Vote en ligne

Source
interstices.info
« Vote par Internet »
Véronique Cortier & Steve Kremer
2017

Aujourd'hui, le vote à distance, par Internet, permet de voter de n'importe où, dès lors que l'on dispose d'une connexion à Internet. Tout comme les machines à voter électroniques, ce système de vote soulève des questions en termes de sécurité et de fiabilité.

Les machines à voter sont désormais utilisées dans de nombreux pays, en phase de tests ou à grande échelle. Aux États-Unis, cette façon de voter est devenue la plus courante, que ce soit avec des bulletins papier qui sont scannés ou par une interaction directe sur un écran tactile. Le manque de transparence de ces machines a créé une polémique. Plusieurs pays, comme les Pays-Bas, l'Irlande ou l'Allemagne, ont décidé d'interdire leur utilisation pour revenir à un scrutin *purement papier*. À l'inverse, certains pays vont plus loin et mettent en place le *vote à distance*, par Internet. Contrairement aux machines installées dans les bureaux de vote, le vote à distance permet de voter de n'importe où, du moment que l'on dispose d'une connexion à Internet.

En matière de vote par Internet, l'Estonie est l'un des pays pionniers. Dès 2005, la possibilité y a été offerte de voter par Internet lors d'élections municipales. En 2007, tous les électeurs ont eu le droit d'utiliser ce mode de scrutin pour des élections parlementaires et, en 2011, cette pratique a gagné en popularité avec 24,3 % des votes par Internet. D'autres pays se lancent dans le vote à distance pour des élections politiques. Des projets pilotes ont par exemple été expérimentés à l'occasion d'élections municipales et régionales en Norvège (expérimentations finalement arrêtées). En Suisse, après des périodes de tests, les cantons de Genève et de Neuchâtel proposent le vote électronique depuis 2015. Lors des élections parlementaires en 2015 de l'état de New South Wales en Australie, les électeurs avaient la possibilité de voter à distance par Internet. Cette élection constitue probablement la plus grande élection par Internet à ce jour. Pour la France également, lors des élections législatives de 2012, les Français de l'étranger ont eu la possibilité de voter par Internet pour élire 11 députés. Cependant en mars 2017, le ministère des Affaires étrangères a annoncé que pour les législatives de 2017, les Français de l'étranger devront voter de manière traditionelle et non électronique, évoquant un risque élevé de cyberattaques et les suspicions sur les élections présidentielles américaines de 2016.

Propriétés essentielles

Le vote par Internet présente des avantages dans certaines circonstances, par exemple lorsque le vote avec urne occasionne de longs déplacements. Ainsi, le vote des Français de l'étranger a lieu traditionnellement dans les ambassades, parfois très éloignées. C'est également le cas pour certains pays comme l'Australie qui ont une faible densité de population. Le vote par Internet permet également une consultation plus fréquente des électeurs et c'est une des raisons pour lesquelles la Suisse cherche à développer le vote électronique.

Cependant, le vote par Internet pose évidemment des problèmes potentiels de sécurité. Ceci est principalement dû à trois raisons. D'une part, les électeurs ne disposent plus d'un bureau de vote avec un isoloir. Il est donc difficile de vérifier l'identité de l'électeur et de s'assurer que cette personne vote librement, sans contraintes. D'autre part, les ordinateurs personnels utilisent de nombreux logiciels peu contrôlables et potentiellement malveillants. Enfin, les électeurs n'ont pas de contrôle sur le système de vote choisi et n'ont pas la capacité de s'assurer que l'urne n'est pas manipulée par des acteurs malveillants, voire par les autorités de l'élection elles-mêmes. De ces constats se dégagent deux types de propriétés de sécurité essentielles pour le vote : l'anonymat et la correction.

L'anonymat

Pour la plupart des élections, l'anonymat du vote est requis. Cela veut dire qu'il doit être impossible de savoir comment un votant particulier a voté, à moins que ce ne soit révélé par le résultat (par exemple si le vote est unanime). Selon l'enjeu des élections, l'anonymat peut ne pas être suffisant. Afin d'éviter la coercition et l'achat de vote, il est également nécessaire que le protocole soit résistant à la coercition : il doit être impossible d'enregistrer des informations qui pourraient convaincre une tierce personne de la valeur du vote.

