Les prestataires de solutions de vote électronique doivent, par ailleurs, transmettre à la CNIL les rapports d'expertise correspondant à la première version et aux évolutions substantielles de la solution de vote mise en place.
Si l'expertise peut couvrir un champ plus large que celui de la présente recommandation, le rapport d'expertise fourni au responsable de traitement doit comporter une partie spécifique présentant l'évaluation du dispositif au regard des différents points de la recommandation.
L'expert doit fournir un moyen technique permettant de vérifier a posteriori que les différents composants logiciels sur lesquels a porté l'expertise n'ont pas été modifiés sur le système utilisé durant le scrutin. La méthode et les moyens permettant d'effectuer cette vérification doivent être dé*crits dans le rapport d'expertise*.

2. La séparation des données nominatives des électeurs et des votes

Le dispositif doit garantir que l'identité de l'électeur ne peut pas être mise en relation avec l'expression de son vote, et cela à tout moment du processus de vote, y compris après le dépouillement.

3. Les sécurités informatiques

Il convient que toutes les mesures physiques (contrôle d'accès, détermination précise des personnes habilitées à intervenir...) et logiques (firewall, protection d'accès aux applicatifs...) soient prises, tant au niveau des serveurs du dispositif que sur les postes accessibles au public, afin de garantir la sécurité des données personnelles et du système de vote dans son ensemble.
Les algorithmes de chiffrement et de signature électronique doivent, dans tous les cas, être des algorithmes publics réputés forts et doivent, si les élections sont mises en place par une autorité administrative, répondre aux exigences prévues dans le référentiel général de sécurité (RGS).
Si un système matériel permet d'héberger plusieurs scrutins, il doit mettre en œuvre une solution technique (par exemple par une virtualisation des systèmes) permettant d'isoler chaque scrutin sur un système informatique distinct de manière à garantir que chaque système soit indépendant et se comporte de manière autonome.

4. Le scellement du dispositif de vote électronique

Avant le début du scrutin, les systèmes de vote électronique utilisés, la liste des candidats et la liste des électeurs doivent faire l'objet d'un scellement, c'est-à-dire d'un procédé permettant de déceler toute modification du système. Avant cette procédure de scellement, il est vérifié que les modules ayant fait l'objet d'une expertise n'ont pas été modifiés. La liste d'émargement et l'urne électronique doivent faire l'objet d'un procédé garantissant leur intégrité durant le vote, c'est-à-dire assurant qu'ils ne peuvent respectivement être modifiés que par l'ajout d'un bulletin et d'un émargement, dont l'intégrité est assurée, d'un électeur authentifié de manière non frauduleuse. Ce procédé doit déceler toute autre modification du système. Après la clôture du vote, la liste d'émargement et l'urne électronique doivent être scellées.
Les procédés de scellement doivent eux-mêmes utiliser des algorithmes publics réputés forts et, le cas échéant, respecter les recommandations du référentiel général de sécurité. La vérification des scellements doit pouvoir se faire à tout moment, y compris durant le déroulement du scrutin. Le bureau de vote doit disposer d'outils dont l'utilisation ne requiert pas l'intervention du prestataire pour procéder à la vérification du scellement, par exemple par une prise d'empreinte numérique.

5. L'existence d'une solution de secours

Tout système de vote électronique doit comporter un dispositif de secours susceptible de prendre le relais en cas de panne du système principal et offrant les mêmes garanties et les mêmes caractéristiques.

6. La surveillance effective du scrutin

La mise en œuvre du système de vote électronique doit être opérée sous le contrôle effectif, tant au niveau des moyens informatiques centraux que de ceux, éventuellement, déployés sur place, de représentants de l'organisme mettant en place le vote ou d'experts désignés par lui. Dès lors, il importe que toutes les mesures soient prises pour leur permettre de vérifier l'effectivité des dispositifs de sécurité prévus pour assurer le secret du vote et, en particulier, les mesures prises pour :

- garantir la confidentialité du fichier des électeurs comportant les éléments d'authentification ;
- garantir le chiffrement ininterrompu des bulletins de vote et leur conservation dans un traitement distinct de celui mis en œuvre pour assurer la tenue du fichier des électeurs ;
- assurer la conservation des différents supports d'information pendant et après le déroulement du scrutin.

Toutes les facilités doivent être accordées aux membres du bureau de vote et aux délégués des candidats, s'ils le souhaitent, pour pouvoir assurer une surveillance effective de l'ensemble des opérations électorales et, en particulier, de la préparation du scrutin, du vote, de l'émargement et du dépouillement.

A ce titre et afin de garantir un contrôle effectif des opérations électorales, le prestataire technique doit mettre à disposition des représentants de l'organisme responsable du traitement, des experts, des membres du bureau de vote, des délégués des candidats et des scrutateurs tous documents utiles et assurer une formation de ces personnes au fonctionnement du dispositif de vote électronique.

7. La localisation du système informatique central

Il paraît hautement souhaitable que les serveurs et les autres moyens informatiques centraux du système de vote électronique soient localisés sur le territoire national afin de permettre un contrôle effectif de ces opérations par les membres du bureau de vote et les délégués ainsi que l'intervention, le cas échéant, des autorités nationales compétentes.

II. — Sur le scrutin
A. — Sur les opérations précédant l'ouverture du scrutin
1. La confidentialité des données

Les fichiers nominatifs des électeurs constitués aux fins d'établir la liste électorale, d'adresser le matériel de vote et de réaliser les émargements ne peuvent être utilisés qu'aux fins précitées et ne peuvent être divulgués sous peine des sanctions pénales encourues au titre des articles 226-17 et 226-21 du code pénal.
La confidentialité des données est également opposable aux techniciens en charge de la gestion ou de la maintenance du système informatique.
Les fichiers comportant les éléments d'authentification des électeurs, les clés de chiffrement/déchiffrement et le contenu de l'urne ne doivent pas être accessibles, de même que la liste d'émargement, sauf aux fins de contrôle de l'effectivité de l'émargement des électeurs.
En cas de recours à un prestataire extérieur, celui-ci doit s'engager contractuellement à respecter ces dispositions par la signature d'une clause de confidentialité et de sécurité et à fournir le descriptif détaillé du dispositif technique mis en œuvre pour assurer cette confidentialité. Le prestataire doit également s'engager à restituer les fichiers restant en sa possession à l'issue des opérations électorales et à détruire toutes les copies totales ou partielles qu'il aurait été amené à effectuer sur quelque support que ce soit.
Le prestataire peut recevoir automatiquement des informations techniques sur le fonctionnement du système de vote pendant tout le déroulement du scrutin. Le prestataire ne doit intervenir sur le système de vote qu'en cas de dysfonctionnement informatique résultant d'une attaque du système par un tiers, d'une infection virale, d'une défaillance technique ou d'une altération des données. Un dispositif technique doit garantir que le bureau de vote est informé automatiquement et immédiatement de tout accès par le prestataire à la plate-forme de vote. Le prestataire doit informer le bureau de vote de toutes les mesures prises pour remédier au dysfonctionnement constaté. Le système de vote doit comprendre un module permettant la remontée automatique de cette information au bureau de vote.
Toutes les actions effectuées sur le serveur de vote ainsi que celles concernant le déroulement du scrutin doivent faire l'objet d'une journalisation. L'intégrité de cette journalisation doit être garantie à tout moment par un procédé cryptographique.
Le bureau de vote, quant à lui, a compétence pour prendre toute mesure d'information et de sauvegarde, et notamment pour décider la suspension des opérations de vote. Le système de vote doit permettre d'informer les électeurs de cette éventuelle décision.

2. Les procédés d'authentification de l'électeur

Le système de vote doit prévoir l'authentification des personnes autorisées à accéder au système pour exprimer leur vote. Il doit garantir la confidentialité des moyens fournis à l'électeur pour cet accès et prendre toutes précautions utiles afin d'éviter qu'une personne non autorisée ne puisse se substituer frauduleusement à l'électeur.

La commission estime qu'une authentification de l'électeur sur la base d'un certificat électronique constitue la solution la plus satisfaisante en l'état de la technique. Le certificat électronique doit être choisi et utilisé conformément aux préconisations du RGS.
Dans le cas du recours à un dispositif biométrique pour l'authentification, le responsable de traitement doit respecter les formalités imposées par la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.
A défaut de recourir aux solutions précitées, dans le cas de la génération d'identifiants et de mots de passe à partir de la liste électorale, le fichier ainsi créé doit faire l'objet d'un chiffrement. Les modalités de génération et d'envoi des codes personnels doivent être conçues de façon à garantir leur confidentialité et, en particulier, que les divers prestataires éventuels ne puissent pas en prendre connaissance.
Dans le cas où le vote s'opérerait par l'enregistrement d'un identifiant permanent apposé sur une carte ou tout autre document ainsi qu'un mot de passe envoyé à chaque électeur, la génération de ces identifiants et mots de passe doit se faire dans les mêmes conditions de sécurité que celles énumérées ci-dessus. Il en va de même de l'envoi du mot de passe.
L'authentification de l'électeur peut être renforcée par un dispositif de type défi/réponse — c'est-à-dire l'envoi par le serveur d'authentification d'une question dont l'électeur est seul à connaître la réponse — ou par l'envoi d'un code par SMS sur le téléphone personnel de l'électeur.
En cas de perte ou de vol de ses moyens d'authentification, une procédure doit permettre à l'électeur d'effectuer son vote et de rendre les moyens d'authentification perdus ou volés inutilisables.
Le vote doit être accessible à tous les systèmes d'exploitation et tous les navigateurs utilisés par les électeurs. A défaut de mettre à disposition du matériel de vote accessible à tous, une procédure manuelle doit être prévue.

3. L'information des électeurs

Il convient de fournir aux électeurs en temps utile une note explicative détaillant clairement les opérations de vote ainsi que le fonctionnement général du système de vote électronique.

4. Le contrôle du système avant l'ouverture du scrutin

Un contrôle du système de vote électronique doit être organisé avant l'ouverture du scrutin et en présence des scrutateurs afin de constater la présence des différents scellements, le bon fonctionnement des machines, que la liste d'émargement est vierge et que l'urne électronique destinée à recevoir les votes est bien vide.

5. Les clés de chiffrement

La génération des clés destinées à permettre le déchiffrement des bulletins de vote doit être publique et se dérouler avant l'ouverture du scrutin. Cette procédure doit être conçue de manière à prouver de façon irréfutable que seuls le président du bureau et ses assesseurs prennent connaissance de ces clés, à l'exclusion de toute autre personne y compris les personnels techniques chargés du déploiement du système de vote. La commission estime que le nombre de clés de chiffrement doit être au minimum de trois, la combinaison d'au moins deux de ces clés étant indispensable pour permettre le dépouillement.
Le système de vote doit garantir que des résultats partiels (hormis le nombre de votants) ne seront pas accessibles durant le déroulement du scrutin.

B. — Sur le déroulement du vote

1. Le vote

Les heures d'ouverture et de fermeture du scrutin électronique doivent pouvoir être contrôlées par les membres du bureau de vote et les personnes désignées ou habilitées pour assurer le contrôle des opérations électorales.

Pour se connecter à distance ou sur place au système de vote, l'électeur doit s'authentifier conformément à la présente recommandation. Au cours de cette procédure, le serveur de vote vérifie l'identité de l'électeur et que celui-ci est bien autorisé à voter. Dans ce cas, il accède aux listes ou aux candidats officiellement retenus et dans l'ordre officiel. Le vote blanc doit être prévu lorsque la loi l'autorise.

