Vote par internet : failles techniques et recul démocratique

Chantal Enguehard

Vote par internet : failles techniques et recul démocratique

Chantal Enguehard
Université de Nantes
Laboratoire d'Informatique Nantes Atlantique
2, rue de la Houssinière
BP 92208
44322 Nantes Cedex 03
France

Résumé

À première vue, voter par internet semble aller de soi. Il n'est pas difficile d'additionner des voix, et de nombreuses transactions bancaires ou commerciales se déroulent via ce nouveau medium. Mais cette opération présente des caractéristiques inédites dans le domaine informatique. Tout d'abord, le secret du vote interdit d'observer la procédure pendant son déroulement. Ensuite, le scrutin ne doit laisser aucune trace permettant de lier chaque électeur à son bulletin. Enfin, depuis que les élections existent, il y a toujours eu des tentatives de fraude à tous les niveaux et ce paramètre ne peut être négligé.

Cet article détaille plusieurs aspects du vote à distance par internet. Il rappelle la signification des élections dans le domaine politique et en trace un brève historique, il présente le vote à distance par internet ainsi que les failles techniques inhérentes. Enfin, il examine la compatibilité du vote par internet avec quelques principes éthiques caractérisant les scrutins démocratiques.

Plusieurs expériences menées dans différents pays sont évoquées et analysées.

Il apparaît que le vote par internet est moins fiable que le vote par correspondance car sa complexité introduit de multiples failles de sécurité tandis que le manque de transparence inhérent à l'outil informatique entraîne inéluctablement des doutes quant à la sincérité des élections.

Mots-clef : vote par internet, démocratie, transparence, fraude, virus, vers, vente de votes, achat de votes, coercition

Abstract

Voting by internet may seem easy. It is not difficult to count ballots. Many banking or commercial transactions take place on the Web. Internet voting, however, presents computer scientists with a new challenge. Firstly, voting secrecy prevents observation of the voting procedure. Secondly, there should be no trace linking a voter with his ballot paper. Lastly, election fraud at all levels has existed for as long as there have been elections and this danger cannot be neglected.

This article presents several aspects of remote internet voting. It points out the significance of the elections and outlines its history. It describes remote Internet voting and the inherent technical risks it causes.

Finally, it examines the compatibility of Internet voting with several principles of democracy.

Several examples which demonstrate the practices of various countries are presented as are the policies of several governmental or international institutions.

It appears that internet voting is less safe than remote voting using traditional mail because its complexity introduces multiples security flaws. In addition, the lack of transparency, which is a common characteristic of all the electronic voting systems, leads to doubt about the validity of election results.

Keywords: Internet voting, democracy, transparency, fraud, virus, worms, vote selling, vote buying, coercicion

Introduction

Cet article fait le point sur l'état de l'art en ce qui concerne le vote à distance par internet. Il détaille les différents modes de vote électronique après avoir rappelé et expliqué les caractéristiques fondamentales des élections démocratiques en usage lors des scrutins politiques. La seconde partie présente les failles techniques de ce nouveau mode de vote tandis que la troisième partie effectue une analyse théorique de la compatibilité entre le vote à distance par internet et la tenue d'élections démocratiques. Ensuite, sont évoquées les expériences réalisées en matière de vote à distance par internet ainsi que leur bilan. Les perspectives d'évolution sont alors examinées.

I. Le vote électronique

I.1. Caractéristiques d'un vote démocratique

Comme le rappelle son étymologie, la démocratie[1] est un régime politique dans lequel le pouvoir appartient au peuple, ce qu'énonce également la formule bien connue issue de l'article 2 de la Constitution de la République Française : « *gouvernement du peuple, par le peuple et pour le peuple* ».