La garantie de correction

Il est bien sûr essentiel que le résultat proclamé corresponde aux intentions de vote des électeurs. Pour les scrutins classiques, des observateurs, comme les votants eux-mêmes, peuvent surveiller l'urne et le processus de dépouillement, afin de garantir la correction, c'est-à-dire la sincérité du scrutin. Lors d'un vote par Internet, garantir la correction du résultat est plus compliqué. Par exemple, comment savoir si le programme exécuté sur l'ordinateur personnel de l'électeur est le bon ? Il se peut en effet que le système soit victime de bugs ou encore qu'un programme différent soit exécuté à cause d'un **virus ou malware**. Comment s'assurer que les bulletins, stockés sur le serveur de l'élection, n'ont subi aucune manipulation ? Aussi, des propriétés plus fortes, de vérifiabilité, sont souhaitables : le protocole doit fournir des preuves mathématiques démontrant la correction du résultat. Un votant doit pouvoir contrôler que son bulletin est présent dans l'urne : on parle alors de vérifiabilité individuelle. La vérifiabilité universelle, quant à elle, assure que le résultat de l'élection a été correctement calculé à partir des votes individuels, d'une manière vérifiable par n'importe quel observateur. Enfin, il faut pouvoir s'assurer que les bulletins ne proviennent que d'électeurs légitimes, pour parer à tout bourrage d'urne éventuel. On parle alors de la vérifiabilité de l'éligibilité. Ces vérifications sont indépendantes du logiciel ayant été utilisé pour voter et dépouiller. Elles permettent ainsi de contourner les problèmes dus à des bugs et malwares.

Quelles sont les difficultés du vote par Internet ?

De manière générale, certains problèmes de sécurité sont inhérents au vote par Internet. Ainsi, des logiciels malveillants comme des virus ou *keyloggers* peuvent enregistrer et divulguer les votes, brisant ainsi l'anonymat. D'autres logiciels peuvent non seulement divulguer les votes mais également changer leur valeur, sans être détectés. Lors des élections législatives en 2012 des Français de l'étranger, Laurent Grégoire, ingénieur français travaillant aux Pays-Bas, en a fait la démonstration en mettant au point un logiciel capable de remplacer le choix de l'électeur pour un parti pirate, au moment où l'électeur votait. En 2007, en Estonie, un étudiant en informatique, Paavo Pihelgas, a également construit un logiciel pour produire des bulletins valides, pour le candidat de son choix. Dans les deux cas, il s'agissait de systèmes de vote dont le fonctionnement et le code source n'étaient pas connus. Ceci démontre que le secret du fonctionnement du système ne garantit pas la sécurité. Au contraire, il est souhaitable que la description du système et le code source soient ouverts pour permettre à un maximum de personnes de procéder à une analyse de sécurité.

Même pour les systèmes les plus sûrs et les plus vérifiables, les mécanismes de vérification font appel à des théories mathématiques complexes dont la compréhension détaillée est réservée à des

experts. Les autres utilisateurs doivent faire confiance à ces experts, contrairement au vote papier où les procédures sont comprises par une vaste majorité des citoyens.

Une autre difficulté importante du vote électronique est l'authentification de l'électeur. Lors d'un vote à l'urne, l'électeur s'identifie au moyen de sa carte d'électeur ou d'une pièce d'identité. Lors d'un vote électronique, l'électeur reçoit en général des identifiants par mail, courrier postal ou SMS. Toute personne ayant accès à ces identifiants peut voter en lieu et place de l'électeur. Il faut donc contrôler toute la chaîne d'envoi de ces identifiants : prestataire chargé de la fabrication des identifiants, opérateurs téléphoniques en cas d'envoi de SMS, opérateurs de messagerie en cas d'envoi de mail. D'autre part, ces identifiants sont faciles à transmettre et peuvent être vendus par un électeur indélicat.