L'électeur doit pouvoir choisir une liste, un candidat ou un vote blanc de façon à ce que ce choix apparaisse clairement à l'écran, indépendamment de toute autre information. Il doit avoir la possibilité de revenir sur ce choix. Il valide ensuite son choix et cette opération déclenche l'envoi du bulletin de vote dématérialisé vers le serveur des votes.

L'électeur doit recevoir immédiatement confirmation de son vote et avoir la possibilité de conserver une trace de cette confirmation.

2. Le chiffrement du bulletin de vote

Le bulletin de vote doit être chiffré par un algorithme public réputé fort dès son émission sur le poste de l'électeur et être stocké dans l'urne, en vue du dépouillement, sans avoir été déchiffré à aucun moment, même de manière transitoire. La liaison entre le terminal de vote de l'électeur et le serveur des votes doit faire l'objet d'un chiffrement distinct de celui qui s'applique au bulletin pour assurer la sécurité tant du procédé d'authentification de l'électeur que la confidentialité de son vote. La mise en place du canal de communication doit intégrer une authentification du serveur de vote.

Par ailleurs, le stockage du bulletin dans l'urne ne doit pas comporter d'horodatage, pour éviter tout rapprochement avec la liste d'émargement.

3. L'émargement

L'émargement doit se faire dès la validation du vote de façon à ce qu'un autre vote ne puisse intervenir à partir des éléments d'authentification de l'électeur déjà utilisés. L'émargement comporte un horodatage. Cette liste, aux fins de contrôle de l'émargement, ainsi que le compteur des votes ne doivent être accessibles qu'aux membres du bureau de vote et aux personnes autorisées.

4. Le dépouillement

La fermeture du scrutin doit immédiatement être suivie d'une phase de scellement de l'urne et de la liste d'émargement, phase qui précède le dépouillement. L'ensemble des informations nécessaires à un éventuel contrôle a posteriori doit également être recueilli lors de cette phase. Ces éléments sont enregistrés sur un support scellé, non réinscriptible et probant.

Le dépouillement est actionné par les clés de déchiffrement, remises aux membres du bureau dûment désignés au moment de la génération de ces clés. Les membres du bureau doivent actionner publiquement le processus de dépouillement.

Les décomptes des voix par candidat ou liste de l'élection doivent apparaître lisiblement à l'écran et faire l'objet d'une édition sécurisée, c'est-à-dire d'un mécanisme garantissant que l'affichage et l'impression des résultats correspondent au décompte de l'urne, pour être portés

au procès-verbal de l'élection. Le cas échéant, l'envoi des résultats à un bureau centralisateur à distance doit s'effectuer par une liaison sécurisée empêchant toute captation ou modification des résultats.
Le système de vote électronique doit être bloqué après le dépouillement de sorte qu'il soit impossible de reprendre ou de modifier les résultats après la décision de clôture du dépouillement prise par la commission électorale.

III. — Sur le contrôle des opérations de vote a posteriori par le juge électoral
1. Les garanties minimales pour un contrôle a posteriori

Pour les besoins d'audit externe, notamment en cas de contentieux électoral, le système de vote électronique doit être capable de fournir les éléments techniques permettant au minimum de prouver de façon irréfutable que :

- le procédé de scellement est resté intègre durant le scrutin ;
- les clés de chiffrement/déchiffrement ne sont connues que de leurs seuls titulaires ;
- le vote est anonyme ;
- la liste d'émargement ne comprend que la liste des électeurs ayant voté ;
- l'urne dépouillée est bien celle contenant les votes des électeurs et elle ne contient que ces votes ;
- aucun décompte partiel n'a pu être effectué durant le scrutin ;
- la procédure de décompte des votes enregistrés doit pouvoir être déroulée de nouveau.

2. La conservation des données portant sur l'opération électorale

Tous les fichiers supports (copies des programmes sources et exécutables, matériels de vote, fichiers d'émargement, de résultats, sauvegardes) doivent être conservés sous scellés jusqu'à l'épuisement des délais de recours contentieux. Cette conservation doit être assurée sous le contrôle de la commission électorale dans des conditions garantissant le secret du vote. Obligation doit être faite, le cas échéant, au prestataire de service de transférer l'ensemble de ces supports à la personne ou au tiers nommément désigné pour assurer la conservation des supports. Lorsqu'aucune action contentieuse n'a été engagée avant l'épuisement des délais de recours, il doit être procédé à la destruction de ces documents sous le contrôle de la commission électorale.

IV. — La publication

La présente délibération sera publiée au Journal officiel de la République française.

Le président,

A. Türk

https://www.cnil.fr/sites/default/files/typo/document/Note_vote_internet_VD.pdf
Note de la CNIL – 28/05/2006
Le vote par internet aux élections politiques, les éléments du débat

L'ensemble des expériences de démocratie électronique, c'est-à-dire d'utilisation des technologies de l'information pour le vote et l'inscription des électeurs, s'insère dans un contexte global de relance du processus démocratique, notamment auprès des jeunes votants ou des nationaux résidant à l'étranger. Le vote par internet aux élections politiques tente ainsi de répondre à plusieurs objectifs : recul de l'abstention, modernisation de l'organisation des opérations de vote, amélioration de la fiabilité des décomptes, baisse du coût des opérations. Le vote à distance via internet, à différencier de la méthode utilisant des machines d'enregistrement électronique direct, comme au Brésil (le vote est enregistré dans une carte à puce, utilisable une fois, traitée dans un bureau fédéral des élections), semble marquer le pas. Si certains pays continuent à avancer, tel la Suisse, l'Estonie ou la Corée du Sud, d'autres ne souhaitent pas poursuivre les expérimentations, peu concluantes. C'est le cas notamment de la Grande-Bretagne, des Etats-Unis et de l'Espagne.

I - Les pays continuant à s'engager dans la voie

Quelques pays continuent à s'engager de manière plus ou moins avancée dans la généralisation des dispositifs de dématérialisation de vote basés sur les technologies de l'information et de la communication.

A – Les pays les plus avancés : l'Estonie et la Suisse

1°) L'Estonie : Le vote par internet à l'échelle nationale lors des élections municipales d'octobre 2005

La plus septentrionale des trois républiques baltes a utilisé pour la première fois cet automne le vote par internet dans un scrutin national : les élections municipales. L'accès à internet étant inscrit comme un droit constitutionnel dans ce pays réputé en pointe dans les nouvelles technologies, les citoyens estoniens effectuent déjà de nombreuses démarches par internet. Dans ce contexte, l'e-vote ne constitue qu'une des modalités de gouvernement électronique, soutenu par 4 des 6 partis représentés au parlement.

a – Un e-vote, basé sur la carte d'identité électronique

En théorie obligatoire, la carte d'identité électronique a déjà été distribuée à près des deux tiers des 1,33 millions d'Estoniens. Dotée d'une puce et d'un code secret, comme sur les cartes de crédit, cette ID Card a donc servi à identifier les votants (résidant en Estonie ou à l'étranger) sur le site sécurisé des élections, ouvert préalablement au scrutin traditionnel pendant 72 heures.

Les électeurs ne possédant pas de lecteur ad hoc sur leur ordinateur personnel ont pu se rendre dans une des nombreuses bibliothèques publiques, offrant des points d'accès gratuit à internet. Quant aux électeurs ne détenant pas de carte d'identité électronique, ou souhaitant s'exprimer selon les modalités traditionnelles, des bureaux de votes ont recueilli leurs bulletins papiers le jour du scrutin.

b – Des annonces ne devant pas masquer un succès d'estime et certaines contestations

Seul 1% du corps électoral estonien s'est exprimé à distance (9317 votants exactement) pour ces élections où la participation est souvent faible (moins de 50% de participation). Le vote via internet n'a donc pas renversé la tendance, ni masqué les contestations de certains partis minoritaires, réclamant un égal accès de tous les citoyens au vote et constatant l'absence de garantie du secret, comme dans l'isoloir.

En pratique, l'e-vote est surtout défendu par les partis libéraux, bien représentés parmi les classes jeunes et urbaines, et espérant étendre encore leur audience au sein de ces mêmes

classes souvent abstentionnistes et technophiles. Moins qu'un conflit générationnel, il s'agit donc d'une véritable stratégie politique et électorale.
En l'absence d'irrégularités graves, les Estoniens auront à nouveau la possibilité de voter en ligne à l'occasion des élections législatives de 2007.

2°) La Suisse : Des expérimentations lors des référendums et des votations entre 2003 et 2005

Le groupe de travail « Avant-projet vote électronique » a vu le jour en juin 2000, sur décision de la Chancellerie fédérale, réunissant en son sein des représentants des cantons de Zurich, de Berne, de Saint-Gall, du Tessin, de Genève et de Neufchâtel.
Les habitants de quelques communes du canton du Zurich ont clos le 27 novembre 2005 la série d'expérimentations prévues par le groupe de travail, à l'occasion du référendum d'initiative populaire « Pour des aliments produits sans manipulations génétiques » et de la votation modifiant la loi sur le travail (ouverture dominicale des commerces).
Matériellement, les électeurs ont reçu par courrier leurs cartes d'électeurs ainsi qu'un code d'accès confidentiel, leur permettant de valider leur vote à distance. Le vote pouvait ensuite s'exprimer via un site sécurisé sur internet ou en envoyant un SMS depuis un téléphone portable. Près de 24% des votants ont utilisé la voie électronique à distance, en préférant l'utilisation d'internet (1154 votes par internet, 243 SMS).
Le groupe de travail rédigera mi-2006 un rapport d'évaluation mettant un terme à la phase pilote, sur la base duquel le Conseil fédéral et Parlement devront décider d'introduire ou non le vote à distance en Suisse comme une alternative de vote. Une loi à ce sujet ne semble toutefois pas attendue dans l'immédiat.

B – La Corée du Sud
Pour sa part, la Corée du Sud, possédant l'un des plus denses réseaux haut débit du monde, s'est fixée comme objectif de proposer le vote généralisé par Internet à ses citoyens d'ici 2012, dans des élections majeures.
Des expérimentations auront lieu entre temps, notamment en 2008 lors d'élections générales.

C – Quelques éléments factuels communs
Chacun de ces pays possède une infrastructure technique avancée et un nombre suffisant d'habitants connectés à internet : taux de pénétration d'internet de l'ordre de 40% en Suisse ; 43% en Estonie ; 58% en Corée du Sud).
Les pays concernés se classent parmi les nations à faible (Estonie : 1,33 million d'habitants ; Suisse : 7,2 millions) ou moyenne (Corée du Sud : 48 millions d'habitants) population. Les enjeux des élections ayant servi de test sont de second plan (municipales en Estonie, modification de la loi sur le travail et introduction des OGM en Suisse), même si ces consultations ont un caractère national.
Enfin, si la mise en œuvre du vote à distance, via internet, pour des élections majeures demeure l'objectif à moyen terme pour l'ensemble de ces pays, la réalisation effective reste conditionnée (en Estonie, analyse de la commission nationale électorale sur les éventuels dysfonctionnements ; en Suisse bilan du groupe « avant-projet vote électronique »). En Corée du Sud, la date de 2012 est trop lointaine pour être certaine.

II - Les pays arrêtant l'expérimentation
De nombreux pays marquent aujourd'hui le pas en matière de vote à distance. Hormis le Canada (expérimentation lors des élections municipales de Markham, Ontario) et l'Australie (discussions dans le cadre d'un forum national Online-Council) qui entendent poursuivre

localement des expérimentations, les Etats-Unis et la Grande-Bretagne ont décidés de mettre clairement un terme à leurs tests de vote électronique à distance, l'Irlande stoppant son projet de recueil électronique des suffrages. L'Espagne temporise enfin la généralisation du vote par internet, du fait de nombreuses critiques quant à la sécurité des opérations.

