Université de Lille

Mémoire présenté pour obtenir le diplôme de Master 2

Faculté des Sciences Juridiques, Politiques et Sociales de Lille

❧

Département droit

Discipline : Droit du Cyberespace

Le Vote Électronique

Entre sécurité et transparence

Par : **Maxime Moisant**

Sous la direction de Marcel Moritz, Maître de Conférences HDR

Membres du jury:

Directeur : Marcel Moritz, Maître de Conférences HDR, Université de Lille

Suffragant : Valentin Gibello, Doctorant en Droit Public, Université de Lille

Date de soutenance : Septembre 2019

Sommaire

Avertissement

La faculté des sciences juridiques, politiques et sociales de Lille n'entend donner aucune approbation ni improbation aux opinions émises dans ce mémoire. Ces opinions doivent être considérées comme propres à son auteur, ou propres à ceux qui les ont émises.
Par ailleurs, l'ensemble de ce travail est édité et publié sous la licence Creative Commons BY-NC-SA 3.0.

Cette licence vous permet de remixer, arranger, et d'adapter l'ensemble de cette œuvre à des fins non-commerciales tant que son auteur est crédité en citant son nom et que les nouvelles œuvres sont diffusées selon les mêmes conditions.
L'ensemble de ce travail est disponible en libre diffusion sur le site de l'auteur : `https://maximemoisant.ovh/` avec actualisation régulière de l'ensemble des points développés selon l'avancée de l'état de l'art ou du droit en la matière. Il est également accessible directement grâce au QR Code ci-dessous.

Date de dernière à jour : **26/08/2019**
En raison de l'utilisation de termes techniques qui viendront directement qualifier et étayer la plupart des éléments de notre réflexion, l'index terminologique est placé avant le développement.

Remerciements

Je tiens en premier lieu à présenter mes respects à Marcel Moritz et à le remercier pour son temps, sa sympathie, sa disponibilité ainsi que son professionnalisme dans la direction de notre Master. Je le remercie d'avoir accepté de prendre la direction de ce mémoire.

Je remercie Valentin Gibello pour la suffragance de ce mémoire, pour le travail accompli durant cette année et pour sa disponibilité pendant les cours. Son expertise technique a apporté une vraie plus-value à l'enseignement de la cybersécurité et de la protection des données dans notre Master.

Je remercie mes collègues Corentin Hellendorff et Gregory Gitsels pour leurs encouragements ainsi que leur sympathie dans le cadre de mon stage à OVH, période durant laquelle ce travail a été réalisé.
Merci à Corentin pour sa relecture attentive et pour ses suggestions intéressantes sur certains points de fond.

La rédaction d'un tel travail n'aurait sans doute pas été possible sans le concours des intervenants suivants :
- Chantal Enguehard, docteure en informatique et maître de conférences à l'université de Nantes, pour son expertise sur le sujet. L'ensemble de ses travaux me furent très précieux pour développer ma réflexion.
- Michaël Tchilingurian, juriste au ministère des Outre-mer, pour avoir accepté de répondre à mes questions à propos de son recours devant le Conseil Constitutionnel sur l'utilisation des machines à voter.
Je remercie enfin et surtout mes proches, à commercer par mes chers parents pour leur soutien infaillible depuis mes premières années d'études, sans lesquels, jamais, je ne serai arrivé là où je suis.

Je leur dédie ce travail, ceux antérieurs, et à venir. Merci Maman et Beau-papa.

Résumé

Le vote électronique est un mode de scrutin existant depuis 1969 en France sous la forme des machines à voter et depuis 2003 sous la forme du vote par Internet. Ces dispositifs soulèvent des questions techniques et juridiques intéressantes au regard de leur fonction : servir le processus démocratique. Permettant de faciliter considérablement le dépouillement et d'accélérer le processus électoral, ces avantages ont un prix et il se paye par une perte du contrôle citoyen du scrutin et de son observation. Si on peut imaginer que la sécurité accrue de ces dispositifs peut remplacer la transparence offerte par le scrutin papier, la réalité est en fait beaucoup plus complexe et nous pose une questions sur la conception que nous avons de la démocratie selon l'importance que nous accordons à la transparence dans le processus électoral. Dernier élément analogique dans un monde qui tend vers la numérisation de toutes les démarches citoyennes, le bulletin de vote peut-il résiter encore longtemps à son informatisation ?

Abstract

Electronic voting is used in France since 1969 in the form of voting machines and since 2003 and in the form of Internet voting. These mechanisms raise interesting technical and legal issues in relation with their function : to serve the democratic process. These advantages are of great value in the process of counting votes and speeding up electoral processes, but these advantages got a price and it is paid for by a loss of citizen control over electoral processes. While we can imagine that the increased security of these devices can replace the transparency offered by the paper ballot, the reality is actually much more complex and asks us questions about the conception we have of democracy according to the importance that we give to transparency in the electoral process. Last analogical element in a world that tends towards the digitization of all the citizen processes, does the ballot paper can resist longer to its computerization ?

Index Terminologique

Adresse IP : Numéro d'identification qui est attribué de façon permanente ou provisoire à chaque périphérique relié à un réseau informatique qui utilise l'Internet Protocol.

AES : Aussi connu sous le nom de Rijndael, est un algorithme de chiffrement symétrique. Il remporta en octobre 2000 le concours AES, lancé en 1997 par le NIST et devint le nouveau standard de chiffrement pour les organisations du gouvernement des États-Unis.

Anonymat : en matière électorale, l'anonymat désigne l'impossibilité de faire correspondre un bulletin vote à un électeur.

Bit : Le bit est l'unité la plus simple dans un système de numération, ne pouvant prendre que deux valeurs, désignées le plus souvent par les chiffres 0 et 1. Un bit ou élément binaire peut représenter aussi bien une alternative logique, exprimée par faux et vrai, qu'un chiffre du système binaire.

Bug : anomalie de fonctionnement d'un programme informatique

Chiffrement : Procédé de cryptographie grâce auquel on souhaite rendre la compréhension d'un document impossible à toute personne qui n'a pas la clé de (dé)chiffrement. Ce principe est généralement lié au principe d'accès conditionnel

Confidentialité : l'électeur exprime son choix en votant seul, à l'abri des pressions.

Dépouillement : opération désignant la révélation des votes et le décompte du nombre de voix attribuées à chaque candidat et du nombre de votes blancs ou nuls.

Disponibilité (des données) : La disponibilité d'un équipement ou d'un système est une mesure de performance qu'on obtient en divisant la durée durant laquelle ledit équipement ou système est opérationnel par la durée totale durant laquelle on aurait souhaité qu'il le soit. On exprime classiquement ce ratio sous forme de pourcentage.

Dispositif de vote électronique / Système de vote électronique : ensemble de matériels et logiciels réalisant le recueil et/ou le décompte de suffrages.

Donnée à caractère personnel : Une donnée à caractère personnel correspond en droit français à toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Exploit : dans le domaine de la sécurité informatique, un exploit est un élément de programme permettant à un individu ou à un logiciel malveillant d'exploiter une faille de sécurité informatique dans un système informatique.
Intégrité (des données) : De manière générale, l'intégrité des données désigne l'état de données qui, lors de leur traitement, de leur conservation ou de leur transmission, ne subissent aucune altération ou destruction volontaire ou accidentelle, et conservent un format permettant leur utilisation.
IPSec : Cadre de standards ouverts pour assurer des communications privées et protégées sur des réseaux IP, par l'utilisation des services de sécurité cryptographiques
Logiciel / Programme : suite d'instructions exécutées par un ordinateur
Métadonnée : Donnée servant à définir ou décrire une autre donnée quel que soit son support.
Modèle OSI : norme de communication, en réseau, de tous les systèmes informatiques qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions.
Octet : Un octet est un multiple de 8 bits codant une information. Dans ce système de codage, s'appuyant sur le système binaire, un octet permet de représenter 28 nombres, soit 256 valeurs différentes.
Paquet : Dans le contexte d'un réseau informatique, le paquet est l'entité de transmission de la couche réseau (couche 3 du modèle OSI).
Sécurité (des données) : En sécurité des systèmes d'information, la sécurité des données est la branche qui s'intéresse principalement aux données, en complément des aspects de traitement de l'information.
Sandbox : Un ou une sandbox (anglicisme signifiant « bac à sable ») est un mécanisme de sécurité informatique qui permet l'exécution de logiciel(s) avec moins de risques pour le système d'exploitation. Ces derniers sont souvent utilisés pour exécuter du code non testé ou de provenance douteuse.
Serveur : un serveur est généralement un ordinateur plus puissant qu'un ordinateur de bureau traditionnel. Il est spécialement conçu pour fournir des informations et des logiciels à d'autres ordinateurs qui lui sont reliés via un réseau.
Sincérité : en matière électorale, la sincérité est la conformité des choix exprimés par les électeurs par rapport aux résultats dépouillés.
Système informatique (SI) : dispositif électronique recevant des informations, disposant d'une capacité de traiter et de stocker les informations et donnant des résultats.

Transparence : les représentants partis, candidats, électeurs et observateurs peuvent suivre le déroulement des opérations électorales. La transparence permet de constater les éventuels dysfonctionnements ou fraudes et d'en présenter des preuves à un juge électoral.

Unicité : en matière électorale, elle garantit que chaque électeur ne peut voter qu'une seule fois.

Violation de donnée (à caractère personnel) : Une violation de données survient lorsque les données dont une entreprise/organisation est responsable subissent un incident de sécurité qui entraîne une violation de la confidentialité, de la disponibilité ou de l'intégrité.

Introduction Générale

Dans la série télévisée américaine dramatique et politique *Scandal* le candidat à la présidence des Etats-Unis Fitzgerald Grant est élu grâce à une fraude organisée à son insu sur des machines à voter dans le Comté de Defiance. La fraude, rendue possible par un logiciel truqué, ne sera jamais détectée. Le concepteur des machines était un conglomérant propriétaire de nombreux casinos, soutenant activement le candidat Grant dans son accession au pouvoir. Pensant avoir été élu en toute légalité et porté par le vote de dizaines de millions d'américains, ce dernier connaîtra la vérité bien plus tard au cours de son mandat et fera tout pour faire taire ceux qui partageaient ce secret.

Les conséquences liées à l'adoption de formes de « vote automatisé » est la source de nombreuses fictions, littéraires ou cinématographiques, qui d'ailleurs, pour la plupart, n'en font pas l'éloge. Dans la réalité cependant, certains affirment que l'informatisation du vote a créé une « citoyenneté digitale » qui amorce l'entrée de la société dans une « cyberdémocratie » et qui annonce tout simplement la fin de la fraude électorale. Les éloges ne manquent pas, mais d'un point de vue moins profane, plus juridique, on ne peut qu'être dubitatif, voire méfiant. En effet, quels sont les enjeux liés à l'évolution de ce protocole républicain saturé de rites ? Annonce-telle une mutation radicale et irréversible de la vie civique ? Ou s'agit-il d'un banal remplacement du vote papier impulsé par une volonté politique et économique ? La réponse à ces questions se trouve dans les nuances des gris.

Le vote est un rituel démocratique existant depuis la Grèce antique permettant à un groupe d'individus de faire, parmi plusieurs propositions, un choix collectif en agrégeant des préférences individuelles. C'est le processus démocratique par excellence. Les choix personnels de chacun sont additionnés, soit en les traitant à égalité, soit en les pondérant en fonction de ceux qui les ont émis, c'est à dire en leur affectant un poids variable en fonction de critères déterminés. Chaque vote contribue ainsi à la formation d'un résultat brut associant une valeur numérique à chaque proposition, donnant un poids final à celle-ci. Ce résultat fait ensuite l'objet de règles d'interprétation et d'un contrôle qui déterminent si un choix collectif a été valablement exprimé et, si oui, de déterminer le choix qui a été fait. Lorsque ce dernier

correspond à la désignation d'une ou plusieurs personnes, on parle d'*« élection »*.

On observe que depuis quelques années, un glissement sémantique s'est opéré. Le système électoral n'est plus simplement un mode de scrutin ou un concept, ou plus largement un principe de fonctionnement. Le système électoral est devenu aujourd'hui un objet tangible, réel : on parle de « système de vote ». Avec l'informatique moderne et l'invention des machines à voter, cette évolution a contribué à créer le terme « système de vote automatisé » pour les dispositifs analogiques, puis le terme « système de vote électronique » [1] pour les dispositifs numériques.

On désigne *« système de vote automatisé »* tout système électoral dans lequel le dépouillement est réalisé par une *« machine »* dont la définition même varie selon sa structure. Nous inclurons dans cette définition le vote grâce à des bulletins à scan optique, de machines à rouages électromécaniques, ou encore grâce à des ordinateurs, qu'ils soient installés dans un bureau de vote ou utilisés pour se connecter à un serveur par l'intermédiaire d'Internet. Plus précisément, ces deux derniers moyens seront l'objet de notre étude. Le vote électronique n'a pas de définition précise en raison de la multitude des vecteurs de vote possibles et d'un manque de base légale, en France, pour les qualifier. Cependant, on peut prendre pour critère, avec le Forum des droits sur l'Internet [2] : l'émission des suffrages au moyen de dispositifs électroniques [3] . Il ne s'agit donc que d'un cas particulier de l'automatisation de l'élection qui a eu lieu à la fin du XXème, phénomène qui correspond à l'informatisation de l'émission des votes et du processus de dépouillement. Cette informatisation de l'élection sera ainsi abordée sous l'angle des machines à voter et sous celui du vote par correspondance électronique, c'est-à-dire le vote par Internet.

L'informatique moderne et le développement d'Internet a tout changé. En effet, le rôle notable des mutations technologiques dans le passage de notre société de l'ère industrielle à l'ère de l'information invite à nous interroger sur la pérennité de nos modèles juridiques et politiques qui eux, restent inchangés depuis de nombreuses décennies. Il est clairement établi que les évolutions technologiques induisent des

1. Commission nationale de l'informatique et des libertés, *Délibération n°2003-036*, Paris, 1er juil. 2003.

2. Le Forum des droits sur l'Internet est une association créée en 2001 avec le soutien des pouvoirs publics, qui a pour mission d'informer les citoyens sur les enjeux liés au développement d'Internet et d'organiser la concertation entre les différents acteurs des réseaux.

3. Forum des droits de l'internet, *Rapport d'activité pour l'année 2003*, sous la dir. de La Documentation française, Paris, 2004, p. 400, isbn : 2-11-0055942-4, url : `https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/044000213.pdf`, voir p. 273.

évolutions politiques. Par exemple, les réseaux sociaux sont devenus la matrice de la plupart des mouvements populaires modernes (Printemps arabe, mouvement des gilets jaunes). Quel est le rôle joué par le vote électronique dans cette transformation ? Quelle place occupe le vote électronique dans ces innovations et plus largement l'informatisation du vote ou de l'opnion ?

Il peut être aussi audacieux que dangereux d'imaginer une société française dans laquelle chaque citoyen doté du droit de vote, à l'aide d'un terminal relié à Internet, voire de son smartphone, puisse voter pour le Président de la République, son député, son maire, voire même voter directement pour ou contre certaines lois. Cette vision politique et militante d'une démocratie directe poussée à son paroxysme peut être très clivante, car bien qu'elle soit théoriquement rendue possible par le développement fabuleux des nouvelles technologies de ces dernières années, il pourrait s'agir d'un immense iceberg dont on ne voit que la surface.

Même si l'on sait que l'article 2 de Constitution de la République Française de 1958 fait mention d'un *« gouvernement du peuple, par le peuple et pour le peuple »* la France est pourtant une démocratie représentative, et en conséquence le pouvoir est exercé par des élus. Les élections nationales constituent un temps fort pour toutes les démocraties, il s'agit de choisir de nouveaux élus auxquels le peuple va confier son pouvoir à de nouveaux représentants. Cette opération change durablement le visage du pays, car elle a une influence sur l'ensemble des pouvoirs régaliens : la police, l'éducation, la justice, la défense... Les irrégularités ou les soupçons de fraudes dans une opération aussi sensible peuvent avoir des effets dévastateurs dans la vie démocratique : manifestations importantes, émeutes et dans le pire des cas, des coups d'état [4].

De la machine à voter à l'ordinateur de vote

Il serait cependant inexact de penser que le vote électronique est une invention nouvelle seulement rendue possible par le développement de l'informatique moderne. La question de la dématérialisation du vote et de sa facilitation de comptage est explorée depuis bien avant l'invention des premiers ordinateurs. L'inventeur de l'ampoule électrique Thomas Edison, dès 1869, imaginait déjà un système électromécanique pour compter les votes populaires, idée qu'il a lui-même repris d'un brevet

4. Les exemples d'élections contestées sont nombreux : Félix Tshisekedi au Congo en 2019, Nicolas Maduro au Venezuela la même année, Ibrahim Boubacar Keïta au Mali en 2018.

déposé en 1850 par Albert Henderson.

A l'époque, le sujet est appuyé par le gouvernement américain : on cherche à gagner du temps lors du décompte des voix pour le vote lors des élections fédérales, car beaucoup de postes sont à pourvoir et le dépouillement à chaque scrutin est chronophage et onéreux. Malheureusement, la machine de Edison, certainement trop en avance sur son temps n'attirera aucune faveur des élus du Congrès, dont même l'un d'entre eux dira, en prophétisant [5], *« if there is any invention on earth that we don't want down here, that is it »* [6]. La machine de Edison subsistera à l'état de brevet... jusqu'en 1906.

Cette année-là, à l'Exposition de Milan, une machine à voter est présentée. Cette étrange boîte porte sur sa face antérieure un nombre convenable de fentes. Le votant introduit dans la fente un disque, que vient de lui tendre le démonstrateur de la machine, un certain Eugenio Boggiano. Ce disque déclenche à l'intérieur deux mécanismes : l'un fait apparaître le total des votes exprimés ; l'autre fait apparaître le nombre des votes émis en faveur de chaque option. Le tout peut être facilement masqué jusqu'à la fin du scrutin. Le disque sort de l'appareil pour être remis au citoyen suivant, et recommencer son office. Boggiano a inventé l'urne mécanique, et devient l'ancêtre du vote électronique. Il aura également inventé, sans en avoir conscience, les principes de bases des machines à sous.

Les inventions et les innovations en la matière vont se succéder rapidement, mais dans l'indifférence générale des démocraties européennes qui auront adoptées le vote à bulletin papier, restant encore aujourd'hui l'une de seules formes de vote, sinon l'unique, qui garantit cumulativement l'unicité, l'anonymat, la confidentialité de chaque voix ainsi que la sincérité du scrutin et surtout la confiance des électeurs en l'issue du scrutin. Ces adjectifs ne sont pas anodins. Ils déterminent la validité d'une élection et seront largement explorés au cours de notre réflexion.

La sémantique du terme « machine » est importante comme nous le disions précédemment. L'une des premières définitions du mot machine indique « Appareil, instrument permettant de réaliser de manière mécanique ou simplifiée les tâches et travaux de la vie courante ». Ce n'est pas un hasard, les premières machines à voter étaient appelées ainsi car elles fonctionnaient avec un système de tringlerie

5. « Thomas A. Edison papers », *in* : *Choice Reviews Online* (1998), ISSN : 0009-4978, DOI : 10.5860/choice.35sup-163.

6. « S'il y a bien une seule invention dont nous ne voulons pas sur Terre, c'est celle-ci »

électromécanique « semblable au compteur kilométrique des anciennes voitures » [7]. En ce temps, les machines à voter ne faisait qu'office « d'urne », c'est-à-dire que l'électeur pressé des boutons mécaniques au travers d'une interaction physique avec la machine, qui se chargeait de transformer ce bouton poussé en un vote collecté et enregistré dans la machine. La nuance est importante, car les nouveaux dispositifs d'aujourd'hui ne sont plus des machines, mais bien des ordinateurs.

Les décennies passant et les évolutions technologiques se produisant, la machine à voter de 1970 et celles de 2007 n'ont ainsi plus rien de semblable, on peut parler aujourd'hui d' « ordinateur de vote » du fait de la numérisation totale du bulletin et de l'urne, alors que les « machines » étaient analogiques et n'avaient que pour seule fonction de compter les voix plus rapidement et de créer une élection plus rapide, plus simple, plus fiable. Cependant le terme « machine à voter » est resté dans le langage commun, bien qu'elles n'ont aujourd'hui de « machine » que le nom. Le mot « ordinateur » se trouve même dans le Littré comme adjectif désignant Dieu qui met de l'ordre dans le monde : allégorie de l'informatique moderne, confinant à la magie pour quiconque la découvre.

La machine à voter en France

Le droit de vote en France est exercé par « tous les nationaux français majeurs des deux sexes, jouissant de leurs droits civils et politiques » auxquels s'ajoutent les citoyens de l'Union Européenne pour les élections européennes et municipales [8]. Ce droit est universel, égal et secret. Depuis la fin du XIXème siècle, ses modalités d'exercice sont globalement restées figées pour l'immense majorité du corps électoral : le bulletin de vote papier, l'enveloppe, l'urne transparente, le passage dans l'isoloir sont autant d'ingrédients constituant la recette d'une république dont le fonctionnement perdure depuis la fin du XIXème siècle.

Le vote électronique, et plus particulièrement l'arrivée des machines à voter dans le paysage électoral en 1969 [9] est l'objet de beaucoup de clivages idéologiques et d'espoirs déçus : les machines à voter de 1973, année de leur première utilisation, sont victimes de nombreuses pannes et autres défaillances. L'état de l'art et de la technologie informatique de l'époque ne pouvant apporter de vraies solutions aux problèmes posés par ces dysfonctionnements, les machines à voter ont été donc progressivement

7. Voir Annexe 1 « Entretien avec Chantal Enguehard »
8. Art. 3 de la Constitution de la Vème République du 4 Octobre 1958
9. Loi n° 69-419 du 10 mai 1969 modifiant certaines dispositions du code électoral

abandonnées dans les années 1980, malgré un élargissement des possibilités d'utilisation de ces machines en 1988 [10] . Trop en avance sur leur temps, ces machines auraient sans doute eu un sort bien différent avec un déploiement au moins trois décennies plus tard.

Remises au gout du jour au début des années 2000 par le ministre de l'intérieur Nicolas Sarkozy, les évolutions technologiques le séparant de Georges Pompidou permettent le développement d'une machine à voter de nouvelle génération, entièrement électronique, plus fiable, et mieux encadrée dans le déploiement comme dans la maintenance : on numérise l'urne, mais aussi le bulletin de vote, car l'ordinateur devient autonome. Afin d'alléger les ressources humaines et financières nécessaires à l'organisation des élections et d'optimiser la durée du dépouillement et la centralisation des résultats, le code électoral permettait alors toujours l'utilisation de moyen de vote électronique nommés sous l'appellation générique de « machines à voter » ; texte qui resta le même depuis 1969 [11].

Le règlement technique de 2003

Pour combler les faiblesses afférentes aux anciens dispositifs, un règlement technique fixant les conditions d'agrément des machines à voter est pris sous la forme d'un arrêté [12] du ministère de l'intérieur en 2003, créant de ce fait un agrément afin d'homologuer ces machines pour une utilisation dans les communes de France. Encore en vigueur aujourd'hui, ce document de 43 pages est composé de 114 exigences et de 15 principes fondamentaux auxquels doivent répondre chaque machine utilisée officiellement dans le cadre des élections politiques nationales et locales.

Ce règlement, bien que souffrant de nombreuses lacunes techniques que nous développerons au cours de notre réflexion a tout de même pour mérite de fixer un cadre normatif spécifique à l'utilisation et la fabrication des machines à voter. En France, les modèles qui sont utilisés proviennent des trois fabricants suivants :

— Nedap : trois modèles très semblables (« 2.07 F », « ESF1 » et « HW 1.06/2 ou FW 4.02) ») ;

10. La Loi n° 88-1262 du 30 décembre 1955 modifiant certaines dispositions du code électoral et code des communes relatives aux procédures de vote et au fonctionnement des conseils municipaux élargie la faculté d'utilisation des machines à voter dans les communes de plus de 3 500 habitants, au lieu de 30 000 jusqu'alors.
11. *Code électoral 2019*, Dalloz-Sirey, déc. 2018, ISBN : 978-2247177578, voir Art. L57-1.
12. JORF n°274 du 27 novembre 2003 p. 20188

— iVotronic : modèle produit par la société Election Systems and Software (ES and S) ;
— Indra : modèle « Point & Vote plus » produit par la société espagnole INDRA SISTEMAS SA et importé en France par Berger-Levrault.

Nedap équipe 20 000 bureaux de vote en Europe, ce qui en fait le leader européen dans la commercialisation des machines à voter.

Le rôle de l'État en la matière est un rôle de régulateur : on peut constater que le marché du vote électronique est un marché comme les autres et que les machines à voter sont des produits techniques comme les autres, dans la mesure où seul l'agrément du ministère de l'intérieur donne le caractère « officiel » à ces machines. De fait, ces machines sont soumises au droit de la propriété industrielle et de celui des brevets : cela soulève d'autres problèmes qui seront abordés au cours de notre réflexion.

Le vote électronique est donc à ce titre un objet de droit qui suscite passions et méfiance. Avènement de la cyberdémocratie pour les uns, source de risques cyber considérables pour les autres, personne n'est indifférent à la façon dont nos dirigeants sont choisis et à la façon dont les élections se déroulent. L'une de ses conséquences majeures du vote électronique est de changer nos habitudes de citoyens, pourtant, le juge ne semble pas disposer à se doter d'une vision technique tangible du vote électronique : son approche reste traditionnaliste comme nous le verrons à travers l'ensemble de sa jurisprudence.

Le vote papier est l'un des derniers éléments analogiques dans un monde qui tend vers la numérisation de toutes les démarches administratives et citoyennes. On pourrait citer la réussite (même relative) que représente la possibilité de déclarer ses impôts en ligne. Si la réussite ne relève pas d'exploit techniques particuliers, elle relève en revanche d'une économie de moyens considérable (ouverture des mairies, timbres, formulaires, temps de présence des agents publics). Si la possibilité de réduire les coûts est un leitmotiv contemporain, alors utiliser ces technologies à des fins électorales semble être un chemin naturel.

Le bulletin de vote papier reste cependant un élément fondamental et traditionnel de notre république. Il permet d'exercer directement le pouvoir souverain dont est détenteur chaque citoyen. Repenser la façon de voter, c'est repenser la démocratie et

la souveraineté du peuple. En ce sens, Edwy Plenel indique dans son livre Le Droit de savoir :
« La souveraineté du peuple, c'est la nation à l'état abstrait, c'est l'âme du pays ; elle se manifeste sous deux formes : d'une main, elle écrit, c'est la liberté de la presse ; de l'autre, elle vote, c'est le suffrage universel. »

Le vote électronique dans le monde

A travers le monde, l'utilisation du vote électronique pour servir le processus politique n'est pourtant pas chose nouvelle. En 2006, les Pays-Bas sont les plus avancés en matière de vote électronique : 90% du corps électoral utilise des machines à voter depuis 1990.

Les États-Unis ont une grande expérience des dispositifs de vote électronique. Au début des années 2000, de nombreuses difficultés sont survenues. Elles n'étaient pas dues au vote électronique, mais à une technologie plus ancienne : les cartes perforées. Pour la plupart mal dessinées, elles ont été difficiles à recompter dans le cadre de l'élection présidentielle de 2000 : concédons toutefois qu'avec cette technologie, il restait possible de vérifier le scrutin, au travers d'un recomptage des voix. En réaction à cette affaire, la loi HAVA [13] a été votée en 2002. Elle a incité à remplacer les technologies anciennes : en 2006, environ 40% des électeurs ont utilisé des ordinateurs tout-électronique, semblables à ceux utilisés en France en 2007. En 2016, cette part a chuté à 33% des votants, tandis que 63% d'entre eux ont opté pour un dispositif de scan optique. Le vote papier ne représente alors, lors de l'élection de Donald Trump, que 1,5% de l'ensemble des bulletins. [14]

Avec la technologie du scan optique, les bulletins de vote sont marqués d'une « croix » et peuvent être scannés sur des systèmes de numérisation optiques situés dans le lieu de vote (« système de dépouillement ») ou dans un système centralisé (« système de dépouillement central »). La plupart des systèmes de numérisation optique plus anciens utilisent la technologie de numérisation infrarouge et les bulletins de vote avec des marques sur les bords afin de numériser avec précision un bulletin de vote papier.

13. American Congress, *Help America Vote Act of 2002*, Washington, 2002, URL : `https://www.congress.gov/bill/107th-congress/house-bill/3295`.
14. Engineering et al., *Securing the Vote : Protecting American Democracy (Cybersecurity)*, National Academies Press, 2018, ISBN : 030947647X, voir TABLE 3-1.

Les systèmes plus récents peuvent utiliser la technologie de « virtualisation », une image numérique de chaque bulletin étant prise pendant le processus de numérisation. Le scan optique est une technologie conçue comme alliant le meilleur des deux mondes : la rapidité offerte par le vote électronique, et la fiabilité offerte par le vote papier. Cependant, cette technologie ne donnant à la machine que la fonction « d'urne » et n'étant utilisé qu'aux Etats-Unis, elle ne sera pas développée davantage dans notre réflexion.

La Belgique a démarré des expériences de vote électronique en 1991. Cela concerne actuellement 50% des électeurs, proportion stagnant depuis 1999. Trois des quatre partis francophones se sont prononcés contre l'utilisation de ce dispositif. Une proposition de loi [15] a imaginé en 2005 d'abandonner le vote électronique et de s'en tenir à l'automatisation du dépouillement : les électeurs votent comme avant, et une machine aide à compter les bulletins, ce projet n'a jamais abouti.

Le 11 juin 2011, le journal L'Avenir annonce que « le gouvernement wallon a décidé d'abandonner le vote électronique dans les 39 communes pilotes. » Le coût réel du vote électronique en Belgique n'a à ce jour fait l'objet d'aucune étude. Selon ses détracteurs, il s'élèverait à trois fois le prix du vote papier traditionnel [16]. Le vote électronique serait plus cher à l'investissement mais aussi en frais d'utilisation que le vote papier.