Pour toutes ces raisons, il semble prématuré d'utiliser le vote par Internet pour des élections à forts enjeux comme des élections politiques importantes. Par contre, il serait réducteur de penser que le vote par Internet est plus dangereux que les autres systèmes de vote en général. Ainsi, le vote par Internet est souvent utilisé pour remplacer le vote par correspondance, qui lui-même n'est pas un système totalement sûr. Contrairement au vote dans un bureau de vote, le processus du vote par correspondance ne peut être observé que par quelques personnes et les électeurs doivent faire pleinement confiance aux organisateurs de l'élection. De plus, le vote par correspondance peut être sujet au bourrage d'urne, comme l'ont montré certaines attaques. En conclusion, le choix d'utiliser un système de vote électronique dépend très fortement du système déjà en place, du type d'élection et des enjeux de sécurité associés.

1. Le vote par internet, tour d'horizon des espoirs déçus

Source
Le Temps
Florian Fischbacher
7 avril 2019

Plusieurs pays occidentaux, à l'image de la Suisse, ont testé l'implémentation de systèmes de vote en ligne. Jusqu'ici ces tentatives sont plutôt infructueuses, sauf en Estonie.

La déconvenue helvétique

Les cantons de Neuchâtel, Fribourg, Bâle-Ville et Thurgovie voulaient que leurs citoyens puissent voter à distance le 19 mai prochain, de manière électronique. Mais le système de vote par internet développé pour La Poste par l'entreprise espagnole Scylt, passé au crible d'un groupe de hackers internationaux, n'était pas à la hauteur. Le programme a été suspendu le 29 mars.

Cette expérience ratée sonne-t-elle le glas du vote électronique en Suisse ? Pas complètement : certains électeurs genevois, vaudois, bernois, argoviens, lucernois et saint-gallois pourront voter en ligne, grâce au système CHVote développé en open source par le canton de Genève. Mais le programme a été interrompu et ne sera opérationnel que jusqu'en 2020, sa mise aux normes exigées par le Conseil fédéral ayant été jugée trop coûteuse.

Les failles principales de ce système concernent une condition jugée essentielle pour que le résultat d'un vote puisse être accepté : la vérifiabilité universelle du résultat, soit la démonstration irréfutable qu'il n'a pas fait l'objet de manipulations. Elle s'oppose à la vérifiabilité individuelle, qui signifie que chaque électeur peut contrôler que son vote a été déposé correctement dans l'urne électronique.

Les restrictions allemandes et françaises

Les Français de l'étranger sont autorisés à voter par internet dans certains cas précis : les élections législatives et les élections des conseillers consulaires. Ceux qui en font la demande reçoivent un authentifiant par e-mail, puis un mot de passe par SMS pour chaque tour de scrutin. Dans le cas de l'élection présidentielle, ou tout autre vote, les Français de l'étranger doivent se rendre à l'isoloir.

En Allemagne, le vote électronique est impossible au niveau fédéral, même pour les résidents étrangers, qui sont tenus de voter physiquement par correspondance. Le Ministère allemand de l'intérieur estime en effet que « la liberté et l'anonymat du vote par internet ne sont pas suffisamment garantis » pour le moment. Une des premières expériences de vote électronique avait pourtant eu lieu dans le pays en 1998 déjà, avec la création d'une élection test virtuelle.

Les errements américains

Aux Etats-Unis, 32 Etats autorisent leurs citoyens installés à l'étranger, notamment les soldats en service, à voter via internet depuis le milieu des années 2000. Mais dans la plupart des cas, il s'agit

d'un simple vote par correspondance, transmis par e-mail, ce qui présente des risques importants de manipulation. Seuls cinq Etats disposent d'un réel portail de vote électronique.

Selon une étude, plus de 100'000 personnes ont voté par internet en 2016. De nombreuses voix commencent à s'élever pour dénoncer les risques liés à ces pratiques, l'Académie américaine des sciences a ainsi officiellement effectué la recommandation suivante en septembre 2018 : « Le vote par internet ne devrait pas être utilisé pour les futures élections, tant que des garanties très robustes de sécurité et de vérifiabilité ne sont pas développées et mises en place. » Et de conclure qu'à ce jour le meilleur moyen de garantir un vote sûr est « low tech » : de bons vieux bulletins en papier, comptés par des humains.