Cependant, il faut bien constater qu'aucun régime de démocratie directe (dans lequel le peuple exercerait directement son pouvoir) ne s'est jamais concrétisé, avant tout pour des raisons pratiques d'organisation. Aussi la plupart des démocraties sont-elles représentatives : le peuple y exerce sa souveraineté par représentants interposés, ces représentants étant choisis lors d'élections. L'analyse historique montre que, paradoxalement, ce système conserve un caractère aristocratique (les élus appartiennent souvent aux classes favorisées) [35], mais il représente cependant un progrès dans le respect de la volonté populaire si on le compare à d'autres systèmes dans lesquels la désignation ou l'hérédité constituent les modes de choix des détenteurs de la souveraineté.

Dans le système de la démocratie représentative, si le peuple est détenteur du pouvoir, il consent à s'en défaire pour le confier à des représentants désignés au moyen du vote. Lors de chaque élection, on peut donc considérer que le pouvoir revient entre les mains du peuple qui désigne de nouveau ses représentants.

Nous constatons que le peuple est l'élément central de cette délégation consentie : il détient le pouvoir et est actif dans la désignation de ses représentants[2].

Le processus de désignation se concrétise dans des élections qui doivent obéir à plusieurs principes de base pour être considérées comme démocratiques et universelles, principes exprimés dans plusieurs déclarations d'organisations internationales, par exemple :

Les Nations Unies, dans la Déclaration Universelle des droits de l'Homme de 1948 (article 21) :

> « La volonté du peuple est le fondement de l'autorité des pouvoirs publics ; cette volonté doit s'exprimer par des élections honnêtes qui doivent avoir lieu périodiquement, au suffrage universel égal et au vote secret ou suivant une procédure équivalente assurant la liberté du vote. » [41]

L'Organisation pour la Sécurité et la Coopération en Europe (OSCE), dans son manuel d'observation des élections :

> « Le concept d'élections honnêtes suppose que le processus électoral se déroule dans la transparence et conformément à l'obligation de rendre des comptes et que l'électorat soit en mesure de faire un choix réel et informé, — ces conditions assurant la confiance des électeurs dans le processus électoral. » [49]

1 "Démocratie" signifie littéralement : pouvoir (kratein = commander) du peuple (dêmos)

2 Ce concept fondamental ne doit pas être confondu avec une mise en perspective opposée et erronée dans laquelle ce sont les représentants qui détiennent le pouvoir et qui consultent le peuple pour leur renouvellement.

Ces déclarations mettent l'accent sur plusieurs caractéristiques essentielles (mais non suffisantes) que doivent respecter des élections démocratiques. Ces caractéristiques (élections honnêtes, suffrage universel, liberté du vote, transparence, etc.) peuvent être exprimées plus clairement sous forme de concepts. Cinq d'entre eux focalisent notre attention :

- transparence : chaque électeur a le droit et la possibilité effective de contrôler toutes les étapes d'un scrutin,
- unicité : un vote par électeur[3],
- confidentialité : chaque électeur peut effectuer son choix en secret,
- anonymat : il est impossible de relier un bulletin à l'électeur qui l'a choisi[4],
- sincérité : les résultats du scrutin reflètent fidèlement la volonté des électeurs.

Du respect de ces principes en toutes circonstances découle la confiance du peuple dans son système électoral. Cette confiance est d'autant plus forte qu'elle est fondée sur le contrôle effectif et direct de la sincérité du scrutin. C'est la transparence qui permet à chaque électeur de participer à l'observation pendant la journée, puis d'assister au dépouillement public, voire d'y prendre part, sans avoir à prévenir quiconque ou à demander une autorisation. Le caractère direct de ce contrôle est essentiel.

Dans le cas contraire où il n'y a pas de transparence directe et la police et l'organisation des élections sont exclusivement déléguées à certains (juges, maires, délégués munis de mandats spéciaux...), les simples citoyens ne jouissent plus d'aucun pouvoir, ni entre les scrutins (le pouvoir est confié aux élus) ni pendant les scrutins (ils ne font pas partie de ceux qui ont le droit de contrôler les votes).