La Suisse est quant à elle un laboratoire et pionnière du vote par Internet (correspondance électronique) ; et même en France, à une échelle plus locale, notamment par l'utilisation de machines à voter dans certaines communes, ou via le vote par Internet lors des élections professionnelles, ou des élections législatives et consulaires pour les français de l'étranger. On observe que la dématérialisation du vote se subordonne à un enchevêtrement de complications juridiques et techniques que nous tâcherons d'explorer au cours de toute notre réflexion.

Le vote électronique est donc utilisé pour qualifier notamment deux façons de voter :

— Les ordinateurs de vote [17] (ou « machines à voter ») ;

15. Proposition de loi visant la suppression du vote automatisé et la généralisation du dépouillement par lecture optique (Nyssens 3-120)

16. Collectif PourEVA, *Position des présidents de parti sur le vote électronique*, 2007, URL : `https://www.youtube.com/watch?v=E0Xii6MW1Sc` (visité le 25/08/2019).

17. Le terme de « machine à voter » est utilisé depuis 1969, époque où il ne s'agissait pas d'informatique. De fait, il n'est plus approprié aux ordinateurs modernes actuellement utilisés.

  - Ils enregistrent les votes et les dépouillent, sans s'occuper de l'identification de l'électeur ni de son émargement. Trois fabricants sont autorisés depuis 2004 : Nedap (néerlandais), ES and S (américain) et Indra (espagnol)
  - Certaines communes en France disposent des telles machines depuis 1988 comme évoqué précédemment
  - Quelques dizaines de villes les utilisent, dont sept de taille moyenne : Amiens, Boulogne-Billancourt, Brest, le Havre, Reims, Le Mans, et Mulhouse
  - D'autres villes les ont jugés insatisfaisants : Cannes, Grenoble, Sceaux et St Denis
  - Depuis 2007, ce sont 66 communes [18] (82 en 2007) représentant au total 3% du corps électoral français, soit 1 300 000 électeurs, qui sont concernées encore aujourd'hui par l'utilisation des machines à voter
- Le vote par Internet (ou vote par correspondance électronique)
  - Le vote transite à travers le réseau Internet, du votant vers des serveurs électoraux qui font office d'urnes. Dans cette forme de vote, chaque citoyen peut théoriquement exercer son pouvoir depuis n'importe quel terminal relié à Internet, et en conséquence, peut le faire depuis n'importe où dans le monde. L'identification et l'émargement sont gérés par le serveur.
  - Si le vote par Internet revêtait il y a encore quelques années un caractère expérimental, de grandes villes comme Genève ont éprouvé cette méthode de vote en tirant des conclusions étonnantes qui seront développés au cours de notre réflexion.
  - En France, l'utilisation de ce dispositif n'est autorisée que dans le cadre des élections professionnelles [19], et dans les élections législatives et consulaires pour les français de l'étranger [20]

Cette liste n'est pas exhaustive, il existe d'autres dispositifs de vote électronique comme les lecteurs à scan optique ou les kiosques de votes. Notre étude va néanmoins se restreindre à aborder la question du vote sur les machines à voter et sur

Cependant, on peut constater que le marketing du fabricant Nedap/France-Élection cherche à faire croire qu'il ne s'agit pas d'informatique, éludant les problématiques inhérentes au fonctionnement d'un ordinateur.

18. Guillemin Christophe, *1,5 million d'électeurs français inaugureront le vote électronique le 22 avril*, 2007, URL : `https://www.zdnet.fr/i/edit/ne/2007/04/communes.html` (visité le 25/08/2019).

19. *Code du travail 2019*, Dalloz-Sirey, déc. 2018, ISBN : 978-2247186433, voir Art. R2314-5.

20. *Code électoral 2019*, voir Art. R176-3.

le vote par Internet. D'une part, la littérature scientifique abondante à ce sujet va permettre de développer notre réflexion mais également parce que le vote par Internet est sans doute la forme de vote électronique la plus prometteuse. Les machines à voter restent les dispositifs de vote électronique les plus traditionnels et les premiers qui viennent à l'esprit pour les profanes lorsque l'on parle de vote électronique.

Par ailleurs, ces deux dispositifs développés ci-dessus sont concernés par des problématiques techniques et juridiques semblables : sécurité et transparence du scrutin, confiance des électeurs dans le résultat du scrutin, influence de la participation à l'élection, coût de l'organisation du scrutin et son monitoring [21]. Cependant le vote par Internet se distingue du fait de sa décentralisation.

En effet, la démocratisation de l'accès à Internet à la fin des années 1990, son omniprésence dans le quotidien et le fonctionnement des pays développés, ainsi que son incroyable pénétration dans les foyers (en France métropolitaine, en décembre 2018, 92.8% des foyers sont connectés à Internet [22]) ont fait naître l'idée que le réseau mondial pouvait permettre un vote à distance. La réalisation pratique d'un tel mode de scrutin apparaît facile à mettre en oeuvre, puisqu'il n'est pas nécessaire de concevoir une machine à voter spécifique : n'importe quel serveur connecté à Internet est suffisant, et seul le logiciel doit être développé.

Le vote par Internet peut ainsi être considéré comme l'avenir du vote électronique, dans sa forme la plus aboutie. Cependant, assurer la sécurité et la transparence d'un tel mode de scrutin est un défi technique et juridique considérable qui s'heurte à une réalité indéniable : Internet est devenu le théâtre et la loge de nouvelles menaces.

Le processus de référendum d'initiative partagée : un premier pas vers le vote par Internet ?

L'utilisation d'Internet afin de consulter le corps électoral pour une prise de décision à portée nationale trouve son exemple dans l'actualité la plus récente. Le 9 Mai 2019, 248 députés et sénateurs de l'opposition ont déclenché un processus de

21. En informatique, le monitoring désigne la mesure, l'observation et le contrôle d'un système et ses composantes : programmes, données manipulées, résultats, utilisation des ressources...

22. Miniwatts Marketing Group, *Data for the 28 Member States of the European Union*, 2019, URL : `https://www.internetworldstats.com/europa.htm#fr` (visité le 25/08/2019).

"référendum d'initiative partagée" en saisissant le Conseil Constitutionnel [23]. Ils ont jusqu'au 12 mars 2020 pour récolter 4,7 millions de signatures sur la question de la privatisation du groupe ADP. (Aéroports de Paris) Si l'objectif est atteint, le gouvernement devra organiser un référendum national courant 2020 afin que les français donnent leur avis sur ce sujet devenu polémique.

Cette consultation constitue une double-nouveauté. D'une part, c'est la première fois que le « RIP », introduit en 2008 dans la loi française est utilisé. Ce dernier nécessite la réunion de plusieurs conditions, et notamment le soutien d'un cinquième des parlementaires puis de 10% du corps électoral. D'autre part, la collecte de signatures se fait en ligne sur le site Internet du ministère de l'intérieur. Chaque citoyen français inscrit sur les listes électorales peut, à l'aide de sa carte d'identité nationale, déposer son soutien au projet de référendum depuis son domicile, par la simple utilisation d'un terminal relié à Internet.

Bien que le site Internet sur lequel se fait la récolte des signatures (site Internet du ministère de l'intérieur) souffre de nombreux dysfonctionnements techniques dès son lancement, il s'agit d'une première expérience de ce à quoi pourrait ressembler un vote par correspondance électronique à portée nationale. Bien entendu les conditions sont bien différentes : la liste de l'ensemble des soutiens est affichée publiquement et peut être consultée en temps réel sur le site du ministère de l'intérieur, et le résultat de cette consultation n'est pas d'application directe car le référendum, s'il est organisé, se fera dans des bureaux avec un bulletin de vote papier.

L'enjeu de la cybersécurité

Si l'on s'intéresse aux conséquences de l'automatisation sur la sécurité des systèmes de vote, on ne peut que constater que le recours à des machines rend possible un grand nombre d'atteintes qui ne sont pas possibles avec des bulletins en papier. Ces atteintes, ou plutôt ces violations, sont rendues possibles par des détournements matériels ou logiciels qui altèrent le fonctionnement des dispositifs. Ce principe de sécurité est aujourd'hui devenu un enjeu majeur, à l'heure de l'interconnexion de machines à voter, et par l'utilisation d'Internet pour le déroulement des élections.

Aux Pays-Bas en 2006, un groupe composé de militants anti-vote électronique

23. Décision n° 2019-1 RIP du 9 mai 2019 du Conseil Constitutionnel

« Wij vertrouwen stemcomputers niet » [24] révéla au public des failles de sécurité critiques dans les machines à voter de marque Nedap, utilisées pour les élections de 2006 aux Pays-Bas, lors d'une émission de télévision nationale de grande écoute. Ces machines sont encore aujourd'hui largement utilisées en Europe.

Le rapport écrit, rendu public par la suite, démontre qu'il est étonnamment facile d'ouvrir la machine à voter ; le boîtier intérieur qui renferme l'électronique n'avait qu'une protection élémentaire : le remplacement du logiciel, le remplacement de composants voire l'ajout de composants s'en trouvait ainsi facilité. Par ailleurs, il a été démontré par la suite que le système logique de la machine n'était même pas chiffré, les données étaient lisibles en clair et les puces pouvaient donc être remplacées.

Le 27 septembre 2007, la commission Korthals-Altes, formée à la suite de la publication du rapport du groupe d'activistes, publie un autre rapport critiquant les machines à voter utilisées comme insuffisamment contrôlables, « car ne fournissant pas de trace papier. Le système ne permet pas non plus de garantir le secret du vote, et les frais élevés de son développement ne sont pas justifiés en regard des maigres avantages que peut procurer un tel système » [25] Le 16 mai 2008, le gouvernement néerlandais annonce l'abandon définitif du vote électronique et le retour au « papier et au crayon ».

En 2016, lors de l'élection de Donald Trump comme président des Etats-Unis, des soupçons de piratage lors de l'élection par une puissance extérieure planent alors sur l'élection et une enquête est ouverte sur le rôle de la Russie dans l'élection de Donald Trump. Le New York Times [26]. constate que plusieurs machines à voter ont été compromises par un accès illicite [27].

Un vent de panique et de méfiance souffle alors sur le marché du vote électronique. À la suite des allégations de piratage par la Russie dont aurait été victime la candidate Hillary Clinton, le gouvernement nééerlandais renonce en janvier 2017 à

24. « Nous ne faisons pas confiance aux machines à voter »

25. Nonnenmacher François, *Les Pays-Bas abandonnent définitivement le vote électronique*, 2008, URL : `https://www.padawan.info/fr/vote_electronique/les_paysbas_abandonnent_definitivement_le_vote_electronique.html` (visité le 25/08/2019).

26. Zeter Kim, *The Myth of the Hacker-Proof Voting Machine*, 2018, URL : `https://www.nytimes.com/2018/02/21/magazine/the-myth-of-the-hacker-proof-voting-machine.html` (visité le 25/08/2019).

27. Par illégal, au sens informatique du terme, il faut entendre par des moyens visant à s'approprier des permissions systèmes qu'un utilisateur normal n'est pas censé détenir.

utiliser le moindre logiciel pour même simplement aider à compter les voix. Force est de constater que les machines à voter ne sont pas invulnérables, mais qu'en plus, certaines d'entre elles peuvent être piratées facilement et que des failles informatiques connues et datant de plusieurs années ne sont pas bouchées, car les mises à jour de sécurité critiques ne sont pas appliquées, comme celles concernant par exemple l'exploit [28] EternalBlue. [29]

La sécurité d'une élection dont le principal vecteur est le vote par Internet est une problématique qui ne saurait se régler par des efforts technologiques ou industriels. L'éternelle course à la sécurité masque des problématiques de transparence évidentes. Cette problématique est d'ailleurs commune à tous les dispositifs de vote électronique : vote par correspondance électronique ou ordinateurs de vote. En effet, dans une élection classique à bulletin papier, l'urne dans laquelle les votes sont déposés est transparente dans les deux sens du terme : l'ensemble des enveloppes est visible de tous. Ce n'est pas par simple fantaisie que l'urne est transparente, il s'agit au contraire d'obéir à une nécessité de transparence dans le cadre de toute élection, car la transparence conditionne la confiance de l'électeur.

Le conflit transparence versus sécurité

Dans une élection dématérialisée, la transparence relève du mythe. C'est d'ailleurs le principe de base de l'informatique moderne en général : les phénomènes physiques qui se déroulent dans un ordinateur sont connus théoriquement, selon des modèles et équations mathématiques éprouvés, mais ne sont pas directement observables : il est impossible de voir un électron se déplacer dans un circuit imprimé. Par ailleurs, même s'il était possible de l'observer, il y aurait des conséquences qui rendraient caduques l'observation, en raison de principes physiques qui ne sauraient être développés au cours de notre réflexion [30] : l'observation d'une particule aussi insignifiante qu'un électron modifierait la nature même de ce qu'on observe.

28. Un exploit, dans le domaine de la sécurité informatique, est un élément de programme permettant à un individu ou à un logiciel malveillant d'exploiter une faille de sécurité informatique dans un système informatique.

29. EternalBlue est un exploit utilisant une faille de sécurité présente dans la première version du protocole SMB. Bien que cette faille de sécurité ait été résolue par Microsoft dans une mise à jour de sécurité publiée le 14 mars 2017 de nombreux utilisateurs de Windows n'avaient toujours pas installé ce correctif de sécurité lorsque, le 12 mai 2017, le ransomware « WannaCry » utilisa cette faille de sécurité pour se propager.

30. Ces principes relèvent de la mécanique quantique, domaine de la science encore mal connu est profondément technique.

Naturellement, on pourrait alors se dire qu'une sécurité accrue d'un dispositif de vote électronique pourrait remplacer ou pallier ce manque de transparence pour l'électeur. Mais est-ce si simple ? Aprés tout, il n'existe aucune loi disposant l'obligation de transparence dans une élection. En matière de vote électronique, seul existe le règlement technique relatif aux machines à voter de 2003, dont justement, l'exactitude scientifique et technique reste contestable et sera largement développée au cours de notre réflexion.

Théoriquement, dans une procédure de vote sur une machine à voter, cette procédure peut être vue comme un système vérifié, dont tous les éléments sont interdépendants : de l'identification jusqu'à l'enregistrement du vote. Pour beaucoup d'acteurs, notamment les politiques et les industriels, le principe général devant gouverner les systèmes de vote est celui de sécurité, de sorte que les règles de droit tendent à garantir la sécurité des systèmes de vote, malheureusement au prix de la transparence.

Dans le contexte d'une élection par vote dématérialisée : l'objet de la confiance de l'électeur n'est plus le même : on ne nous invite plus à faire confiance en l'issue du scrutin, mais on nous invite davantage à faire confiance en un dispositif destiné à recueillir notre vote et à tout un ensemble de règles et de certifications qui sont censés garantir la sincérité du scrutin. La différence n'est pas anecdotique et a des conséquences sur l'acceptation du scrutin.

Les procédés techniques mis en œuvre dans les systèmes de vote électronique sont souvent d'une grande complexité, à base notamment de techniques de chiffrement, ce qui nécessite généralement, pour les évaluer, le recours à une expertise tierce. Mais cette expertise se limite le plus souvent à quelques aspects du système et ne va rarement, sinon jamais, au cœur du système lui-même. En outre, la plupart des éditeurs de ces systèmes se réfugient derrière le secret industriel pour ne rien révéler sur le fonctionnement réel de leur produit, ce qui constitue d'ailleurs un obstacle majeur quand on cherche à encourager la confiance de l'électeur ou quand on cherche naturellement à s'assurer de l'efficacité ou de la fiabilité technique de la partie « logiciel », ou même de la partie « matériel » dans le cadre d'un audit. Mais un audit serait-il suffisant pour chasser le doute ? La réponse est complexe et dépend du protocole de conception et de vérification employé.

La course à la sûreté et à la fiabilité

Le dispositif technique déployé dans le cadre d'une élection présente souvent des négligences flagrantes sous certains aspects pourtant essentiels à la préservation de l'anonymat du vote : il en est ainsi de certains procédés de vote à distance pour lesquels l'électeur, par exemple, s'authentifie par un nom et un mot de passe. Ces informations étant éditées par un sous-traitant puis distribuées par courrier ordinaire non recommandé, voire transmis en main propre par un service de la mairie sans qu'aucune mesure de protection particulière ne soit prise pour les préserver leur confidentialité, comment certifier l'intégrité et l'authenticité de ces informations ?

Devant l'installation d'un nombre croissant de systèmes de vote automatisé depuis le début des années 2000, de nombreux experts se sont intéressés à la sécurité de ces dispositifs, qui, comme l'a souligné le Conseil de l'Europe, doit être garantie par les États [31]. Les études sur la question se sont multipliées, et ont porté sur les machines employées lors des votations populaires, car les votations parlementaires sont le plus souvent publiques : contrôlables, vérifiables avec le nom de chaque parlementaire associé à son vote.

Il ressort notamment des expertises que les possibilités d'atteinte à la disponibilité et à l'intégrité des systèmes sont nombreuses. Il convient de souligner ici que ces études présentent un ensemble de potentialités, en faisant abstraction des problèmes ayant pu se poser concrètement, ce qui suffit à établir l'insécurité des systèmes.

L'analyse des études montre avant tout que les atteintes à la sécurité proviennent de la complexité des dispositifs. En effet, les fabricants ont toujours eu pour objectif de simplifier au maximum l'interface entre les électeurs et la machine, il leur a fallu pour cela accroître sans cesse la complexité interne des systèmes, qui étaient souvent, lors de leur introduction, à la pointe de la technologie.

Or, d'une manière générale, il est admis que plus un système est complexe, plus il est difficile de garantir sa sécurité, principalement parce que les interactions entre les composants deviennent trop nombreuses pour être totalement comprises, que ce soit par les experts qui peuvent être mandatés par l'État, ou même par les concepteurs eux-mêmes.

31. Council of Europe, *Legal, Operational And Technical Standards for E-voting - Recommendation Rec (2004)11 And Explanatory Memorandum*, Council of Europe, mai 2005, ISBN : 9287156352, voir norme 28.

En somme, personne ne peut imaginer l'ensemble des événements qui se déroule sur les circuits imprimés d'une machine, qu'ils soient d'origine volontaire ou involontaire, pouvant conduire à une défaillance, et les ingénieurs en sont généralement réduits à corriger les problèmes qui se sont déjà posés et qui ont été identifié, sans pour autant garantir qu'un système soit exempt de défauts.

L'ensemble des remarques précédentes s'appliquent surtout et en particulier à la partie « logiciel », qui équipe la plupart des machines et qui constitue la principale source de problèmes de sécurité. Selon le père du logiciel libre et de la licence GNU, Richard Stallman, un système informatique complexe équipé d'un logiciel donné, aussi perfectionné et contrôlé soit-il ne peut être exempt d'erreurs d'exécution ou de « bugs » [32].

Cependant, il faut garder à l'esprit, comme évoqué précédemment, qu'il ne s'agit pas de jouer aux apprenti-sorciers : tous les modèles mathématiques et physiques que les ingénieurs utilisent pour concevoir ces systèmes sont des modèles éprouvés, mis en œuvre dans chaque dispositif électronique de notre quotidien et qui, au fil des décennies, ne cessent d'être améliorés.

Dans le cadre du vote par correspondance électronique, lorsqu'un système de vote est accessible en réseau, comme c'est notamment le cas des serveurs de vote par Internet, il est possible que des attaquants exploitent une ou plusieurs vulnérabilités présentes dans les applications, les protocoles réseau ou dans le système d'exploitation et prennent le contrôle de la machine à distance.

Il devient alors possible de remplacer certains composants de l'application électorale par des versions modifiées, d'introduire des programmes dont la fonction est d'altérer le fonctionnement du logiciel de vote ou de modifier le programme utilisé, le tout par le biais d'attaques informatiques distantes. Dans une certaine mesure, il est également possible de violer le secret du vote des électeurs en pouvant « ouvrir » l'enveloppe virtuelle contenant le bulletin qui transite sur le réseau sans que ni le serveur de vote, ni l'électeur n'en ait conscience.

La problématique de la sûreté des machines est une réelle préoccupation : le cas

32. LINUXCARE, *Richard Stallman's Interview*, 1999, URL : `https://lists.gnu.org/archive/html/help-gnu-emacs/2010-12/msg00744.html` (visité le 25/08/2019).

de l'élection de Donald Trump a engendré beaucoup d'enquêtes et d'études sur la fiabilité des systèmes de vote sans pour autant mettre en doute officiellement la sincérité du scrutin de la présidentielle américaine de 2016. Par exemple, le magazine en ligne américain The Intercept [33], publie un article le 17 Juin 2017 en rendant public un rapport classifié de la NSA mentionnant que des hackers du renseignement militaire russe ont essayé à maintes reprises de pénétrer dans les systèmes électoraux américains. [34]

Bien que l'article original ne le mentionne pas explicitement, il n'est cependant pas clairement établi à ce jour que l'élection présidentielle américaine de 2016 ait été biaisée du fait de l'ingérence russe sur le plan médiatique ou sur le plan informatique [35]. Cependant, ces seuls soupçons auront suffi pour persuader les Pays-Bas de prolonger leur moratoire sur les machines à voter [36].

Un nouveau protocole de vote

Les atteintes possibles à la disponibilité, à l'intégrité et au secret rendent donc indispensable une évolution du cadre normatif lié à l'utilisation des systèmes de vote automatisé. Le règlement technique rédigé et publié en 2003, évoqué précédemment, n'est plus adapté aux nouveaux enjeux liés à la sécurité moderne des systèmes d'information : des solutions doivent être trouvées afin de restaurer la confiance. En effet, s'il est possible, comme évoqué, de corriger ponctuellement certains problèmes, la multiplication des mesures de sécurisation rend paradoxalement les systèmes plus complexes et donc plus fragiles.

L'essor du vote par Internet, promesse de campagne de Emmanuel Macron est

33. The Intercept est une plateforme journalistique qui révéle des documents classifiés de la NSA. Fondé par Glenn Greenwald, journaliste qui a hautement contribué dans la publication des révélations d'Edward Snowden sur les programmes de surveillances de la NSA.

34. Esposito Richard, *Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election*, 2017, URL : `https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/` (visité le 25/08/2019).

35. Vinogradoff Luc, *Le spectre de la désinformation russe derrière les « fake news » sur Internet*, 2016, URL : `https://www.lemonde.fr/big-browser/article/2016/11/30/le-spectre-de-la-desinformation-russe-derriere-les-fake-news-sur-internet_5040983_4832693.html` (visité le 25/08/2019).

36. Lausson Julien, *Les Néerlandais tournent le dos à la gestion électronique des élections législatives*, 2017, URL : `https://www.numerama.com/politique/229515-les-neerlandais-tournent-le-dos-a-la-gestion-electronique-des-elections-legislatives.html` (visité le 25/08/2019).

encore aujourd'hui incertain. Concernant les machines à voter, le gouvernement d'Edouard Philippe a annoncé que le statu quo sur le moratoire, en vigueur depuis plus de dix ans, serait maintenu, empêchant ainsi toute nouvelle commune d'opter pour de tels appareils. Le ministère de l'Intérieur a toutefois annoncé, en septembre 2017, peu après la nomination de Gérard Collomb, que différentes mesures de simplification en matière de :

> sécurité informatique, juridique et matérielle des scrutins électoraux [serait] proposées, parmi lesquelles la dématérialisation de la propagande électorale, la normalisation des bulletins de vote et l'interdiction des machines à voter.

Cette mesure a déclenché une levée de boucliers de certains parlementaires de la majorité présidentielle, partisans du vote électronique, notamment au travers de questions écrites, comme celle posée par la députée Isabelle Florennes en Aout 2018, dont la réponse écrite n'a été publiée au Journal Officiel qu'à la fin du mois de Juillet 2019 [37]. Elle évoquait ainsi dans sa question le point suivant :

> « Les machines à voter permettent d'éviter les erreurs humaines qui surviennent généralement lors du dépouillement. En cela, elles représentent un véritable gain de temps. Et, contrairement au vote via Internet, souvent mis en avant, les machines à voter ne peuvent faire l'objet de détournement ou de cyberattaque puisqu'elles ne sont pas connectées, preuve supplémentaire de leur fiabilité. »

Le ministère de l'Intérieur a répondu que les machines à voter continuent de soulever de « sérieuses difficultés » :

> « allongement des temps d'attente dans les bureaux équipés, coût élevé pour les communes et l'État (entre 4 000 et 6 000 euros en 2007 pour l'achat d'une machine, auxquels s'ajoutent les frais d'entretien, de stockage et de formation), et surtout méfiance des citoyens devant l'impossibilité de recompter physiquement des bulletins de vote » [38] .

Il est par conséquent préférable de rechercher des solutions d'ensemble permettant, en particulier, de contourner le fait que les machines à voter apparaissent comme des « boîtes noires » impossibles à contrôler, ce qui résoudrait d'une part la recherche de la transparence et d'autre part l'opacité des systèmes de vote. La seule solution tangible semble être d'imaginer de nouveaux protocoles de vote, moins dépendant

37. Florennes Isabelle, *Possible suppresion des machines à voter - Question écrite*, 2018, URL : `http://questions.assemblee-nationale.fr/q15/15-11516QE.htm` (visité le 25/08/2019).

38. Prunaud Christine, *Interdiction des machines à voter - Question écrite*, 2017, URL : `http://www.senat.fr/basile/visio.do?id=qSEQ171101801` (visité le 25/08/2019).

des personnes privées et davantage relevant d'une initiative souveraine et ouverte.

Si l'on admet à propos des systèmes de vote électroniques que la sécurité ne peut remplacer la transparence [39], alors qu'il est en même temps difficilement envisageable de pouvoir faire en sorte qu'un système informatique soit transparent dans son fonctionnement, une question centrale se pose alors : **Comment assurer l'équilibre entre transparence et sécurité dans les dispositifs de vote électronique ?**

39. Voir Annexe 1 « Entretien avec Chantal Enguehard »

L'utilisation des nouvelles technologies à des fins électorales reste dans l'ensemble un succès relatif. Si Internet a par exemple permis à l'ensemble des partis politiques de développer leur propagande électorale et de toucher une masse d'électeurs toujours plus grande et dans une certaine mesure, beaucoup plus ciblée, l'utilisation des ordinateurs dans le dispositif électoral reste très anecdotique, mais juste dans le nombre de machines déployées : moins d'une centaine de communes en France sont équipées de machines à voter, mais leur fonctionnement reste révolutionnaire. Si le Juge reste doté d'une approche méfiante et traditionnaliste de sa jurisprudence en matière de contention électoral face au vote électronique, le développement du vote par Internet ainsi que du marché qu'il a créé sans oublier les technologies développées à cet effet, ne sont certainement pas à négliger, bien au contraire. [**Partie 1**] Si les machines à voter sont destinées à tomber en désuétude comme le voudrait le président Emmanuel Macron, le vote par Internet va quant à lui subsister et se développer. Les machines à voter ou le vote par Internet sont des techniques indéniablement porteuses de changement dans la vie démocratique. On peut d'ailleurs observer que les citoyens eux-mêmes se sont emparés du sujet, au travers de groupes de réflexions ou de militants. Ces technologies, comme si elles étaient dotées d'une force qui leur était propre, permettent des découvertes sur le plan informatique, et peuvent laisser songeur sur le devenir juridique et politique qu'est l'acte du vote. [**Partie 2**]

Première partie

La modernisation du vote par l'automatisation : la voix mécanisée du peuple

Le cadre normatif du vote électronique révèle un attachement de l'État aux principes de sécurité et de fiabilité des élections organisées par voie électronique : machines à voter ou vote par correspondance. Ces dernières années, le Sénat a également eu l'occasion de se prononcer au travers de la production de deux rapports sur la pratique du vote électronique en France au sens large. Tout d'abord un rapport en 2014 abordant la question de la transparence des machines et des conclusions sur des expériences sur le vote par Internet dans l'Union Européenne, et un autre rapport en 2018, doté d'une approche plus partisane et plaidant pour le retour des machines à voter, l'extension de leur utilisation et un encouragement fort sur le développement du vote par Internet. Nous verrons que ce dernier rapport, en particulier, a une approche plus politique que scientifique de cette question. La question de l'évolution de la jurisprudence du juge et de sa compétence sera également posée. **(Chapitre 1)** Si le vote électronique est un objet juridique fascinant, d'où notre étude, nous verrons qu'il échappe en vérité à un très large public : le juge, les parlementaires, les électeurs. D'une part, il n'est pas nécessairement compris par ceux qui en font l'utilisation, et d'autre part son contrôle échappe aux acteurs étatiques de par son opacité. Or, on sait qu'en matière de sécurité informatique, la sécurité par l'obscurité est la pire des solutions envisageables. Les atteintes techniques rendues possibles par le vote électronique ainsi que les problématiques inhérentes à l'utilisation de tout système informatique seront développées car leurs conséquences sont importantes sur plan juridique et sur le plan technique. Du fait de ces considérations, une méfiance de l'électorat et des acteurs étatiques s'est naturellement développée malgré encore la présence de beaucoup de partisans chez les industriels et les politiques. **(Chapitre 2)**

Chapitre 1

Un cadre juridique stable mais de plus en plus inadapté

La forme la plus ancienne de vote électronique est la machine à voter. Elles sont autorisées depuis 1969, mais réellement utilisées depuis les années 2000 en raison des améliorations apportées aux machines traditionnelles et rendues possibles par l'informatique moderne. Le règlement technique de 2003 vient fixer des règles pour encadrer leur utilisation, et le vote par Internet est autorisé pour les élections professionnelles. (1.1) Cette informatisation du vote a des conséquences juridiques importantes, notamment concernant les recours, on annonce tout simplement la fin du contentieux électoral. Quel est par ailleurs le rôle du juge dans la régulation de ces dispositifs ? (1.2) Le vote électronique est aujourd'hui devenu un sujet politique : un rapport du sénat encourage la fin du moratoire et la reprise de la commercialisation des machines pour les communes. Le vote électronique et plus particulièrement le vote par Internet est par ailleurs au centre d'une promesse électorale du président Emmanuel Macron. (1.3)

1.1 Le vote électronique comme expérience juridique et politique

Globalement le résultats liés au vote électronique en France sont insatisfaisants. La plupart des mairies qui accueilleront en 1969 ces machines ne les verront pas d'un bon œil **(1.1.1)** néanmoins ces machines furent une tentative d'imposer un nouveau standard pour les processus électoraux. **(1.1.2)** Ces échecs de mise en œuvre ont contribué à l'abandon temporaire des machines à voter, puis à leur relance et leur modernisation **(1.1.3)** et dans un souci de modernité et de simplicité, des expérimentations relatives au vote par Internet furent lancées **(1.1.4)**

1.1.1 Des débuts difficiles et une diminution des prérogatives du maire

En 1969, une première tentative d'installation de machines à voter est faite en région parisienne et en Corse. Comme évoqué en introduction, la loi du 10 mai 1969, promulguée dans l'intérim entre la présidence de Charles de Gaulle et celle de Georges Pompidou autorise et codifie l'emploi de machines à voter (elles se présentent alors sous forme d'urnes rudimentaires électromécaniques) dans certaines communes de la banlieue parisienne et en Corse.