Le contre-exemple estonien

Les Estoniens seront les seuls citoyens de l'UE qui pourront voter par internet lors des élections européennes, le 26 mai 2019. Ce mode de scrutin existe depuis les élections municipales de 2005 dans le pays. Le vote électronique ne rencontre que peu de résistance, même si la possibilité de « corriger un vote » en cas d'erreur ou de vote forcé surprend les observateurs. À ce jour, aucune fraude n'a jamais été signalée.

Lors des législatives de mars 2019, 44 % ont voté à l'aide du système en ligne baptisé i-Voting. En 2009, ils étaient 16 % à avoir choisi ce canal. En Suisse, à titre de comparaison, 54,75 % des inscrits qui ont voté pour la votation du 18 juin 2018 à Genève l'ont fait de manière électronique.

Pourquoi voter par internet ?

En 2017, une étude de l'Université de Zurich, menée dans les cantons de Genève et de Zurich a montré que, contrairement aux arguments souvent avancés par ses partisans, l'e-voting n'était pas un facteur déterminant pour améliorer la participation aux votations et élections. Confirmant le constat du Conseil d'Etat genevois en 2013 : « Cette nouvelle façon de voter se substitue au vote par correspondance ou à l'urne. »

L'enjeu est plutôt celui de l'égalité. En novembre 2018, l'Organisation des Suisses de l'étranger a ainsi remis à Berne une pétition rassemblant plus de 11'000 signatures. Elle demande l'introduction du vote électronique pour toutes les Suissesses et les Suisses de l'étranger d'ici à 2021, rappelant qu'il s'agit du seul canal qui puisse permettre à la Cinquième Suisse de participer pleinement aux élections et votations fédérales.

Source
The Conversation
Poorvi Vora
7 mai 2019

2. Comment l'Inde fait voter plus de 600 millions de personnes

Près de 600 millions d'électeurs indiens ont été appelés à voter sur une période de 39 jours, soit jusqu'au 19 mai, pour élire leurs députés.

L'Inde compte environ 900 millions de citoyens, dont les deux tiers se rendent habituellement aux urnes.

Je travaille sur la sécurité des systèmes de vote électronique depuis plus de 15 ans. Comme certains de mes collègues, je me suis intéressée à la façon dont une nation peut comptabiliser autant de votes sur une aussi longue période. L'Inde utilise des postes de vote électroniques conçus et fabriqués localement (jusqu'à 4 millions dans plus d'un million de bureaux de vote certains étant situés dans les localités les plus reculées).

La toute première version du poste de vote électronique indien a été mise en service lors des élections législatives au Kerala en 1982. Cette machine est maintenant utilisée dans tout le pays.

Comment fonctionnent les postes électroniques ?

Quand un électeur arrive au bureau de vote, il présente une pièce d'identité avec photo au responsable du bureau qui vérifie qu'il figure bien sur les listes électorales. Un assesseur utilise alors l'appareil de contrôle du poste de vote électronique pour déverrouiller la machine, qui est prête à recevoir le vote.

L'interface du poste est très simple : une série de boutons portent les noms des candidats et leurs emblèmes. Pour voter, il suffit d'appuyer sur le bouton correspondant au candidat de son choix.

Une fois le bouton pressé, le choix du votant est imprimé sur papier. La personne dispose de quelques secondes pour vérifier que son vote a été enregistré correctement, après quoi le papier est déposé dans une urne scellée.

Tout le système fonctionne sur batterie afin de ne pas dépendre du système électrique.

Lorsque le bureau de vote ferme, à la fin de la journée, les postes de vote électronique et les urnes contenant les papiers de contrôle sont scellés avec de la cire et du ruban adhésif portant les signatures des représentants des différents candidats à l'élection, puis entreposés sous la surveillance de gardes armés.

Après les élections, lorsqu'il est temps de compter les votes, les machines électroniques sont récupérées, les sceaux, brisés, et le décompte des votes de chaque appareil de contrôle est lu à voix haute sur le tableau d'affichage. Les assesseurs additionnent à la main les totaux de toutes les machines pour obtenir les résultats de chaque circonscription.