A – Les Etats-Unis

Suite à un rapport d'experts du 21 janvier 2004, le projet SERVE (Secure Electronic Registration and Voting Experiment) a été abandonné du fait des nombreuses failles de sécurité détectées.
Le projet devait permettre aux citoyens expatriés (notamment les forces armées stationnées en Irak) de participer aux élections présidentielles de novembre 2004, via un dispositif de vote à distance par internet.
Pour les auteurs du rapport remis au Pentagone, le système présentait de « nombreuses failles de sécurité l'exposant à une grande variété d'attaques bien connues », d'une manière d'autant plus sensible que l'envergure de l'opération lui offrait une exposition particulière.
En conséquence, « au vu de l'impossibilité de garantir la légitimité des votes » en l'état actuel des technologies, le rapport préconisait l'arrêt immédiat du projet jusqu'à ce que « les infrastructures Internet et informatiques domestiques n'aient pas été totalement repensées ».

B – La Grande-Bretagne
[…]

C – L'Espagne
[…]

D – Un désengagement essentiellement motivé par l'immaturité des technologies
Sans réduire la problématique du vote électronique à son environnement technique, l'absence de sécurité dans les technologies mises en œuvre fonde tous les revirements étudiés.
L'ensemble des pays ayant stoppé leurs expérimentations de vote via internet entendent se réinvestir dans de tels projets, à moyen terme, dès que les technologies permettront d'organiser d'une manière totalement sécurisée la transparence des opérations. Toutefois, même dans l'hypothèse technique la plus sûre, d'autres réflexions majeures relanceront le débat, certains percevant dans le vote par internet une totale régression démocratique : en votant depuis son domicile plutôt que d'un isoloir, le vote demeure-t-il indépendant ? Le récent exemple italien démontre bien que, dans le cadre d'élections aux enjeux majeurs, il restera délicat de fonder entièrement un processus électoral sur le vote à distance.

https://en-marche.fr/emmanuel-macron/le-programme/vie-politique-et-vie-publique
La République En Marche, programme d'Emmanuel Macron

[...]

Objectif 3 : Des élites plus efficaces.

Nous moderniserons nos institutions.

« Je demande à la politique qu'elle soit efficace, qu'on perde pas tant de temps et d'énergie : 2 mois sur l'affaire Valbuena, 6 sur la déchéance de nationalité, un sur la question du voile à l'université. Il y a plus urgent et pertinent »
– Pierre, 20 ans, Paris – La Grande Marche

Aujourd'hui, les responsabilités politiques sont diluées : trop d'acteurs, trop d'interventions successives, trop de lenteurs.

Au Parlement, un député représente sept fois plus de personnes aux États-Unis qu'en France. C'est aussi le cas au gouvernement : seuls quatre gouvernements de la Vème République ont compté moins de 15 ministres, et sous le quinquennat de François Hollande, 74 hommes et femmes politiques ont exercé des fonctions ministérielles.

Demain, nous concentrerons les énergies sur les sujets prioritaires en limitant la bureaucratie gouvernementale et parlementaire. Nous favoriserons la procédure accélérée pour l'adoption des textes.

Plus d'efficacité, c'est aussi plus de numérique : nous avons besoin de numériser notre démocratie, en instituant un vote électronique qui élargira la participation, réduira les coûts des élections et modernisera l'image de la politique.

- ➔ Interdire que des amendements écartés en commission soient à nouveau examinés en séance publique. La procédure parlementaire doit être plus efficace et plus rapide.
- ➔ Pendant les débats de la loi sur le mariage pour tous, plus de 5 000 amendements ont été déposés à l'Assemblée nationale, ce qui nuit à la qualité du travail parlementaire.
- ➔ Limiter le nombre de mois pendant lequel on légifère et consacrer plus de temps parlementaire à l'évaluation de l'action du gouvernement.
- ➔ Appliquer par défaut la procédure accélérée devant le Parlement, avec une seule lecture initiale par chambre.
- ➔ Généraliser le vote électronique d'ici 2022.
- ➔ Nous réduirons le nombre de parlementaires au Sénat comme à l'Assemblée nationale

http://www.senat.fr/notice-rapport/2018/r18-073-notice.html
Rapport d'information n°73. Session ordinaire du Sénat 2018-2019 – 24/10/2018
Réconcilier le vote et les nouvelles technologies (Jacky Deromedi et Yves Détraigne)

SYNTHESE

[…]

Sécuriser le vote par Internet pour les Français de l'étranger

Le vote par Internet, un dispositif essentiel pour les Français de l'étranger

Issu d'une initiative du sénateur Robert del Picchia, le vote par Internet est circonscrit à deux scrutins : l'élection des députés représentant les Français de l'étranger et les élections consulaires.

Le vote par Internet fait l'objet de quatre contrôles de sécurité : ceux du bureau de vote par voie électronique (BVE), de la Commission nationale de l'informatique et des libertés (CNIL), de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) et du juge électoral.

En pratique, cette modalité de vote reste complexe pour les électeurs, notamment parce que leurs codes d'identification doivent être envoyés par au moins deux canaux de transmission (courriel et sms). Sur le plan sociologique, le vote par Internet ne semble pas avoir d'influence sur le taux de participation des électeurs établis hors de France, qui dépend principalement des enjeux du scrutin.

Ce dispositif constitue toutefois une garantie essentielle pour les Français de l'étranger, certains devant parcourir des centaines de kilomètres pour se rendre aux urnes. Lors des élections législatives de 2017, un seul bureau de vote était ouvert en République centrafricaine, deux en Colombie (uniquement à Bogota) et trois en Russie.

En pratique, les Français de l'étranger utilisent massivement le vote par Internet : plus de la moitié d'entre eux ont voté en ligne lors des élections législatives de 2012.

La sécurisation du vote par Internet, un impératif démocratique

Les élections législatives de 2017 ont été un échec : l'État et son prestataire ne sont pas parvenus à garantir l'intégrité de la plateforme de vote et les Français de l'étranger n'ont pas été autorisés à s'exprimer par Internet.

Cet échec résulte d'un niveau de menaces particulièrement élevé (contexte géopolitique) mais également des imperfections structurelles de la plateforme (calendrier de mise en œuvre trop optimiste, tests grandeur nature peu concluants, pilotage insuffisant de l'administration, etc.).

Dès lors, les rapporteurs préconisent quatre mesures pour sécuriser le vote par Internet en vue des élections consulaires de 2020 et législatives de 2022.

Proposition n° 5 : Garantir l'organisation du vote par Internet pour les élections consulaires de 2020, notamment en :

- augmentant le nombre de tests grandeur nature (TGN) et en les organisant avec suffisamment d'anticipation pour corriger les difficultés constatées ;
- s'appuyant sur la direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) pour renforcer le pilotage du projet.

Proposition n° 6 : Préparer le vote par Internet pour les élections législatives de 2022 en :

- renforçant les moyens alloués à sa sécurisation ;
- rationalisant la procédure d'achat de la plateforme de vote, notamment en organisant un dialogue compétitif pour mieux définir les exigences d'ergonomie et de sécurité et en lançant la procédure de mise en concurrence plus en amont.

Proposition n° 7 : Sécuriser l'identification des électeurs participant au vote par Internet en créant une véritable identité numérique, le cas échéant à partir d'outils biométriques.

Proposition n° 8 : Prévoir l'obligation pour le Gouvernement de consulter l'Assemblée des Français de l'étranger (AFE) avant, le cas échéant, d'annuler le recours au vote par Internet.

RAPPORT

[…]

II. Sécuriser le vote par Internet pour les français de l'étranger

[…]

Les modalités de vote prévues pour les Français de l'étranger

<table>
<tr><th>Scrutin concerné</th><th>Vote à l'urne</th><th>Vote par Internet</th><th>Vote par correspondance papier</th><th>Vote par remise de pli à l'administration</th></tr>
<tr><td>Élection du Président de la République</td><td rowspan="9">Oui</td><td rowspan="2">Non</td><td rowspan="2">Non</td><td rowspan="3">Non</td></tr>
<tr><td>Référendum national</td></tr>
<tr><td>Élection des députés</td><td>Oui</td><td>Oui</td></tr>
<tr><td>Élection des sénateurs</td><td rowspan="3">Non</td><td rowspan="2">Non</td><td>Oui</td></tr>
<tr><td>Élection des représentants au Parlement européen</td><td>Non</td></tr>
<tr><td>Élection des conseillers de l'Assemblée des Français de l'étranger (AFE)[3]</td><td rowspan="2">Non</td><td>Oui</td></tr>
<tr><td>Élection des conseillers consulaires</td><td>Oui</td><td>Non</td></tr>
</table>

[…]

Les risques de piratage du vote par Internet

Les risques de piratage portent sur la plateforme de vote par Internet, d'une part, et sur les ordinateurs des électeurs, d'autre part. Les cyberattaques contre la plateforme de vote par Internet peuvent remettre en cause l'ensemble du scrutin, par exemple en :

- générant des requêtes artificielles pour saturer totalement ou partiellement la plateforme, créer un « déni de service » et empêcher les électeurs de s'exprimer ;
- « défigurant » la plateforme pour y afficher des messages extérieurs, comme en avril 2015 lorsque des messages de soutien à une organisation terroriste ont été publiés sur les réseaux sociaux de TV5 Monde ;
- s'introduisant dans le système (« cheval de Troie ») pour y exfiltrer des informations confidentielles ou modifier les résultats. Dans cette hypothèse, une simple rumeur d'attaque peut décrédibiliser les résultats du scrutin.

Les risques de piratage portent également sur les ordinateurs des électeurs eux-mêmes. Comme l'a souligné l'Observatoire du vote, le vote est « effectué sur des ordinateurs ou des smartphones connectés d'un bout à l'autre par Internet. Or, ceux-ci sont soumis à de nombreuses failles informatiques qui peuvent mettre en danger l'anonymat ou la sincérité de ce vote ». De même, certains appareils ne sont pas suffisamment mis à jour, ce qui laisse perdurer des failles informatiques pourtant connues des fabricants.

Entendue par vos rapporteurs, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) considère d'ailleurs que les attaques contre les ordinateurs personnels sont les plus difficiles à maîtriser, chaque électeur choisissant librement son terminal de vote.

[…]

C. LA SÉCURISATION DU VOTE PAR INTERNET, UN IMPÉRATIF DÉMOCRATIQUE

Le maintien du vote par Internet pour les élections législatives et consulaires est indispensable pour garantir un droit de vote effectif à nos compatriotes établis hors de France. Comme pour

les machines à voter, si le « risque zéro » n'existe pas, l'enjeu est de sécuriser le dispositif pour réduire les craintes de cyberattaques.

Cette exigence répond d'ailleurs à un engagement du Président de la République, qui a déclaré en octobre 2017 devant l'Assemblée des Français de l'étranger (AFE) : « si nous ne sommes pas en capacité pour les prochaines élections de nous organiser pour avoir un système de vote [par Internet] étanche à toute attaque, ça ne s'appelle plus la France, notre pays ! [...] Nous nous en donnerons les moyens parce que c'est un intérêt d'abord démocratique mais c'est une question aussi de crédibilité et de souveraineté qui est la nôtre ».

1. La sécurisation du vote par Internet, une question de moyens

a) À court terme : veiller à la sécurisation de la plateforme de vote, en lien avec l'actuel prestataire

Son marché public n'ayant pas été résilié, la société SCYTL est toujours chargée de mettre en œuvre le vote par Internet pour les élections consulaires de 2020. Il faudra attendre la préparation des élections législatives de 2022 pour lancer une nouvelle procédure de mise en concurrence.