Le gouvernement annonce, pour appuyer cette expérimentation, des objectifs de transparence, de modernisation du processus électoral, de simplification de l'environnement administratif de l'acte électoral et la poursuite d'un objectif de réduction des dépenses publiques. En réalité, il s'agit surtout de lutter contre la fraude électorale : on constate des irrégularités manifestes dans les scrutins organisés dans certaines mairies tenues par les communistes autour de la région parisienne et d'autres cas de fraude en Corse. Malgré les réserves du ministère des Finances, le ministre fait importer des États-Unis les premières machines à voter.

Le 27 décembre 1972, Raymond Marcellin, alors ministre de l'intérieur fixe par décret publié au Journal Officiel de la République Française du 28 décembre 1972 [1] la liste des communes où est autorisée l'utilisation des machines à voter. Mêlant villes de droite et villes communistes le tout pour masquer l'intention initiale, le décret prévoit également pour appuyer cette sélection un critère de taille : 30 000 habitants. Dans l'opinion et chez la plupart des maires, cette liste sera perçue comme

1. JORF du 28 décembre 1972 p. 13590

infâmante, car elle labélise les pratiques de certaines mairies comme déviantes. Ce qu'on peut constater, c'est que le contexte de la mise en place de ces machines n'est pas le même entre celui de leur instauration en 1969 et celui de leur remise au goût du jour dans les années 2000 : le premier était clairement appuyé par une volonté politique de diminution des fraudes, le second est marqué par une volonté de réduction des coûts et une modernisation de l'acte électoral.

L'une des conséquences juridiques notables de l'utilisation dès 1973 des machines à voter est une diminution drastique du rôle du maire dans le contrôle du bon déroulement des élections dans les communes. En effet, le code général des collectivités territoriales accorde une grande importance à la place du maire dans le processus institutionnel en général.

Article L2212-1 du Code Général des Collectivités Territoriales

Le maire est chargé, sous le contrôle administratif du représentant de l'État dans le département, de la police municipale, de la police rurale et de l'exécution des actes de l'État qui y sont relatifs.

Le maire dispose également d'autres prérogatives régies par le Code Électoral. Les articles R42 à R71 font intervenir le maire dans la plupart des étapes liées aux procédures électorales, comme la présidence des bureaux de vote [2], la désignation des assesseurs [3], la mise à disposition des bulletins nécessaires aux élections [4] ou encore la proclamation des résultats [5].

Avec l'utilisation des machines à voter, le maire est délesté de la plupart de ces prérogatives : s'il reste garant symbolique de l'autorité de l'État au sein de sa commune, c'est la machine qui est placée au centre du dispositif et non plus la logistique organisée par le maire.

2. *Code électoral 2019*, voir Art. R43.
3. *Ibid.*, voir Art. R44 et 45.
4. *Ibid.*, voir Art. R55.
5. *Ibid.*, voir Art. R69.

Article R55-1 du Code Électoral

Avant le scrutin, le maire fait procéder à la mise en place sur la machine du dispositif indiquant les candidatures, telles qu'elles figurent sur la liste adressée par le préfet.

Ce changement bouleverse les standards électoraux mis en place à travers le pays depuis la révolution de 1789.

1.1.2 De nouveaux standards et dispositifs électoraux

Avec l'utilisation des machines à voter, une rupture de l'uniformité des dispositifs électoraux se créé : certaines communes auront recours à des urnes électromécaniques tandis que d'autres devront s'en tenir (jusqu'en 2004) à l'urne transparente classique. C'est la première fois sous la république qu'une diversité des dispositifs est impulsée par l'État. En effet, depuis les premières élections libres de 1791 en France, on a pu constater une recherche constante de procédures standardisées et de dispositifs communs à l'ensemble du territoire, comme l'isoloir ou les enveloppes [6].

L'uniformisation du dispositif a une valeur symbolique et une valeur juridique qui ont deux objectifs communs : d'une part n'importe quel électeur vote de la même façon et dans les mêmes conditions, donnant une forme d'unité nationale [7] ; d'autre part cette uniformisation permet de respecter beaucoup plus facilement les principes directeurs du droit électoral évoqués au début de notre réflexion, encourageant la sincérité du scrutin.

Il faut toutefois noter qu'en comparaison avec le processus de vote traditionnel, la plupart des étapes sont conservées : présence d'un isoloir contenant la machine, marquage du nombre de votants sur un compteur pouvant être lu pendant les opérations de vote, obligation de possibilité d'enregistrement du vote blanc, total des suffrages obtenus par liste ne pouvant être lu qu'à la clôture des scrutins ou encore l'obligation d'émargement à côté des machines à voter.

6. Olivier Ihl, « L'urne électorale. Formes et usages d'une technique de vote », fre, *in* : (1993), ISSN : 0035-2950, DOI : 10.3406/rfsp.1993.394716, URL : https://www.persee.fr/doc/rfsp_0035-2950_1993_num_43_1_394716.

7. Yves Déloye et Olivier Ihl, « Introduction. De l'élection à l'acte de vote », FR, *in* : *L'acte de vote*, Références, Paris : Presses de Sciences Po, 2008, p. 11–29, ISBN : 9782724610581, voir Chapitre I.

Le code électoral dispose que chaque bureau de vote est équipé d'une unique machine à voter [8]. Si les dispositions ne le mentionnent pas explicitement, le Conseil Constitutionnel énonce que l'article utilise le terme « la machine » au singulier. En conséquence, on peut considérer une machine à voter comme une urne, laquelle ne peut être placé qu'à hauteur d'un exemplaire unique par bureau. [9]

L'encadrement juridique des machines à voter de 1973 reste solide car leur fonctionnement reprend celui de la machine de Bagianno de 1906 mais en plus abouti. Ici, la machine ne fait qu'office d'urne. Le votant presse des boutons mécaniques pour exprimer son choix, le fonctionnement de la machine reste analogique et l'utilisation de circuits imprimés ne sert qu'à alimenter la machine afin d'éclairer des lampes pour l'affichage de son panneau. De ce fait, la réglementation technique reste très anecdotique et n'énonce que des principes fonctionnels. Les machines à voter doivent être d'un modèle agréé par arrêté du ministre de l'intérieur et satisfaire aux conditions techniques suivantes :

Article L51-1 du Code Électoral

(...)
- ne pas permettre l'enregistrement de plus d'un seul suffrage par électeur ;
(...)
- ne pouvoir être utilisées qu'à l'aide de deux clefs différentes, de telle manière que, pendant la durée du scrutin, l'une reste entre les mains du président du bureau de vote et l'autre entre les mains de l'assesseur tiré au sort parmi l'ensemble des assesseurs.

Malgré tout, l'expérience tourne à l'échec : la résistance de certaines mairies à adopter ces nouveaux dispositifs ainsi que les pannes techniques contraignent le ministère de l'intérieur à rapatrier la plupart des machines dans les locaux du ministère. Ces machines seront pour la plupart condamnées à y rester sans que les communes ne les utilisent à nouveau. La maintenance de ces machines était difficile et les incidents techniques pouvaient être d'une grande gravité. « Il pouvait arriver qu'à la fin d'une journée de scrutin, lorsqu'on consultait les compteurs pour connaître les

8. *Code électoral 2019*, voir Art. R63.
9. Décision n°2007-3872 du 4 octobre 2007 du Conseil Constitutionnel

résultats, ils soient encore à zéro. » [10]

1.1.3 Un abandon... pour une modernisation progressive

De la machine à l'ordinateur

L'encadrement juridique des machines à voter va continuer d'évoluer progressivement pour une accélaration à partir du début des années 2000. Si le texte est resté le même sans renforcement du périmètre technique depuis 1969, la donne commence à changer en 1988. En effet, une nouvelle exigence technique est apportée au texte initial :

Article L51-1 du Code Électoral

(...)
- permettre plusieurs élections de type différent le même jour à compter du 1er janvier 1991 ;
(...)

Cette nouvelle condition vient mettre un terme à l'utilisation de l'ensemble des machines à voter utilisées jusqu'à cette date. Il n'était effectivement pas possible d'installer la machine afin de permettre plusieurs scrutins en raison de limitations technologiques : les compteurs devaient être remis à zéro, la machine était soumise à divers tests avant chaque tenue d'élection. Le législateur pousse l'utilisation de l'informatique qui, en 1988, est encore balbutiante.
En 2005, la loi n° 2005-102 du 11 février 2005 pour l'égalité des droits et des chances, la participation et la citoyenneté des personnes handicapées vient rappeler l'exigence d'un vote universel. Elle impose en effet l'obligation pour les personnes handicapées de pouvoir voter seules, quel que soit leur handicap :

Article L51-1 du Code Électoral à jour de la loi n°2005-102

(...)
- permettre aux électeurs handicapés de voter de façon autonome, quel que soit leur handicap ;
(...)

10. Voir Annexe 1 « Entretien avec Chantal Enguehard »

La plupart des modèles agréés par le ministère de l'intérieur étaient déjà conforme à cette disposition en 2005. Le 17 novembre 2003, Nicolas Sarkozy, Ministre de l'interieur, de la sécurité intérieure et des libertés locales réglemente les conditions d'agrément des machines à voter dans un arrêté portant approbation du règlement technique fixant les conditions d'agrément des machines à voter. Cet arrêté publié au Journal Officiel de la République Française le 27 novembre 2003 constitue, en son temps, une avancée majeure pour le vote électronique [11].

Un règlement technique aux nombreuses lacunes techniques

Ce règlement, censé faire entrer les machines à voter dans l'ère de l'informatique moderne prévoit ainsi que chaque machine fasse l'objet d'un audit par un organe de certification indépendant. Il donne lieu à un rapport confidentiel, transmis au ministère qui accorde ou non l'agrément. Dès sa publication cependant, le règlement est pourtant critiqué pour ses lacunes scientifiques et techniques. Parmi les principes fondamentaux, le règlement impose celui de « transparence » ou encore celui de « vérifiabilité » du scrutin.

Pour Chantal Enguehard, la vérifiabilité des résultats d'une machine à la fin d'une journée de scrutin n'est possible que par l'intégration d'un système de double-vérification avec des bulletins papiers (le machine génère un vote papier pour chaque voix émise) : en d'autres termes, une trace palpable est nécessaire afin de pouvoir mener à bien des vérifications. Cependant, aucune machine à voter utilisée en France n'intègre à ce jour un tel dispositif. Les scrutins ne peuvent donc pas être vérifiés : seule fait foi la mémoire de la machine.

De même, le règlement impose le principe de « transparence ». Or, dans un système informatique, la transparence n'a pas de sens : le vote est « transformé » plusieurs fois pendant son parcours sur les circuits imprimés de la machine, passant d'un mouvement de bouton, à une conversion en courant électrique complexe pour finir par être stocké sur une puce. De plus l'électeur n'a pas connaissance du fonctionnement exact de la machine ni de son logiciel, on entretient une opacité difficilement acceptable. Par exemple les rapports d'expertise de ces systèmes ne sont pas consultables publiquement, les logiciels utilisés dans ces machines sont des logiciels propriétaires, l'électeur n'a pas un moyen direct et fiable de vérifier son vote...

11. Arrêté du 17 novembre 2003 portant approbation du règlement technique fixant les conditions d'agrément des machines à voter (NOR/INT/X/03/06924/A)

De plus, le périmètre technique du règlement n'intègre pas la partie logique de la machine à voter, pourtant fondamentale dans un système informatique : les mots « code source » n'apparaissent nulle part, le mot « logiciel » n'est évoqué que dans un contexte fonctionnel : il est nécessaire au bon fonctionnement de la machine et le mot « transparence » n'apparaît que dans sa propre définition sans donner les moyens de la mettre en œuvre. Le règlement ne fixe ainsi aucun principe gouvernant le logiciel : son développement, sa compilation, son déploiement ou sa maintenance. [12]

Le règlement de 2003 est resté inchangé depuis sa publication et s'applique toujours aux machines à voter utilisées dans les communes de France. Au total, ce sont près de 1 300 000 électeurs concernés dans toute la France par l'utilisation des machines à voter encore aujourd'hui, soit plus de 3% du corps électoral. Rapidement le gouvernement va réfléchir à la mise en place d'autres modes de scrutins. La même année que l'adoption du règlement technique sur les machines à voter en 2003, une nouvelle expérience est tentée : le vote par Internet.

1.1.4 L'expérience du vote par Internet

Les français de l'étranger : pionniers du vote par Internet

Un rapport du Forum des droits de l'Internet remis au gouvernement en 2003 préconise un déploiement méthodique du vote électronique dans le domaine des élections politiques nationales et celui des élections professionnelles, notamment, tout un chapitre sur le vote par Internet y est consacré [13]. Une première expérience de vote par Internet pour des élections nationales a donc eu lieu en 2003 lors de l'élection des représentants à l'Assemblée des Français de l'étranger sur les deux circonscriptions aux Etats-Unis. Elle a été reconduite en 2006 sur l'ensemble des circonscriptions électorales des français de l'étranger. Dans l'intervalle un expert est cependant missionné pour auditer ce système car des doutes subsistent sur sa fiabilité.

Cet audit donne lieu à un rapport qui émet des réserves sur la possibilité de réaliser un scrutin sincère et fiable lorsque le suffrage de l'électeur est entièrement dématérialisé. Selon le rapport, le recours à l'isoloir dans un environnement électoral contrôlé tel qu'un bureau de vote traditionnel reste le meilleur moyen afin de

12. Voir Annexe 1 « Entretien avec Chantal Enguehard »
13. Forum des droits de l'internet, *op. cit.*

maintenir le secret du scrutin la liberté du vote de l'électeur. Toujours selon le rapport, il s'agirait de la seule façon d'assurer la sincérité du processus électoral. Les recommandations de ce rapport seront globalement ignorées, jusqu'en 2010.

En effet, la CNIL s'est intéressée de près au vote électronique dans le cadre d'une délibération de 2010 [14]. Elle pose un socle de réglementation commun au vote par Internet et au vote par machines à voter. La délibération porte sur « la sécurité des systèmes de vote électronique » sans distinction de moyen. La principale nouveauté de cette délibération est la mise en avant de dispositions servant à garantir la sécurité logicielle des dispositifs. La CNIL recommande ainsi de nombreuses mesures qui n'étaient alors pas mises en oeuvre. Ces préconisations couvrent entre autres : expertise du code source du logiciel, expertise des mécanismes de chiffrement utilisé, notamment pour le chiffrement du bulletin de vote sur le poste de l'électeur, expertise des échanges réseau, et enfin le fait que l'expertise doit être réalisée par un expert indépendant. Ces dispositions donneront lieu en 2013 à une inscription, certes rudimentaire, dans la loi de ces exigences de secret du vote et de sincérité du scrutin lié au système de vote utilisé [15].

Elles seront mises en œuvre pour les français de l'étranger jusqu'en 2017 dans le cadre des élections législatives et consulaires. Les recommandations en matière de sécurité vont également être reprises pour l'utilisation du vote électronique dans les élections professionnelles. Si on semble assister à une généralisation prudente du vote électronique, cette dématérialisation n'est pas sans conséquence juridique pour les électeurs ou pour le juge. Le vote électronique vient développer un nouveau type de contentieux, ou plus exactement, comme nous le verrons, il pourrait mettre fin au contentieux électoral. Comment la jurisprudence électorale s'adapte-t-telle à cette évolution ?

14. Délibération n° 2010-371 du 21 octobre 2010 de la Commission Nationale Informatique et Libertés

15. *Code électoral 2019*, voir Art. L33 et suivants.

1.2 Le vote électronique et l'adaptation d'un nouveau contentieux électoral

Pour contester une élection, cette contestation doit s'appuyer sur des preuves solides au-delà de simples suspicions. A ce titre, le contrôle du scrutin, notamment par son observation, donne les preuves requises pour appuyer une requête en annulation. (1.2.1) Dans le cadre du vote électronique sur des machines à voter ou même par Internet, la fourniture de ces preuves est cependant plus complexe. (1.2.2)

1.2.1 L'importance du contrôle du scrutin en matière contentieuse

L'informatisation du vote est soumise aux mêmes principes que le vote papier, en conséquence, l'informatisation ne résout pas les possibles irrégularités liées au vote papier qui peuvent engendrer l'annulation du scrutin. La violation de ces principes, peut ainsi avoir pour conséquence que la volonté réelle des électeurs « ne peut pas être connue de manière certaine, et donc qu'il est impossible de connaître avec certitude le choix majoritaire des électeurs » [16]. Dans le cas où plus particulièrement la sincérité du scrutin est atteinte, le juge annule l'élection. Dans ce cas, naturellement, l'élection est annulée par le juge. Ces principes fondamentaux d'ailleurs, comme évoqués en introduction sont l'égalité, la liberté et le caractère secret du vote [17].

Le respect cumulatif de ces principes vise à assurer la sincérité du scrutin. En conséquence, l'observation des élections est cruciale, car elle a justement pour but de s'assurer de la sincérité du scrutin. C'est l'observation qui permet de révéler au juge des manquements aux principes mentionnés afin d'obtenir l'annulation de l'élection. Lors d'une élection par vote à bulletin papier, les procédures électorales, de l'identification de l'électeur jusqu'au dépouillement, se déroulent en présence de personnes autorisées à contrôler les opérations électorales, leur permettant une observation concrète des procédures dans les limites de leurs sens : ouïe, toucher, vue, etc [18].

Dans le cadre d'une élection dématérialisée, via un vote par Internet ou par l'utilisation des machines à voter, la situation est bien différente : on assiste à un glissement de la plupart des procédures électorales vers un environnement virtualisé

16. Richard Ghevontian, éd., *La sincérité du scrutin*, fre.
17. *Ibid.*
18. Chantal Enguehard et Tatiana Shulga-Morskaya, « De l'annulation d'élections par Internet par le moyen des insuffisances du système de vote », *in* : *Les convergences du droit et du numérique*, Bordeaux, France, 2017, URL : https://hal.inria.fr/hal-01730380.

et non contrôlé : identification de l'électeur, expression de l'intention du vote, envoi du vote, comptage du nombre de votes... rendant l'observation des opérations électorales beaucoup plus complexe, voire impossible.

De ces obstacles découle une première conclusion importante : comment démontrer au juge que la sincérité d'une élection est atteinte pour obtenir son annulation ? Les requérants, souvent simples électeurs ou candidats ne sont pas en capacité de détecter l'ensemble des irrégularités et de les prouver. On pourrait imaginer que le juge essayerait d'appliquer sa jurisprudence « traditionnelle » que nous développerons dans quelques instants, mais cette application rencontre très vite sa limite liée à l'utilisation de ce nouveau procédé.

1.2.2 La difficulté de soulever des moyens techniques

La compétence du juge est déterminée en fonction de la nature de l'élection : le juge constitutionnel (et donc administratif) est compétent pour les contentieux liés aux élections politiques, et le juge judiciaire est compétent pour ceux liés aux élections professionnelles. De façon générale, il est difficile de faire annuler une élection par les seuls moyens liés au fonctionnement technique du système de vote.

Le juge constitutionnel annule l'élection lorsque sa sincérité est atteinte [19] :

> « Vue de loin, on peut définir la sincérité du scrutin comme le révélateur de la volonté réelle de l'électeur. Dès lors que celle-ci ne peut pas être connue de manière certaine, et donc qu'il est impossible de connaître avec certitude le choix majoritaire des électeurs, l'élection est annulée par le juge »

Autrement dit, si une irrégularité est constatée dans un système de vote électronique, il faut que cette irrégularité ait affecté le calcul des voix, et que l'écart constaté, du fait de cette irrégularité, a provoqué un écart assez important en comparaison avec d'autres bureaux de vote. On constate dans la jurisprudence que ni les insuffisances liées à l'organisation du scrutin [20], ni les insuffisances liées alléguées au dispositif de vote [21] ne sont suffisantes à elles seules pour donner lieu à une annulation par le juge.

De même, les insuffisances de fonds ne peuvent se suffire à elles seules pour donner lieu à une annulation du scrutin : le fait que certaines recommandations de la

19. Ghevontian, *op. cit.*
20. Décision n°2012-4554 AN du 15 février 2013 du Conseil Constitutionnel
21. Décision n°2012-4597/4626 AN du 15 février 2013 du Conseil Constitutionnel

CNIL n'ont pas été mises en œuvre dans la définition des modalités du vote n'est pas suffisant dès lors qu'il n'y avait pas de preuve que ces circonstances aient affecté les résultats du scrutin.

L'approche du juge judiciaire est sensiblement identique à celle du juge constitutionnel : « il n'y a pas lieu d'annuler un scrutin dès lors qu'une irrégularité est relevée » [22]. Dans un arrêt du 13 Janvier 2010, la Cour de Cassation a l'occasion de clarifier les causes d'annulation [23] :

> « à moins qu'elles soient directement contraires aux principes généraux du droits électoral, les irrégularités commises dans l'organisation et le déroulement du scrutin ne peuvent constituer une cause d'annulation que si elles ont exercé une influence sur le résultat des élections (...) si, s'agissant du premier, elles ont été déterminantes de la qualité représentative des organisations syndicales dans l'entreprise ou du droit pour un candidat d'être désigné délégué syndical. »

Il semble que le juge judiciaire soit plus enclin à recevoir des moyens techniques de preuve pourvu que les irrégularités soient de nature à fausser le scrutin [24]. La distinction de conception du juge judiciaire et du juge constitutionnel est importante : le juge judiciaire accepte de reconnaître les irrégularités qui pourraient fausser le scrutin , là où le juge constitutionnel a une approche plus pragmatique : l'irrégularité doit d'abord s'être produite, mais en plus, elle doit avoir faussé le scrutin. En outre, il n'est pas simple d'obtenir l'annulation de l'élection en s'appuyant exclusivement sur les moyens techniques.

Ainsi, un dysfonctionnement technique d'un système de vote électronique énonçant des résultats non-sincères pourrait tout à fait passer inaperçu, comme nous tâcherons de le démontrer plus tard dans notre démonstration. Sur le plan contentieux, la tâche devient d'autant plus délicate car seule une partie réduite des insuffisances techniques est susceptible de servir de preuve entraînant l'annulation de l'élection par le juge. Peut-on espérer un changement et de vraies garanties légales entourant le recours aux ordinateurs de vote et au vote par Internet ? Un récent rapport du sénat plaide pour la fin du moratoire de 2008 sur les machines à voter et pour une expérimentation plus large du vote par Internet. La « modernisation » du système électoral était d'ailleurs une promesse du président Emmanuel Macron. Qu'en-est-il aujourd'hui ?

22. Marie-Laure Morin, *Le guide des élections professionnelles et des désignations de représentants syndicaux dans l'entreprise*, Dalloz-Sirey, nov. 2015, isbn : 2247138527, voir p. 1247.
23. Cour de cassation, civile, Chambre sociale, 13 janvier 2010, n°09-60.203
24. Cour de cassation, civile, Chambre sociale, 10 Mars 2010, n°15-19.544

1.3 Un retour du vote électronique ?

D'abord annulé en 2017 sur fond de menace cyber au profit d'une élection au format papier, les élections législatives de 2017 pour les français de l'étranger, qui devaient se dérouler par Internet, sont révélatrices de faiblesses techniques importantes qui ont justifié leur annulation (1.3.1) Cette annulation a poussé le sénat a lancé des travaux en vue de la production d'un nouveau rapport d'information sur le vote électronique plutôt étrange, qui plaide en faveur d'un retour du vote électronique et de son extension (1.3.2)

1.3.1 L'annulation du vote par Internet des élections législatives pour les français de l'étranger en 2017

« Si nous ne sommes pas en capacité pour les prochaines élections de nous organiser pour avoir un système de vote étanche à toute attaque, ça ne s'appelle plus la France, notre pays ! »

Ces propos, tenus en octobre 2017 par Emmanuel Macron, n'ont pas été oubliés par les Français de l'étranger, notamment par ceux qui ont dû parcourir de très longues distances, quelques mois auparavant, pour rejoindre leur ambassade ou consulat, afin d'élire leur député.

En effet, au début de l'année 2017, suite aux incidents survenus pendant la campagne américaine et afin de contrer toute perturbation de l'élection par une puissance étrangère, la France a pris la décision de ne pas permettre à ses ressortissants étrangers de voter par Internet pour les élections législatives de 2017. Dans un communiqué, le gouvernement cite des raisons de sécurité afin de motiver sa décision, notamment des propos énoncés par le Quai d'Orsay (ministère des Affaires Etrangères) :

> « Cette décision a été prise sur la base des recommandations des experts de l'Agence nationale de la sécurité des systèmes informatiques et en tenant compte du niveau de menace extrêmement élevé de cyberattaques qui pourrait affecter le déroulement du vote électronique. En raison de ce contexte, il a été jugé préférable de ne prendre aucun risque de nature à compromettre le scrutin législatif pour les Français de l'étranger » [25].

25. Leloup Damien, *Législatives : les Français de l'étranger privés de vote électronique pour des raisons de sécurité*, 2017, URL : `https://www.lemonde.fr/pixels/article/2017/03/06/`

Guillaume Poupard, directeur général de l'ANSSI avait développé ces propos :

> « On ne peut exclure un risque sur la sincérité, mais ce qui est plus probable, en termes de faisabilité, c'est une attaque majeure qui rende le système indisponible, détruise des bases, etc. avec un impact important sur l'image du fonctionnement de la démocratie. »

Selon lui, laisser le vote se dérouler aurait pu donner lieu à « des manipulations fines, pourquoi pas la publication de la liste des Français qui ont voté pour tel candidat » [26].

Cette annulation va avoir pour principale conséquence de produire un très récent rapport d'information du sénat sur le vote électronique : le « Rapport d'information n°73 sur la réconciliation du vote avec les nouvelles technologies » adopté en commission le 24 octobre 2018 dont les premiers travaux remontent à 2017. Ce rapport liste huit propositions visant tout d'abord à « faire davantage confiance aux communes qui souhaitent utiliser des machines à voter » et ensuite à « sécuriser le vote par Internet pour les français de l'étranger »

Entre autres, le rapport préconise la fin du moratoire mis en place depuis 2008 sur les machines à voter et un renforcement, sinon une extension, du vote par Internet. Ce rapport est cependant critiquable, sur le fond comme sur la forme.

1.3.2 Le rapport d'information n°73 du sénat

Une vision militante du vote électronique...

Ce qui transparaît entre les pages du rapport d'information n°73 du sénat est une vision partisane, sinon militante du vote électronique. La vision adoptée par ce rapport est critiquée par le milieu scientifique et notamment par les intervenants du milieu universitaire qui ont été appelés à participer aux travaux et aux auditions.

Pour Chantal Enguehard, la sécurité d'un système de vote ne peut remplacer sa transparence . Or, le rapport insiste avec appui sur la question de la sécurité des

---

`legislatives-le-gouvernement-ne-recourra-pas-au-vote-electronique-pour-les-francais-de-l-etranger-pour-des-raisons-de-securite_5090026_4408996.html` (visité le 25/08/2019).

26. Rees Marc, *L'ANSSI s'explique sur l'annulation du vote électronique des Français de l'étranger*, 2017, URL : `https://www.nextinpact.com/news/103560-lanssi-sexplique-sur-annulation-vote-electronique-francais-l-etranger.htm` (visité le 25/08/2019).

ordinateurs de vote [27], mais n'interroge pas la question de la transparence de l'opération électorale et de son contrôle citoyen. La question est d'ailleurs à peine évoquée lorsqu'il est fait référence au « rituel républicain », concernant le vote papier, pour l'évacuer immédiatement [28].

La question de la confiance en l'élection est également éludée. Il est important de rappeler que dans le contexte d'une élection par vote dématérialisée, l'objet de la confiance de l'électeur n'est plus le même : on ne nous invite plus à faire confiance en l'issue du scrutin, mais on nous invite davantage à faire confiance en un dispositif destiné à recueillir notre vote et à tout un ensemble de règles et de certifications qui sont censés garantir la sincérité du scrutin. La différence n'est pas anecdotique et a des conséquences sur l'acceptation du scrutin [29].

Un autre rapport, plus complet, datant de quelques années plus tôt allait d'ailleurs en ce sens et mettait en exergue la problématique liée à la transparence des opérations électorales liées aux ordinateurs de vote [30]. Il recommandait même de pérenniser « en l'état » du moratoire de 2008 sur les machines à voter en attendant de se doter d'une réglementation plus solide et d'un règlement technique de 2003 amélioré dans un objectif de « mieux assurer la clarté des opérations électorales » et de « renforcer les conditions d'agrément des machines ».

On a cependant pu constater, à la lumière de nos développements précédents, que le législateur comme les politiques ont délaissé les machines à voter en prolongeant le moratoire de 2008 sans prendre de nouvelles mesures allant dans le sens d'une mise à niveau juridique visant à encadrer le périmètre technique des machines à voter.

Dans les intervenants du récent rapport n°73 du sénat, figurent parmi les inter-

27. Jacky Deromedi et Yves Détraigne, *Réconcilier le vote et les nouvelles technologies - Rapport d'information n°73 fait au nom de la commission des lois*, rapp. tech., Paris, France : Sénat, 2018, p. 96, url : `https://www.senat.fr/notice-rapport/2018/r18-073-notice.html`, voir p. 10-12 et p. 20-23.

28. *Ibid.*, voir p. 18.

29. Selon Chantal Enguehard, cela revient à infantiliser l'électeur : on le persuade de faire confiance à un dispositif que des personnes qu'il ne connait pas et ne connaîtra jamais ont certifié comme étant fiable. Confier son vote à un dispositif électronique dont le fonctionnement même échappe à ceux qui sont destinés à l'utiliser fait appel à bon nombre de considérations psychologiques et philosophiques.