Si la procédure de vote est faussée, par exemple par des fraudes, ou si la transparence est insuffisante pour maintenir la confiance, les perdants ne seront pas convaincus de leur défaite, les représentants mal élus risquent de perdre leur légitimité et de voir leur pouvoir contesté. Cette situation est un facteur d'instabilité, voire de crise politique grave, puisqu'il n'y a alors plus de détenteurs du pouvoir clairement identifiés.

Historiquement, on peut remarquer que l'application des cinq principes que nous observons s'est lentement mise en place puis améliorée au cours du temps. En France, par exemple, le premier scrutin (semi-)universel[5] s'est tenu en 1848. À l'époque, on note son choix sur un papier que l'on confie au président du bureau de vote pour que celui-ci le dépose dans l'urne. Il est alors quasi impossible de garder son choix secret et les pressions sont d'autant plus fortes dans les milieux ouvriers ou paysans que l'un des candidats est souvent le maître ou le propriétaire. L'isoloir est introduit en 1913 ainsi que l'usage d'une enveloppe, améliorant considérablement la confidentialité du vote. Les dernières innovations interviennent en 1988 avec l'usage obligatoire d'une urne transparente visible de tous et la signature du registre d'émargement par chaque électeur [44]. Depuis cette date, en France, il n'y a presque plus d'annulation de scrutin pour cause de fraude durant la procédure de vote.

Il s'agit d'examiner l'inscription du vote par internet dans ce processus historique.

---

3 C'est l'unicité qui donne au scrutin son caractère universel. Chaque personne en âge de voter (et non déchue de ses droits civiques) possède une et une seule voix. Il n'existe pas d'autres critères limitant le droit de vote comme cela pu être le cas en France avec le suffrage censitaire (un revenu minimum était exigé) ou le déni de droit de vote aux femmes, encore d'actualité dans quelques pays.

4 Confidentialité et anonymat traduisent les deux aspects du secret du vote.

5 Les femmes ne votent pas.

II.2 Typologie du vote électronique

Le vote par internet (i-vote) fait partie d'un ensemble plus large appelé vote électronique (e-vote). Sous ce dernier terme sont regroupées toutes les formes de vote faisant intervenir un dispositif électronique.

► Il peut s'agir d'un simple ordinateur de vote[6].

Les électeurs doivent se rendre dans leur bureau de vote habituel où ils votent à l'aide d'ordinateurs. La plupart de ces dispositifs enregistrent directement chaque vote dans une mémoire (Direct Recording Electronic - DRE). Certains produisent une preuve de vote (un bulletin) qui est collectée dans une urne après que l'électeur l'ait vérifiée au moment de son vote. Il existe encore d'autres modèles qui enregistrent chaque vote sur un support individuel (carte magnétique par exemple), non vérifiable par l'électeur puisque celui-ci ne peut voir directement ce qui est enregistré sur la carte qu'il a utilisée.

La gestion de la liste d'émargement se déroule encore souvent de manière traditionnelle, à l'aide d'un registre signé par les votants. En France, le dépouillement est effectué localement par chaque ordinateur de vote qui imprime un ticket mentionnant les résultats qui sont ensuite recopiés sur un procès-verbal transmis à l'organisme centralisateur. Dans d'autres pays, les résultats sont transmis sous forme électronique ou via un réseau (Italie, Canada par exemple[7]).

La grande faiblesse des ordinateurs de vote reste que la plupart ne produisent pas de preuve de vote vérifiée par l'électeur, leurs résultats sont donc invérifiables. Dès 2002, la Commission de Venise du Conseil de l'Europe a estimé que l'impression de chaque suffrage sur support papier est un complément judicieux au vote électronique [15]. L'Association for Computing Machinery a considéré qu'il est indispensable que tout système de vote produise des traces matérielles directement vérifiables (par opposition à des enregistrements uniquement informatiques) qui permettent d'attester de son bon fonctionnement ou de détecter des dysfonctionnements [1]. En 2006, l'institut national nord-américain des standards et technologies a produit une recommandation affirmant que la vérification ou le contrôle des résultats d'un système de vote ne doit pas être confié à des logiciels qui, eux aussi, peuvent connaître des dysfonctionnements [43]. Ces résultats ont été confirmés de nombreuses études universitaires [20] [30] [38] [55], la commission indépendante irlandaise sur le vote électronique [7] [8] ou encore des institutions internationales [46].