Entendus par vos rapporteurs, les représentants du ministère des affaires étrangères ont affirmé leur volonté de travailler avec le prestataire d'ici 2020 pour sécuriser la plateforme de vote et tirer les conséquences des difficultés rencontrées en 2017. Les risques de piratage paraissent au demeurant moins élevés pour des élections consulaires (dont les enjeux sont principalement locaux) que pour des élections législatives (dont les enjeux sont nationaux).

Aujourd'hui, il est toutefois impossible d'assurer que le dispositif de vote par Internet sera bien opérationnel en 2020, tant les efforts à fournir sont nombreux à un an et demi du scrutin.

Pour atteindre cet objectif, l'État doit se donner les moyens de piloter ce projet d'envergure et de veiller à son bon avancement.

À titre de comparaison, le canton de Genève (Suisse) développe depuis 2003 sa propre solution de vote électronique, sans recourir à des prestataires extérieurs. À l'inverse, l'ANSSI a déploré « la relative faiblesse du pilotage technique du marché, en raison du manque de compétence [du ministère français des affaires étrangères] en matière de pilotage de grands projets informatiques ».

Il pourrait notamment être fait appel aux informaticiens de la direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) pour renforcer les compétences techniques du maître d'ouvrage. […]

Dans la même logique, au moins trois tests grandeur nature (TGN) pourraient être organisés avant chaque utilisation de la plateforme de vote 3 (contre un seul TGN pour les élections consulaires de 2014 et deux TGN pour les élections législatives de 2017).

Proposition n°5 : […] (voit plus haut)

b) À moyen terme : préparer les élections législatives de 2022

Certes, l'actuelle plateforme de vote par Internet représente un coût non négligeable de 6,72 millions d'euros sur quatre ans. Les sommes déjà investies semblent d'ailleurs suffisantes pour sécuriser le vote par Internet pour les élections consulaires de 2020.

Toutefois, ce budget pourrait être augmenté en prévision du nouveau marché qui sera lancé pour les élections législatives de 2022 et, éventuellement, les élections consulaires de 2026. Face à l'aggravation du risque de cyberattaques, un tel investissement permettrait notamment de renforcer les exigences de sécurité et d'intéresser de nouveaux prestataires.

Pour financer cette dépense, vos rapporteurs proposent d'envisager la dématérialisation de la propagande électorale des élections législatives pour les seuls Français de l'étranger disposant d'une adresse électronique, comme cela est déjà le cas pour les élections consulaires.

Lors des élections législatives de 2017, l'envoi aux Français de l'étranger de la propagande électorale sous format papier a par exemple représenté un coût de 3,27 millions d'euros.

En outre, les travaux en cours pour refondre la liste électorale consulaire, notamment grâce au nouveau répertoire électoral unique, doivent permettre de fiabiliser les coordonnées des Français de l'étranger et de réduire les échecs de connexion à la plateforme de vote en ligne.

Enfin, la procédure de passation du marché public doit être revue afin de renforcer l'efficacité et la sécurité de la plateforme de vote par Internet.

En termes de calendrier, le marché doit être attribué au moins dix-huit mois avant le scrutin (contre douze mois pour les élections législatives de 2017) afin d'être en mesure de corriger les imperfections constatées lors des tests grandeur nature.

La Cour des comptes propose d'exiger des candidats qu'ils réalisent des tests fictifs pendant la procédure d'attribution du marché pour « permettre l'évaluation de la qualité technique de leur offre ».

De même, le Gouvernement pourrait recourir à un dialogue compétitif, procédure qui permet, contrairement aux appels d'offres, d'échanger avec les candidats sur la meilleure manière de répondre aux besoins de l'administration. Une telle procédure avait d'ailleurs été etenue en 2009 pour la conception de la première plateforme de vote par Internet, avant d'être écartée en 2015 au profit d'un appel d'offres.

À titre complémentaire, le droit de la commande publique autorise explicitement le ministère des affaires étrangères à mener une « consultation préalable de marché » (ou « sourçage ») en consultant les entreprises compétentes en amont de la mise en concurrence. Ce « sourçage » permettrait notamment de mieux connaître les solutions de vote électronique mises sur le marché et de mieux définir les besoins en matière d'ergonomie et de sécurité.

Proposition n°6 : […] (voit plus haut)

Vos rapporteurs appellent également à la mise en œuvre des propositions de bon sens formulées en 2014 par notre collègue Antoine Lefèvre et notre ancien collègue Alain Anziani, qu'il s'agisse du renforcement de l'information des électeurs sur le mode de fonctionnement du vote par Internet, de l'adaptation des infractions pénales à cette modalité de vote et de la

possibilité pour les électeurs d'adresser des observations écrites au bureau de vote par voie électronique (BVE).

c) À long terme : développer une véritable identité numérique

L'identification des électeurs représente l'une des principales difficultés du vote par Internet : l'identité de la personne qui se connecte sur la plateforme est difficilement vérifiable, en particulier lorsque plusieurs membres d'une famille votent sur le même ordinateur.

Dès lors, il paraît nécessaire de sécuriser l'identification des électeurs, notamment en ayant recours à des techniques biométriques. Cette identité numérique pourrait aussi ouvrir l'accès à d'autres services administratifs, sous réserve de la nécessaire protection des données à caractère personnel.

En cours de développement par l'Agence nationale des titres sécurisés (ANTS), le prototype ALICEM pourrait constituer une première réponse : il permet d'identifier un individu à distance, en comparant la photographie prise de son téléphone portable et celle de son passeport biométrique (reconnaissance faciale). ALICEM n'est toutefois pas directement transposable au vote par Internet des Français de l'étranger, plus de 20 % d'entre eux ne disposant d'aucun passeport.

De manière alternative, il pourrait être envisagé de sécuriser la « carte consulaire », que les ambassades et consulats remettent aux expatriés, et d'y insérer des éléments biométriques. Ce projet pourrait être financé par la dématérialisation de la propagande électorale des Français de l'étranger. Entendu par vos rapporteurs, un industriel évalue son coût initial à environ 960 000 euros, somme à laquelle s'ajouterait un coût de maintenance de 50 000 euros par an.

Un tel dispositif permettrait également de simplifier la procédure de connexion à la plateforme de vote, en supprimant l'envoi des codes d'identification par courriel et sms.

Proposition n° 7 : [...] (voir plus haut)

L'exemple estonien illustre les possibilités offertes par l'identité numérique, notamment en termes de simplification des démarches administratives. Ce modèle n'est toutefois pas directement transposable en France car il nécessite de centraliser de nombreuses données à caractère personnel au sein d'un même dispositif informatique.

L'identité numérique estonienne
L'Estonie s'est dotée d'une carte d'identité numérique en 2004. Ce dispositif est aujourd'hui utilisé par 98 % de la population estonienne, soit environ 1,27 million de personnes. En dehors des mariages, des divorces et des achats immobiliers, qui nécessitent la présence physique des individus, toutes les démarches administratives peuvent être effectuées en ligne, à partir de la carte d'identité numérique. Concrètement, cette carte d'identité permet de voter, de payer ses impôts, d'accéder aux transports en commun, d'être informé des résultats scolaires de ses enfants, d'effectuer une demande de subvention et même de se voir délivrer une ordonnance médicale. Les autorités estiment économiser environ 2 % du PIB estonien grâce aux économies et aux gains de temps générés.

L’Estonie a également créé un statut de « e-résident » pour les étrangers, détenu par environ 35 000 personnes : il permet à toute personne (ressortissants étrangers inclus) de créer et de gérer son entreprise à distance, sans être installé sur le territoire estonien.

L’Estonie a aussi développé une plateforme dénommée « X-Road » qui permet à toutes les administrations de stocker et d’échanger des données à caractère personnel. Une fois l’information transmise à l’État, elle devient accessible à toute autre administration habilitée.

Des mesures de protection sont indispensables pour sécuriser cette identité numérique : en 2007, un piratage de grande ampleur a perturbé pendant plus de deux semaines le fonctionnement de sites institutionnels estoniens, de banques mais aussi de médias.

Depuis, l’Estonie stocke chaque type de données sur des serveurs différents. De même, elle a ouvert un relai numérique au Luxembourg (« data embassy ») pour diversifier les lieux de stockage de ses données.

[…]

http://pagesperso.ls2n.fr/~enguehard-c/note_technique_internet_2014.pdf
Publication LINA - UMR CNRS 6241 - 11/07/2014
Note technique sur le vote par internet (Chantal Enguehard)

[…]

1. Le vote par internet

Le vote par internet est aussi désigné par les termes "vote en ligne" et "vote à distance par voie électronique".
Les électeurs procèdent depuis n'importe quel ordinateur connecté à internet, que cet ordinateur soit chez eux, au travail, dans un lieu public ou un cybercafé. Le vote par internet est un mode de vote à distance, il peut donc être comparé au vote par correspondance postale. La connexion avec internet est parfois réalisée via un réseau intranet intermédiaire (par exemple, le réseau intranet de l'école, de l'université ou de l'entreprise d'où l'électeur procède à son vote) lui-même connecté à la toile internet. Le centre serveur de vote est composé de plusieurs serveurs ou systèmes virtuels hébergés sur une seule machine se chargeant de différentes tâches : authentification des électeurs, réception des bulletins, gestion des émargements, stockage des bulletins, dépouillement, etc. Ces serveurs et systèmes sont souvent dupliqués afin de faire face à d'éventuelles pannes.

2. Enjeux et difficultés

Unicité
Pour assurer le respect du principe d'unicité (un électeur - une voix), le système de vote par internet doit tenir à jour une liste des émargements afin d'empêcher tout vote multiple. Il est donc indispensable que, pour chaque bulletin reçu, le centre serveur ait connaissance des codes ayant autorisé le vote.

Lorsqu'un vote est émis, deux types de données sont donc utilisées : un code d'autorisation (séparée du vote) et le vote lui-même. Une difficulté est que, afin de préserver l'anonymat il est nécessaire de mettre en place des mécanismes sophistiqués visant à ne pas révéler ces informations aux dispositifs relayant l'information sur la toile depuis le poste de la personne ayant voté jusqu'au centre serveur de vote. Le centre serveur de vote lui-même ainsi que les personnes ayant accès aux machines de vote ne doivent pas être mesure de reconstituer le lien entre un vote et le code d'autorisation qui l'accompagnait.

Sincérité

Lorsque qu'un électeur vote via internet, il exprime son choix par un clic de souris. Cette force mécanique de quelques joules est convertie en une impulsion électrique, elle-même transformée en une information codée en binaire susceptible de connaître ensuite d'autres traitements (comme le chiffrage, etc.). Tous les votes, sans exception, sont donc soumis à plusieurs transformations. Du fait de la protection du secret du vote, l'ensemble de ces transformations ne peut être suivi pas à pas. Par conséquent, des transformations modifiant le sens du vote de certains bulletins pourraient passer inaperçues, y compris si une grande quantité de bulletins étaient affectés.

Sur ce point, le vote par internet diffère considérablement du vote par correspondance pour lequel les bulletins dénombrés sont censés être ceux que les électeurs ont envoyés, sans aucune transformation intermédiaire. De plus, l'identité de l'électeur peut être établie d'après des éléments accompagnant l'enveloppe fermée contenant le bulletin de vote. La transformation, l'ajout ou le retrait de bulletins en grande quantité peuvent difficilement être dissimulés du fait de la manipulation de bulletins matériels, des nécessaires complicités, des éventuels témoignages, etc.

Dans le cas du vote par internet, il apparaît finalement que personne (ni les électeurs, ni les candidats, ni les experts, ni les partis, ni le ministère, etc.) ne peut être certain que les choix des électeurs n'ont pas été modifiés avant leur comptage ou même que les votes apparemment recensés aient été émis par les électeurs eux-mêmes.