30. Alain Anziani et Antoine Lefevre, *Vote électronique : Préserver la confiance des électeurs - Rapport d'information n°445 fait au nom de la commission des lois*, rapp. tech., Paris, France : Sénat, 2014, p. 85, url : `https://www.senat.fr/rap/r13-445/r13-445.html`, voir p. 24-35.

venants auditionnés dans l'élaboration de ce rapport plusieurs représentants de la société France Election : la société distributrice des machines à voter Nedap largement utilisées dans les communes de France, qui utilisent encore à ce jour des machines à voter. Leur participation marque certains points du rapport notamment concernant la promotion de nouvelles machines à voter [31].

Aucun argument de sécurité logique ou physique n'est avancé pour justifier la promotion offerte à ces machines à voter au travers de ce rapport. Le rapport ne mentionne aucune évaluation de ces machines par des services de sécurités de l'État ou par une évaluation indépendante.

Le rapport est également porteur de nombreuses lacunes méthodologiques et scientifiques que nous allons développer.

...pourtant lacunaire et profane

Les rapporteurs affirment que « La fraude, en outre, s'avère impossible compte tenu des l'installation de scellés préalablement au vote, au besoin par huissier de justice. » [32]

En mettant de côté l'originalité que constituerait l'intervention d'un huissier de justice au coeur du processus éléctoral, on observe que les rapporteurs font abstraction de la partie logique de la machine à voter. Rappelons-le : le périmètre du règlement technique de 2003 sur les machines à voter ; largement repris dans le rapport ; ne consacre pas une ligne sur la sécurité logique des machines à voter. Il est bien sûr question à plusieurs reprises de « scellés » préalables à toute élection afin de protéger la machine. Mais les scellés ne peuvent pas protéger contre les fraudes électroniques, c'est-à-dire les fraudes cachées à l'intérieur du logiciel de la machine. La pose de scellés, plus largement, est également inefficace en cas de bugs ou d'erreurs d'exécution même s'ils sont susceptibles d'affecter la sincérité des résultats.

En contraste, le rapport précédent, celui de 2014 ; si l'on met de côté l'usage d'un vocabulaire inexact [33] recommandait dans l'une de ces douze propositions de « Réviser et compléter le règlement technique des machines à voter » en prenant compte les évolutions technologiques en matière de sécurité informatique produites

31. Deromedi et Détraigne, *op. cit.*, voir p. 20.
32. *Ibid.*, voir p. 58.
33. Le rapport parle de « cryptage » au lieu de « chiffrement »

au cours des dix dernières années séparant ce rapport du règlement technique de 2003. Par ailleurs, ce rapport reprend à bon compte les conclusions d'un groupe de travail du ministère de l'intérieur en 2007 ; qui a motivé en partie la mise en place du moratoire ; déplorant la faiblesse du règlement qui :

> se révèle largement insuffisant sur certains points en ce qui concerne la sécurité informatique des machines, ce qui explique également que les trois modèles agréés présentent des niveaux de sécurité relativement différents.

34

Comme nous l'avons développé précédemment, le juge n'est pas en mesure de statuer en cas d'atteinte à la sincérité du scrutin car il est impossible d'en apporter directement la preuve. Il s'agit d'une conséquence de l'opacité du vote électronique et donc d'une affirmation juridiquement et techniquement fausse.

Ainsi, notamment pour Chantal Enguehard, le rapport n°73 du Sénat (2018-2019) « n'est pas scientifique. Dans un rapport scientifique, il y a une méthodologie, une bibliographie et une expertise du propos. Ce rapport prouve que le Sénat n'est pas une institution scientifique. » Pour achever notre analyse de ce rapport riche en enseignements sur la volonté de l'appareil politique concernant le vote électronique, on pourrait émettre la critique désormais traditionnelle qu'il met en relief une incompréhension flagrante de la technologie et des conséquences de l'informatisation sur le droit. Selon les rapporteurs, la sécurité informatique n'est d'ailleurs « qu'une question de moyens » [35]...

Nous allons maintenant démontrer que, le vote électronique reste un mécanisme technique avant d'être un mécanisme juridique. De ce fait, il est soumis aux lois traditionnelles de la sécurité informatique où la confidentialité, la disponibilité, l'intégrité et la sécurité des données véhiculées par le dispositif doivent être maintenues. Rendre un dispositif toujours plus complexe ne contribue en rien à sa transparence. La sécurité par l'obscurité (soustraire au regard d'autrui les composantes et les fonctionnement d'un système afin de ne pas en rendre visibles les failles) n'est pas une méthode viable pour garantir cette dernière. Puis nous démontrerons que la poursuite de la sécurité représente une faiblesse des systèmes de vote. Elle présente d'abord une faiblesse quant à la compréhension du public auquel s'adresse ce dispo-

34. Anziani et Lefevre, *op. cit.*, voir p. 34.
35. Deromedi et Détraigne, *op. cit.*, voir p. 42.

sitif : l'électorat. Elle présente également une faiblesse sur l'image que nous avons de notre démocratie. C'est l'ensemble de ces points que nous allons à présent développer.

Chapitre 2

Le vote électronique : entre dysfonctionnement et sécurité

Les enjeux liés à la cyber sécurité sont majeurs lorsqu'on vient à parler de vote électronique. En effet, si l'on imagine une société démocratique dont le suffrage repose entièrement sur les dispositifs de vote électronique, comme les machines à voter ou le vote par Internet, les conséquences liées à une cyberattaque ou un dysfonctionnement de grande envergure seraient désastreuses. D'une part, comme tout système informatique, les systèmes de vote électronique sont soumis aux dysfonctionnement. (2.1) D'autre part, si l'on se penche plus particulièrement sur le vote par Internet, si sa simplicité théorique de mise en place est confondante, ses vulnérabilités le sont tout autant. Nous expliquerons à cette occasion comment transitent les données sur un réseau, comment ces données sont conçues et comment est-il possible de compromettre la sincérité d'un vote par Internet tout comme sa disponibilité (2.2). Cette informatisation présente un autre problème important : la qualité de celui qui l'opère. Comme nous l'avons vu, ce n'est pas l'Etat qui intervient pour mettre en place ces dispositifs. Ce sont des personnes privées. (2.3)

2.1 Des défauts inhérents aux systèmes informatiques

Les ordinateurs sont des objets complexes, et avec cette complexité vient des faiblesses, tels que les bugs informatiques (2.1.1) des faiblesses non-détectables (2.1.2) et concernant plus spécifiquement les machines à voter, la plupart sont aujourd'hui dépassées et représentent un coût pour les communes qui les utilisent encore (2.1.3)

2.1.1 Les bugs de programmation et les fraudes logicielles

Lors du dépouillement des élections communales à Saint-Josse en Belgique le 14 octobre 2018, le collège des experts a détecté une anomalie importante, qui, rectifiée, a modifié le résultat de l'élection : dans un bureau de la ville, seuls 58 votes avaient été comptabilisés alors que 885 tickets avaient été scannés [1].

Outre le fait que nous sommes ici en Belgique, il s'agit en l'espèce d'un incident traitant de la vérifiabilité du vote électronique (que le règlement technique de 2003, en France, dispose pourtant alors qu'il n'est pas appliqué [2]) la question de la fiabilité des logicielles doit être explorée : les machines à voter, comme les serveurs et autres terminaux numériques ne sont pas infaillibles et peuvent rencontrer des dysfonctionnement liés à la façon dont leur logiciel interne est conçu : bugs, comportements inattendus, limitations du logiciel ou du matériel...

Une contremesure pour s'en prémunir est d'entreprendre des tests techniques et des expertises, comme le recommande le règlement technique [3] de 2003 ou les délibérations de la CNIL [4] en la matière, mais ces mesures ne sont pas suffisantes. La délibération de la CNIL ne contient qu'une seule ligne à propos des tests devant être menés :

> « Un test du système de vote électronique doit être organisé avant l'ouverture du scrutin et en présence des scrutateurs afin de constater la

1. Belga Marc, *Vers un recomptage partiel des votes à St-Josse suite à un bug*, 2018, URL : `https://www.lanouvellegazette.be/297372/article/2018-10-22/vers-un-recomptage-partiel-des-votes-st-josse-suite-un-bug` (visité le 25/08/2019).

2. Voir notamment le principe de « Vérifiabilité » du scrutin disposé dans le règlement

3. Le règlement ne documente pas la façon dont les tests sur les machines doivent se dérouler, mais il exige que des tests se déroulent. On suppose, en lisant les exigences associées que les constructeurs doivent élaborer leur propre protocole de test, car les machines à voter sont issues de modèles et de constructeurs différents

4. Délibération n°03-036 du 1er juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique.

> présence du scellement, le bon fonctionnement des machines, la remise à zéro du compteur des voix et que l'urne électronique destinée à recevoir les votes est bien vide et scellée. »

La formule utilisée par la CNIL pose davantage de problèmes qu'elle n'en résout :

— Que veut dire « remise des compteurs à zéro » au sens informatique ? Vider la mémoire vive ? Effacer le contenu du disque dur ?

— Que veut dire « vérifier que l'urne électronique destinée à recevoir les votes est bien vide » ? La CNIL tente d'appliquer des principes de sécurité et de transparence liés aux anciennes machines à voter, mais cette transposition est bien délicate à mettre en oeuvre sur le plan technique.

Tester les ordinateurs de vote en conditions réelles n'est pas envisageable : si des tests à échelle réduite peuvent être entrepris pour éprouver une fiabilité (qui ne serait pas alors démontrée dans les conditions réelles) il est impossible de faire déplacer des millions des personnes pour le simple prétexte de tester la fiabilité de ces machines.

Le logiciel de la machine est aussi un vecteur de choix pour des pirates expérimentés : un logiciel interne leur permettrait de contrôler à distance la machine, modifier les votes qui seraient entrer par l'électeur, la rendre inutilisable pendant le vote ou effacer ce qu'elle contient. Ce type d'attaque est également envisageable avec le vote par Internet et peut avoir des conséquences bien plus graves qu'une atteinte ciblée sur une machine à voter dans un certain bureau de vote.

Dans l'hypothèse théorique où la partie logique de la machine à voter serait exempte de défaut, le problème lié à la sécurité ou la transparence du processus électoral est-il résolu ? Pas totalement.

Sur le plan de la transparence tout d'abord, si l'on se réfère au système d'exploitation en tant que tel, il n'est pas le seul logiciel à opérer au sein du dispositif électronique : toute une série de micrologiciels propriétaires développés par les fabricants des composants de la machine fonctionnent en support au système d'exploitation, il s'agit le plus souvent de logiciels dont la conception est d'une part protégée par le secret industriel et par des brevets et d'autre part dont la conception n'est pas souveraine.

Sur le plan de la sécurité, la partie logique ne se suffit pas à elle seule : elle doit coopérer avec la partie physique de la machine. Si le périmètre du règlement

technique de 2003 encadre la conception physique de la machine à voter, elle reste soumise à des lois physiques qui nous échappent totalement, comme l'exemple de l'incident de Schaerbeek en 2003.

2.1.2 L'incident de Schaerbeek et la corruption non détectée de données

Lors du dépouillement des élections communales du 18 mai 2003 dans la ville de Schaerbeek, un des bureaux de vote constate une anomalie étonnante : un candidat a reçu plus de votes qu'il n'y avait de participants inscrits dans le bureau. Cette anomalie technique est communiquée dans la soirée même et une batterie de tests est effectuée la semaine suivante : expertise de la machine, expertise du code source... Les conclusions du rapport sont étonnantes [5] :

> « L'incident d'un bureau de Schaerbeek est très vraisemblablement un incident isolé (...) Par ailleurs, cet incident n'a pu être reproduit. Il a pu y être remédié et il n'y a dès lors aucune incidence sur le résultat des élections. (...) Étant donné qu'aucune erreur n'a été trouvée dans le logiciel, et vu la structure interne du programme, le collège conclut que l'erreur a très probablement été occasionnée par une inversion spontanée et aléatoire d'une position binaire (ce phénomène est abondamment décrit dans la littérature spécialisée). »

Effectivement, bien que ce phénomène ait pu très rarement être à la fois observé et détecté dans l'informatique moderne, on sait que ; de par l'échelle des particules que manipulent les ordinateurs pour opérer ; ils sont sensibles aux rayonnements cosmiques qui balaient la Terre en continu [6]. Pour schématiser, les interférences provoquées par le rayonnement ont transformé au sein de la mémoire vive de la machine un « 0 » en « 1 », d'où le terme « inversion binaire ». Le rapport se veut cependant rassurant :

> « Même si les systèmes ne sont pas parfaits, l'ensemble des contrôles effectués permet de s'assurer du bon fonctionnement global du déroulement du vote électronique. L'objectif visé, à savoir émettre les votes, les enregistrer, les visualiser et les compter selon les dispositions légales, a été atteint. »

En vérité, un tel incident comme celui de Schaerbeek n'a aujourd'hui aucune chance de se reproduire dans les mêmes circonstances que celles de 2003 et avec

5. Collectif PourEVA, *18/05/2003 : Rapport concernant les élections du 18 mai 2003*, 2003, URL : `https://www.poureva.be/spip.php?article32` (visité le 25/08/2019).

6. J. F. Ziegler, « Terrestrial cosmic ray intensities », *in* : *IBM Journal of Research and Development* (1998), ISSN : 00188646.

des technologies plus récentes. Depuis 2010, un nouveau type de mémoire vive pour ordinateur est disponible : la mémoire RAM ECC [7]. Il s'agit d'une mémoire vive « autonome » qui en plus de remplir sa fonction habituelle de stockage de l'information pour un traitement à court terme par le processeur est équipée de puces dédiées à la vérification des données stockées, afin de détecter toute altération due à des perturbations extérieures, comme l'électromagnétisme ou les rayons cosmiques en vue d'identifier et de corriger la corruption non détectée de façon traditionnelle.

Aujourd'hui cette technologie est devenue un standard équipant la plupart des infrastructures critiques. Elle est utilisée dans les ordinateurs où une corruption de donnée est inacceptable : calcul scientifique, domaine financier, médical, militaire. La plupart des cartes mères et des processeurs utilisés pour des applications moins critiques ne sont pas conçus pour soutenir la correction d'erreurs dans le but de maintenir leurs prix au plus bas niveau possible.

Cette technologie rend-elle le vote électronique plus transparent ? Non, mais elle permet de donner une plus grande importance à la partie logique des machines à voter. Elle fait poser également la question de la qualité et de la pertinence des composants utilisés dans les machines à voter modernes afin d'assurer leur fiabilité technique, avant même de poser la question de la fiabilité de la partie logique de la machine. A ce titre, le règlement technique de 2003 est aujourd'hui terriblement obsolète, de même que la plupart des machines encore utilisées aujourd'hui, en France ou ailleurs.

2.1.3 Des technologies coûteuses et obsolètes

L'achat des machines à voter est à la charge des communes qui les utilisent [8]. De manière générale, l'achat d'une machine à voter est un investissement qui pour les communes doit s'amortir car elle est destinée à remplir sa fonction pendant de nombreuses années et de nombreuses élections d'autant plus qu'une commune qui souhaite s'équiper intégralement en machines à voter doit multiplier l'achat par le nombre de bureaux de votes présents dans la commune.

Lors de l'adoption du règlement technique par arrêté en 2003, le gouvernement a

7. ECC : Error Correcting Code
8. Ministère de l'intérieur - Circulaire portant instruction permanente relative aux machines à voter (NOR/INT/A/04/00065/C)

souhaité promouvoir, sous l'emprise d'une certaine techno-fascination, l'achat de ces équipements par les communes en promettant une prise en charge à hauteur de 400 à 800 euros par machine équipée [9]. Selon les modèles actuellement agréés en France, une machine à voter coûte aux environs de 5 000 euros l'unité [10]. En fonction du prestataire et du fabricant de la machine, la maintenance préventive et curative de la machine peut parfois ne pas être incluse. En raison des problématiques liées à l'agrément délivré par le ministère de l'intérieur ces machines ne peuvent pas par la suite être modifiées de façon substantielle [11].

On pourrait faire l'analogie avec le matériel électronique ferroviaire : la plupart des composants électroniques qui équipent les trains à grande vitesse ne bénéficient au cours de leur durée de mise en circulation d'aucune optimisation technologique. Si un composant subit une défaillance technique, on le remplace dans son procédé de fabrication original, même si ce procédé est ancien par rapport à ce que peut produire le nouvel état de l'art.

Les trois modèles agréés par le ministère de l'intérieur (« ESF1 du fabricant Nedap, le modèle « iVotronic » du fabricant ES & S et le modèle « Point & Vote » de la société espagnole Indra Sistemas [12]) risqueraient de perdre leur agrément en cas de mise à jour de leur logiciel ou de leur architecture technique. On peut supposer que ces conditions sont en faveur des fabricants en raison des coûts recherches et développement que de telles machines pourraient impliquer.

Une ville comme Lille qui souhaiterait intégralement s'équiper en machines à voter pour équiper ses bureaux de vote (130 bureaux aux élections européennes de 2019 [13]) représenterait un investissement de plus 500 000 euros. Rappelons cependant que depuis 2008, les préfets n'autorisent plus de nouvelles communes à s'équiper de telles machines, en raison d'un moratoire imposé par l'exécutif qui s'est perpétué entre les changements de gouvernements. Au 1er Janvier 2008, 66 communes en France utilisent encore des machines à voter.

9. Deromedi et Détraigne, *op. cit.*, voir p. 54.
10. *Ibid.*, voir p. 54.
11. Ministère de l'intérieur - Circulaire portant instruction permanente relative aux machines à voter (NOR/INT/A/04/00065/C)
12. Ces agréments ont été respectivement délirés par les arrêtés du ministre de l'intérieur du 12 avril 2007, du 15 février 2008 et du 7 mai 2004
13. Ministère de l'intérieur, *Liste des bureaux de vote par circonscription - Lille*, 2019, url : `https://www.lille.fr/content/download/25855/380120/file/Liste+des+bureaux+de+vote+par+circonscription++Lille+-+Hellemmes+et+Lomme.pdf` (visité le 25/08/2019).

Les deux tiers de ces communes sont situés dans huit départements différents, et on constate également une forte concentration des machines à voter en Île-de-France, avec 23 communes utilisatrices [14].

Cette obsolescence liée aux machines est source de vulnérabilités informatiques dangereuses. Il y a un équilibre à trouver entre les arguments des fabricants des machines à voter, les promoteurs du vote par Internet, et les chercheurs en cybersécurité qui dénoncent qu'en l'état, l'utilisation de tels dispositifs représente un danger juridique, mais aussi un danger démocratique. Quelles seraient les conséquences en cas de piratage de la démocratie ?

14. Deromedi et Détraigne, *op. cit.*, voir p. 9.

2.2 Le piratage de la démocratie

Il va s'agir ici des éléments techniques (2.2.1) pour comprendre les enjeux liés aux tentatives de fraudes et de piratage (2.2.2) et exposer l'ampleur des conséquences liées à ces attaques, qui seraient démesurées. (2.2.3)

2.2.1 Quelques éléments techniques : Adresses IP et paquets réseaux

Imaginons une situation dans laquelle un électeur vote depuis son domicile, par exemple, dans le cadre d'une élection professionnelle ou une élection politique ; comme ce fut le cas pour les français de l'étranger en 2012 lors des élections législatives et consulaires. Nous allons analyser de quelle façon le bulletin de vote transite du terminal de l'électeur vers le serveur électoral.

Dans les communications sur Internet, le modèle OSI [15] se traduit par le protocole TCP/IP qui consiste en l'empilement de sept couches. Chaque ordinateur ou serveur connecté à Internet dispose d'une adresse IP spécifique et unique pour l'identifier au sein du réseau. Cette adresse dans le protocole IPv4 mesure 32 bits (par exemple 194.254.129.22) et dans le protocole IPv6, 128 bits (par exemple 2001 :0db8 :0000 :85a3 :0000 :0000 :ac1f :8001).

Afin que les données soient transmises à travers Internet, une adresse IP « expéditrice » ainsi qu'une adresse IP « destinataire » sont donc requises ainsi qu'un compartiment dédié à la donnée transportée. Ainsi on peut schématiser que l'électeur, expéditeur du bulletin, conçoit sur son terminal le bulletin de vote, qui est envoyé vers le serveur électoral, destinataire, que l'on peut représenter sous forme d'urne. L'enveloppe papier se transforme ici en « paquet » (TCP/IP), semblable à un colis, qui trouve son chemin entre routeurs et fibres optiques jusqu'à son destinataire. Cette relation expéditeur/destinataire n'est pas seulement utilisée dans vote électronique, mais c'est également ce qui rend possible l'existence même d'Internet.

L'information circule donc sur Internet sous forme de « paquets ». La circulation de ces paquets est articulée par le protocole TCP/IP, on parle alors de « paquet IP

15. Il s'agit d'une norme de communication, en réseau, de tous les systèmes informatiques. C'est un modèle de communications entre ordinateurs proposé par l'Organisation Internationale de Normalisation (concevant les normes ISO) qui décrit les fonctionnalités nécessaires à la communication et l'organisation de ces fonctions.

(Internet Protocol)[16] ». Ces paquets peuvent avoir une longueur maximale de 216 bits, soit un peu plus de 65 mégaoctets par paquet. Bien sûr, il s'agit d'une limite théorique, la plupart des paquets IP circulant sur le réseau ne pèsent que quelques Ko selon l'information transportée. On représente un paquet TCP/IP de la façon suivante :

Paquet TCP/IP		
Charge utile	**En-tête TCP**	**En-tête IP**
Données d'application : URL, contenu d'un mail, contenu d'une page web, vidéo, image etc En-tête d'application : version de l'application, etc	Port expéditeur Port destinataire	IP Expéditrice IP Destinataire
Couche 5 TCP/IP (Couches OSI 5, 6 et 7)	Couche 4 TCP/IP	Couche 3 TCP/IP

On constate qu'en l'état, on ne parle pas de confidentialité de l'information (car un paquet est une information). La raison est simple : Internet a été conçu pour faciliter le transport de l'information et non pour faciliter sa sécurisation. Cette faiblesse va appuyer notre mise en situation, en imaginant qu'un attaquant souhaite compromettre la confidentialité du vote de l'électeur, voire même le modifier.

2.2.2 Les atteintes possibles au vote par Internet

l'attaque « man in the middle »

Une intervention du type homme au milieu (man in the middle) consiste à se faire passer pour le serveur vis-à-vis de l'ordinateur de l'électeur et à se faire passer pour l'électeur vis-à-vis du serveur. L'attaquant peut ainsi connaître le vote, et pire encore, le modifier. En effet les paquets réseaux ne sont pas conçus dans leur nature comme étant « sécurisés » ou « confidentiels ». Techniquement, cette sécurisation du paquet s'appelle le chiffrement.

Pour comprendre l'importance du chiffrement, il faut d'abord saisir ce qu'il désigne. Le chiffrement est un processus qui sécurise les données ou informations. Lorsque les données ou les informations sont chiffrées, il devient « presque impos-

16. Sciences Institute Information, *Internet Protocol - DARPA Internet Program*, 1981, URL : `https://tools.ietf.org/html/rfc791` (visité le 25/08/2019).

sible »[17] pour un tiers non autorisé d'en connaître le contenu. Tout intermédiaire malveillant n'a ainsi plus la possibilité de le lire de façon claire. Si un paquet chiffré est lu, il sera de toute façon inexploitable. Le chiffrement du vote peut ainsi offrir une protection solide contre ce type d'attaque si la clef publique du chiffrement envoyée à l'électeur n'a pas été interceptée par le fraudeur, et là est toute la difficulté du vote par Internet : il s'agit d'un vote qui peut se dérouler dans le monde entier.

Cela appelle à tirer des conséquences simples : il est strictement impossible de garantir que le bulletin de vote virtuel[18] ou le premier contact avec le serveur électoral se déroule en toute confidentialité. De plus, même si la clef de chiffrement qui est utilisée pour protéger le bulletin de vote virtuel n'est pas connue de l'attaquant ou des dispositifs qu'il utilise, il est tout à fait possible de « capturer » le vote et l'effacer avant qu'il n'arrive au serveur électoral.

Il lui suffit d'utiliser une méthode consistant à « scanner » les paquets transitant dans son périmètre réseau et de les filtrer par en-tête de paquet[19]. L'électeur se retrouve ici privé de son droit de vote, l'atteinte est extrêmement grave d'autant plus qu'il est facile de renvoyer un message sur le terminal de l'électeur afin de lui faire croire que son vote a bien été enregistré.

Cette attaque, d'un certain degré technique est pourtant à la portée de tout pirate motivé puisque les dates des élections sont connues longtemps à l'avance. Si l'on admet que les applications de vote utilisées par les électeurs soient coûteuses à développer, il s'en suivra un amortissement qui s'étendra sur plusieurs élections : ce temps permettra aux plus motivés de se procurer les applications, de les décompiler[20], et de connaître en détail le fonctionnement avec suffisamment de talent pour tromper un électeur qui n'en a, dans la majorité des cas qu'une connaissance très rudimentaire[21].

17. Si l'on veut être rigoureux, la sécurité d'un algorithme de chiffrement dépend d'abord de son fonctionnement, mais aussi et surtout de la longueur de la clé utilisée. Il est aujourd'hui inenvisageable de s'estimer en sécurité avec des clés d'une longueur inférieure à 128 bits dans le chiffrement des communications sur Internet aujourd'hui.

18. Par commodité, nous appellerons « bulletin de vote virtuel » l'ensemble des paquets réseaux constituant le vote de l'électeur.

19. Nous venons de voir précédemment que l'en-tête du paquet TCP/IP contient au minimum l'adresse expéditrice et l'adresse destinataire. Le plus souvent, selon l'ampleur du scan, on peut connaître la couche protocole, facilitant grandement le filtrage et le contrôle du flux des paquets sur le réseau.

20. La décompilation d'un logiciel est une opération qui permet de reconstituer le code source d'un logiciel à partir d'un programme exécutable dans un format binaire. On emploie parfois le terme d'ingénierie-inverse (reverse engineering)

21. Pour certains politiques, notamment l'ancien sénateur Philippe Kaltenbach, la question de

Un autre type d'attaque beaucoup plus sournoise consiste en l'utilisation de virus informatique pour altérer les terminaux des électeurs voire le serveur électoral central.

l'attaque par virus informatique

En 2017, le bilan de la cyber-attaque mondiale provoquée par le virus WannaCry [22] fut l'un des plus lourds de l'histoire de l'informatique moderne : 300 000 postes infectés répartis dans 174 pays différents pour des dégâts chiffrés à plusieurs milliards d'euros par les entreprises impactées [23]. Cet exemple illustre à quel point un virus informatique bien conçu peut être dévastateur.

WannaCry était un virus conçu pour rendre indisponible les terminaux infectés. Il n'avait pas pour fonction d'être discret et ne servait aucun but particulier, sinon celui du profit. On peut tout à fait imaginer un virus développé avec moyens étatiques (comme pour WannaCry) conçu à partir d'un logiciel de vote décompilé qui en affecterait son fonctionnement. Ce mode d'attaque peut tout à fait être envisageable. Il serait d'ailleurs le plus probable et le plus intéressant sur le plan technique comme le plan juridique.

Techniquement, un virus peut facilement infecter un grand nombre d'ordinateurs sans être détecté : on sait que les antivirus sont inopérants face à des programmes comme WannaCry qui sont conçus pour leur échapper. Les concepteurs du virus peuvent également payload [24] le virus le jour du vote, affectant irrémédiablement la machine de l'électeur : le virus pourrait alors transmettre les identifiants de l'électeur sur un serveur distant avant son vote, modifier le vote de l'électeur avant le processus de chiffrement, rendre le terminal de l'électeur inutilisable. Il s'agit certainement de la menace la plus grave qui pèse sur un scrutin par Internet : l'ensemble des propriétés liées à la sécurité sont altérées : disponibilité, intégrité, confidentialité.

l'utilisation des ordinateurs pour et leur accessibilité au large public, notamment les personnes âgées, est une question loin d'être anecdotique.

22. WannaCry est un logiciel malveillant de type « ransomware ». Il s'agit d'un logiciel qui chiffre toutes les données du poste infecté, prenant en otage les données chiffrées en échange d'une rançon que l'utilisateur devra payer (en crypto-monnaie) pour recouvrer l'accès au poste infecté

23. Vanuxem Solène, *Infographie : Wannacry, l'heure du bilan !*, 2017, URL : `https://www.wisper.io/fr/infographie-wannacry/` (visité le 25/08/2019).

24. En sécurité informatique, la payload d'un virus (charge active) consiste à ce que le virus exécute l'action pour laquelle il a été conçu via un déclencheur précis : ping régulier vers un site Internet qui active la payload, date et heure précise, etc...

2.2.3 Les conséquences juridiques sur le vote

Juridiquement, les conséquences seraient impensables : il reviendrait au juge, en vertu de nos développement précédents, d'apprécier l'irrégularité conséquente du virus afin de déterminer si cette infection a permis de fausser le scrutin. Or :

- Le virus peut avoir eu des effets latéraux qui n'ont pas visé directement le scrutin
  - Comment le juge peut-il déterminer si le scrutin a été faussé par la seule présence du virus sur les terminaux des électeurs ?
- Le virus peut avoir modifié le vote de l'électeur sans que ce dernier ne le sache tout comme il pourrait n'être qu'un faux positif
  - Le juge peut-il annuler l'élection en vertu d'un « principe de précaution » fictif qu'il inventerait ?
  - On peut réellement parler de précaution : si les applications de vote sont conçues pour ne pas relier l'électeur à son vote, le juge serait incapable de dire si la sincérité du scrutin est altérée.
- Le virus peut avoir transmis des informations d'identification de l'électeur permettant à d'autres personnes d'usurper son identité
  - Comment le juge va-t-il apprécier l'ampleur de cette usurpation ?
  - Comment l'électeur peut-il prétendre avoir été usurpé ?
  - Dans quelles proportions le juge peut-il prendre la décision d'annuler l'élection en raison de l'altération de la sincérité du scrutin ?