Système de sécurité et failles

Les postes de vote électronique indiens utilisent principalement des micrologiciels et du matériel spécialisé, contrairement aux machines utilisées aux États-Unis, qui s'appuient sur les systèmes SIS. En d'autres termes, ils sont faits exclusivement pour voter, ce qui leur évite de dépendre d'un système d'exploitation standard comme Windows qui nécessite d'être régulièrement mis à jour pour réparer les failles de sécurité détectées.

Chaque machine n'a besoin que d'une connexion entre le poste de vote et l'appareil de contrôle. Il n'existe aucun moyen de connecter l'une de ces machines au réseau d'un ordinateur, encore moins à Internet, y compris sans fil.

Après la clôture du scrutin, les postes de vote électronique sont scellés à l'aide d'une technique antédiluvienne : la cire.

Ce fonctionnement offre une certaine protection contre d'éventuelles falsifications des résultats. La Commission électorale indienne a affirmé à plusieurs reprises que ces postes de vote électronique rendaient toute fraude impossible. Cependant, une étude menée par des chercheurs a démontré qu'il existait des moyens de trafiquer les machines. La façon dont elles sont conçues les rend particulièrement vulnérables aux attaques les plus simples, comme l'interception et la modification du signal transmis par le câble de la machine.

La Commission électorale n'ayant apparemment procédé à aucune évaluation de sécurité indépendante, il est difficile de savoir exactement ce qu'il est possible ou non de faire. Les partis politiques défaits aux élections soupçonnent souvent une manipulation des résultats et remettent en question la fiabilité de l'équipement.

Fabrication des machines

Comme mes collègues et moi-même avons pu le constater, au moment de la fabrication des machines, de nombreuses occasions se présentent de les trafiquer d'une façon impossible à détecter lors des vérifications qui précèdent les élections. Le logiciel des machines est conçu, programmé et testé par deux sociétés nationales : Bharat Electronics et Electronics Corporation of India.

Les puces des machines sont fabriquées à l'étranger. Pour les premières versions, le fabricant inscrivait aussi le code de la machine dans la puce. Aujourd'hui, ce sont les sociétés d'électronique qui s'en chargent.

À tout moment durant la fabrication, les essais et la maintenance des appareils, il est possible d'introduire des puces contrefaites ou d'autres composants qui permettraient à des pirates informatiques de manipuler les résultats.

La Commission électorale assure que toute manipulation ou erreur serait forcément détectée puisque les postes sont fréquemment contrôlés et que les représentants des candidats ont l'occasion de participer à un simulacre de scrutin juste avant qu'une machine ne soit utilisée lors des véritables élections. Toutefois, il est possible d'effectuer des changements indétectables. Les essais de contrôle peuvent ne révéler qu'une partie des failles, et l'absence de problèmes durant les essais ne signifie pas qu'il n'y en a pas.

Vérification des résultats fournis par les machines

Il existe néanmoins un moyen de détecter les attaques éventuelles : le papier imprimé indiquant le vote de l'électeur et stocké en toute sécurité avec l'équipement électronique. Suite à une directive de la Cour suprême datant de 2013, la Commission électorale a instauré ce procédé afin de préserver l'intégrité du scrutin.

Dans chaque circonscription, les résultats de cinq postes de vote électronique sont vérifiés par comparaison entre un décompte à la main des votes imprimés et celui des votes électroniques (ce qui implique 1 à 2 % des machines de chaque circonscription). Les partis d'opposition ont demandé à la Cour suprême d'ordonner la vérification des résultats de la moitié des postes, mais cela ne sera peut-être pas le cas cette année.

Bien que le système de vote électronique soit utile et opérationnel, les représentants du gouvernement et les observateurs ne doivent pas présumer qu'il n'existe aucun risque de fraude. La Commission électorale doit continuer à améliorer les procédures de contrôle et fournir au public des rapports de commissions de sécurité indépendantes. Aucune technologie n'étant infaillible, chaque résultat d'élection, quel qu'il soit, doit être vérifié manuellement pour s'assurer qu'il est correct.