Portée de l'expertise d'un système de vote électronique.

L'expertise d'un système de vote électronique ne peut porter sur l'entièreté du système de vote puisqu'une partie importante de celui-ci (les ordinateurs à partir desquels les votes sont émis) ne peut être inspectée. Or ces ordinateurs sont susceptibles d'être le siège d'attaques externes visant à la fois la sincérité des élections et le secret du vote. […]

Du côté du centre serveur de vote, plusieurs mois seraient nécessaires pour une expertise complète, sans garantie de trouver tous les bugs ou éventuelles fraudes.

La portée de l'expertise d'un système de vote électronique apparaît donc réduite : des dysfonctionnements ou des fraudes peuvent se produire sans être détectés, même s'ils concernaient un nombre important de suffrages.

Efficacité du chiffrement du bulletin de vote

Bien que cette mesure soit efficace une fois qu'elle a été effectuée (sous réserve que les clés de chiffrement n'aient pas été divulguées ou obtenues frauduleusement), il reste toujours possible qu'un programme malveillant hébergé sur le poste de l'électeur copie ou modifie le bulletin de vote avant chiffrement. Cette mesure ne peut donc garantir que le vote de l'électeur n'a pas été modifié avant le dépouillement et qu'il est resté secret.

3. Conclusion

Le vote par internet apparaît donc plus fragile que le vote par correspondance postale car les bulletins sont modifiés en dehors de toute surveillance : le vote porté par un grand nombre de bulletins pourrait être changé par un bug malencontreux, ou du fait d'une manœuvre frauduleuse d'un individu isolé, sans que cette atteinte majeure à la sincérité de l'élection ne soit remarquée. […]

« En outre, il est impossible à l'électeur de savoir si l'information enregistrant son vote a correctement retranscrit le choix qu'il a effectué et si cette information, à la supposer correcte, n'a pas été modifiée en cours d'acheminement jusqu'au serveur collectant les "bulletins électroniques".»
« En d'autres termes, l'électeur valide son choix sur son ordinateur mais n'a aucune garantie que son vote ait été bien pris en compte, ni que le sens de son vote n'a pas été altéré. »
« Autre point d'achoppement : on ne peut savoir avec certitude quel a été le vote émis. Il n'est pas sûr, pour des raisons techniques, que ce soit le même que le vote enregistré. »
« En matière de vote à distance, la sécurité est d'autant plus délicate à garantir que la puissance publique n'a aucune prise ou moyen de contrôle sur le terminal qui sert à l'électeur à voter. L'électeur choisit librement le terminal de vote, le plus souvent un ordinateur personnel. Or, comme le rappelaient les représentants de l'agence nationale de sécurité des systèmes d'information (ANSSI), les moyens pour parer tous les risques informatiques sont hors de prix pour un simple particulier. Ce risque est d'autant plus fort que selon les électeurs, les terminaux varient, de même que les logiciels et les navigateurs. »
« En fait, le vote électronique relève aujourd'hui d'une modernité obsolète. » […]
https://www.alain-bensoussan.com/avocats/vote-electronique-garanties-minimales
Cabinet d'avocats Alain Bensoussan – 18/10/2017
Le vote électronique requiert des garanties minimales (Emmanuel Walle)

Le vote électronique nécessite un cadre technique apportant toutes les **garanties de fiabilité**. Parmi les garanties minimales : la transparence par le recours systématique à l'expertise indépendante et **l'accès au code source des logiciels**.

La fiabilité et les modalités de mise en œuvre du vote électronique sont soumises quasiment chaque année à l'examen du juge. Plus d'un a pu se dire surpris de la contradiction apparente entre la jurisprudence du Conseil d'État et celle de la Cour de cassation relativement à l'obligation de réaliser une **expertise indépendante** préalablement à chaque scrutin recourant au vote électronique.

En mars 2015, le Conseil d'État a jugé nécessaire la réalisation d'une telle expertise avant chaque scrutin, afin de garantir de manière certaine « **la sincérité des opérations électorales »**.

En septembre 2016, la Cour de cassation indique « qu'il résultait de l'expertise indépendante conduite entre juillet et octobre 2012 que le **système de vote électronique** utilisé pour le scrutin ne présentait aucune modification substantielle depuis celle qui avait été diligentée en 2005 lors de sa mise en place, le tribunal a exactement décidé qu'il avait été satisfait aux prescriptions des articles R. 2314-12 et R. 2324-8 du code du travail ».

On voit ici le problème qui se pose à l'organisateur d'un scrutin désireux de satisfaire à ses obligations mais aussi désireux de gérer au mieux les coûts occasionnés par l'organisation du vote électronique :

- Faut-il ou non diligenter une expertise indépendante, alors que la solution de vote a été expertisée auparavant ?

Une circonstance est de nature à jeter un trouble encore plus grand lorsque l'on sait que le même système de vote a été utilisé dans les deux cas, objet de ces jurisprudences apparemment contradictoires, mais pour des élections différentes. Le problème n'est qu'apparent et la contradiction peu fondée (…).

https://www.nextinpact.com/news/102944-le-numero-l-anssi-defavorable-au-vote-electronique.htm
NextImpact.com - 18/01/2017
Le numéro un de l'ANSSI défavorable au vote électronique (Xavier Berne)

Guillaume Poupard, le directeur général de la très sérieuse Agence nationale de la sécurité des systèmes d'information (ANSSI) a déclaré ce matin à l'Assemblée nationale qu'il n'était « *pas en faveur du vote électronique* ». S'appuyant sur ses propos, un député a décidé de demander au gouvernement d'interdire les machines à voter pour les prochaines élections.

Si François Fillon a promis de généraliser le vote électronique, rappelons que son usage est aujourd'hui assez limité. S'agissant du vote par Internet, il est uniquement proposé aux Français de l'étranger (sur la base du volontariat), et pour quelques scrutins seulement. En 2017, cette faculté leur sera ainsi offerte pour les législatives, mais pas pour la présidentielle. Quant aux machines à voter, officiellement autorisées depuis la fin des années 60, seules quelques communes continuent de les utiliser, suite à l'adoption d'un moratoire, courant 2007.

Poupard favorable à une extension du moratoire sur les machines à voter

Interrogé lors d'une audition par le député socialiste Sébastien Pietrasanta, Guillaume Poupard a eu du mal à cacher sa réticence face à ces dispositifs. Le numéro un de l'ANSSI s'est tout d'abord dit « *très en faveur* » d'une « *extension* » du moratoire concernant les machines à voter. Sachant qu'aucune nouvelle commune ne peut aujourd'hui rejoindre la cinquantaine de villes qui font encore de la résistance, on imagine que cette nouvelle étape se traduirait par un abandon de ces appareils électroniques.
« *Ces machines ont le défaut d'être assez différentes les unes des autres, elles sont difficiles à aller évaluer une par une... Il faut peut-être même simplement se reposer la question de l'intérêt de ces machines, mais là c'est un avis un peu personnel* », a déclaré ce spécialiste de la cryptographie.

Les bulletins traditionnels jugés plus rassurants que le vote par Internet

Même son de cloche au sujet du vote par Internet : « *En toute franchise, je ne suis pas en faveur du vote électronique, parce qu'aujourd'hui quand on met en regard les capacités de sécurisation que l'on a – même en faisant beaucoup d'efforts, même avec des gens très sérieux – et le niveau des attaquants potentiels (...), on a du mal à totalement rassurer.* »
Tout en affirmant que les cybermenaces ne devaient pas être « *tétanisantes* », Guillaume Poupard a plaidé en faveur du système traditionnel. « *De fait, ce processus encore très concret, avec des bulletins, des enveloppes... Ça, c'est de nature à me rassurer.* »

Le directeur général de l'ANSSI, qui figure d'ailleurs dans le « *bureau du vote électronique pour les élections des Français établis hors de France* », a rapidement été entendu par Sébastien Pietrasanta. Dans un tweet, l'élu a « *solennellement* » demandé au ministre de l'Intérieur, Bruno Le Roux, « *d'interdire les machines à voter* » pour les prochaines élections. […]

https://www.lemonde.fr/pixels/article/2017/03/09/pourquoi-le-vote-electronique-des-francais-de-l-etranger-pour-les-legislatives-a-t-il-ete-annule_5092022_4408996.html
Lemonde.fr - 09/03/2017
Pourquoi le vote électronique des Français de l'étranger pour les législatives a-t-il été annulé ? (Damien Leloup et Martin Untersinger)

Deux audits de sécurité ont montré que la plateforme de vote pouvait être fortement ralentie par une attaque, et une fuite de données a achevé d'emporter la décision.

En annonçant, lundi 6 mars, que les Français de l'étranger ne pourraient pas voter par Internet aux législatives, comme c'était initialement prévu, le ministère des affaires étrangères, Jean-Marc Ayrault, a déclenché de très vives protestations de la part de candidats et d'électeurs.

Selon les informations du *Monde*, la décision d'annuler ce vote électronique a été prise au terme d'un long processus et de deux audits, en décembre 2016 et en février, qui ont conduit l'Agence nationale de sécurité des systèmes d'information (l'Anssi, chargée de la sécurité numérique de l'Etat) à rendre un avis défavorable.
L'annulation n'est pas liée à une menace particulière ou précise, ni à des informations laissant entendre qu'un groupe ou qu'un Etat chercherait à perturber ou à influencer le vote. Le contexte géopolitique, les actions de groupes étatiques ou para-étatiques, et le déroulement de la campagne électorale aux Etats-Unis, ont cependant pesé – le système de vote déjà utilisé en 2012 étant considéré comme insuffisamment robuste.
La principale faiblesse identifiée du système de vote qui devait être utilisé était qu'il pouvait être vulnérable à une attaque dite de « déni de service », c'est-à-dire à une saturation du système l'empêchant de fonctionner correctement. Ce qui pouvait entraîner, en cas d'attaque, des retards de plusieurs heures, voire empêcher une partie des électeurs de voter. Même si le nombre d'électeurs concernés était faible, une telle perturbation aurait eu *« un impact important sur l'image du fonctionnement de la démocratie »*, expliquait cette semaine Guillaume Poupard, le directeur de l'Anssi, au site *NextInpact*.

Une fuite de données

Pour autant, les résultats du premier audit, demandé fin 2016, n'avaient pas souligné de graves défauts structurels dans le système de vote, et le gouvernement comme les experts ont semble-t-il espéré qu'il pourrait être mis en place. Mais en février, lors du second audit, les experts ont découvert une fuite de données ayant eu lieu lors d'un test interne réalisé par le prestataire chargé du système de vote, qui aurait pu permettre à un attaquant doué d'altérer en partie les données du système électoral. La fuite aurait potentiellement pu être détectée par des pirates étrangers, ce qui a conforté l'Anssi dans sa décision de rendre un avis négatif et convaincu le gouvernement d'annuler le vote électronique pour les législatives.
Plus encore que l'annulation elle-même, c'est le calendrier qui avait suscité la colère des députés des Français de l'étranger, dont l'ancienne secrétaire d'Etat Axelle Lemaire (PS) et Frédéric Lefebvre (LR), furieux qu'elle intervienne deux mois avant le scrutin. François Fillon avait lui aussi critiqué cette décision, prise en conseil des ministres, estimant qu'il

s’agissait d’un *« déni de démocratie »* et d’un *« gâchis d’argent public »* – le ministre des affaires étrangères lui avait répondu que la décision avait été prise en raison du *« niveau élevé de la menace »*, et que *« le développement d’un nouveau système de vote électronique se poursuit en vue de son utilisation lors de prochaines échéances électorales à l’étranger »*.

https://www.nextinpact.com/news/103636-avant-suppression-vote-electronique-dysfonctionnements-pointes-lors-tests.htm
NextImpact.com - 11/03/2017
Retour sur la suppression du vote électronique pour les élections législatives 2017 (Marc Rees)

La suppression du vote par Internet pour les Français de l'étranger fait suite à une chaude recommandation de l’ANSSI. Cependant, elle ne laisse pas insensibles les élus. La sénatrice Joëlle Garriaud-Maylam met en cause les faiblesses du ministère, plus que le risque d’un piratage extérieur. D’autres voix vont dans le même sens. Sauf au ministère.