En vérité, bien au-delà de poser des problématiques techniques, de telles hypothèses d'atteinte posent de réelles questions juridiques qui désarmeraient le juge et amènent à nous interroger sur la pertinence même du vote électronique. Doit-on pour autant le condamner ? Il s'agit d'un équilibre à trouver et à explorer comme nous le faisons actuellement dans notre réflexion. Nous aurions tort de penser qu'un scrutin par Internet en apparence réussi serait une victoire démocratique et technologique : le fait qu'aucune attaque n'ait été répétée ne prouve pas qu'il n'y en ait pas eu. Certains acteurs l'ont pris compris : chercheurs, électeurs, et politiques.

Le vote électronique, qu'il concerne le vote par Internet ou le vote par machine est gouverné par les mêmes règles de sécurité informatique, il est donc logique qu'une méfiance se soit créée. Néanmoins, il existe une problématique sérieuse liée au recours à des prestataires ou des sous-traitants dans l'organisation des votes. D'une certaine façon, l'élection est privatisée.

2.3 La privatisation des processus électoraux

Le recours à des personnes privées ou des prestataires pour l'organisation d'élections par voie électronique ou sur des machines à voter dépossède l'État d'une de ces prérogatives premières, l'organisation d'élection, devenu un marché comme un autre (2.3.1) Il y également d'autres problèmes issus de l'encadrement légal de ces dispositifs : leur protection juridique par la propriété intellectuelle (2.3.2)

2.3.1 Processus électoraux et marchés publics

Il faut souligner l'importance que constitue l'entrée des acteurs privés dans ce qui constitue depuis le début de la république un sanctuaire : les processus électoraux. Concernant les machines à voter, on peut ne plus aujourd'hui parler de marché concurrentiel : trois acteurs se partagent l'ensemble des 66 communes qui utilisent encore des machines à voter, dont un qui n'équipe seulement que deux communes.

Concernant le vote par Internet, la situation est bien différente et beaucoup plus riche. Il faut distinguer le vote politique et le vote pour les élections professionnelles. Concernant le vote pour les élections politiques, c'est-à-dire pour les élections législatives et consulaires pour les français de l'étranger, le prestataire doit répondre à un cahier des charges précis imposé par des recommandations de la CNIL et des recommandations de l'ANSSI concernant les moyens de sécurisation du vote par Internet. En mai 2016, le marché a été attribué à la société SCYTL pour une durée de quatre ans et un montant de 3,73 millions d'euros, somme à laquelle il faut ajouter 2,99 millions d'euros de prestations annexes, confiées à d'autres entreprises. SCYTL présentait en apparence de solides références, notamment parce qu'elle était intervenue comme sous-traitant de l'entreprise ATOS Origin pour concevoir la précédente plateforme de vote en ligne [25].

Cependant l'élection par Internet n'a pas eu lieu : calendrier trop ambitieux, tests de sécurité et d'ergonomie non concluants. Les responsabilités ont été partagées entre l'administration et le prestataire. L'ANSSI évoque tout de même que le projet, mis en œuvre plus tôt et avec des moyens plus conséquents aurait pu être un succès : « surchauffe d'un projet fondamentalement ambitieux quoique pas irréaliste

25. Deromedi et Détraigne, *op. cit.*, voir p. 41.

»

Le marché public n'a, pour autant, pas été résilié et reste encore vigueur aujourd'hui malgré l'échec de la mise en œuvre des élections de 2017. La société SCYTL est toujours chargée de mettre en œuvre le vote par Internet pour les élections consulaires de 2020.

La mise en œuvre du vote par Internet pour les élections législatives et consulaires pour les français de l'étranger reste une priorité, d'une part car il s'agit d'une promesse de campagne qui semble tenir à cœur au président Emmanuel Macron, et d'autre part car les acteurs privés chargés de l'exercice de cette prestation ont une certaine « vision » du vote. Jean Souto, directeur des ventes-mondes chez SCYTL, disait en 2012 :

> « Cette génération a bien compris que dans le futur, nous ne voterons même plus à partir d'un ordinateur portable, mais à partir d'un smartphone. En France, le Ministère de l'Éducation nationale a utilisé nos services pour les élections syndicales. Laissons les français pouvoir voter d'où ils veulent, quand ils veulent, pour qu'ils se sentent concernés ! Apportons un peu de modernité dans le système électoral »

Ce recours à des personnes privées ne pose pas que des problèmes relatifs à la conception du rôle de l'État, elle pose un problème insoluble de transparence lié à la protection de dispositifs par la propriété intellectuelle.

2.3.2 Propriété industrielle et transparence

Une décision du Conseil Constitutionnel illustre parfaitement notre propos [26]. Pour Michaël Tchilingurian, auteur de ce recours devant le Conseil Constitutionnel [27] :

> « Il n'y a aucune assurance à ce que le choix de l'électeur soit respecté au moment où il enregistre son vote [sur la machine à voter]. A cela s'ajoute le fait que le logiciel de ces machines est protégé par le secret industriel et commercial, car il s'agit de logiciels propriétaires. Il n'y a donc aucun moyen de s'assurer que ces logiciels sont bien paramétrés pour respecter ces principes. »

La décision du Conseil Constitutionnel du 20 décembre 2007 est pourtant formelle. Pour les sages, la publication des Codes Sources ne représente pas une atteinte à la liberté du vote ou à la sincérité du scrutin :

26. Décision n° 2007-3742/3947 AN du 20 décembre 2007 - Conseil Constitutionnel
27. Nous l'avons retrouvé et contacté par mail dans le but de lui poser quelques questions relatives à son recours

> « 14 - Considérant, en cinquième lieu, qu'en s'abstenant de prévoir la publicité des tests de conformité pratiqués sur chaque modèle de machines à voter par les organismes de certification agréés par le ministre ainsi que la publication des « codes sources » des logiciels utilisés, lesquels sont protégés par le secret industriel et commercial, le règlement technique fixant les conditions d'agrément des machines à voter approuvé par l'arrêté ministériel susvisé du 17 novembre 2003 ne méconnaît ni le principe de liberté du vote, ni le principe de sincérité des opérations électorales ; »

Ce considérant du Conseil Constitutionnel est très étonnant et peut évoquer une certaine méconnaissance technique des Sages sur le fonctionnement d'un système informatique : la non-publication du code source d'un dispositif électronique, surtout une machine à voter, n'aide ni à sa sécurité (nous évoquions précédemment la sécurité par l'obscurité) et encore moins à sa transparence. Le Code la propriété intellectuelle protège les inventions brevetées et les œuvres de l'esprit [28]. La structure interne d'une machine à voter peut être protégée par la première et le code source peut être protégé par la seconde.

Cette situation tolérée par le CPI, est défendue à bien des niveaux par l'article L61-1 qui protège les droits du propriétaire en lui réservant un monopole économique sur invention pendant la durée légale de protection : « le brevet est une arme industrielle et économique, il constitue un véhicule technologique [29]. »

Le ministère de l'intérieur exige néanmoins des fabricants des machines à voter un accès total aux dispositifs afin d'éprouver les spécificités fonctionnelles de chaque modèle par rapport aux 114 exigences du règlement technique de 2003 et des recommandations de la CNIL . Ces expertises sont conduites par des cabinets d'experts en audit informatique « indépendants » [30]. Ces rapports demeurent confidentiels au motif de cette protection industrielle et en vue de la préservation des intérêts commerciaux des personnes privées. Les pratiques liées aux conditions d'agréments qui demeurent obscures et de la protection industrielle de la structure physique et logique des machines amènent à un constat amer : le déclin silencieux du contrôle citoyen des élections.

Garantir sécurité et transparence pour les dispositifs de vote électronique relève

28. Cette protection est garantie respectivement par les articles L6116-1 et L111-1 du Code la Propriété Intellectuelle

29. Jacques Azéma, *Droit de la propriété industrielle*, Dalloz-Sirey, sept. 2017, ISBN : 2247153062, voir p. 92.

30. JORF n°274 du 27 novembre 2003 p. 20188

d'un défi, autant pour les industriels que pour les politiques et les électeurs. Nous avons étudié jusqu'à présent que le maître mot, obsession des politiques et des industriels pour l'élaboration du vote sur machine à voter et sur des plateformes en ligne était la sécurité. Cette sécurité est pourtant difficile à atteindre, d'une part car les systèmes d'informations souffrent de défauts inhérents à leur conception et d'autre part même le moins faillible des systèmes reste tout de même faillible et que les conséquences démocratiques peuvent être un désastre en cas de cyberattaque.

Le juge a tenté d'adapter sa jurisprudence à ces nouveaux systèmes. Cette adaptation révèle rapidement ses limites car les conditions de fonctionnement des machines à voter mettent tout requérant dans une position de faiblesse en cas de contentieux. Dans le cadre du vote par Internet l'équilibre entre les salariés et l'employeur sur l'accès aux différentes pièces du dossier liées à la mise en œuvre des élections professionnelles, comme le rapport d'expertise ou le cahier des charges, est également rompu.

En France, depuis 2008, l'État applique un moratoire sur les machines à voter, qui empêche non seulement l'utilisation de ces appareils par de nouvelles communes mais également la modernisation des équipements existants. Les communes équipées de machines à voter doivent ainsi organiser les scrutins nationaux sur des machines qui sont aujourd'hui largement obsolètes. Faute d'avoir anticipé à temps les risques de piratage informatique, le Gouvernement a abandonné en 2017, sur fond de menace cyber, le vote par Internet pour les élections législatives, au détriment de l'expression démocratique des Français de l'étranger, c'est ce que d'ailleurs regrette le président Emmanuel Macron qui appelle de ses vœux au retour du vote électronique, sans quoi,« la France ne serait plus la France. »

On pourrait considérer que cette déclaration du président de la république peut relever de la techno-fascination, mais malgré tout, les apports du vote électronique sont nombreux. Tout d'abord, il s'agit d'un apport technologique : l'objectif de sécurité qui doit être atteint pour des dispositifs aussi sensibles que ceux destinés à exprimer la volonté du peuple doit être éprouvé, ce qui a par exemple encouragé le développement de nouveaux procédés de chiffrement ou de nouveaux dispositifs de reconnaissance optique largement utilisés aux Etats-Unis. Ensuite, il s'agit d'un apport juridique : le vote électronique permet au juge de se confronter à un objet technique complexe et de mettre à l'épreuve sa jurisprudence traditionnelle. On ne peut raisonnablement dire que le vote électronique est un apport à la vie démocra-

tique par rapport à ce que prétendent ses promoteurs.

L'apport du vote électronique que nous n'avons pas évoqué jusqu'à présent et qui va être développé dans la seconde partie de nos réflexions, c'est le fait que le vote électronique a développé la sensibilisation de chercheurs, politiques et militants sur ce qui est annoncé comme l'avenir de la démocratie.

Deuxième partie

L'éveil de la citoyenneté électronique ?

Le développement des nouvelles technologies a contribué à créer des nouvelles formes de militantisme et le vote électronique est devenu un enjeu démocratique majeur duquel ce sont saisis scientifiques, citoyens et militants. Tous s'accordent sur le fait que ce qui doit être la priorité, c'est la transparence du processus électoral. Or, nous l'avions étudié, concilier transparence et sécurité n'est pas simple, c'est ce qui constitue le cœur de notre réflexion. Le vote électronique peut-il d'ailleurs simplement répondre favorablement à cet impératif de transparence ? Des essais prometteurs ont été tentés à travers des formes de vote dites « vérifiables » censées allier le meilleur des deux mondes entre transparence et sécurité. Par ailleurs, les possibilités offertes par Internet pour la mise en place d'initiatives locales ou nationales sont nombreuses et parmi elles, nous étudierons le pétitionnement électronique. **(Chapitre 3)**. Que pourrait-il advenir du vote électronique durant les prochaines décennies ? Peut-on imaginer une société dans laquelle on voterait pour le président de la république, nos députés, nos maires ou même les lois directement sur notre smartphone ? Ou le vote électronique est-il condamné à rester marginalement utilisé et à demeurer un objet technique rempli de méfiance et d'incompréhension des électeurs ? **(Chapitre 4)**

Chapitre 3

Entre contestations et solutions

Depuis le début des années 2000, le développement des technologies de vote électronique, machines à voter ou vote par Internet, ou même des technologies de l'information en général a créé de nouveaux mouvements militants dont le principal objectif est de lutter pour une société démocratique plus transparente. Nous étudierons cette mouvance sous l'angle du besoin de transparence relatif aux machines à voter (3.1) Dans cette recherches de solutions, il y a donc eu nécessité d'imaginer de nouveaux systèmes de vote électronique et parmi eux, nous étudierons les dispositifs vérifiables (3.2)

3.1 Une prise de conscience citoyenne et politique

Bien entendu, en raison de l'ensemble de ce que nous avons développé précédemment, un mouvement de contestation concernant les machines à voter s'est développé, composé de différents acteurs avec différents méthodes (3.1.1) Il est devenu urgent de mener des études sérieuses sur l'apport du vote électronique dans notre société au lieu de procéder à un développement sans réel fondement (3.1.2)

3.1.1 Une opposition aux multiples visages

Une opposition militante technicienne

Nous évoquions au début de notre réflexion le groupe de réflexion citoyenne néerlandais « Wij vertrouwen stemcomputers niet » constituant également un groupe de chercheurs en informatique. Ce groupe a choisi d'entreprendre des actions militantes de sensibilisation de l'opinion aux Pays-Bas en rendant publiques des failles informatiques dont souffrent les machines à voter. Ils se sont également livrés à une démonstration d'un piratage d'une machine à voter à l'occasion d'un direct télévisé. Leur argumentaire repose sur le registre de l'opacité des machines. Le manque de transparence ou encore la pauvreté ergonomique.

Si les actions de ces groupes peuvent être louables, les lois françaises peuvent sévèrement sanctionner ce genre de comportement. Depuis la loi pour la confiance en l'économie numérique de 2004, l'application de la loi en matière d'intrusion dans les systèmes d'information est indifférente de la finalité des intentions du pirate.

Tout d'abord au regard de la loi, on sait que depuis 1980, dès lors qu'il y a intrusion, il y a infraction et potentiellement application d'une sanction pénale [1]. Depuis 2004, le fait de détenir un programme informatique destiné à faciliter l'intrusion est aussi sanctionné [2] : il y a une indifférence de la loi quant aux intentions du pirate, aussi louables soient-elles, comme celles de montrer les failles d'un système de vote électronique. Cette disposition rend difficile, en France, le combat pour des dispositifs de vote électronique sécurisés.

L'autre pilier argumentaire servant de revendication aux groupes de réflexion citoyenne ou aux militants concernés par le vote électronique tient dans le transfert de la compétence électorale du citoyen vers le technicien. Le vote électronique procède en effet d'une reconfiguration inédite de la division du travail électoral. Les citoyens passent du statut d'acteurs à celui d'observateurs de la machine qui enregistre, comptabilise et dépouille. Par la privatisation de l'élection, l'électeur se voit donc retirer la surveillance de la gestion du scrutin en faveur de techniciens.

Le piratage du vote électronique comme sport

Aux Etats-Unis, la « DEF CON Hacking Conference » est un événement international qui convie les experts en sécurité informatique du monde entier autour d'événements et de conférences sur le thème de la cyber-sécurité. Depuis quatre ans cette année, la DCHC organise un défi devenu récurant, celui de pirater une machine à voter [3]. Si les exemplaires de ces machines vendus en France ont un prix fixé entre 4 000 et 6 000 l'unité, la DCHC accueille chaque année une machine à

1. Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique

2. Le fait d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle- même ou pour l'infraction la plus sévèrement réprimée.

3. Collier Kevin, *At hacking conference, Pentagon's transparency highlights voting companies' secrecy*, 2019, URL : `https://edition.cnn.com/2019/08/12/politics/defcon-voting-village-darpa-dominion/index.html` (visité le 25/08/2019).

voter expérimentale dont le prix est fixé par le constructeur à dix millions de dollars [4].

Si une telle machine a peu de chance d'être déployée à grande échelle en raison de son prix et des technologies utilisées pour la fabriquer, elle révèle une ambition assumée des fabricants : «Its endgame goes way beyond securing the vote. The agency hopes to use voting machines as a model system for developing a secure hardware platform » [5].

Le fabricant va jusqu'au bout de sa démarche en spécifiant que les logiciels utilisés par cette machine sont open sources, qu'aucune puce ni aucun composant n'est accablé par un logiciel prioritaire comme ceux de Intel ou de AMD qui détiennent des logiciels propriétaires dans leurs processeurs et autres puces.

Les enjeux aux Etats-Unis sont d'une importance capitale : l'utilisation des machines à voter est beaucoup plus poussée qu'en France et leur sécurité relève des questions de sécurité nationale [6]. En France, justement, il existe également une opposition institutionnelle au vote électronique, dont la suppression est d'ailleurs souhaitée par des partis et quelques personnalités politiques.

Une opposition politique institutionnelle

Dans certains programmes politiques, la suppression du vote électronique est devenue une promesse électorale, comme c'est le cas par exemple du parti Europe Ecologie Les Verts [7]. Certains politiques de sensibilités différentes sont également des militants que l'on pourrait qualifier « d'anti-machines » comme l'ancien sénateur Philippe Kaltenbach.

Le 22 juillet 2014, Philippe Kaltenbach, a présenté une proposition de loi « visant

4. Hay Newman Lily, *Hackers Take on Darpa's 10 Million dollars Voting Machine*, 2019, URL : `https://www.wired.com/story/darpa-voting-machine-defcon-voting-village-hackers/?verso=true` (visité le 25/08/2019).

5. « L'enjeu va bien au-delà de sécuriser le vote. L'agence espère utiliser les machines à voter afin de développer une architecture matérielle sécurisée »

6. Braun Jake Blaze Matt, *Report on Cyber Vulnerabilities inU.S. Election Equipment, Databases, and Infrastructure*, 2018, URL : `https://www.defcon.org/images/defcon-26/DEF%20CON%2026%20voting%20village%20report.pdf` (visité le 25/08/2019).

7. Paradoxalement, le parti organise ses élections internes et ses consultations par voie électronique, comme ce fut le cas en 2018 afin de préparer la stratégie à adopter pour les élections européennes de 2019 : `https://eelv.fr/newsletter_archive/elections-europeennes-vote-des-adherent%C2%B7e%C2%B7s-sur-la-strategie/`

à supprimer le recours aux machines à voter pour les élections régioales » [8]. En 2015, le sénateur Kaltenbach a proposé une loi visant à interdire purement et simplement les machines à voter en France au vu des problèmes qui leur sont inhérents. En plus des arguments habituels avancés, Philippe Kaltenbach indique qu'en raison de la technologie, les personnes âgées sont obligées de se faire aider. La technologie des machines à voter ne permet pas d'aider ces personnes sans voir ce qu'elles votent, ce qui casse une fois de plus le secret du vote [9].

Pour lui, le développement des machines à voter dans les scrutins officiels serait principalement motivé par un enjeu financier lié aux coûts des machines à voter et au développement d'un marché. L'activité des groupes qui sont opposés aux machines à voter sert deux objectifs.

Tout d'abord certains plaident pour un retour au vote papier, estimant que l'informatique et ses failles n'ont pas leur place dans un processus aussi sensible que l'expression de la démocratie. Ensuite, il s'agit de faire avancer l'état de l'art en plaidant pour davantage de transparence : sensibiliser les électeurs aux enjeux liés au vote électronique est un enjeu qui pourrait d'ailleurs faire l'objet d'une mission régalienne.

Une remise en question de l'exécutif ?

Par ailleurs, comme évoqué en introduction, il semblerait que le ministère de l'intérieur ait parfaitement conscience des faiblesses techniques liées aux machines à voter et des coûts liés à leur exploitation :

> « allongement des temps d'attente dans les bureaux équipés, coût élevé pour les communes et l'État (entre 4 000 et 6 000 euros en 2007 pour l'achat d'une machine, auxquels s'ajoutent les frais d'entretien, de stockage et de formation), et surtout méfiance des citoyens devant l'impossibilité de recompter physiquement des bulletins de vote » [10]

A ce jour l'incertitude demeure sur le sort qui est réservé aux machines à voter qui équipent les 66 communes depuis l'installation du moratoire en 2008. On sait

8. Kaltenbach Philippe, *Proposition de loi visant à supprimer le recours aux machines à voter pour les élections générales*, 2014, URL : `http://www.senat.fr/leg/ppl13-763.html` (visité le 25/08/2019).

9. de Villaines Astrid, *3 questions à... Philippe Kaltenbach, l'homme qui ne veut plus de machines à voter*, 2015, URL : `http://www.lcp.fr/actualites/3-questions-philippe-kaltenbach-lhomme-qui-ne-veut-plus-de-machines-voter` (visité le 25/08/2019).

10. Christine, *op. cit.*

que le gouvernement d'Edouard Philippe souhaite réformer le vote électronique et plus particulièrement le vote par Internet. Les conditions d'agrément demeurent cependant obscures. Les soupçons de collusions entre les politiques et les fabricants de machines ont poussé l'exécutif a adopté une nouvelle approche de la question « épineuse »[11] des machines à voter. Nous apprenions ainsi lors d'une réponse à une question écrite d'une députée le 25 Juillet 2019 que l'exécutif allait engager une réflexion au sujet des machines à voter mais maintiendrait en l'état le moratoire :

> « C'est pourquoi, conformément à la feuille de route du ministère de l'intérieur communiquée en septembre dernier, le Gouvernement a engagé une réflexion visant à réexaminer le cadre applicable aux machines à voter, y compris pour ce qui concerne l'homologation et l'autorisation de nouveaux modèles. En attendant, le moratoire est maintenu. »

L'étranger n'a pas attendu pour s'atteler à de nouvelles expériences en vue de constater les effets du vote électronique sur le scrutin. En Suisse, pays dont les logiciels équipant les dispositifs de vote électronique sont disponibles en libre accès sur Internet, l'exécutif helvétique s'est attelé à une expérience à Genève dont les conclusions méritent d'être étudiées.

Les conclusions de l'expérience de Genève

En 2013, la commission externe d'évaluation des politiques publiques de Suisse publie un rapport dressant un bilan d'une expérience qui a été menée dans le cadre des élections cantonales à Genève. Il s'agissait, en parallèle aux autres modes de scrutin (vote à l'urne et par correspondance) de rendre également possible le vote par Internet pour l'ensemble des électeurs du canton et d'en observer les conséquences sur l'élection et ses résultats. Cette expérience avait pour objectif de constater les effets du vote électronique d'une part sur les résultats de l'élection, sur la participation à l'élection, de dresser un profil des votants en ligne et enfin de tester la viabilité technique du dispositif[12]. En Suisse, on peut distinguer deux systèmes de vote par Internet aux origines différentes.

11. Terme utilisé dans le rapport n°445 du Sénat.

12. Commission externe d'évaluation des politiques publiques, *Voter par internet : évaluation des effets du vote électronique à Genève*, rapp. tech., Genève : République et Canton de Genève, 2013, p. 64, URL : `https://www.ge.ch/document/rapport-commission-evaluation-politiques-publiques-quant-impact-introduction-du-vote-electronique-geneve/telecharger`, voir p. 6.

Trois systèmes de vote par Internet étaient disponibles depuis 2004 [13] : celui de la Poste fédérale (en partenariat avec la société SCYTL, également prestataire auprès de l'État Français), celui du niveau Cantonal (principalement Genève, et développé par des fonctionnaires en open source, celui sur lequel se base le rapport de la commission) et une version alternative issue d'un « fork » de cette dernière utilisée à Zurich et qui a depuis cessé d'être utilisée. Aucun incident n'a été décelé à ce jour, mais lors de tests de sécurité réalisés en 2018 sur le système de la Poste, des failles ont été découvertes.

Le rapport de la commission donne des conclusions favorables en vote électronique. Nous noterons quelques remarques intéressantes issues du rapport :

- Le rapport évoque une participation similaire en référence aux autres modes de scrutins : le vote par Internet n'attire pas de nouveaux votants par rapport aux modes de scrutins [14] ;
- Les votants en ligne sont surtout des votants appartenant aux catégories socio-professionnelles moyenne-supérieure : on constate que les votants en ligne ont un niveau de connaissances politiques plus élevé que les votants par correspondance ou aux urnes [15] ;
- Les votants en ligne sont surtout de gauche : on retrouve en majorité des votes en ligne qui plaident pour une taxation des hauts revenus, une appartenance de la Suisse à l'Union Européenne [16] ;
- Le rapport à l'informatique des votants en ligne est important : les personnes qui utilisent régulièrement Internet et qui considèrent avoir de bonnes connaissances en informatique ou qui ont confiance dans les communications et les transactions en ligne, utilisent significativement plus le vote par Internet que les autres [17].

Le rapport recommandait ainsi en 2013 une extension du vote électronique, tout en renforçant « les exigences de sécurité ». Le rapport se base en partie sur une étude de la Haute Ecole spécialisée bernoise (HESB) qui fut mandatée pour expertiser les systèmes de vote par Internet suisses. L'étude conclue :

« « Aucun des trois systèmes de vote électronique utilisés en Suisse n'est vérifiable par l'électeur lui-même, ni transparent à 100% » » [18]

Si le rapport de 2013 se voulant encourageant et satisfait de l'expérience menée,

13. *Ibid.*, voir p. 19.
14. *Ibid.*, voir p. 46.
15. *Ibid.*, voir p. 47.
16. *Ibid.*, voir p. 6.
17. *Ibid.*, voir p. 47.
18. *Ibid.*, voir p. 20.

la situation politique aujourd'hui est bien différente : au niveau fédéral les partis sont opposés au vote par Internet. Mais il ressort d'une consultation organisée par le Conseil fédéral début 2019 que 19 des 26 Cantons y sont favorables. Autrement dit une écrasante majorité de la population y est favorable tandis que la classe politique y est opposée. Concrètement, les deux systèmes ont été suspendus pendant une période d'au moins quatre ans : plutôt étonnant pour une démocratie qui se revendique aux yeux du monde comme « directe »...

3.2 Rendre les dispositifs de vote électronique plus véri(fiables)

Parmi les difficultés rencontrées afin de rendre une élection plus fiable et transparente, il y a celle de la vérifiabilité. Nous le savons, il s'agit d'une exigence majeure qui est imposée en France par le règlement technique de 2003. Seulement, le principe de vérifiabilité pose plusieurs problèmes. Reprenons par exemple les termes du règlement technique de 2003 à ce sujet : « caractère vérifiable : les résultats du vote peuvent être vérifiés après le dépouillement du scrutin ; » [19]

Imaginons un votant qui souhaite avoir la preuve que son vote a été effectivement pris en compte :

- Si cette preuve était affichée publiquement, le votant perdrait son anonymat.
- Si cette preuve était imprimée, elle pourrait être exigée par un tiers exerçant des pressions, ou exploitée comme justificatif pour vendre son vote.
- Pour le vote par Internet, si cette preuve était renvoyée par mail à l'électeur pour confirmer que son vote bien a été pris en compte, il y aurait alors une trace dans le système qui l'associerait à son vote, faisant perdre son anonymat.

À ce titre le principe d'anonymat et celui de vérifiabilité ne sont pas si différents, on pourrait même dire qu'ils sont les deux faces d'une même pièce. Pour Steve Kremer, chercheur à l'INRIA :

> « Pour préserver l'anonymat, il faudrait donner au votant une preuve mathématique, une sorte de code qu'il serait seul à comprendre. Ainsi, il pourrait montrer ce code à un tiers avec la possibilité de lui mentir délibérément afin de ne pas révéler son choix réel et échapper à des mesures de rétorsion » [20]

19. JORF n°274 du 27 novembre 2003 p. 20188

20. INRIA, *Apporter des réponses pour des échanges plus sûrs*, 2011, URL : `https://www.inria.fr/centre/saclay/actualites/apporter-des-reponses-pour-des-echanges-plus-surs` (visité le 25/08/2019).

Si théoriquement la solution de Steve Kremer est envisageable il faut se rendre à l'évidence en admettant que l'écrasante majorité de l'électorat n'est pas pourvue de connaissances techniques assez développées pour rendre un tel système envisageable à l'échelle d'une nation. C'est d'ailleurs tout le problème du vote électronique : on assiste à un glissement de prérogative du citoyen vers le technicien, et le citoyen ne disposant pas des connaissances techniques afférentes aux systèmes de vote est condamné, soit à devoir faire confiance au technicien, soit à devoir se saisir de sujets qu'il ne maitrisait pas auparavant afin de pouvoir comprendre comment son vote est exprimé, manipulé et transformé au sein des systèmes de vote électronique. L'appel à la transparence et à la vérifiabilité du scrutin, au-delà d'être un enjeu simplement juridique est également un enjeu démocratique.

3.3 Les dispositifs de vote électronique « vérifiables »

Dans un scrutin à bulletins papier, la vérifiabilité du scrutin ne se pose pas : l'observation du scrutin suffit à elle seule pour prouver sa sincérité. Avec l'utilisation des machines à voter et du vote Internet, la vérifiabilité devient plus délicate (3.2.1) Devant ces difficultés, de nouveaux moyens censés compenser le manque de transparence ont été imaginé (3.2.2)

3.3.1 Sincérité et observation du scrutin

La vérifiabilité du vote par matérialisation du bulletin

Prenons le cas d'une élection avec un scrutin qui s'effectue à l'urne, comme pour les élections présidentielles en France. Le principe de vérifiabilité est très facile à mettre en œuvre avec les éléments analogiques que sont les enveloppes et les bulletins papiers. Lorsque le bulletin est enveloppé et déposé dans l'urne, nous avons la certitude que ce bulletin sera pris en compte dans le comptage des voix, en raison de la présence des assesseurs qui, à l'aide de leurs sens, ont pour mission de garantir l'intégrité du l'urne et la sincérité du scrutin.

Dans le cas de figure ; qui est le plus probable ; où les assesseurs ont rempli leur office et que l'urne et son contenu ont effectivement été surveillées pendant toute la durée du scrutin, la seule proclamation des résultats à l'issue du dépouillement suffira pour manifester la sincérité du scrutin. Pourquoi ? Car les enveloppes déposées au cours de la journée n'auront pas été modifiées sans que cette modification ait pu

être constatée ou visible par un ou l'ensemble des assesseurs. Comme le dit Chantal Enguehard, le bulletin de vote est composé « des mêmes particules physiques » [21] entre le moment où l'enveloppe est déposée et le moment où elle est ouverte pour dépouillement.