► Il peut s'agir aussi de kiosques à voter.

Les électeurs peuvent voter depuis n'importe quel bureau de vote puisque la gestion des émargements est réalisée par un serveur central. Ce serveur recueille également les choix des électeurs au fur et à mesure du déroulement de la journée et fournit les résultats du vote en fin de journée.

Cette technologie est toujours présentée comme expérimentale bien qu'aucun dispositif scientifique d'expérimentation ne l'encadre. Elle présente les mêmes faiblesses que les ordinateurs de vote, notamment quant au manque de transparence du processus et à sa vulnérabilité.

► Enfin, il peut s'agir de vote par internet.

La procédure de vote par internet ne disposant pas de modèles organisationnels, légaux et technologiques définis par des standards et des normes internationales, elle ne se déroule pas toujours exactement de manière identique. Voici cependant le schéma général qui est suivi dans ses grandes lignes par les procédures usuelles de vote par internet dites sécurisées. Les électeurs se

6 Les "ordinateurs de vote" sont également nommés "machines à voter" mais ce terme de "machines à voter", introduit dans le code électoral en 1969, époque où il ne s'agissait pas d'informatique, n'est plus approprié aux ordinateurs actuellement utilisés.

7 L'Italie a définitivement abandonné la transmission électronique des résultats de vote en décembre 2006, le principe en est sérieusement remis en cause au Canada.

connectent sur un site officiel de vote depuis n'importe quel ordinateur relié au réseau internet comportant un navigateur compatible avec l'application de vote s'exécutant sur le site officiel. Ils doivent alors s'identifier (donner leur identité) et s'authentifier (prouver leur identité), avant de voter. Un serveur recueille les votes et les stocke jusqu'à la clôture du scrutin. Il produit les résultats du vote à la clôture du scrutin.

Comme tous les électeurs ne disposent pas d'un ordinateur connecté à Internet, ce mode de vote doit être toujours mis en place en supplément de la procédure traditionnelle de vote, il n'est jamais obligatoire[8]. Le vote par internet se déroule généralement sur plusieurs jours, avant le vote traditionnel qui se tient dans les bureaux de vote.

II. Failles techniques du vote par internet

II.1 Méthodologie d'évaluation

Tous les systèmes de vote présentent des vulnérabilités, il n'existe pas de système de vote idéal garantissant le strict respect des principes d'un scrutin démocratique et donnant des résultats parfaitement justes. Notre analyse veillera à comparer le vote par internet avec le vote par correspondance qui permet également de voter à distance et dont les vulnérabilités et qualités sont bien connues. Cette approche nous permettra de déterminer si les risques sont supérieurs, comparables ou inférieurs.

Il faut donc rappeler la mise en œuvre du vote par correspondance postale.

Chaque électeur reçoit le matériel de vote par la poste. Il comprend les bulletins de vote (ou l'unique bulletin de vote dans le cas du modèle dit "bulletin australien"[9]), une enveloppe anonyme et une enveloppe de correspondance. Pour voter, l'électeur met le bulletin de son choix dans l'enveloppe anonyme qu'il scelle, puis il glisse cette enveloppe dans l'enveloppe de correspondance. Il inscrit sur celle-ci son identité, l'authentifie (par exemple par sa signature) puis l'envoie, par la poste, au bureau centralisateur des élections.