À quelques encablures de l’élection législative, le ministère a décidé d’annuler le vote électronique des députés des Français de l’étranger. La décision a été très critiquée, de Frédéric Lefebvre à Axelle Lemaire, en passant par François Fillon. Guillaume Poupard, directeur général de l’ANSSI, nous a expliqué lundi 6 mars les raisons de son avis, conduisant à cette décision : « *Jusqu’au dernier moment, nous avons essayé de faire en sorte que la plateforme soit d’un bon niveau (…) si la plateforme est clairement meilleure qu’en 2012, le niveau de la menace est aujourd’hui bien supérieur* ». Et celui-ci de craindre un risque trop important « *sur l’image du fonctionnement de la démocratie.* »

Une sénatrice pointe les faiblesses des prestataires retenus par le ministère

Cependant, cette présentation mesurée n’a visiblement pas convaincu Joëlle Garriaud-Maylam. La sénatrice plaide à la porte du ministère des Affaires étrangères pour le maintien du vote par Internet lors des législatives de 2017. Elle conteste surtout l’existence de « *menaces nouvelles* », préférant dénoncer « *plutôt des problèmes techniques déjà identifiés en 2012* ».
Dans une question parlementaire tout juste adressée au Quai d’Orsay, elle estime donc que c’est « *moins à l'environnement international qu'aux faiblesses éventuelles des prestataires retenus par le ministère que seraient imputables les difficultés mises en évidence lors de ce test* ».
Ces propos corroborent ceux glanés le 8 mars par l’AFP auprès d’une source proche du dossier, toujours au même ministère. Dans deux tests réalisés en novembre 2016 et février 2017, seuls 2 500 des 12 000 électeurs volontaires ont pu arriver au bout de la procédure de vote. Et c’est dans le contexte de cette piteuse expérience que l’Agence nationale de la sécurité des systèmes d'information (ANSSI) a finalement soufflé son avis négatif.
Next INpact a recueilli un autre témoignage venant charger la barque. Jean Lachaud, conseiller honoraire à l'Assemblée des Français de l'étranger, délégué général du Souvenir Français pour les États-Unis, a fait partie de ces testeurs.
Il nous rappelle d’entrée qu’« *il va sans dire qu’il est impossible, par principe, d’avoir confiance dans un scrutin par internet, l’urne (à savoir le traitement n’étant par définition pas transparente, d’une part, et le risque de sabotage (interne) ou de piratage (externe) étant bien réel, d’autre part* ».

L’intérêt du vote par Internet

Seulement, le vote électronique reste une composante jugée essentielle : outre l'éloignement des bureaux de vote, se pose un problème de transmission du matériel électoral pour ceux qui voudraient passer par la voie du vote par correspondance. « *Si, en France, le courrier est distribué suffisamment rapidement, il n'en est pas de même à l'étranger* ».
Et pour cause, nous rappelle ce conseiller honoraire, « *compte tenu des délais de déclaration des candidatures pour le deuxième tour, d'impression et de mise sous enveloppe du matériel électoral correspondant, l'expérience démontre amplement que ce matériel n'est quasiment jamais reçu par les électeurs avant le deuxième tour, en dehors de quelques pays limitrophes de la France* ». Le manque de temps et l'éloignement des Français de l'étranger rendent du coup très difficile, voire impossible l'organisation de telles opérations.
Ceci dit, insiste-t-il, « *la raison pour laquelle le vote par internet est supprimé n'a rien à voir, en tout cas directement, avec des "risques de piratage", lesquels existent depuis toujours* ».
Notre contact témoigne que « *le système mis en place par le nouveau prestataire du ministère des Affaires étrangères a très mal fonctionné lors des deux essais en grandeur nature* ».
Dans le passé, le marché du vote électronique attribué initialement à ATOS et à l'entreprise espagnole Scytl avait « *connu, à l'occasion de chaque scrutin pour lequel il a été mis en œuvre, à des dysfonctionnements considérables qui, s'ils avaient été connus du grand public, auraient causé un scandale* » affirme Jean Lachaud.
Quelques exemples pointés du doigt : « *non réception des identifiants, codes d'accès et autres mots de passe par un nombre non négligeable d'électeurs, impossibilité de voter pour un grand nombre de celles et ceux ayant malgré tout reçu les codes nécessaires, soit pour des raisons d'accès au site* ». Il y avait en outre des incompatibilités dues à Javascript, « *entre la version (...) du système et celle tournant sur les machines utilisées par les électeurs* ».

Des tests peu glorieux

Pour le scrutin de 2017, un nouvel appel d'offres a donc été lancé par le ministère des Affaires étrangères, remporté par l'entreprise espagnole. Consécutivement, « *deux essais ont eu lieu, les dysfonctionnements du premier (deux tours en novembre) ayant entraîné un autre essai, apparemment non prévu, le mois dernier* ».
« *La semaine dernière, quelques jours après le deuxième tour de ce deuxième essai, j'avais pronostiqué (sans trop d'audace) l'annulation du vote par internet pour 2017. En effet, le nouveau système proposé fonctionne encore plus mal que le système ATOS. Il était manifestement impossible de le corriger à temps* » insiste Jean Lachaud.
Florilège de quelques bugs ayant émaillé les courriers échangés avec l'organisateur : le ministère annonçait par exemple aux testeurs qu'un « *problème technique a empêché l'accès au portail de vote* ». Jean Lachaud se plaignait préalablement ne pas avoir reçu le SMS qui lui aurait permis de participer au vote. « *Le site electeur.voteraletranger.gouv.fr ne reconnaissant pas l'ensemble identifiant/mot de passe qui me permettait d'accéder au site monconsulat.fr du temps où celui-ci était en activité, j'ai essayé de m'y enregistrer comme un nouvel utilisateur. Après plus de 15 tentatives, je n'ai pas réussi à seulement m'enregistrer sur le site de vote* ».

Des recours contre l'organisation du vote par correspondance ?

Voilà pourquoi celui-ci partage le sentiment selon lequel « *l'annonce d'un « risque de piratage » n'est qu'un habillage destiné à détourner l'attention* ». Il craint donc que les principaux responsables de ce fiasco ne soient les organisateurs de ces opérations.

Il reste que le basculement du vote électronique au vote par correspondance ne va pas se faire sans risque, nous explique l'avocat franco-américain Pierre Ciric, qui avait provoqué l'annulation de l'élection législative de Corinne Narassiguin dans la première circonscription des Français de l'étranger en 2013.
Puisqu'il est très difficile si ce n'est impossible d'adresser à temps le matériel électoral à l'ensemble des électeurs Français disséminés dans le monde, surtout dans le cas du deuxième tour, le scrutin sera sans nul doute attaqué pour irrégularités dans les onze circonscriptions concernées. Il pourrait même être annulé si des irrégularités concernant le traitement des votes par correspondance impactent un nombre de voix supérieur à l'écart de voix, indique Me Pierre Ciric.

« Une très forte recommandation de l'ANSSI »

Confrontée à ces témoignages, une source proche du dossier au ministère reconnait l'existence de bugs sur la plateforme, avant d'insister : la décision a bien été prise « *suite à une très forte recommandation de l'ANSSI liée aux menaces cybernétiques d'un niveau nettement plus élevé qu'en 2012* ».
« *Clairement,* poursuit notre interlocuteur, *il y a eu des dysfonctionnements sécuritaires et fonctionnels. On a donné malgré tout sa chance au produit d'où ce test grandeur nature organisé à nouveau en février, achevé voilà une dizaine de jours. Nous avons eu encore un peu d'insatisfaction au plan fonctionnel, mais l'expérience a bien été polluée par une série d'aspects en terme de capacités d'accès à la plateforme et surtout des problèmes réellement sécuritaires* ».
Sur le chiffre des 12 000 inscrits aux tests, mis en avant par l'AFP, effectivement 2 500 personnes ont réussi à voter de bout en bout. Le taux d'échec serait cependant inférieur à ce que laissent entendre une simple comparaison, car tous les participants n'auraient pas participé à l'opération. « *L'ordre d'échec est plutôt d'environ 1 500 personnes* ».
Ce serait donc la combinaison de ces éléments qui a poussé le ministère à prendre cette décision. « *L'une des difficultés est que le vote doit rester secret, lisible ni par des tiers, ni par le ministère. Le secret du vote est un principe constitutionnel, ce qui rend les choses plus compliquées.* »
Quels sont justement les risques épinglés ? « *Des attaques par déni de service, des tentatives de déstabilisation destinées à jeter le doute sur la sincérité du scrutin, le risque de modification du vote par des tiers. Il y a des partisans du vote électronique, d'autres aussi qui émettent de gros doutes* ». Du coup, « *l'ANSSI nous a déconseillé de mettre en œuvre la plateforme pour ces élections, sans nous dire que telle attaque allait arriver, mais en nous alertant du niveau de menace.* »

Le marché avec Scytl n'est pas remis en cause

En attendant, le marché passé avec l'entreprise Scytl pour quatre années reste intact.
« *Développement, test grandeur nature, les unités prévues ont été respectées. L'avenir sera de continuer à mettre au point une solution satisfaisante* ». Pour contextualiser, le cahier des charges de ce marché avait été rédigé avec l'ANSSI. L'appel fut lancé en décembre 2015 et les offres ramassées en février 2016. Seuls deux candidats se sont présentés, l'espagnol Scytl et le français Docapost, une filiale de la Poste qui n'a finalement pas été retenue.
Cette mise entre parenthèses du vote électronique sera donc sans conséquence, nous assure-t-on. « *Il n'y a aucune raison de remettre en cause la relation contractuelle. Nous continuons avec Scytl sans la considérer fautive.* »

En attendant, contrairement à Me Pierre Ciric, notre source reste confiante sur l'organisation des législatives 2017, prenant pour exemple l'épisode des présidentielles de 2012 où les étrangers ont pu voter aussi par urne ou procuration. « *Quand les gens veulent voter à l'urne, ils vont voter* ». De plus, pour les législatives, des tournées consulaires seront organisées pour faciliter cette expression citoyenne. Bilan après le 18 juin 2017.

https://www.maddyness.com/2017/06/20/tribune-vote-electronique-blockchain/
Maddyness.com - 20/06/2017
Vote électronique, vers la fin des réticences grâce à la blockchain ?

Alexandre David, cofondateur et directeur des Produits à Eureka Certification, estime que les craintes concernant le vote électronique peuvent être levées grâce à la blockchain.

On en entend beaucoup parler tant il a déjà été adopté outre-Atlantique. Le vote par voie électronique fait débat en ces périodes électorales. Vanté par certains, décrié par d'autres, ce système de vote numérique ne fait pas l'unanimité au sein des sociétés et gouvernements. Et pour cause, les fraudes récurrentes pendant les scrutins sont évoquées comme principaux freins à la démocratisation de ce nouveau dispositif.