De même, comme évoqué précédemment, l'urne transparente, au-delà d'être un symbole, remplit une mission qui aide indirectement à la sincérité du scrutin : déposer son enveloppe dans une urne opaque susciterait la méfiance de l'électeur, du seul fait de l'opacité de l'urne. C'est pourtant ce qui se produit dans un ordinateur de vote qui dématérialise le bulletin.

l'opacité comme obstacle à la sincérité

Si le règlement technique de 2003 impose le principe de vérifiabilité, alors ce principe n'est tout simplement pas respecté par les ordinateurs de vote actuellement déployés en France dans les 66 communes utilisatrices de ces dispositifs, de même que celui de « transparence », en référence à ce même règlement.

En effet, qu'il s'agisse d'un vote par Internet ou d'un vote sur des ordinateurs de vote à bulletins dématérialisés, la volonté de l'électeur subit des transformations dont il n'a même pas conscience : sa volonté est transformée en une impulsion électrique qui va être traitée par des composants de l'ordinateur afin de transformer cette impulsion électrique en une suite de 0 et de 1 qui pourra être comprise par le processeur central de l'ordinateur avant de, peut-être, subir d'autres transformations.

Ces transformations au sein du système ne sont pas observables, mais pourtant vont servir à la proclamation des résultats. Si les résultats dépendent de processus qui n'ont pas pu être observés et si on considère que la sincérité du scrutin découle de l'observation du processus électoral, alors la sincérité d'un scrutin par ordinateur de vote à bulletins dématérialisés seul, ne peut se manifester.

Ainsi faut-il élaborer des dispositifs dotés de mécanismes qui garantissent une vérifiabilité et une « traçabilité » [22] des votes.

21. Voir Annexe 1 « Entretien avec Chantal Enguehard »

22. Par traçabilité, nous entendons ici le fait que chaque vote ait une origine authentifiée qui soit nécessairement liée à la volonté d'un électeur et que cet électeur existe. Nous ne parlons pas de la nécessité de lier chaque vote à son votant, en raison du principe de l'anonymat du vote

3.3.2 Compenser l'absence de transparence

Les ordinateurs de vote avec bulletin papier en clôture de scrutin

Il existe deux types de machines, en plus de l'ordinateur de vote à bulletin dématérialisé, qui contrairement à cette dernière utilisent des traces papiers en plus de leur mémoire interne pour remplir leur fonction de machine à voter.

La première de ces machines ; que nous n'évoquerons que très brièvement, car présentant les mêmes défauts qu'un ordinateur de vote à bulletin dématérialisé ; imprime des tickets papiers correspondant à chaque bulletin stocké dans sa mémoire interne lors du dépouillement. Il s'agit des ordinateurs de vote à bulletin matérialisé. La principale faiblesse de cette machine est, nous la devinons, qu'elle est sensible aux dysfonctionnements logiques qui affectent sa mémoire interne. De plus cette machine, bien que dotée d'une trace, déplace le problème de la transparence et de la vérifiabilité : les bulletins imprimés sont bien sûr anonymes, mais avec ce système, les électeurs ne peuvent pas vérifier que leur vote a bien été pris en compte.

En conséquence, cette machine dispose des mêmes faiblesses technico-juridiques que les ordinateurs de vote à dématérialisation [23]. A noter toutefois qu'une telle machine pourrait théoriquement remplir le critère de vérifiabilité tel qu'il est écrit dans le règlement technique de 2003 car la vérifiabilité intervient « après » le scrutin. Le deuxième type d'ordinateur de vote qui pourrait représenter une solution alliant vérifiabilité et transparence est l'ordinateur de vote à bulletin papier individuel.

Les ordinateurs de vote avec bulletin papier individuel

Leur fonctionnement est le suivant : pour chaque scrutin et à chaque vote exprimé, l'ordinateur imprime un bulletin papier en même temps que le vote est exprimé. Le votant, isolé avec la machine, voit le bulletin papier imprimé et peut dès lors vérifier que le vote qu'il a préalablement saisi sur la machine correspond à ce qui est inscrit sur le bulletin imprimé. Il peut alors soit confirmer son vote, soit le modifier [24]. S'il confirme son vote, le bulletin n'est pas récupéré par l'électeur : il est versé dans une urne scellée au sein de la machine avec les autres bulletins papiers. S'il choisit de modifier son vote, alors le bulletin papier est détruit.

23. Bar-el Hagai, *Why secure e-voting is so hard to get*, 2015, URL : `https://www.hbarel.com/analysis/cyber/secure-e-voting-is-hard-to-get` (visité le 25/08/2019).

24. Schneier, *The Problem with Electronic Voting Machines*, 2004, URL : `https://www.schneier.com/blog/archives/2004/11/the_problem_wit.html` (visité le 25/08/2019).

Avec une telle machine, d'une part l'électeur vérifie que son vote a bien été pris en compte et d'autre part l'urne remplie de bulletins papiers représente une sécurité analogique en cas de dysfonctionnement de l'ordinateur. Il devient ainsi possible d'effectuer un double comptage des voix entre les résultats annoncés par l'ordinateur et les bulletins papiers intégrés dans l'urne de la machine [25]. Seulement, l'utilisation de cette machine souffre de nombreux défauts. Ces défauts, en dehors de ceux qui sont simplement liés à l'utilisation de l'informatique relève des procédures électorales : sous quelles conditions pourrait-on effectuer le comptage des bulletins papiers ? Tout l'intérêt de l'utilisation d'une telle machine réside dans la réponse à cette question : si le recomptage des bulletins papiers est systématique, il n'y aucun intérêt à proposer l'utilisation d'une machine à voter.

Intervalles de confiance et degré de certitude

La nuance est grande : des résultats vérifiables ne sont pas forcément des résultats vérifiés. En cas de discordance les bulletins papiers et la mémoire qui est stockée dans l'ordinateur, un support peut-il prévaloir sur l'autre ? De notre avis, si le comptage de l'urne papier ne correspond pas à la mémoire interne de l'ordinateur il convient d'annuler les votes associés au bureau de vote.

La vérification des urnes pourrait se faire selon un protocole désignant aléatoirement des bureaux de vote dans différents endroits comme c'est le cas depuis 2019 en Inde où les machines à voter de ce type sont utilisées massivement à travers le pays qui comporte un million de bureaux de vote [26] et plus de 900 millions de personnes inscrites sur les listes électorales.

Le rôle des mathématiques est important : un système nommé « vérification à risque limité », que l'on pourrait comparer à un audit de risques, peut permettre d'établir à un niveau de certitude élevé si le vote se déroule convenablement ou s'il y a des erreurs, le tout en n'étudiant que quelques milliers de bulletins. Les principales notions mathématiques déployées en la matière sont justement les intervalles de confiance et de fluctuation.

25. Pruthi Rupali, *What is VVPAT ? How does VVPAT work ?*, 2019, URL : `https://www.jagranjosh.com/current-affairs/what-is-vvpat-machine-with-evm-how-does-vvpat-work-1555312059-1` (visité le 25/08/2019).

26. MoneyControl, *Lok Sabha polls 2019 : Number of polling booths, voters and other key facts*, 2019, URL : `https://www.moneycontrol.com/news/india/lok-sabha-polls-2019-number-of-polling-booths-voters-and-other-key-facts-3631851.html` (visité le 25/08/2019).

La méthode semble tout à fait fiable, et sa capacité d'autorégulation (puisqu'elle ajuste elle-même le nombre de bulletins à étudier) la rend extrêmement économique en termes d'opérations à réaliser. Rapidité, économie et fiabilité mathématique sont dans un pays aussi peuplé que l'Inde essentiels où les élections sont amenées à se dérouler en continu durant un mois entier [27].

Vérifiabilité et faillibilité

Dans le cas dans d'un dysfonctionnement pour une quelconque raison de l'ordinateur de vote qui amènerait à changer le vote de l'électeur sur le bulletin papier, on pourrait difficilement imaginer une solution à apporter à cet électeur qui viendrait à se plaindre que son vote ne correspond pas à celui qu'il a saisi dans la machine. Nous connaissons l'adage selon lequel « un ordinateur ne se trompe pas ». Nous avons exposé dans notre démonstration jusqu'à présent que cela était faux.

Cependant, dans la mesure où ces machines doivent répondre à un cahier des charges précis, qu'elles sont censées suivre un procédé de fabrication contrôlé de bout en bout pour que le fabricant puisse l'obtenir le précieux agrément du ministère de l'intérieur, on pourrait supposer que le juge, s'il venait à se prononcer sur un cas d'espèce, douterait de la sincérité de l'électeur.

Imaginons qu'à l'issue d'un scrutin cependant, des électeurs, par dizaines viennent à se plaindre que le vote que la machine a enregistré est différent de celui qu'ils ont saisit : la pression exercée de fait sur le juge serait-elle suffisante pour faire annuler le scrutin du bureau de vote cible ? Il serait plus probable que ce dernier demande une expertise de la machine afin d'identifier des fraudes ou des dysfonctionnements qui auraient pu affecter la sincérité du vote que de simplement se fonder sur la sincérité des électeurs, d'autant plus que ces contestations, qui interviendraient après le dépouillement, pourraient n'avoir que pour but d'annuler le scrutin du bureau de vote en question en raison de résultats insatisfaisants pour ces électeurs.

27. HINDUSTANTIMES, *Lok Sabha election 2019 schedule Highlights | Tried to cover left-wing extremism affected areas at one go, says EC*, 2019, URL : `https://www.hindustantimes.com/lok-sabha-elections/lok-sabha-election-2019-schedule-live-updates-countdown-for-lok-sabha-polls-begins-with-ec-s-announcement-today/story-6RWOYDUJp1IaJdW248pgyL.html` (visité le 25/08/2019).

L'insolubilité du problème d'achat de voix

On sait que le code électoral sanctionne pénalement le fait pour quiconque « promettre des libéralités, des faveurs ou des dons » afin d'influencer l'issue d'un scrutin [28]. En la matière, c'est la tentative d'influence le vote qui est condamnée et non l'obligation de résultat en la matière. On comprend pourquoi : pour un votant qui souhaite apporter la preuve de son vote, il peut être difficilement envisageable qu'il apporte une preuve vidéo où ce dernier se filmerait de bout en bout entre l'insertion du bulletin dans l'enveloppe et le passage devant l'urne. Concernant le fait de pouvoir se prendre en photo dans un isoloir, rien n'est précisé explicitement, excepté à l'article L59 du Code électoral : « Le scrutin est secret ». Le ministère de l'intérieur a eu l'occasion de préciser cet article dans la presse généraliste lors des municipales en 2014 :

« Si le "selfie" n'est pas en lui-même source de trouble à l'ordre public, il n'apparaît pas recommandé de le faire car le simple fait de le faire et a fortiori de le publier peut générer un soupçon sur l'indépendance de l'électeur quant à son vote. En effet, rien ne peut garantir que cette publication n'ait été exigée, notamment par des pressions. [29] »

L'article R49 du Code électoral permet au président du bureau de vote de procéder à toute expulsion en cas de trouble à l'ordre public. L'usage d'une caméra, de la sortie de l'isoloir jusqu'à l'urne pourrait aisément rentrer dans ce cadre.

Pourquoi ce développement concernant l'achat de votes est important ? Il existe en fait un problème commun à l'ensemble des machines à voter que nous n'avons pas encore soulevé : celui de l'achat des voix ou des pressions qui peuvent être exercés sur les votants afin qu'ils votent pour un certain candidat. En effet, l'environnement des machines à voter rend facile pour tout électeur de produire la preuve d'un vote en la faveur d'un certain candidat en se filmant de bout en bout pendant son vote, bien plus facile donc que dans une élection à bulletin papier car l'ensemble du processus se fait à l'abris des regards. La confirmation par la machine que son vote a bien été pris en compte suffit à elle seule comme preuve de vote.

On peut constater que par bien des aspects, les « solutions » de vote électronique, concernant les machines à voter ne représentent pas de réelles solutions en ce qu'elles

28. *Code électoral 2019*, voir Art. L106.
29. Cette déclaration a été reprise par de nombreux articles de presse en ligne

sont elles-mêmes sources de problèmes dans leur déploiement et leur utilisation. Le développement du vote par Internet est porteur de nombreuses innovations démocratiques qui peuvent nous amener à remettre en question certaines règles afférentes au fonctionnement de nos institutions.

Chapitre 4

Un mode de scrutin porteur de changements

Les récents mouvements politiques et sociaux ne peuvent nier le rôle crucial qu'a joué Internet dans leur constitution : l'influence du réseau dans la vie démocratique est de plus en plus importante. Internet a donné un regain d'intérêt inédit à un droit qui semblait oublié : le droit de la pétition. En effet, le pétitionnement électronique est une conséquence naturelle de la possibilité qu'ont désormais les individus de s'exprimer sur Internet et même d'y voter (4.1) L'exemple de cette innovation peut laisser songeur sur les évolutions à venir dans notre démocratie. Mais dans une vision cartésienne de l'apport de cette technologie à la démocratie, est-ce vraiment une avancée ? (4.2)

4.1 Pétitionnement électronique et vote électronique

Remis au goût du jour avec l'essor des technologies de l'information, le pétitionnement électronique et le vote électronique ont des origines communes (4.1.1) Il s'agit d'un phénomène de société pourtant négligé par les politiques et le Législateur qui est handicapé par un manque de loi pour l'encadrer et un contrôle assez restreint de ces plateformes quant à l'usage des données des utilisateurs (4.1.2) C'est pourtant une erreur, tant les enjeux liés à la protection des utilisateurs de ces plateformes est importante (4.1.3) Les conséquences liées à une utilisation à des fins politiques de ces données sont dangereuses et concrètes (4.1.4) D'ailleurs une époque où l'action militante et politique se déporte de plus en plus sur les réseaux, peut-on parler de cyberdémocratie ? (4.1.5) Que ce soit le vote électronique ou le pétitionnement électronique, il est regrettable que l'État ne ce soit pas emparer du sujet pour en faire des services souverains. (4.1.6)

4.1.1 Une pétition électronique contre le vote électronique

On peut définir le pétitionnement électronique comme tout dispositif numérique dont la fonction est de récolter des signatures en vue de saisir un ou plusieurs décideurs d'une question ou d'une proposition. Si le mécanisme de pétitionnement papier classique était destiné à tomber dans l'oubli à l'heure des nouvelles technologies, ce sont pourtant elles qui vont lui donner une nouvelle jeunesse [1].

Par ailleurs, il est aujourd'hui attesté que l'une des premières grandes pétitions électroniques en France porte justement sur le vote électronique. Le 28 Février 2007, le site ordinateurs-de-vote.org a lancé une pétition contre l'utilisation des machines à voter et du vote électronique en France. Cette pétition cumulera près de 110 000 signatures virtuelles qui totalisent en fait trois types de signature :

— Les signatures papiers classiques envoyées par courrier ;
— Les signatures électroniques, c'est-à-dire celles obtenues via le remplissage d'un formulaire ;
— Les signatures scannées, c'est-à-dire les signatures papiers, mais scannées au lieu d'être envoyées par courrier.

Le site ordinateurs-de-vote.org est un site que l'on pourrait qualifier de militant anti-vote électronique produisant des publications scientifiques mixtes qui plaident en faveur d'un vote plus transparent et vérifié par l'électeur. Soutenant l'idée que le vote électronique est dangereux pour la démocratie, il compile les dépêches d'agence et les articles traitant de cette thématique [2]. Aujourd'hui le site existe toujours, mais n'est visiblement plus maintenu depuis quelques années.

Le succès de cette pétition sera très limité : seul le moratoire de 2008 sur les machines à voter vient donner un coup d'arrêt temporaire à l'expansion du vote électronique. L'ironie du sort, c'est que le succès de cette pétition va faire des émules et même créer une multitude de plateformes qui auront pour principale fonction de créer des pétitions, d'en faire la promotion et de récolter les soutiens [3] à ces pétitions, donnant à Internet une dimension revendicative qui n'existait pas jusqu'alors,

1. Laurent Jeanneau, *Les nouveaux militants*, Les Petits Matins, mar. 2008, isbn : 2915879346, voir p. 211.
2. Collectif ODV, *Pourquoi ce site ?*, 2004, url : `https://www.ordinateurs-de-vote.org/Pourquoi-ce-site.html` (visité le 25/08/2019).
3. Il est beaucoup plus sage de parler de soutien que de signature électronique. Si l'on veut être rigoureux, nous nous accorderons à dire que le terme de « soutien » est générique alors que celui de signature électronique obéit à une définition stricte, qui permet garantir l'intégrité d'un document électronique et d'en authentifier l'auteur. La signature électronique signifie l'engagement contractuel alors qu'un soutien n'a pas de valeur juridique et ne correspond, en somme qu'à une adhésion.

et pourtant, nous sommes déjà en 2007. Hasard du calendrier, le règlement technique sur les machines à voter de 2003 adopté par arrêté ministériel le fut la même année que l'acte II de la décentralisation via la loi constitutionnelle n°2003-276 du 28 mars 2003 qui constitutionnalisa le droit de pétition dans les collectivités territoriales.

4.1.2 Des tentatives et des échecs

Nous avons pu constater précédemment que malgré les innovations qui se poursuivent en la matière, le droit de vote reste globalement hermétique aux nouvelles technologies et les expérimentations menées via les machines à voter ou le vote par Internet restent à ce jour, en France, un succès mitigé.

Concernant les pétitions électroniques, la quasi-absence de cadre juridique convenable sur le plan national a laissé libre court au développement d'une multitude de plateformes dont certaines sont cependant un véritable succès. Cette quasi-absence s'exprime par un droit de la pétition qui n'a jamais vraiment été formalisé, ni par le Législateur, ni par le Juge jusqu'en 2003. Les pétitions les plus populaires sont même reprises par les médias comme un baromètre de l'intensité d'une revendication démocratique, comme ce fut le cas en 2016 à l'occasion des revendications contre la loi travail[4] donnant lieu à une pétition qui totalisa plus d'un million de soutiens. Cette pétition et cette revendication plus particulièrement ont même créé des mouvements citoyens autonomes comme « Nuit Debout ».

Certes, l'État a tenté de s'adapter en ouvrant progressivement des plateformes officielles afin que les citoyens puissent directement déposer des propositions qui peuvent ensuite donner lieu à des débats et pourquoi pas des projets de lois, mais ces innovations n'ont de charme que ce qu'elles représentent sur le papier. Parfois il s'agit simplement de la possibilité de donner avis et de faire des propositions relatifs aux politiques publiques comme sur le site de l'assemblée nationale[5].

Mais tout porte à croire qu'il s'agit d'un échec : à ce jour cette initiative n'a donné lieu à aucun retrait d'une loi qui pouvaient être contestée ou donné l'occasion à une proposition de loi d'émerger. Le site présente des dysfonctionnements importants et ne semblent plus être maintenu correctement. Pour preuve, il s'agit

4. Loi n° 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels

5. Il y a une rubrique "déposer votre contribution" en parallèle avec la procédure d'examen des projets de loi : `http://etudesimpact.assemblee-nationale.fr/`

d'un site institutionnel, et pourtant le protocole SSL n'y est même pas activé, les communications sont envoyées en clair et ne sont ni chiffrées ni sécurisées...

4.1.3 Un dispositif négligé par l'État

Il semblerait donc, malgré l'importance considérable de cette évolution démocratique que constitue l'usage des réseaux pour défendre des revendications, que le pouvoir politique continue de négliger les pétitions électroniques et les forces dont elles peuvent se doter. Pourtant, l'État, et plus particulièrement le Législateur devrait se saisir de cette question pour deux raisons majeures :

Tout d'abord le pétitionnement électronique, certainement au même titre que le vote électronique, répond à un besoin citoyen, celui de pourvoir revendiquer et de défendre des propositions en dehors des échéances électorales. Ce besoin, qui saurait être expliqué et développé sous l'angle de la science politique peut difficilement trouver sa place dans nos développements, bien qu'il puisse également trouver comme origine secondaire le vote électronique.

La seconde raison, moins évidente, est que le déficit juridique en matière pétitionnement électronique a contribué a créer une jungle : si les plateformes de pétitionnement sont nombreuses et peuvent rassembler des centaines de milliers de soutiens ou de signatures, les règles entourant le fonctionnement de ces plateformes restent assez floues, encourageant des pratiques douteuses.

4.1.4 L'importance de la sécurité des données

La protection ou la sécurité des données des citoyens sur Internet ; et plus particulièrement celles des citoyens européens ; est devenu un enjeu capital depuis ces dernières années avec l'entrée de l'application du règlement européen sur la protection des données [6] en Mai 2018. Cette législation n'est pas sans conséquence ni sur le vote électronique, ni sur le pétitionnement électronique. La conformité des plateformes de pétitionnement électronique soulève des questions importantes de même que le fonctionnement des plateformes de vote par Internet.

6. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

Dans la plupart des cas, afin de pouvoir utiliser les services d'une plateforme de pétitionnement électronique, il faut au préalable lui communiquer un certain nombre de données nous concernant, comme le nom, le prénom, l'adresse postale et une adresse mail. Etrangement, ces informations sont également demandées par les plateformes commerciales afin de pouvoir nous envoyer des offres de biens et de services adaptés à nos préférences.

De plus, ces informations, additionnées à nos interactions sur ces plateformes peuvent révéler, par déduction, des données très sensibles, comme les opinions politiques, philosophiques ou religieuses. Si l'on considère que la récolte de données personnelles en vue de soutenir une pétition est un traitement, quelle est sa finalité au sens du règlement européen [7] ? Le plus souvent, il s'agit du consentement. Il faut garder en tête que ces services de pétitionnement en ligne à destination de la France sont hébergés, parfois, en dehors de l'Union Européenne [8], dans des pays où on ne s'attend pas à trouver de tels services : Iles Vierges Britanniques, Bahamas, etc.

Cette problématique est au cœur de nos préoccupations quand nous venons à parler de sécurité du vote électronique. Nous ne parlons pas ici de sécurité du dispositif électronique, mais de quelques choses de plus profond : la sécurité de nos opinions.

4.1.5 Vote électronique et réseaux sociaux

Cambridge Analytica était une société travaillant en collaboration avec Facebook spécialisée dans les outils d'exploration et d'analyse de données. Le lanceur d'alerte Christopher Wylie affirme dans un entretien accordé à plusieurs journaux européens, dont Libération, que la société Cambridge Analytica a joué un « rôle crucial » dans le vote en faveur du Brexit [9].

Selon lui, le profilage de dizaines de millions d'utilisateurs, rendu possible par l'accumulation massive de données transmises par Facebook, combiné à une campagne de publicité ciblée en faveur du Brexit ont permis de faire pencher le corps

7. L'article 5 du Règlement Européen sur la Protection des données impose une finalité pour le traitement de données à caractère personnel

8. On peut raisonnablement douter que l'ensemble des préconisations imposées par le RGPD pour garantir la bonne tenue et la légalité du traitement hors de l'Union Européenne soient respectées.

9. Delesalle Sonia, *"Sans Cambridge Analytica, il n'y aurait pas eu de Brexit"*, 2018, URL : `https://www.liberation.fr/planete/2018/03/26/sans-cambridge-analytica-il-n-y-aurait-pas-eu-de-brexit_1638940` (visité le 25/08/2019).

électoral britannique du côté d'une sortie de l'Union Européenne lors du Référendum britannique le 23 juin 2016. Il n'est cependant pas clairement établit à ce jour que cette campagne fut si importante au point d'avoir déclencher le Brexit [10]. L'enquête est d'ailleurs toujours en cours.

Ce qu'illustre ce cas d'espèce très ancrée dans l'actualité, c'est que des données personnelles exploitées à des fins politiques entre des mains de sociétés sans scrupules peuvent faire basculer un pays et faire tomber des gouvernements : rappelons que David Cameron a démissionné suite au référendum britannique, les résultats n'allant pas le sens attendu par le parti travailliste.

Quel rôle joue le vote électronique, et plus particulièrement le vote par Internet à la lumière de cette histoire ? Au-delà des faiblesses techniques dont peuvent souffrir le dispositif, l'élément clé dans un vote, c'est l'électeur. Dans une campagne publicitaire confinant à de la propagande politique ciblée, l'électeur peut se retrouver manipuler : il peut voir des articles de presse qui le sensibilisent à des causes qu'il n'aurait pas défendues autrement et il peut être conditionné par des publicités récurrentes. Pour cette raison, la réelle problématique qui est liée à la protection des données des citoyens européens, quand on vient à parler de vote par Internet pour des élections politiques, ce n'est pas le piratage du système qui pose le plus de problèmes, c'est le piratage des esprits.

Bien entendu, on sait qu'en France le code électoral à son article L49 garantit une période de « silence électoral » : « « A partir de la veille du scrutin à zéro heure, il est également interdit de diffuser ou de faire diffuser par tout moyen de communication au public par voie électronique tout message ayant le caractère de propagande électorale. » »

En vérité cette interdiction relève cependant davantage d'un principe que d'une règle : le phénomène #RadioLondres phénomène qui apparaît sur plusieurs réseaux sociaux, communiquant des résultats partiels accessibles en dehors du territoire national et provenant par exemple de pays limitrophes où ne s'appliquent pas de telles restrictions de silence électoral sur les élections étrangères. Les comptes anonymes sur les réseaux sociaux véhiculant de la propagande politique avant de disparaitre, les groupes privés sur les réseaux sociaux... La propagande électorale, malgré elle, ne

10. Rathi Rahul, *Effect of Cambridge Analytica's Facebook ads on the 2016 US Presidential Election*, 2019, URL : `https://towardsdatascience.com/effect-of-cambridge-analyticas-facebook-ads-on-the-2016-us-presidential-election-dacb5462155d` (visité le 25/08/2019).

s'arrête plus comme elle le devrait le jour précédant le scrutin. On pourrait d'ailleurs considérer qu'une telle saturation d'informations peut affecter la sincérité du scrutin et cette disposition est censée s'appliquer dans ce but.

Il convient, à la lumière de nos développements de renforcer la protection des données à caractère personnel à travers le monde afin que les futures élections, qu'elles se déroulent à l'urne ou sur notre ordinateur se déroulent comme un lancer de dé pipé.

A ce titre, sur le plan international, les événements qui entourent l'élection de Donald Trump et le vote du Brexit suscitent un certain nombre d'interrogations et surtout un constat : le support privilégié pour la propagande politique est désormais Internet. Si le vote continue de résister à son informatisation, il poursuit, avec le pétitionnement électronique, un but précis : l'avènement de la cyberdémocratie.

4.2 La cyberdémocratie et ses conséquences

4.2.1 La banalisation du débat public

Les objectifs de la modernisation de l'État par le vote électronique comme à travers l'espace numérique contribuent implicitement à une banalisation et une dévalorisation des scrutins publics. Les votations sont comprimées dans un formalisme cadré, qui se construit non plus dans un mouvement collectif cohérent mais avec des habitudes qui relèvent davantage de la simple consommation du vote. Le débat idéologique va progressivement être déconsidéré et négligé à l'occasion des grandes consultations nationales puisqu'il suffirait simplement, à partir d'images et de textes sur un écran et d'une touche à effleurer pour exercer son devoir de citoyen. Dans le cadre du vote par Internet, l'électeur ne se déplace plus au bureau de vote : il y a une rupture dans la relation physique que ce dernier entretenait jusqu'alors avec les scrutins.

4.2.2 Vote électronique et sondages

La tentation du référendum permanent vient avec le vote électronique, soit pour soumettre des questions dont il faut se demander pourquoi celles-ci et pas d'autres, soit pour soumettre la légitimité d'une proposition ou même d'une autre élection qui s'est déroulé peu de temps avant. En vérité, le principal danger politique du vote électronique, c'est que le débat public se transforme en opinion public et que le vote électronique dégénère sans s'en rendre compte en sondage électronique. En effet, dans le cadre d'un recours au vote électronique, celui-ci serait généralisé afin de pouvoir mettre le citoyen au coeur du processus institutionnel : on pourrait imaginer que celui-ci viendrait à se prononcer pour ou contre une certaine loi, que l'on mette en place un seuil de voix minimal afin qu'une proposition de loi soit soumise à consultation nationale.

Les dispositions constitutionnelles liées au référendum [11] n'auraient plus de raison d'être et seraient vidées de leur importance au profit d'un système de vote électronique rapide et national. Dans le cadre d'un sondage, la réponse de l'électeur n'a qu'une valeur indicative, elle n'a aucune signification juridique n'a aucun effet mesurable sur la politique en général. Le vote électronique, c'est mettre en jeu sa part de souveraineté propre à chacun de nous : il a un cadre officiel, solennel. Mais

11. Surtout l'Art. 11 de la Constitution du 4 Octobre 1958

paradoxalement, on pourrait imaginer qu'une interface de sondage électronique soit identique à une interface de vote en ligne. Les moyens pourraient être exactement les mêmes, mais pour des fins diamétralement opposées.

On pourrait également considérer qu'il y aurait une rupture dans sa relation psychique avec la chose publique : le vote serait devenu quelque chose de banal et d'acquis, détaché du sens profond que celui-ci pouvait porter grâce au cérémonial du vote en communauté dans un bureau de vote avec l'urne transparente et les enveloppes qui s'y accumulaient autrefois. Néanmoins, dans les sociétés démocratiques contemporaines comme la notre, ainsi que de nombreux observateurs l'ont démontré, le succès de la démarche impliquée par le vote électronique, quelle que serait sa forme, dépend moins des techniques mises en oeuvre que des contextes sociaux ou politiques [12].

4.2.3 L'omniscience du système de vote

Selon Chantal Enguehard, un dispositif de vote par Internet, constitué entre un terminal et un serveur, est une série de dialogues entre ces deux dispositifs. Lors d'une élection, l'électeur entre des identifiants afin d'être reconnu par le système et de déterminer s'il a déjà voté pour l'élection en cours. Selon les dernières recommandations de la CNIL, l'électeur doit pouvoir confirmer son vote lorsqu'il choisit un candidat [13]. La requête est alors envoyée au serveur électoral puis, par rebond, revient sur le terminal du votant afin qu'il puisse confirmer son vote.

Cette disposition technique a une conséquence extrêmement importante : entre l'instant où le serveur reçoit la requête et l'instant où l'électeur confirme son choix, le serveur électoral est capable d'identifier l'électeur et de l'associer à son vote. Si l'on peut vraisemblablement supposer que cette correspondance n'est établie que le temps du traitement de l'information, alors pendant un très bref instant, le secret du vote et son anonymat ne sont plus garantis.