Le bureau des élections collecte les enveloppes au fur et à mesure de leur réception. Le dépouillement se déroule en deux phases. D'abord, les enveloppes de correspondance sont ouvertes et le registre d'émargement est mis à jour en conséquence. Les enveloppes anonymes qu'elles contiennent sont rassemblées et brassées afin de ne pas conserver de lien entre celles-ci et les enveloppes de correspondance. Ensuite les enveloppes anonymes sont ouvertes. Les bulletins qu'elles contiennent sont dénombrés afin d'établir l'issue du vote.

Nous ne présenterons ici ni les questions liées au rituel du vote qui ont déjà été largement traitées (voir par exemple [14] et [25]), ni les aspects concernant la fracture numérique ou l'accessibilité [5].

II.2 Risques de fraudes externes

Les fraudes externes interviennent hors du bureau des élections, soit chez l'électeur, soit pendant l'acheminement du vote jusqu'au bureau des élections. L'acheminement d'informations sensibles depuis le bureau de vote jusqu'à l'électeur est également visé puisque ces informations peuvent être utilisées pour frauder. A priori, les fraudeurs ne sont pas des personnes directement impliquées dans l'organisation du vote.

Le vote par correspondance postale est tributaire des services d'acheminement du courrier dont la fiabilité varie beaucoup selon les pays. Ce canal doit être considéré comme un tunnel opaque sur

8 À l'exception notable de la France où le décret n°2007-554 du 13 avril 2007 relatif aux modalités d'élection par voie électronique des conseils de l'ordre des infirmiers dispose « Le vote peut avoir lieu par voie électronique. Le vote électronique exclut toute autre modalité de vote. »

9 Le bulletin australien mentionne les différentes alternatives, l'électeur exprime ses choix en cochant à l'aide d'un stylo.

lequel il n'est pas envisageable d'exercer une surveillance systématique (car l'acheminement de courrier se déroule en divers lieux et à différents moments). Plusieurs types d'incidents peuvent subvenir : le service postal peut connaître des dysfonctionnements ou fonctionner selon des délais incertains ; les enveloppes peuvent être bloquées en fonction de leur provenance : les enveloppes de vote par correspondance, facilement identifiables, peuvent faire l'objet de substitutions ; même si les services postaux sont censés respecter le secret des missives, les enveloppes peuvent être ouvertes et les votes dévoilés, au mépris de la confidentialité du vote et il existe aussi des techniques pour connaître le contenu d'enveloppes sans même les ouvrir. Il serait théoriquement envisageable de sécuriser les services postaux en généralisant l'utilisation de courriers recommandés et d'enveloppes inviolables, mais, outre le coût démesuré de telles mesures, il semble illusoire de l'étendre à des pays où n'existe même pas la notion de courrier recommandé.

Toutefois, une telle fraude, lorsqu'elle est menée à grande échelle, implique un grand nombre de personnes qui doivent être physiquement présentes et intervenir. Il y a alors de fortes chances qu'un témoin dénonce ces actes et que la fraude soit sanctionnée. En France, c'est d'ailleurs à la suite de fraudes massives dans le vote par correspondance que ce mode de vote a été banni des élections politiques en 1975 [33].

Lors d'un vote par internet, les fraudeurs peuvent opérer depuis n'importe quel point du globe, quels que soient le lieu d'où l'électeur vote et le trajet suivi par son bulletin. Une personne seule peut suffire pour attaquer un scrutin[10] il peut aussi s'agir d'une organisation étrangère bien financée [27]. Si l'attaque est correctement menée, il est impossible d'en retrouver les auteurs.

Plusieurs types d'attaques peuvent être menées.

Le déni de service (denial of service) consiste à bombarder le serveur de demandes de vote afin d'empêcher les électeurs légitimes de voter. Le serveur, saturé, ne pourra répondre à toutes les demandes et est même susceptible de tomber en panne. Cette attaque est extrêmement simple à mener, ses effets sont visibles.