Et pourtant, avec l'évolution des nouvelles technologies, et notamment le protocole blockchain, des solutions innovantes apparaissent pour implémenter un vote dématérialisé, en toute sécurité, grâce à un stockage de données numériques décentralisé. A l'heure où le vote électronique et son fonctionnement suscitent des réserves, doit-on voir la blockchain comme un outil de sécurisation numérique et démocratique ?

Qu'est-ce que la blockchain ?

La blockchain est un registre numérique public, sécurisé et transparent qui fonctionne sans organe central de contrôle. Il contient des informations horodatées et regroupées sous forme de blocs, qui s'empilent les unes sur les autres pour former une chaîne : la blockchain.

Depuis l'explosion de la bulle Internet dans les foyers, toutes les interactions (e-mails, messages instantanés, envoi de documents…) reposent davantage sur un système de partage que sur un système d'échange. Autrement dit, lorsque l'on envoie un fichier à un autre utilisateur, il ne reçoit pas réellement le fichier en question, mais plutôt sa copie. Cette dimension *peer-to-peer* se complique lorsque l'échange de valeurs entre en jeu. Par exemple, si 30 euros sont envoyés d'un individu *X* à un individu *Y,* il est primordial que l'individu *X* n'ait plus accès à ces 30 euros. Une évidence qui s'applique également au vote électoral. Mais alors, comment s'assurer qu'un électeur n'ait pas accès deux fois à la même élection ?

La blockchain va révolutionner le vote

L'application de la blockchain au vote permet d'envisager un dispositif sécurisé. Son utilité est double : elle permet à la fois de simplifier le déroulement des élections et le dépouillement des bulletins de vote. Au-delà de ces facilités, elle réduit aussi considérablement les possibilités de fraude, grâce aux résultats transparents et précis qu'elle prévoit et qui font d'elle une véritable arme numérique contre les menaces informatiques.

Les champs de possibilités qu'offre cette application sont larges et sur le point de bouleverser les systèmes politiques et hiérarchies sociales traditionnels. La blockchain peut aller jusqu'à révolutionner le concept même du vote. En effet, dans un futur proche, plutôt que de donner sa voix à un candidat lors d'une élection, les citoyens pourront, s'ils le souhaitent, s'exprimer pour des décisions, et ceci en temps-réel. En effet, la blockchain peut rapidement et facilement dégager la position d'un peuple, et ce quasiment sans coûts économiques. En somme, elle rend possible la mise en place d'un référendum, organisé en peu de temps et auquel chaque citoyen pourra participer. Une participation qui était jusque là impensable dans nos sociétés actuelles.

La blockchain : un rempart contre la triche

Dans le cadre de la mise en place du vote électronique, la réponse habituelle aux questions de triche est de passer par un organe de contrôle externe. Néanmoins, un tel acteur n'est pas nécessairement exempt de défauts, bien au contraire. Les menaces encourues peuvent comprendre les cyberattaques, les bugs ou encore la fraude interne. Quoi qu'il en soit, dans le contexte du vote, le fait de faire appel à un acteur centralisé peut entrainer une remise en cause de l'ensemble des résultats d'une élection. C'est de cette dimension faillible que le vote électronique tire sa mauvaise réputation.

La solution décentralisée offerte par la blockchain permet de contourner ce problème. Mais à partir du moment où la blockchain est indépendante, qui est garant de sa sécurité ? En l'absence de tout autre acteur, elle doit assurer elle-même son bon fonctionnement. Heureusement, des mécanismes ont été conçus pour rendre impossible toute tentative de falsification ou d'attaque du réseau.

Pour commencer, chaque utilisateur est identifié sans faille sur le réseau grâce à un mécanisme d'identifiant unique. On sait alors précisément qui a réalisé quelle action dans le registre. Il est alors impossible de falsifier ou de réfuter les opérations enregistrées : chaque information inscrite dans le registre l'est définitivement, sans pouvoir n'être ni transformée ni altérée. Ensuite, un réseau est composé d'une multitude de nœuds. Puisqu'il existe non pas un mais plusieurs serveurs, si l'un d'entre eux venait à cesser son activité le reste prendrait le relai instantanément. De ce fait, si quelqu'un souhaite s'en prendre à la chaîne, il faut absolument qu'il fasse tomber tous les nœuds pour y parvenir.

Entre système infaillible imperméable à la triche et potentiel tremplin démocratique, la technologie blockchain a toute sa place dans l'organisation des élections. Le vote électronique, qui jusqu'à lors souffrait d'une mauvaise réputation, dispose donc aujourd'hui de moyens pour proposer à la société de demain une alternative plus qu'intéressante.

https://www.ledevoir.com
Le vote par Internet, une technologie mûre

Récemment, le directeur général des élections du Québec Pierre Reid proposait aux élus de l'Assemblée nationale d'implanter le vote par Internet au Québec. Pour le DGE, un tel système pourrait aider à résoudre le problème du faible taux de participation comme ce fut le cas aux dernières élections municipales. À la suite des avancées sur le plan technique et des succès de divers systèmes de votation par Internet dans le monde, la proposition du DGE doit être appuyée et concrétisée afin de permettre au Québec d'amorcer la transition d'un système de votation du XIXe siècle vers un système de votation du XXIe siècle.

Le Canada est un pays relativement avancé dans ce domaine. Six provinces ont adapté leurs lois afin de permettre le vote par Internet. Le Québec n'en fait pas partie. La ville de Markham, en Ontario, permet le vote par Internet depuis 2003 et, en 2014, 97 municipalités en Ontario offraient la possibilité de voter par Internet. C'est aussi le cas de plus de la moitié des municipalités en Nouvelle-Écosse. En Alberta, l'entrée en vigueur du vote par Internet était prévue pour les élections municipales de 2013, mais un problème technique a fait en sorte qu'elle a dû être reportée.

Ailleurs dans le monde, c'est également au niveau municipal ou local que la plupart des systèmes de vote par Internet ont été adoptés. La Lettonie représente le seul exemple d'implantation réussie à l'échelle nationale. Dès 2002, le gouvernement de la Lettonie a décidé de développer le vote par Internet et, depuis 2005, les Lettons peuvent choisir entre le bulletin de vote traditionnel et le vote par Internet aux niveaux local, national ou aux élections européennes.

Diverses instances se sont investies dans ce domaine. Depuis plus de dix ans, l'Organisation de sécurité et de coopération en Europe (OSCE) développe une expertise sur les systèmes de vote par Internet. À l'invitation du gouvernement letton, des observateurs de l'OSCE ont suivi les élections nationales de 2011. Leur rapport suggérait diverses améliorations, qui ont été entérinées par le gouvernement de la Lettonie et mises en place lors des élections de 2015, où les observateurs de l'OSCE étaient également présents. De son côté, le Conseil de l'Europe a établi un ensemble de lignes directrices sur les aspects légaux, opérationnels et techniques pour les systèmes de votation par Internet.

Certaines tentatives ont échoué. En 2013, en Norvège, le gouvernement en place envisageait l'implantation du vote par Internet au niveau national, mais l'opposition était farouchement contre. Le gouvernement en place a tergiversé, et ce n'est qu'au printemps 2013 qu'il a autorisé l'utilisation du vote par Internet pour l'automne suivant. Avec si peu de temps, les responsables n'ont pu développer et tester convenablement le système, ce qui a mené à des défaillances.

L'enjeu de la sécurité

L'aspect sécuritaire est l'une des principales inquiétudes invoquées au sujet du vote par Internet. Or des systèmes de vote bien conçus s'inspirent d'approches utilisées avec succès dans d'autres domaines. Les systèmes sécuritaires utilisés aujourd'hui pour effectuer des transactions financières par Internet — paiement de factures, paiement par carte de crédit, dépôts directs, etc. — sont aussi utilisés pour transmettre le vote du citoyen vers le système de votation. Quant au décompte des votes, des systèmes efficaces le font en sauvegardant les votes reçus sur un serveur qui n'est pas connecté à Internet afin de l'isoler du piratage, une technique aussi utilisée par les banques pour conserver une trace des transactions effectuées.

Après une douzaine d'années d'utilisation, aucun problème important n'est apparu lors des élections municipales en Ontario et en Nouvelle-Écosse, ni aux niveaux national ou municipal en Lettonie. Les échecs recensés des différents essais tiennent davantage de la précipitation, comme le cas de la Norvège, de la mauvaise planification ou de choix technologiques douteux. L'approche « par étape » proposée pour le Québec par le DGE reprend celles suivies par les expériences réussies : on commence par un projet-pilote et on déploie plus tard l'outil à plus large échelle.

Les réussites et l’expertise accumulée depuis quinze ans montrent qu’aujourd’hui le vote par Internet a atteint un seuil de maturité qui permet d’envisager son déploiement à large échelle. L’État encourage les citoyens à faire leur déclaration de revenus par Internet, avec tous les renseignements personnels qui y sont contenus. Si un système de votation par Internet a ses particularités, il utilise des technologies connues, qui ont fait leurs preuves et que l’État utilise déjà. De plus, comme le montre la coopération entre l’OSCE et la Lettonie, le système peut être amélioré une fois mis en place.

Deux avantages principaux sont avancés en faveur d’un système de votation par Internet. Le premier concerne les coûts. Si l’implantation d’un système de votation par Internet a un prix, une fois en place il peut entraîner de substantielles réductions de frais lors de la tenue d’un vote. Et comme le soulignait le DGE, le même système peut servir au niveau municipal et au niveau national. Le second avantage est de faciliter l’acte de voter, qui peut se faire à n’importe quel moment avant la date du scrutin et à partir de chez soi.

Ces deux caractéristiques offrent la possibilité de multiplier le nombre de sujets sur lesquels les citoyens et les citoyennes peuvent se prononcer. Et ici, on parle non seulement de consultation, mais surtout de décision. Dans cette perspective, un système de votation par Internet peut permettre de donner un sens à l’expression « souveraineté du peuple ».

Le vote par Internet sera tôt ou tard une réalité. Les élus de l’Assemblée nationale doivent donner suite à l’initiative du DGE afin de doter le Québec des outils de décision politique du XXIe siècle.

https://inria.fr
Vote électronique : le logiciel Belenios s’ouvre au grand public

La plate-forme de vote électronique Belenios , conçue dans les équipes-projets communes Inria-Loria Pesto et Caramba, est désormais ouverte au public.

Chacun peut en effet organiser une élection qu’il soit ou non expert en informatique. Depuis septembre 2016, plusieurs élections de structures académiques se sont ainsi déroulées via ce logiciel et ont montré que d’autres personnes que les concepteurs pouvaient aisément mettre en place une élection grâce à cet outil. Les concepteurs Véronique Cortier et Pierrick Gaudry, directeurs de recherche CNRS ainsi que Stéphane Glondu, ingénieur Inria s’enthousiasment du succès de leur logiciel Belenios , déjà utilisé pour des élections de comités nationaux de partenaires académiques. Ouvert à tous, il est, pour le moment, davantage utilisé dans le milieu académique qu’associatif. « La contrainte pour utiliser ce logiciel est qu’il faut disposer des adresses mails de toutes les personnes qui sont susceptibles de voter, ce qui n’est pas forcément le cas dans toutes les structures associatives », complète Véronique Cortier.

Que permet le logiciel Belenios ?

Belenios assure la confidentialité des votes et permet la transparence des scrutins car, l’urne étant publique, le votant peut vérifier à tout moment que son bulletin (chiffré) est bel et bien déposé dans l’urne, grâce au code remis en amont par mail. Ce code étant un "droit" de vote, l’urne ne connaît que la partie publique des codes de vote. Ainsi, le bourrage d’urne n’est pas possible. Outre la confidentialité, Belenios garantit la vérifiabilité. Si chaque votant peut vérifier que son bulletin est dans l’urne (vérifiabilité individuelle), tout le monde peut vérifier

que le résultat correspond aux bulletins dans l'urne (vérifiabilité universelle) et tout le monde peut vérifier que les bulletins proviennent de votants légitimes (vérifiabilité de l'éligibilité)
En quoi est-il sûr ?