4.2.4 L'expression de la liberté du vote

Selon Chantal Enguehard :

12. Éric Maigret et Laurence Monnoyer-Smith, « Le Vote en ligne », FR, *in* : *Réseaux* 112-113.*2-3* (2002), p. 378–394, voir p. 378.
13. Délibération n°2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet

« « Pour que l'électeur vote en toute liberté, il faut qu'il puisse voter pour Marine Le Pen alors qu'il est dans une famille qui vote Jean-Luc Mélenchon, ou l'inverse, c'est ça la liberté de vote. » [14] »

Or, dans un vote par Internet, l'électeur le plus craintif et le plus sensible peut croire qu'une trahison de sa famille politique pourra être connue par autrui : il ne connait rien du système qu'il utilise et doit faire confiance à des experts dont il ne pourra jamais consulter les rapports traitant de l'expertise de l'application de vote par Internet, tenus secrets en raison d'un secret industriel.

4.2.5 Une vision néolibérale

On sait depuis le début du XXème siècle que certaines missions de service public peuvent aisément être confiées à des entreprises privées [15], la question de la délégation des missions relatives à la mise en œuvre d'élections politiques peut s'avérer plus délicate.

La décision du Conseil Constitutionnel en la matière [16] évoquée précédemment conclue cependant à la parfaite légalité de l'usage des machines à voter dans les communes qui l'ont souhaité dès lors que la machine à voter dispose de l'agrément du ministère de l'intérieur et que le préfet a préalablement autorisé le recours à ces machines.

Concernant le pétitionnement électronique, la situation est différente : le cadre normatif du pétitionnement électronique est beaucoup plus restreint que celui du vote électronique car l'État ne s'est, en fait, pas donné les moyens de son ambition. Certes, la loi pour une république numérique [17] a considérablement développé les outils étatiques afin de mettre à disposition des administrés les outils dont ils ont besoin pour être plus proches des gouvernants. Si la volonté de mettre en place un "gouvernement ouvert" est encore timide, la prochaine réforme devra sans doute passer par une étude sérieuse du sujet du pétitionnement en ligne et du vote par Internet pour certaines élections. Le seul problème, désormais récurrent, dans les projets visant à intégrer l'outil numérique dans les démarches administratives et citoyennes est le retrait de l'État des initiatives qu'il impulse.

14. Voir Annexe 1 « Entretien avec Chantal Enguehard »
15. Conseil d'Etat, du 4 mars 1910, 29373 "Therond"
16. Décision n° 3742/3947 du 20 décembre 2007 du Conseil Constitutionnel
17. Loi n° 2016-1321 du 7 octobre 2016 pour une république numérique

En effet, le début des années 2000 a étémarqué par le déploiement de nouvelles conceptions de l'État de son rôle avec nouvelles lois de décentralisation s'accompagnant d'une exigence d'autonomie plus grande pour les collectivités locales , la marge de liberté laissée aux communes pour l'organisation des élections peut se lire dans cette perspective. Mais, au-delà des enjeux spécifiques à la décentralisation, les théories néolibérales invitent à une remise en cause radicale des manières de penser l'État moderne.

Selon cette conception, l'État devrait laisser sa place à des acteurs jugés plus pertinents au titre de leur compétence, ou de leur domaine : c'est la conception ordo-libérale. Dans cette conception l'État est régulateur : il fixe un cadre légal mais n'intervient pas du tout. On peut à ce titre regretter que l'État recourt à des personnes privées pour exercer des missions d'une importance capitale pour le fonctionnement démocratique comme les élections, via des machines à voter et des plateformes de vote par Internet conçues par des personnes privées.

Si le vote électronique est porteur d'avenir, cet avenir ne sera bon que par le développement de solutions souveraines, ouvertes, et contrôlables par le plus grand nombre. Il ne suffit pas de chercher bien loin pour constater le savoir-faire français dans les technologies de l'information : l'ANSSI a par exemple développé son propre système d'exploitation open sources du nom du clip OS [18] en 2018. L'application de messagerie sécurisée Tchap, également française est une réussite dans le domaine des communications sécurisées de bout en bout [19]. A quand une solution de vote par internet française libre, vérifiable et transparente ?

18. https ://www.ssi.gouv.fr/administration/services-securises/clip/
19. http ://www.tchap.fr/

Conclusion

Platon, quatre siècles avant notre ère, exposa dans le Livre VII de La République une allégorie illustrant parfaitement notre propos. Dans une caverne souterraine dont l'entrée donne sur l'extérieur, des hommes sont enchainés entre eux. Ils n'ont jamais vu ni la surface ni les rayons du soleil qui peinent à leur parvenir au fond de cette caverne. Ils ne connaissent de la vision du monde que les ombres et les formes émanant d'un feu brûlant derrière eux depuis toujours. Ils ne connaissent des sons du monde que leurs échos lointains et confus. C'est l'allégorie de la caverne. Dans cette allégorie, le soleil symbolise « l'idée du bien, source la science et de la vérité en tant qu'elles sont connues ».

Dans cette quête de transparence et de sécurité dans les systèmes de vote électronique, nous sommes, malgré nous, comme ces hommes, persuadés que ce que nous voyons sur l'écran, de notre terminal ou de celui d'une machine à voter est la vérité. Nous maîtrisons la technologie, nous avons confiance en nos dispositifs et pour beaucoup d'entre nous, nous avons la certitude qu'un ordinateur exécute uniquement les instructions qui lui ont été saisies. Une part très restreinte de la population a pourtant pleinement conscience du fonctionnement complexe de l'ordinateur et savent de fait qu'il est faillible. François Pellegrini dit à ce sujet :

> « [l'électeur] ne peut plus faire confiance à ses sens pour attester de la réalité d'actions immatérielles, se produisant au sein d'équipements informatiques dont seule l'existence peut être attestée, et dont les effets ne sont perceptibles qu'à travers d'autres dispositifs techniques »

Chantal Enguehard évoque quant à elle une « nature chimérique du vote électronique », résultant, selon elle d'une « incompatibilité» entre transparence directe, respect de l'anonymat et dématérialisation des votes. Dans la mythologie grecque, la chimère est une créature fantastique, utilisée aujourd'hui pour représenter les espoirs fous confinant à l'illusion ou la fantaisie.

Si la transparence repose effectivement sur l'observabilité de l'élection, alors le vote électronique ne saurait, par essence, être transparent sans faire d'atteinte à l'anonymat du vote, condition de validité essentielle de toute élection dans les démocraties modernes. Est-ce une fatalité pour autant ? Nous avons pu constater au

cours de nos développements que des solutions peuvent exister et que les conditions nécessaires à leur apparition sont réunies : une expérience suisse qui tire des conclusions favorables, des élections indiennes qui réussissent à se tenir soupçons d'irrégularité avec une méthode relative fiables...

En vérité, il n'existe aucune disposition légale qui impose l'obligation de transparence dans l'élection. Le mot « transparent » ou « transparence » n'apparaît d'ailleurs, dans un contexte électoral, qu'une seule fois dans le Code Electoral à l'article L63 : « L'urne électorale est transparente [...] »

Cette transparence peut être comprise à la lumière de l'ensemble du processus électoral par vote papier. Si l'urne qui recueille les bulletins est transparente, c'est d'abord pour obéir à une disposition légale, mais c'est également pour lui faire revêtir une valeur symbolique et philosophique qui impose la sincérité du scrutin quand les procédures sont correctement respectées par les assesseurs.

Le principe de transparence peut également être considéré comme le dénominateur commun des piliers du droit électoral que sont l'anonymat, l'unicité, la convivialité, la confidentialité, et la sincérité. Réduire la transparence à une simple question de philosophie politique serait pour autant une erreur.

Cependant, on constate que de nombreuses élections se déroulent aujourd'hui par vote dématérialisé sans que le manque de transparence lié à ces élections n'entache leur validité. C'est le cas des élections professionnelles mais aussi celui des élections législatives pour les français de l'étranger dans le cadre du vote par Internet. C'est également le cas pour plus d'un million de français qui utilisent à chaque élection des machines à voter pour exprimer leur volonté, malgré, du fait de leur obsolescence, des dysfonctionnements.

Nous avons pu constater que l'expérience menée à Genève en 2013 citée infra n'avait pas d'impact significatif sur le résultat des élections. Pour autant l'étude de la Haute Ecole spécialisée bernoise (HESB) relève que les dispositifs utilisés n'étaient pas 100% transparents. Il semblerait que cet impératif de transparence tend à s'estomper par l'utilisation du vote par Internet.

Selon un sondage réalisé fin octobre 2015 par Harris Interactive pour le quotidien Le Parisien, 56 % des Français interrogés souhaiteraient pouvoir voter par Internet aux élections politiques sans avoir à se déplacer jusqu'à leur bureau de vote. Autre

donnée intéressante, on apprend que 58 % des abstentionnistes lors des précédents scrutins déclarent que, s'ils pouvaient voter par Internet, ils le feraient. Ce nombre grimpe à 79 % chez les 18-25 ans.

A l'heure de l'hyper-connexion entre les nouvelles générations et les ordinateurs, le vote par Internet est sans doute le mode de vote électronique qui est destiné à se développer. Nous pouvons conjecturer que les machines à voter, en France, sont destinées disparaitre au profit du vote par Internet pour les élections politiques et que le vote à l'urne sera remplacé, pour certaines élections parmi les moins porteuses d'enjeux nationaux, par un vote dématérialisé.

Le vote par Internet, d'ailleurs, est propice à un certain développement car les bases sont posées depuis un moment avec le vote par Internet aux élections professionnelles et par le mécanisme de la pétition électronique.

Nous avons évoqué au départ de notre réflexion qu'Internet était d'ailleurs un outil destiné à être de plus en plus utilisé à des fins politiques pour faire vivre la démocratie. Nous avons à ce titre évoqué l'exemple du Référendum d'initiative partagée dont la consultation se fait sur le site du ministère de l'intérieur.

L'action citoyenne tend à quitter la rue pour s'installer de plus en plus sur les réseaux. La dématérialisation de la propagande électorale aurait pour avantage de garantir des économies considérables à l'ensemble des partis politiques, y compris les plus minoritaires d'entre eux, qui sont parfois obligés de lever des fonds pour simplement transmettre leurs bulletins aux bureaux de vote pour donner la possibilité aux électeurs de voter pour ses sensibilités politiques. Dès lors, les électeurs les plus convaincus doivent imprimer leur bulletin chez eux par leurs propres moyens pour soutenir leurs candidats, augmentant le risque que le bulletin ne soit pas valide pour des raisons de formes parfois très strictes. Ce problème ne se pose pas avec le vote électronique en général : le bulletin nul n'existe plus.

Marcel Moritz interroge d'ailleurs la soutenabilité de notre modèle institutionnel face à l'essor des nouvelles formes d'expression démocratique comme le pétitionnement électronique et la remise en question de procédures qui perdurent depuis maintenant des décennies sur le plan électoral :

> « (...) est-il acceptable que des structures privées (...) pallient aux yeux du public une mission qui devrait être assurée par la puissance publique, avec parfois des conditions d'utilisation extrêmement discutables ? (...) il nous semble essentiel de nous interroger sur l'évolution des pratiques dé-

> mocratiques qui pourrait être induite par le développement des pétitions en ligne. »

Si l'article original dont est tiré cette interrogation traite du pétitionnement électronique et du développement des initiatives locales pour faire vivre la démocratie, on peut aisément constater qu'à la lumière de nos développements, le pétitionnement électronique et le vote électronique sont en réalité les deux faces d'une même pièce.

L'un a une approche se fondant sur le soutien quantitatif d'une part connue de la population à une proposition, c'est le pétitionnement électronique ; l'autre a une approche se fondant sur la pondération des voix accordées par le corps électoral à une proposition ou un candidat en tout anonymat, c'est le vote électronique. Les deux se font par l'usage du même support : Internet.

Pour Benjamin Bayart, militant pour les libertés fondamentales dans la société de l'information, ingénieur français, président de l'association FDN et co-fondateur de la Quadrature du Net, « Internet aura à terme, le même effet sur notre société que la découverte de l'écriture. » Selon lui, de grands bouleversements économiques et politiques vont se produire grâce à Internet, et la possibilité pour une nation de s'organiser via l'utilisation des seuls réseaux est sans doute l'une de ces révolutions à venir.

Il est tout à fait possible de considérer que le vote électronique, en France, serait une non-solution à un non-problème : après tout, le scrutin à bulletin papier a prouvé sa sécurité et sa transparence depuis le début de son utilisation dans notre république. Les circonstances qui devront amener à un changement progressif et généralisé en faveur d'un autre mode de scrutin comme le vote par Internet devront se justifier par bien d'autres choses qu'une simple recherche d'économie ou de modernité.

Qu'il s'agisse de faire l'impasse sur la transparence afin de rendre le vote électronique possible pour les élections politiques nationales ou de réfléchir à de nouveaux modèles démocratiques, les prochains grands bouleversements démocratiques se feront par l'impulsion des citoyens eux-mêmes. Les experts en sécurité informatique, seront, peut-être, les assesseurs de demain.

Bibliographie

Ouvrages et Rapports

Alvarez, R. Michael et Thad E. Hall, *Electronic elections : The perils and promises of digital democracy*, 2010, isbn : 9781400834082.

Anziani, Alain et Antoine Lefevre, *Vote électronique : Préserver la confiance des électeurs - Rapport d'information n°445 fait au nom de la commission des lois*, rapp. tech., Paris, France : Sénat, 2014, p. 85, url : https://www.senat.fr/rap/r13-445/r13-445.html.

Azéma, Jacques, *Droit de la propriété industrielle*, Dalloz-Sirey, sept. 2017, isbn : 2247153062.

Commission externe d'évaluation des politiques publiques, *Voter par internet : évaluation des effets du vote électronique à Genève*, rapp. tech., Genève : République et Canton de Genève, 2013, p. 64, url : https://www.ge.ch/document/rapport-commission-evaluation-politiques-publiques-quant-impact-introduction-du-vote-electronique-geneve/telecharger.

Council of Europe, *Legal, Operational And Technical Standards for E-voting - Recommendation Rec (2004)11 And Explanatory Memorandum*, Council of Europe, mai 2005, isbn : 9287156352.

Déloye, Yves et Olivier Ihl, « Introduction. De l'élection à l'acte de vote », FR, *in* : *L'acte de vote*, Références, Paris : Presses de Sciences Po, 2008, p. 11–29, isbn : 9782724610581.

Deromedi, Jacky et Yves Détraigne, *Réconcilier le vote et les nouvelles technologies - Rapport d'information n°73 fait au nom de la commission des lois*, rapp. tech., Paris, France : Sénat, 2018, p. 96, url : https://www.senat.fr/notice-rapport/2018/r18-073-notice.html.

Engineering et al., *Securing the Vote : Protecting American Democracy (Cybersecurity)*, National Academies Press, 2018, isbn : 030947647X.

Enguehard, Chantal, « Les dispositifs de vote électronique dits vérifiables », *in* : *Le vote électronique*, sous la dir. d'Olivier Ihl Gilles Guglielmi, Eyrolles, 2015, url : https://hal.archives-ouvertes.fr/hal-01199032.

Enguehard, Chantal. et Robert (19..-....). Panico, *Technologies et usages de l'anonymat sur internet*, 2010, isbn : 9782296131088.

Forum des droits de l'internet, *Rapport d'activité pour l'année 2003*, sous la dir. de La Documentation française, Paris, 2004, p. 400, isbn : 2-11-0055942-4, url : https://www.ladocumentationfrancaise.fr/var/storage/rapports-publics/044000213.pdf.

Guglielmi, Gilles-J, Olivier Ihl et Collectif, *Le vote électronique*, LGDJ, 2015, isbn : 2275044663, url : https://www.lgdj.fr/le-vote-electronique-9782275044668.html.

Jeanneau, Laurent, *Les nouveaux militants*, Les Petits Matins, mar. 2008, isbn : 2915879346.

Klay, Francis et al., *Retour d'experience sur la Validation du Vote Electronique*, rapp. tech., 2006.

Morin, Marie-Laure, *Le guide des élections professionnelles et des désignations de représentants syndicaux dans l'entreprise*, Dalloz-Sirey, nov. 2015, isbn : 2247138527.

Pellegrini, François, *Chaînes de confiance et périmètres de certification : le cas des systèmes de "vote électronique"*, Research Report RR-8553, 2014, p. 30, url : https://hal.inria.fr/hal-01010950.

Articles et Publications

Abandah, Gheith A. et al., « Secure national electronic voting system », *in* : *Journal of Information Science and Engineering* (2014), issn : 10162364.

Boukamel, Owen, « Le rôle des réseaux d'acteurs dans l'innovation publique complexe : le cas du vote électronique dans le canton de Genève », *in* : *Politiques et management public* (2017), issn : 0758-1726, doi : 10.3166/pmp.34.2017.0010.

Chaum, David et al., « Scantegrity : End-to-end voter-verifiable optical-scan voting », *in* : *IEEE Security and Privacy* 6.*3* (2008), p. 40–46, issn : 15407993, doi : 10.1109/MSP.2008.70.

Contamin, Jean-Gabriel, Thomas Léonard et Thomas Soubiran, « Les transformations des comportements politiques au prisme de l'e-pétitionnement », *in* : *Réseaux* (2017), issn : 0751-7971, doi : 10.3917/res.204.0097.

Cortier, Véronique et Ben Smyth, « Attacking and fixing Helios : An analysis of ballot secrecy », *in* : *Journal of Computer Security* 21.*1* (2013), p. 89–148, url : http://www.bensmyth.com/publications/2012-attacking-ballot-secrecy-in-Helios/.

Enguehard, Chantal, « Blockchain et vote électroniqueBlockchain and Electronic Voting », *in* : *Terminal* (2019), issn : 0997-5551, doi : 10.4000/terminal.4190.

— « Introduction à l'analyse de chimères technologiques, le cas du vote électronique », *in* : *Cahiers Droit, Sciences & Technologies* (2010), ISSN : 1967-0311, DOI : 10.4000/cdst.244.
— « Le vote électronique en France : opaque & invérifiable », *in* : *Terminal 99-100* (2007), p. 199–214, URL : https://halshs.archives-ouvertes.fr/halshs-00085071.
— « Transparency in Electronic Voting : the Great Challenge Abstract : Keywords : » *in* : *Political Science* (2008).
— « Vote papier, vote mécanique, vote électronique », *in* : *Le Genre humain* (2011), ISSN : 0293-0277, DOI : 10.3917/lgh.051.0041.
— « Vote par internet : failles techniques et recul démocratique », 2007, URL : https://hal.archives-ouvertes.fr/hal-00181335.

ENGUEHARD, Chantal et Jean-Didier GRATON, « Machines à voter et élections politiques en France : étude quantitative de la précision des bureaux de vote », *in* : *Cahiers Droit, Sciences & Technologies* (2014), ISSN : 1967-0311, DOI : 10.4000/cdst.326.

GHEVONTIAN, Richard, éd., *La sincérité du scrutin*, fre.

HÉLÈNE-MARION, Michel, « Les cartes cognitives du vote électronique : une approche exploratoire des systèmes de représentations des citoyens », *in* : *Systèmes d'Information et Management* (2005), ISSN : 12604984.

IHL, Olivier, « L'urne électorale. Formes et usages d'une technique de vote », fre, *in* : (1993), ISSN : 0035-2950, DOI : 10.3406/rfsp.1993.394716, URL : https://www.persee.fr/doc/rfsp_0035-2950_1993_num_43_1_394716.

KIM, Keonwoo et Dowon HONG, *Electronic Voting System using Mobile Terminal*, 2007, DOI : 10.5281/zenodo.1082527, URL : https://doi.org/10.5281/zenodo.1082527.

KLING, Rob et David LYON, « The Electronic Eye : The Rise of the Surveillance Society . », *in* : *Contemporary Sociology* (1995), ISSN : 00943061, DOI : 10.2307/2077688.

LI, Yan Jiang, Chuan Gui MA et Liu Sheng HUANG, « Electronic voting scheme », *in* : *Ruan Jian Xue Bao/Journal of Software* (2005), ISSN : 10009825, DOI : 10.1360/jos161805.

LOADER, B D et D MERCEA, « Networking Democracy ? Social media innovations and participatory politics », *in* : *Information, Communication and Society* 14.6 (2011), p. 757–769, DOI : 10.5281/zenodo.571345, URL : https://doi.org/10.5281/zenodo.571345.

Maigret, Éric et Laurence Monnoyer-Smith, « Le Vote en ligne », FR, *in* : *Réseaux* 112-113.*2-3* (2002), p. 378–394.

Morel, Benjamin, « Les enseignements des expériences européennes du vote électronique », *in* : *Revue française de droit constitutionnel* (2018), issn : 1151-2385, doi : 10.3917/rfdc.114.0371.

Moritz, Marcel, « Gouvernements ouverts et pétitions électroniques - Quel impact sur les politiques publiques locales ? », *in* : *Revue Internationale de droit des données et du numérique* 3 (2017), p. 79–94, issn : 2553-6893.

Nessmann, Philippe, « Le vote électronique, pour quelles élections ? », *in* : *CNRS Le Journal* (2015).

« Thomas A. Edison papers », *in* : *Choice Reviews Online* (1998), issn : 0009-4978, doi : 10.5860/choice.35sup-163.

Venturini, Tommaso et Richard Rogers, « "API-based research" or how can digital sociology and journalism studies learn from the Cambridge Analytica affair », *in* : *Digital Journalism* (2019), url : https://hal.archives-ouvertes.fr/hal-02003925.

Ziegler, J. F., « Terrestrial cosmic ray intensities », *in* : *IBM Journal of Research and Development* (1998), issn : 00188646.

Extraits d'Ouvrages

Enguehard, Chantal, « Internet voting : Situation, questions, and trends », *in* : *Transforming Politics and Policy in the Digital Age*, 2014, isbn : 9781466660397, doi : 10.4018/978-1-4666-6038-0.ch012.

— « Transparence, élections et vote électronique », *in* : *Machines à voter et Démocratie*, sous la dir. d'Elsa Forey et Christophe Geslot, questions contemporaines, L'Harmattan, 2011, p. 89–106, url : https://hal.archives-ouvertes.fr/hal-00435966.

Noizat, Pierre, « Blockchain Electronic Vote », *in* : *Handbook of Digital Currency : Bitcoin, Innovation, Financial Instruments, and Big Data*, 2015, isbn : 9780128023518, doi : 10.1016/B978-0-12-802117-0.00022-9.

Suaudeau, Hervé, *Contribution de Hervé Suaudeau pour le rapport de la Commission des lois du Sénat sur le vote électronique le 25 Janvier 2018*, Other, Sénat, 2018, url : https://hal.archives-ouvertes.fr/hal-01960749.

Wojcik, Stéphanie, « La démocratie électronique, mythe et réalité », *in* : *Les défis actuels de la démocratie*, 2010.

Colloques et Conférences

Enguehard, Chantal, « Vote électronique et preuve papier », *in* : *14 ème Colloque international "De l'insécurité numérique à la vulnérabilité de la société"*, Paris, France, 2007, publication électronique, URL : https://halshs.archives-ouvertes.fr/halshs-00409469.

Enguehard, Chantal, Walter De Abreu Cybis et Gabriel Michel, « Vote électronique : informatiser au service des électeurs », *in* : *Colibri*, Bento Gonçalves, Brazil, 2009, publication électronique, URL : https://hal.archives-ouvertes.fr/hal-00410660.

Enguehard, Chantal et Tatiana Shulga-Morskaya, « De l'annulation d'élections par Internet par le moyen des insuffisances du système de vote », *in* : *Les convergences du droit et du numérique*, Bordeaux, France, 2017, URL : https://hal.inria.fr/hal-01730380.

Vollan, Kåre, « Voting in uncontrolled environment and the secrecy of the vote », *in* : *Electronic Voting 2006 - 2nd International Workshop*, 2006.

Xenakis, Alexandros et Ann Macintosh, « Procedural security analysis of electronic voting », *in* : *ACM International Conference Proceeding Series*, t. 60, 2004, p. 541–546, ISBN : 1581139306, DOI : 10.1145/1052220.1052288.

Textes de Loi

American Congress, *Help America Vote Act of 2002*, Washington, 2002, URL : https://www.congress.gov/bill/107th-congress/house-bill/3295.

Assemblée nationale, *Loi n°2016-1088 relative au travail, à la modernisation du dialogue social et à lasécurisation des parcours professionnels*, Paris, 8 août 2016.

— *Loi n°2016-1321 pour une république numérique*, Paris, 7 oct. 2016.

— *Loi n°69-419 modifiant certaines dispositions du code électoral*, Paris, 10 mai 1969.

— *Loi n°88-1262 modifiant certaines dispositions du code électoral*, Paris, 30 déc. 1988.

— *Loi n°88-19 relative à la fraude informatique*, Paris, 5 jan. 1988.

Les Journaux Officiels, *Journal Officiel de la République Française*, Paris, 28 déc. 1972, p. 13590.

— *Journal Officiel de la République Française*, Paris, 27 nov. 2003, p. 20188.

Parlement Européen, *Règlement (UE) 2016/679 du Parlement européen et du Conseil*, 27 avr. 2016.

République Française, *Constitution de la Vème République*, Paris, 4 oct. 1958.

Codes

Code du travail 2019, Dalloz-Sirey, déc. 2018, ISBN : 978-2247186433.

Code électoral 2019, Dalloz-Sirey, déc. 2018, ISBN : 978-2247177578.

Code général des collectivités territoriales 2019, Dalloz-Sirey, déc. 2018, ISBN : 978-2247177530.

Jurisprudences

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération n°2003-036*, Paris, 1er juil. 2003.

— *Délibération n°2010-371*, Paris, 21 oct. 2010.

— *Délibération n°2019-053*, Paris, 25 avr. 2019.

CONSEIL CONSTITUTIONNEL, *Décision n°2007-3742/3947*, 20 déc. 2007.

— *Décision n°2007-3872*, 4 oct. 2007.

— *Décision n°2007-3947*, 20 déc. 2007.

— *Décision n°2012-4554 AN*, 15 fév. 2013.

— *Décision n°2012-4597/4626*, 15 fév. 2013.

— *Décision n°2019-1 RIP*, 9 mai 2019.

CONSEIL D'ETAT, *29373 "Therond"*, Paris, 4 mar. 2010.

COUR DE CASSATION CHAMBRE SOCIALE, *n°09-60.203*, Paris, 13 jan. 2010.

— *n°15-19.544*, Paris, 10 mar. 2010.

Webographie

BLAZE MATT, Braun Jake, *Report on Cyber Vulnerabilities inU.S. Election Equipment, Databases, and Infrastructure*, 2018, URL : `https://www.defcon.org/images/defcon-26/DEF%20CON%2026%20voting%20village%20report.pdf` (visité le 25/08/2019).

CHRISTINE, Prunaud, *Interdiction des machines à voter - Question écrite*, 2017, URL : `http://www.senat.fr/basile/visio.do?id=qSEQ171101801` (visité le 25/08/2019).

CHRISTOPHE, Guillemin, *1,5 million d'électeurs français inaugureront le vote électronique le 22 avril*, 2007, URL : `https://www.zdnet.fr/i/edit/ne/2007/04/communes.html` (visité le 25/08/2019).

Collectif PourEVA, *18/05/2003 : Rapport concernant les élections du 18 mai 2003*, 2003, URL : https://www.poureva.be/spip.php?article32 (visité le 25/08/2019).

— *Position des présidents de parti sur le vote électronique*, 2007, URL : https://www.youtube.com/watch?v=E0Xii6MW1Sc (visité le 25/08/2019).

Damien, Leloup, *Législatives : les Français de l'étranger privés de vote électronique pour des raisons de sécurité*, 2017, URL : https://www.lemonde.fr/pixels/article/2017/03/06/legislatives-le-gouvernement-ne-recourra-pas-au-vote-electronique-pour-les-francais-de-l-etranger-pour-des-raisons-de-securite_5090026_4408996.html (visité le 25/08/2019).

François, Nonnenmacher, *Les Pays-Bas abandonnent définitivement le vote électronique*, 2008, URL : https://www.padawan.info/fr/vote_electronique/les_paysbas_abandonnent_definitivement_le_vote_electronique.html (visité le 25/08/2019).

Group, Miniwatts Marketing, *Data for the 28 Member States of the European Union*, 2019, URL : https://www.internetworldstats.com/europa.htm#fr (visité le 25/08/2019).

Hagai, Bar-el, *Why secure e-voting is so hard to get*, 2015, URL : https://www.hbarel.com/analysis/cyber/secure-e-voting-is-hard-to-get (visité le 25/08/2019).

hindustantimes, *Lok Sabha election 2019 schedule Highlights | Tried to cover left-wing extremism affected areas at one go, says EC*, 2019, URL : https://www.hindustantimes.com/lok-sabha-elections/lok-sabha-election-2019-schedule-live-updates-countdown-for-lok-sabha-polls-begins-with-ec-s-announcement-today/story-6RWOYDUJp1IaJdW248pgyL.html (visité le 25/08/2019).

Information, Sciences Institute, *Internet Protocol - DARPA Internet Program*, 1981, URL : https://tools.ietf.org/html/rfc791 (visité le 25/08/2019).

INRIA, *Apporter des réponses pour des échanges plus sûrs*, 2011, URL : https://www.inria.fr/centre/saclay/actualites/apporter-des-reponses-pour-des-echanges-plus-surs (visité le 25/08/2019).

Isabelle, Florennes, *Possible suppresion des machines à voter - Question écrite*, 2018, URL : http://questions.assemblee-nationale.fr/q15/15-11516QE.htm (visité le 25/08/2019).

Julien, Lausson, *Les Néerlandais tournent le dos à la gestion électronique des élections législatives*, 2017, URL : https://www.numerama.com/politique/229515-

les-neerlandais-tournent-le-dos-a-la-gestion-electronique-des-elections-legislatives.html (visité le 25/08/2019).

Kevin, Collier, *At hacking conference, Pentagon's transparency highlights voting companies' secrecy*, 2019, URL : https://edition.cnn.com/2019/08/12/politics/defcon-voting-village-darpa-dominion/index.html (visité le 25/08/2019).

Kim, Zeter, *The Myth of the Hacker-Proof Voting Machine*, 2018, URL : https://www.nytimes.com/2018/02/21/magazine/the-myth-of-the-hacker-proof-voting-machine.html (visité le 25/08/2019).

Lily, Hay Newman, *Hackers Take on Darpa's 10 Million dollars Voting Machine*, 2019, URL : https://www.wired.com/story/darpa-voting-machine-defcon-voting-village-hackers/?verso=true (visité le 25/08/2019).

Linuxcare, *Richard Stallman's Interview*, 1999, URL : https://lists.gnu.org/archive/html/help-gnu-emacs/2010-12/msg00744.html (visité le 25/08/2019).

Luc, Vinogradoff, *Le spectre de la désinformation russe derrière les « fake news » sur Internet*, 2016, URL : https://www.lemonde.fr/big-browser/article/2016/11/30/le-spectre-de-la-desinformation-russe-derriere-les-fake-news-sur-internet_5040983_4832693.html (visité le 25/08/2019).

Marc, Belga, *Vers un recomptage partiel des votes à St-Josse suite à un bug*, 2018, URL : https://www.lanouvellegazette.be/297372/article/2018-10-22/vers-un-recomptage-partiel-des-votes-st-josse-suite-un-bug (visité le 25/08/2019).

Marc, Rees, *L'ANSSI s'explique sur l'annulation du vote électronique des Français de l'étranger*, 2017, URL : https://www.nextinpact.com/news/103560-lanssi-sexplique-sur-annulation-vote-electronique-francais-l-etranger.htm (visité le 25/08/2019).

Ministère de l'intérieur, *Liste des bureaux de vote par circonscription - Lille*, 2019, URL : https://www.lille.fr/content/download/25855/380120/file/Liste+des+bureaux+de+vote+par+circonscription++Lille+-+Hellemmes+et+Lomme.pdf (visité le 25/08/2019).

MoneyControl, *Lok Sabha polls 2019 : Number of polling booths, voters and other key facts*, 2019, URL : https://www.moneycontrol.com/news/india/lok-sabha-polls-2019-number-of-polling-booths-voters-and-other-key-facts-3631851.html (visité le 25/08/2019).

ODV, Collectif, *Pourquoi ce site ?*, 2004, URL : https://www.ordinateurs-de-vote.org/Pourquoi-ce-site.html (visité le 25/08/2019).

PHILIPPE, Kaltenbach, *Proposition de loi visant à supprimer le recours aux machines à voter pour les élections générales*, 2014, URL : http://www.senat.fr/leg/ppl13-763.html (visité le 25/08/2019).

RAHUL, Rathi, *Effect of Cambridge Analytica's Facebook ads on the 2016 US Presidential Election*, 2019, URL : https://towardsdatascience.com/effect-of-cambridge-analyticas-facebook-ads-on-the-2016-us-presidential-election-dacb5462155d (visité le 25/08/2019).

RICHARD, Esposito, *Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election*, 2017, URL : https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/ (visité le 25/08/2019).

RUPALI, Pruthi, *What is VVPAT ? How does VVPAT work ?*, 2019, URL : https://www.jagranjosh.com/current-affairs/what-is-vvpat-machine-with-evm-how-does-vvpat-work-1555312059-1 (visité le 25/08/2019).

SCHNEIER, *The Problem with Electronic Voting Machines*, 2004, URL : https://www.schneier.com/blog/archives/2004/11/the_problem_wit.html (visité le 25/08/2019).

SOLÈNE, Vanuxem, *Infographie : Wannacry, l'heure du bilan !*, 2017, URL : https://www.wisper.io/fr/infographie-wannacry/ (visité le 25/08/2019).

SONIA, Delesalle, *"Sans Cambridge Analytica, il n'y aurait pas eu de Brexit"*, 2018, URL : https://www.liberation.fr/planete/2018/03/26/sans-cambridge-analytica-il-n-y-aurait-pas-eu-de-brexit_1638940 (visité le 25/08/2019).

VILLAINES ASTRID, de, *3 questions à... Philippe Kaltenbach, l'homme qui ne veut plus de machines à voter*, 2015, URL : http://www.lcp.fr/actualites/3-questions-philippe-kaltenbach-lhomme-qui-ne-veut-plus-de-machines-voter (visité le 25/08/2019).

Annexes

Annexe 1 - Entretien avec Chantal Enguehard

Le texte suivant est la retranscription d'un entretien téléphonique du 17 Juillet 2019 entre l'auteur et Chantal Enguehard, docteure en informatique et Maitre de Conférences à l'Université de Nantes, spécialiste du vote électronique. Le texte a été revu et corrigé sans impacter le propos exprimé.

MM : Qu'avez-vous pensé de ce rapport n°73 du Sénat et quel est selon vous son apport scientifique ?

CE : Ce n'est pas un rapport scientifique. Dans un rapport scientifique, il y a une bibliographie, il y a des démonstrations. Le sénat n'est pas une institution scientifique. Il ne fait aucune production scientifique, ce rapport en est une preuve.

MM : Lorsque le rapport a été rendu public, vous avez en réponse publié votre analyse de ce rapport. L'un des premiers points que vous critiquez est l'absence de la question de la confiance des électeurs dans le vote électronique. En quoi pensez-vous que c'est important ?

CE : L'idée de confiance dans les résultats d'un vote vient des sciences politiques. Les sciences politiques nous disent que ce n'est pas très grave si un système de vote n'est pas juste à une voix près ou quelques voix près. Ce qui est essentiel, c'est que les gens qui ont voté soient convaincus que la personne qui est désignée gagnante de l'élection est celle qui devait l'être, celle qui a eu le plus de suffrages. Si ce n'est pas le cas, il peut y avoir des émeutes dans les rues, des désordres publics. L'élection est une manière de prendre une décision extrêmement difficile à beaucoup de personnes en un temps réduit tout en maintenant la paix publique. Imaginez, si on devait choisir le prochain président de la république juste en discutant, au consensus, ça prendrait longtemps ! Dans une élection, si les gens pensent que le résultat est honnête, ou « sincère » au sens

juridique, il n'y a pas d'émeutes. Il peut y avoir des contestations, mais elles seront anecdotiques. La confiance dans les résultats d'une élection est un élément essentiel qui maintient la paix publique.

MM : Pensez-vous qu'un logiciel open source servirait la confiance en le vote électronique quant à l'utilisation des machines à voter ?

CE : Cela ne résout pas le problème, on ne peut pas être certain que le logiciel qui est utilisé est effectivement celui qui a été rendu public. Quant au code source, même s'il est public, il est transformé par un compilateur pour être ensuite exécuté. Le "pape" du Logiciel Libre Richard Stallman s'est d'ailleurs exprimé très clairement à ce sujet : un code source public ne peut pas résoudre les problèmes de confiance quant au vote électronique. Même si le code source est ouvert, les intentions de vote des électeurs sont transformées d'une manière qui échappe à nos sens, sans compter les bugs et les erreurs d'exécution afférant à n'importe quel logiciel.

MM : A propos des erreurs d'exécution. Je souhaiterais aborder l'incident de Schaerbeek de 2003 : une inversion binaire, dû au rayonnement cosmique. Vous en parlez dans certains de vos travaux. Aujourd'hui la technologie a évolué et il existe maintenant la mémoire RAM ECC, destinées à éviter ce genre d'incident. Pensez-vous que ce genre de technologie pourrait servir la crédibilité des machines à voter ?

CE : La question de la transparence se pose toujours. L'incident de Schaerbeek a été vu un peu par hasard, mais nous avons aujourd'hui des machines à voter qui sont utilisées en France, rien ne nous dit qu'elles nous donnent les bons résultats : on ne peut pas vérifier si les résultats sont justes. D'ailleurs, dans le règlement technique des machines à voter de 2003, il y a une liste de 15 « principes à respecter ». Parmi ces principes, figure le caractère « vérifiable » de l'élection, ce qui n'est pas mis en œuvre aujourd'hui. J'avais à l'époque envoyé une lettre recommandée interrogeant le premier ministre à ce sujet, je n'ai jamais eu de réponse. Sans parler du principe de « transparence » qui figure aussi dans cette liste avec la précision « le processus doit pouvoir être examiné et vérifié » : en informatique, cela ne veut rien dire car le respect du secret du vote interdit de suivre les étapes de transformation des expressions des votes.

Avant mon audition au sénat, j'avais fourni des démonstrations écrites au sujet de la nécessaire transparence des élections et de l'impossibilité de vérifier les résultats électoraux issus des machines à voter. J'ai pu expliquer ces démonstrations lors de mon audition. Aucune de ces démonstrations n'a été reprise dans le rapport n°73 du sénat.

MM : Peut-on dire que ceux qui ont écrit ce règlement technique avaient des notions d'informatique relativement limitées ? Oui, parce qu'il y a beaucoup d'exigences qui portent sur des principes physiques : lâcher la machine à un mètre de haut, la soumettre à certaines températures... Il n'y a rien sur la qualité logicielle de la machine. Il n'y a même pas une disposition à des tests élémentaires : on pourrait imaginer que dans les mairies il y ait un moyen de vérifier qu'il s'agit de la bonne machine. Par exemple, dans les entreprises, les machines à timbrer sont toutes certifiées unes à unes, alors que les machines à voter n'ont aucune certification individuelle.

CE : Une certification ou une labélisation propulsée par le ministère public pourrait-elle pallier ce problème ? Cela ne résout de toute façon pas le problème de fond. Le ministère public pourrait décréter que l'on puisse se déplacer instantanément dans l'espace, mais les lois de la physique nous en empêcheront quand même. On peut écrire et décréter tout ce que l'on souhaite, mais il y a des choses qui restent à ce jour impossibles, comme rendre vérifiable le résultat d'une élection par vote électronique sans trace papier, ou rendre une élection électronique aussi transparente que les élections politiques telles que nous les pratiquons en France.

MM : Que pensez-vous, justement, de l'approche du juge quant à cette impossibilité de prouver qu'il y a eu fraude dans un scrutin électronique ?

CE : Le juge se repose sur les textes. Si un texte dispose qu'un papier certifiant la conformité de la machine est juste nécessaire pour attester de la validité de la machine, alors tout va bien. Il n'y a aucune loi qui dispose que l'élection se doit d'être transparente, car la transparence n'est pas définie juridiquement.

MM : Pensez-vous que le juge a une approche traditionnaliste sur les machines à voter ?

CE : En fait, ce n'est pas dans ses compétences. Le problème, c'est que ce n'est ni dans les compétences du juge, ni dans les compétences des avocats et ni dans les compétences des législateurs. Les machines à voter sont autorisées par une loi de 1969, d'ailleurs à l'époque, les machines ne sont pas électroniques, elles sont mécaniques, c'est pour cette raison que l'on emploie le terme « machine », ce qui n'est, déjà, pas sans défaut. Les machines de première génération sont tombées peu à peu en désuétude parce qu'il y avait dedans un système de tringlerie, un peu comme dans les vieux compteurs de voiture, et qu'il y a eu des pannes. Ce qu'il faut comprendre, la grosse différence, c'est qu'avec le vote papier, le bulletin dépouillé au soir est le même qui a été déposé par l'électeur, c'est-à-dire que ce sont les mêmes molécules de papier, les mêmes molécules d'encre, il n'y a aucune modification, évidemment dans la mesure où l'urne a bien été surveillée. Dans le vote électronique, c'est cet aspect qui est problématique : la volonté de l'électeur est transformée à plusieurs reprises et est dématérialisée.

MM : L'anonymat sur internet est une question aujourd'hui pleine d'enjeux. En tant que docteure en informatique, existe-t-il selon vous un moyen de dissocier le vote de celui qui l'a émis ?

CE : C'est une question complexe. Des cryptologues travaillent sur ce thème, il y a des conférences, etc. Mais, vous savez, ce qui est important, c'est le point de vue l'électeur. Pour que l'électeur vote en toute liberté, il faut qu'il puisse voter pour Marine Le Pen alors qu'il est dans une famille qui vote Jean-Luc Mélenchon, ou l'inverse, c'est ça la liberté de vote. Avec le vote par internet, on est dans un vote par correspondance et donc, rien ne garantit que l'électeur soit seul devant son ordinateur ou son portable, mais dissocions les problèmes. L'électeur doit confier à un même système, dont il ne contrôle rien et dont il ne sait rien, son identité et son vote. L'électeur, en toute bonne foi, peut douter que son vote va rester secret. Cela peut l'amener à ne pas voter en toute liberté et donc, à changer son vote, comme voter blanc par exemple. Le problème, c'est qu'on demande à quelqu'un de faire confiance à un système dont il connait rien, qui a été certifié par des experts dont il ne connait pas le nom et dont il ne verra jamais les rapports. Et ça, c'est quelque chose qui est profondément infantilisant. On enseigne aux enfants à ne pas faire

confiance aux inconnus, mais en tant qu'adulte et citoyen on exige des électeurs qu'ils fassent confiance à des gens qu'ils ne connaissent pas.

MM : On peut demander à l'ordinateur d'oublier, certains systèmes sont conçus pour ne conserver des informations que le temps du traitement.

CE : On peut lui demander d'oublier, on peut nous dire que l'ordinateur est conçu ainsi, mais on est de nouveau dans le registre de la foi et pas dans le registre de la raison. Quand je vote par correspondance papier, et pourtant ce type de vote est globalement peu satisfaisant et critiquable, le système est conçu pour que les dispositions pour garantir le secret du vote soient visibles : la première enveloppe, qui porte la signature et l'identité de l'électeur et permet d'effectuer l'émargementest ouverte pour révéler une seconde enveloppe sans aucune marque concernant l'identité de l'électeur. Une fois cette opération effectuée pour tous les votes, les secondes enveloppes sont mélangées avant d'être ouvertes. Ce processus, je n'ai pas à le croire, car, pour y avoir assisté plusieurs fois, je l'ai vu. Et, à chaque dépouillement, il y a des représentants des candidats qui voient le déroulement ce processus. Toute la différence est là.

MM : Pensez-vous justement que regarder le dépouillement et devoir l'enveloppe tomber dans l'urne transparente relève d'une valeur qui conditionne la validité du vote ou s'agit-il avant tout d'une valeur symbolique ?

CE : Il y a effectivement toute une signification symbolique dans laquelle je ne souhaite pas rentrer. Ce que je vois c'est avant tout l'aspect pratique de ces objets. Ce sont des objets qui ont des propriétés physiques tout à fait utiles pour le vote. Il y a une quantité phénoménale de publications sur l'aspect cérémonial du vote, mais pour moi ce n'est pas le sujet. Le vote n'est pas une messe. Le fait de surveiller l'urne toute la journée, ce n'est pas parce que c'est une relique, c'est parce que cette surveillance est nécessaire pour que la sincérité du vote soit manifeste. Or la surveillance constante des bulletins n'est pas possible avec le vote par correspondance. Il faut noter que le vote par internet est une nouvelle forme de vote par correspondance, or le vote par correspondance papier qui existait jusqu'en 1975, avait été abandonné en raison de fraudes mas-

sives.

MM : En 2017 le Quai d'Orsay a décidé d'annuler le vote par internet pour les français de l'étranger pour les élections législatives et consulaires sur fond de menace cyber. Qu'en pensez-vous ?

CE : C'est une sage décision. Intervention russe ou pas, ne pas faire de vote par internet est une sage décision.

MM : D'ailleurs, vous défendez une position particulière sur le vote par internet ou les machines à voter ?

CE : Moi je n'ai rien contre le vote électronique, si un jour on arrive à faire un vote électronique transparent. Je suis informaticienne, je n'ai rien contre l'informatique, mais la façon avec laquelle le vote électronique est aujourd'hui organisé, ça ne va pas. Je ne vois pas comment on peut faire aujourd'hui un vote électronique transparent. je constate que pour l'instant, le vote est extrêmement résistant à l'informatisation. En informatisant le vote je pense qu'on y perd, vraiment. On perd en transparence, et la transparence est essentielle pour les élections.

MM : En dehors de toute considération scientifique, que pensez-vous de l'attitude du Sénat ou même de celle de l'État par rapport au vote électronique ? Pensez-vous que c'est dangereux ?

CE : Le vote électronique peut être dangereux oui. Le danger premier, c'est la négation du résultat par ceux qui n'y croient pas, et vous n'avez pas la possibilité de leur démontrer le contraire. Les effets peuvent être très néfastes. Dans le code électoral, inciter les gens à ne pas voter c'est pénalement répréhensible. On peut, de ce fait, imaginer que douter des résultats d'une machine à voter et tenter de le démontrer pourrait relever aussi du pénal. Que puis-je dire à part faire mon travail de scientifique ? Tout est écrit dans mes travaux. On voit bien quand même que dans ce rapport du sénat, et j'espère l'avoir démontré, que les sénateurs ce sont fait le relais d'un fabricant de machines à voter.

MM : A ce sujet, peut-on parler d'un marché concernant les machines à voter ?

Est-ce mauvais ?

CE : Tout à fait. Mais le coût n'a jamais été estimé en France. En Belgique une étude a été menée, mais jamais en France en ce qui concerne le vote papier et son impact d'une part et le vote par machines à voter d'autre part. Mais tout marché n'est pas forcément mauvais, il peut y avoir des marchés qui se développent pour de bonnes raisons !

MM : Avez-vous constaté au cours de vos études un impact de la participation par l'utilisation des dispositifs de vote électronique ?

CE : Concernant les machines à voter, j'ai constaté que l'impact n'était ni négatif ni positif. J'aurais bien aimé le faire concernant le vote par internet, notamment pour les élections professionnelles, mais je manque de données et il n'y a pas eu d'étude sur ce sujet, ce qui est bien dommage d'ailleurs. Chez les estoniens, on constate une augmentation de la participation, mais il est clair que l'Estonie sert de laboratoire sur ce sujet spécifique. Les estoniens ont connu le stalinisme, ils étaient dans l'URSS, donc on peut penser que pour eux, voter, même par internet, c'est déjà formidable par rapport au passé.

MM : Avez-vous eu à ce jour un retour du sénat suite à votre demande de retrait de votre nom de ce rapport ?

CE : Non. J'ai écrit à Gérard Larcher, j'ai eu une réponse m'indiquant qu'il avait transmis ma réponse à Mr. Bas. Ce dernier a commencé par me répondre que « [le] rapport fait état des informations que [les rapporteurs] ont recueillies] ». C'est à la suite de cette réponse que j'ai rédigé une analyse pour justement démontrer que le rapport en question ne comporte aucune de mes réflexions, j'ai renvoyé ma demande à Gérard Larcher qui a transmis a M. Bas et depuis silence radio. Mais je n'aurai pas de réponse. Je ne me fais aucune illusion.

MM : C'est la première fois que vous êtes auditionnée par les institutions pour votre expertise ?

CE : Je suis intervenue précédemment pour le rapport de 2014 du sé-

nat des sénateurs Lefèvre et Anziani et également pour le ministère de l'intérieur en 2007, donc non ce n'est pas la première fois, mais à chaque fois les rapports ne sont pas complètement satisfaisants. Le problème est que le sénat ne fonctionne pas avec des principes scientifiques. C'est-à-dire, il auditionne des gens, parmi lesquelles des experts, reprend ce que disent ces personnes, alors qu'ils peuvent parfois dire des choses fausses ou des contrevérités scientifiques. Par exemple, quand un fabricant de machines à voter montre que son dernier modèle fonctionne avec des « touches de vote digitalisées » cela suffit à qualifier le machine de « nouvelle génération » et à lui attribuer une « amélioration » sur le plan ergonomique qui n'est nullement démontrée. Donc, il n'y a pas de validité scientifique sur les rapports du sénat et il faudrait que le sénat se réforme profondément. En tant que scientifique, chaque chose que l'on énonce doit être démontrée, par citation ou expérience, etc. Le sénat ? Rien. L'ANSSI, a contrario, fait de superbes publications en la matière, c'est d'ailleurs eux qui ont appuyé la décision qu'il ne fallait pas faire de vote par internet pour les français de l'étranger. On voit aussi que notre président de la république est déconnecté de la chose scientifique, en disant qu'on allait remettre en place le vote par internet et l'étendre car sinon la France ne serait plus la France, ou quelque chose approchant . Mais il y a des gens qui travaillent sur la santé ou l'écologie qui ne sont pas écoutés non plus, et c'est beaucoup plus grave et cela peut engendrer des morts. Les constats sont identiques. La pensée scientifique ne semble pas irriguer la politique. Il peut y avoir des exceptions, mais globalement, ce n'est pas le cas. Le rapport n°73 du sénat a été voté à l'unanimité par la commission des lois sans que personne ne se dise qu'il ne fallait pas le faire.

MM : On pourrait penser que déployer le vote électronique à grande échelle pourrait se retourner contre ceux qui l'ont promu ?

CE : Les alternances politiques ne changent pas vraiment l'idée que l'on a sur le vote électronique. En France, plus d'un million de français utilisent des machines à voter, ce n'est pas rien. Et, vous qui êtes juriste, faites vous à l'idée que les machines à voter, c'est la fin du contentieux électoral concernant la sincérité du vote. C'est énorme. Les fraudes électroniques ne pouvant être démontrées, le contentieux n'existe plus. C'est conster-

nant.

MM : Pourquoi pensez-vous que le pentesting (fait pour un expert de sécurité en informatique d'exploiter les vulnérabilités d'un système informatique afin de les exploiter et de les révéler) n'est pas scientifique ?

CE : Alors, à ce sujet, ce qu'il s'est passé en Suisse dernièrement est très intéressant. Des personnes trouvent une faille, les auteurs du logiciel la bouchent et ils disent : maintenant c'est bon. La course à la sécurité, c'est une course sans fin. Ce qui compte, ce n'est pas la sécurité, c'est la transparence. Ce qui est intéressant, c'est que ce sont les industriels qui ont amené le thème de la sécurité, car sur la transparence, ils ont tout de suite perdu. Le vote papier n'a pas à être sécurisé car en cas d'un incident, il y a des preuves et des traces, il y a des éléments à présenter devant un juge.

MM : Pensez-vous que le juge devrait être doté d'une expertise technique ?

CE : S'il avait une petite formation, ça ne serait pas mal. Mais, comment vous dire, si on savait faire des programmes sans bug, on le ferait, croyez-moi. Aujourd'hui tout le monde a un ordinateur ou un téléphone portable qui sont eux aussi des ordinateurs, et on constate dans la vie de tous les jours que parfois il y a des bugs, et parfois ça se remet à bien marcher sans raison apparente. L'informatique est une science extrêmement jeune. On ne sait pas faire des programmes sans bugs.

Annexe 2 - Entretien avec Michaël Tchilingurian

Le texte suivant est la retranscription d'un entretien par mail du 8 Aout 2019 entre l'auteur et Michaël Tchilingurian, auteur du recours devant le Conseil Constitutionnel pour la décision n°2007-3947 Le texte n'a subit que peu de retouches.

MM : Pouvez-vous vous présenter succinctement au travers de votre parcours ?

MT : Je suis fonctionnaire de l'Etat au ministère des outre-mer où j'occupe une fonction de juriste. Je suis rentré dans la fonction publique via le concours des IRA (instituts régionaux d'administration), après avoir décroché un DEA de droit public.

MM : Qu'entendez-vous par « illégalité du dispositif » à la lumière de la décision rendue par le Conseil Constitutionnel ?

MT : J'ai introduit un contentieux (demande d'annulation de l'élection de mon député devant le Conseil constitutionnel), car je contestais l'usage des machines à voter dans ma commune. J'estime (et je pense ne pas être le seul à le penser) que l'usage des machines à voter lors de scrutins pose un problème "démocratique". Dans le vote traditionnel (papier), le système respecte le principe du secret et du choix de vote de chaque électeur. L'usage de l'enveloppe anonyme dans lequel est glissé le bulletin à l'abri du regard (passage dans l'isoloir) permet de respecter ces deux principes. De plus, cette opération est transparente et contrôlable par tous les citoyens : on utilise une urne transparente (afin d'éviter le bourrage d'urne) et le dépouillement des bulletins est assuré par les citoyens eux-mêmes en public, après la clôture du vote. Or, avec les machines à voter, ces principes ne sont pas respectés : ces machines fonctionnent avec un logiciel informatique qui doit permettre l'attribution du vote de l'électeur tout en assurant le secret de son vote, de manière dématérialisée. Or, ceci est contradictoire : comme le secret du vote doit être assuré, on ne doit pas pouvoir "pister" le vote de l'électeur au moment où il enregistre son vote. Donc il n'y a aucune assurance à ce que le choix de l'électeur soit respecté au moment il enregistre son vote. A cela s'ajoute le fait que le logiciel de ces machines est protégé par le secret industriel et commercial, car il s'agit de logiciels propriétaires. Il n'y a donc aucun moyen de s'assurer que ces logiciels sont bien paramétrés pour respecter ces principes. Plus

globalement, le recours aux machines à voter fonctionnant avec un logiciel informatique, soumet l'opération électorale, au contrôle d'informaticiens (donc des experts, des techniciens), seuls à pouvoir vérifier et disséquer l'opération, et non au contrôle des citoyens. Dans le vote à l'urne classique, n'importe quel citoyen peut contrôler l'opération de vote. En cas de vote électronique, seul un technicien informatique pourra le faire, sauf à ce que chaque électeur soit informaticien, ce qui est loin d'être le cas aujourd'hui. La dématérialisation du vote par l'usage de machines à voter est par nature anti-démocratique, car il soumet le fonctionnement de notre démocratie au contrôle d'experts informaticiens. J'ai tenté de "sensibiliser" le Conseil constitutionnel sur ces questions (considérant 14 de la décision) : j'ai soulevé le fait que c'était contraire à certains principes constitutionnels ou conventionnels (liberté de vote, sincérité des opérations électorales - principes sur lesquels s'appuyaient à l'époque la JP constitutionnelle), mais je n'ai pas été suivi par cette juridiction.

MM : Estimez-vous que les machines à voter peuvent constituer un apport positif dans la vie démocratique en France ?

MT : Absolument pas ! Pour les raisons indiquées ci-dessus. En fait, l'usage de machines à voter pourrait, à la rigueur, être utilisé en France, si on organisait plusieurs scrutins en une seule journée, comme c'est le cas aux États-Unis. Mais ce n'est pas le cas en France : on se limite toujours à un ou deux scrutins le même jour ! Donc le recours aux machines à voter est inutile. En plus, le vote papier comme il est organisé en France fonctionne très bien et permet largement de respecter les principes démocratiques rappelés plus haut.

MM : Avez-vous un avis sur la pertinence de l'arrêté ministériel du 17 novembre 2003 réglementant les machines à voter et leur agrément ? Que manquerait-il selon vous dans ce règlement pour servir la sécurité et la transparence d'une élection par vote électronique ?

MT : Concernant cet arrêté, j'avais contesté le fait qu'il n'imposait pas le recours à un logiciel dont le code source serait public. Les logiciels utilisés par les machines agréées en France fonctionnent sous un régime propriétaire. Donc, hormis le recours à un test grandeur nature de ces

machines, il n'est pas possible de vérifier que ces logiciels respectent le choix de l'électeur. Ce qui constitue un problème démocratique à mon sens majeur, comme expliqué plus haut. Si on veut vraiment recourir à des machines à voter en France, il faudrait dans ce cas doubler le vote électronique par une trace/vote papier afin de pouvoir vérifier, une fois l'opération électorale close, l'absence d'écart entre les votes enregistrés par la machine à voter et le vote/trace papier émis et contrôlé par l'électeur lui-même. Mais exiger une trace papier pour des raisons de transparence revient à remettre en cause le principe même du recours à des machines à voter fondée sur la dématérialisation du vote. Donc, le respect des principes de transparence et de contrôle démocratique des opérations électorales exclurait, dans tous les cas, et à mon sens, le recours aux machines à voter. En conclusion, je suis pour l'abrogation de cet arrêté et non pour sa modification.

MM : Avez-vous lu ou pris connaissance du rapport n°73 du sénat sur le vote électronique et avez-vous des commentaires à faire sur sa pertinence technique et scientifique ?

MT : Je ne connaissais pas le rapport, je le découvre donc en répondant à votre questionnaire. Je savais qu'il y avait un moratoire sur l'extension des machines à voter depuis 2007, mais je suis heureux d'apprendre que ce moratoire va conduire prochainement à l'obsolescence des machines actuellement autorisés... Ce qui devrait bientôt conduire à leur abandon si rien ne se passe... Plus sérieusement, le rapport insiste beaucoup sur la question de la sécurité de ces machines (afin d'éviter des bugs ou des piratages conduisant à fausser le résultat), mais n'interroge pas la question de la transparence de l'opération électorale et de son contrôle citoyen (que j'ai développé au dessus). La question est à peine évoqué dans un entrefilet lorsqu'il est fait référence au "rituel républicain", concernant le vote papier, pour l'évacuer immédiatement. Cf. I, A, 2, a) : "De même, les machines à voter remettraient en cause le « rituel républicain », comme l'ont souligné deux spécialistes du vote auditionnés par vos rapporteurs, MM. Gilles Guglielmi et Gilles Toulemonde. Le président du bureau de vote prononce, certes, le traditionnel « a voté » mais l'électeur ne passe pas par l'isoloir et ne peut plus contribuer au dépouillement en tant que scrutateur." Je trouve ce silence (volontaire ?) étonnant de la part d'élus

qui, normalement devraient être sensibles au respect des principes démocratiques, même si, en tant que sénateurs, ce sont des élus non élus directement par les citoyens (puisque élus par les élus locaux). A mon sens, la question de la sécurité est consécutive au choix de la méthode de recensement des votes papier/électronique : Dans les deux cas, il existe toujours un problème de sécurité ouvrant la possibilité de fraude. Le rapport fait d'ailleurs référence à l'affaire de la "fraude à la chaussette" qui s'est déroulé à Perpignan aux élections municipales de 2008 (I, B, 2). De même qu'il rapporte l'incident de Schaerbeek (Belgique, 2003) concernant les machines à voter. Mais il est plus facile à mon sens de détecter une fraude/anomalie avec le vote papier que dans le cadre d'un vote électronique : dans le premier cas, tout citoyen scrutateur peut le voir, car c'est à portée de tout citoyen lambda ; dans le second cas, il faut forcément faire appel à des informaticiens, d'où la perte de contrôle démocratique au profit d'un contrôle par des experts.

Table des matières