Le principe cryptographique de base est que le chiffrement se fait avec une clé publique et le déchiffrement avec une clé privée qui est partagée entre les autorités, souvent au nombre de trois. On parle de chiffrement à clé multiple dès lors que plusieurs clés sont nécessaires pour déchiffrer. Lors du dépouillement, seul le résultat final est déchiffré.
À quand l'utilisation du logiciel Belenios dans le milieu politique ?

Le logiciel Belenios n'est pas adapté aux élections politiques car le vote électronique reste du vote par correspondance. Il n'y a pas de réel isoloir et il faut faire confiance à l'ordinateur. Or, un ordinateur peut être infecté. L'informaticien Laurent Grégoire avait d'ailleurs montré, lors des législatives de 2012, qu'il était possible de modifier le choix d'un électeur au moment de l'envoi du bulletin dans l'urne électronique pour les Français vivant à l'étranger. Le vote papier reste plus sûr que le vote électronique.

Belenios permet d'organiser des élections qui n'existaient pas auparavant et de remplacer des outils comme Google Form ou Lime Survey , des outils initialement conçus pour des sondages et non des élections, en garantissant à la fois confidentialité et transparence. Une nouvelle version du logiciel Belenios vient de sortir, et la partie client de celui-ci est désormais distribuée sous Debian (Linux). Il n'est pas nécessaire de l'installer pour voter mais grâce à cet outil, tout électeur peut désormais contrôler facilement le bon déroulement de son élection.

https://lejournal.cnrs.fr
Le vote électronique, pour quelles élections ?

Pour lutter contre l'abstention dans les grandes élections, certains hommes politiques souhaitent que l'on puisse bientôt voter chez soi, par Internet. Mais cette mesure est-elle envisageable ?

L'électeur se cale dans son siège, connecte son ordinateur au site officiel du gouvernement, entre son identifiant et son mot de passe, clique sur le bulletin de vote de son choix et le valide. A voté ! Selon un sondage réalisé fin octobre 2015 par Harris Interactive pour le quotidien Le Parisien, 56 % des Français interrogés souhaiteraient pouvoir voter ainsi, sans avoir à se déplacer jusqu'à leur bureau de vote. Mieux : 58 % des abstentionnistes lors des précédents scrutins déclarent que, s'ils pouvaient voter par Internet, ils le feraient. Et ce nombre grimpe à 79 % chez les 18-25 ans !

À une époque où l'abstention est devenue un problème préoccupant, plusieurs responsables politiques, de droite comme de gauche, ont réagi à ce sondage en estimant urgent de mettre en place un tel système. Mais est-ce techniquement possible ? Le vote en ligne est-il aussi fiable que le vote à l'urne ?

« Pour le moment, non ! », estime Véronique Cortier, chercheuse au Laboratoire lorrain en recherche informatique et ses applications (Loria)1. Récente lauréate du prix Inria-Académie des sciences du jeune chercheur, elle et son équipe, constituée principalement de Stéphane Glondu et de Pierrick Gaudry, travaillent au développement de Belenios, un logiciel de vote par Internet. « Les problèmes à résoudre sont nombreux, estime-t-elle. Ils tiennent à deux

éléments essentiels, mais a priori contradictoires, de tout scrutin politique : le secret du vote, qui interdit de pouvoir établir un lien entre un votant et son bulletin, et la vérifiabilité, qui assure au votant que son bulletin a bel et bien été pris en compte pendant le dépouillement. »
Belenios, un logiciel libre et ouvert

Lors d'un vote classique, ces deux conditions sont remplies. Dans l'isoloir, l'électeur place le bulletin de son choix dans une enveloppe puis, devant le président du bureau de vote, le glisse dans une urne transparente. Le secret du vote est donc bien respecté. Et la vérifiabilité aussi : le votant peut s'en convaincre, s'il le souhaite, en restant dans la salle jusqu'à la fin du dépouillement.

« Les logiciels développés par les entreprises privées, remarque Véronique Cortier, se concentrent sur la confidentialité du vote, une condition d'ailleurs exigée par la Commission national de l'informatique et des libertés. La transparence du scrutin, elle, n'est pas à la hauteur : le fonctionnement de ces systèmes est secret et l'électeur ne peut rien vérifier par lui-même. »

Belenios, le programme développé au Loria, est une amélioration de Helios, un logiciel sous licence libre conçu en 2008 par Ben Adida, de l'université d'Harvard. Ce dernier a été utilisé avec succès en 2009 pour l'élection du président de l'université de Louvain (en Belgique) et, depuis 2010, pour l'élection de l'équipe dirigeante de l'Association internationale pour la recherche en cryptologie. Comme Helios, Belenios est sous licence libre et chacun pourra, s'il le veut et s'il en a la capacité, en connaître le code et le fonctionnement.
Multiplier pour mieux additionner

« Comme pour toute élection, poursuit Véronique Cortier, le scrutin électronique se compose d'une phase de vote, suivie d'une phase de dépouillement. Le votant s'identifie et sélectionne le bulletin de son choix. Ce bulletin est ensuite crypté à l'aide d'une clé publique, puis envoyé à un serveur. Sur l'écran de son ordinateur, l'électeur voit son bulletin tomber dans une urne virtuelle et rejoindre les bulletins cryptés des autres votants. »

Afin de renforcer la confidentialité du dépouillement, le décompte des voix se fait sans que les bulletins soient préalablement déchiffrés. « Belenios utilise un chiffrement de type El Gamal, qui possède une propriété homomorphique très intéressante : en combinant ensemble les bulletins cryptés, on obtient directement le résultat du vote. Mais ce résultat est crypté, et il faut le déchiffrer avant de pouvoir l'annoncer au public. »

Pour ce faire, les responsables du scrutin possèdent chacun un fragment d'une clé privée. Il faut la mise en commun des différents fragments pour permettre le déchiffrement du dépouillement. Ainsi, un responsable mal intentionné ne peut pas, avec son seul morceau de clé, avoir accès au résultat du vote et être tenté de le modifier.
Réduire les risques de fraude

Pour réduire au minimum les risques de fraude, l'équipe du Loria a multiplié les systèmes de protection. « Chaque votant possède un jeton de vote à usage unique, explique Véronique Cortier. Le bulletin est signé grâce à ce jeton, et chacun peut vérifier que les bulletins présents dans l'urne sont tous valables. Si quelqu'un attaque le serveur pour bourrer l'urne, cela se verra immédiatement… »

Imaginons maintenant qu'un hacker parvienne à intercepter un bulletin chiffré avant qu'il n'arrive dans l'urne. Puisque la clé de cryptage est la même pour tous, le hacker pourrait déduire le contenu du bulletin en le comparant avec des bulletins qu'il aurait cryptés sur son ordinateur. Le secret du vote en serait alors brisé. Pour empêcher cela, l'ordinateur de l'électeur génère, avant l'envoi du bulletin, un nombre aléatoire qui est utilisé dans le chiffrement. Ainsi, un même vote, généré à deux instants distincts, produit deux bulletins chiffrés différents.

« Mais le système n'est pas parfait, met en garde Véronique Cortier. Par exemple, lors d'un scrutin, nul ne doit pouvoir forcer la main d'un électeur. Avec un vote à l'urne, le citoyen est seul dans l'isoloir. Avec Internet, comment être sûr que, chez lui, il n'est pas menacé par quelqu'un ? Et comment s'assurer que son ordinateur n'est pas infesté par un virus capable de modifier le vote avant l'envoi ? »

Les expériences de vote électronique en France

Ces imperfections empêcheront-elles la mise en œuvre du vote en ligne en France ? En réalité, le vote électronique y a déjà été expérimenté, sous deux formes différentes. En 2003, une loi a fixé les conditions d'agrément de machines à voter électroniques : présentes dans les bureaux de vote, elles remplacent à la fois l'isoloir et l'urne. En 2007, 83 villes les avaient adoptées – Brest, Mulhouse, Le Havre, Courbevoie, Nevers… –, pour un million et demi d'électeurs, soit 3 % du corps électoral. Cependant, cette année-là, le premier tour de l'élection présidentielle a été entaché par plusieurs problèmes techniques et juridiques, comme lorsque deux machines ont été installées dans chaque bureau de vote de Reims pour écourter le temps d'attente2. Un moratoire a alors été instauré, interdisant l'adoption de ce système par de nouvelles communes.

Autre vote électronique testé lors de scrutins réels : à l'occasion des élections législatives de 2012 et consulaires de 2014, les Français résidant à l'étranger ont pu voter soit à l'urne en se rendant dans leur consulat, soit par correspondance avec un bulletin papier et des enveloppes, soit par Internet. Un votant sur deux s'est exprimé en ligne lors de ces législatives, mais sans effet notable sur le taux de participation, contrairement à ce qui était espéré.

En 2014, dans un rapport sur le vote électronique en France, les sénateurs Alain Anziani et Antoine Lefèvre se sont montrés très réservés à ce sujet. Devant l'opacité du fonctionnement des machines à voter, ils ont demandé le maintien du moratoire sur ces machines. Et, face aux imperfections du vote par Internet, ils se sont déclarés opposés à son extension au territoire métropolitain, mais favorables à son maintien pour les Français de l'étranger (le vote par correspondance, l'autre solution pour ceux qui résident loin du consulat, étant encore moins bien sécurisé que le vote en ligne).
Le vote en ligne, pour quelles élections ?

Le bilan des expérimentations menées ailleurs en Europe est, selon les deux sénateurs, lui aussi mitigé. Seules la Suisse et l'Estonie continuent à développer le vote par Internet. La seconde, surnommée « e-Estonie », investit beaucoup et depuis longtemps dans les services électroniques mis à la disposition de ses citoyens : e-carte d'identité, e-impôts, e-police, e-services de santé, e-école et, bien sûr, e-élections. Pour tous les scrutins, les Estoniens ont le choix entre le vote à l'urne et le vote à distance. En 2013, 21 % du corps électoral a voté électroniquement.

Partout ailleurs en Europe, le vote électronique stagne ou recule. L'Irlande a abandonné son programme en 2004 en raison d'un manque de fiabilité des machines à voter. En Allemagne, la Cour constitutionnelle fédérale a déclaré les machines contraires à la loi, leur exactitude n'étant pas vérifiable par le citoyen. Aux Pays-Bas, le vote par Internet a été arrêté en 2008 après une rupture de la confiance dans la fiabilité des résultats. Idem au Royaume-Uni, où le vote à distance a été testé lors d'élections locales de 2002 à 2007.

Si le vote par Internet n'est pas aussi fiable que le vote à l'urne, il est tout de même promis à un bel avenir, mais pas pour les grandes élections politiques », note Véronique Cortier. En novembre 2014, les 268 000 militants de l'UMP ont ainsi été appelés à élire leur président par Internet. En décembre 2014, les élections professionnelles à l'Éducation nationale se sont faites en ligne. En décembre 2015, les étudiants de l'Institut national des langues et civilisations orientales choisiront leurs représentants également en ligne.

« Et courant 2016, nous rendrons Belenios utilisable par tous, conclut Véronique Cortier. En allant sur un serveur dédié, les associations, les comités d'entreprise, les communes et tous ceux qui souhaitent organiser un scrutin en ligne pourront le faire librement et gratuitement. » Chacun pourra alors se faire sa propre idée sur les élections version 2.0. En attendant, un jour peut-être, de choisir un président de la République depuis son ordinateur personnel…