Les interventions du type homme-au-milieu (man-in-the-middle) consistent 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, le fraudeur peut ainsi modifier le vote qui a été émis. Le cryptage du vote offre une bonne protection contre cette attaque si la clef publique de chiffrement envoyée à l'électeur n'a pas été interceptée par le fraudeur. Celle-ci doit donc lui être envoyée dans un courrier sécurisé, comme les informations qui lui permettent de s'identifier. Par contre il n'est pas nécessaire de connaître la clef de chiffrement pour capturer le bulletin et le détruire, privant l'électeur de l'exercice de son droit de vote. Il est facile de renvoyer un message sur le poste de l'électeur afin de lui faire croire que son vote a été bien enregistré. Cette intervention, bien qu'assez technique, est à la portée de tout informaticien motivé puisque les dates des élections sont connues longtemps à l'avance, et que, pour des raisons de rentabilité, les applications de vote seront amorties sur plusieurs élections. Il est donc possible de les connaître en détail et d'imiter leur fonctionnement avec suffisamment de talent pour tromper un électeur qui n'en a qu'une connaissance très partielle [52].

L'utilisation de virus et de vers[11] est bien plus redoutable. Comme la plupart des antivirus ne peuvent détecter que les virus déjà connus, les nouveaux virus ne sont pas détectables avant de passer à l'action. Par exemple, en 2001 le vers Code Rouge (Code Red worm) a infecté 360 000

10 « L'utilisation d'Internet comme moyen de communication, ainsi que l'usage de l'ordinateur banalisé de l'électeur, constituent un changement radical par rapport aux envois par correspondance, en terme de portée de nuisance d'un fraudeur potentiel. En effet, avec le système actuel d'envoi postal aux bureaux de vote, un fraudeur ne peut s'interposer physiquement que sur le cheminement d'un nombre réduit de suffrages, que ce soit pour les détruire ou les falsifier. Il en va bien autrement avec Internet. » F. Pellegrini [50]

11 Un vers est un virus qui a la capacité de se propager seul en utilisant le réseau.

ordinateurs en seulement quatorze heures avant d'être détecté et qu'un antivirus puisse agir. Les vers plus récents sont encore plus virulents et se propagent en utilisant de multiples méthodes, ils sont capables de passer les firewalls et autres défenses, et sont difficiles à analyser [39] [53]. Les attaquants peuvent créer de nouveaux virus, ou modifier des virus qui existent déjà pour éviter leur détection. Il existe sur internet des kits de construction de virus. Les attaquants ont l'avantage de tester leurs créations à l'aide des anti-virus communément distribués et qu'utilisent leurs victimes potentielles.
Un virus peut donc facilement infecter un grand nombre d'ordinateurs sans être détecté et rester dormant jusqu'au jour du vote. Il est susceptible de réaliser différents types d'actions, à l'insu de l'électeur, comme capturer les informations nécessaires à la connexion avant qu'elles ne soient transmises au serveur et les communiquer à un tiers, modifier le vote de l'électeur avant cryptage, ou rediriger l'électeur vers un site imitant le site officiel (spoofing) : l'électeur croit voter sur le site officiel alors qu'en fait il est en train d'interagir avec un site qui se contente d'imiter le site officiel.

Une fraude beaucoup plus simple mais de portée limitée est l'usurpation d'identité par une personne de l'entourage de l'électeur. Il suffit de prendre connaissance des informations qui permettent à l'électeur de s'identifier et de voter. Généralement, il s'agit de l'identifiant, du mot de passe et de la clef de chiffrement qui ont été envoyés par courrier postal. Des informations supplémentaires, comme la date de naissance, sont quelquefois demandées mais il n'est pas difficile de se les procurer. Les services de la poste sont considérés comme suffisamment fiables pour envoyer ces informations sensibles. Pourtant, plusieurs personnes habitant souvent le même domicile, le courrier peut être intercepté lorsqu'il est parvenu à destination. Seul l'usage de courriers recommandés peut garantir que le courrier est effectivement délivré à son destinataire. Cette mesure coûteuse n'est jamais mise en œuvre.

Le grand danger est qu'une élection par internet peut se dérouler apparemment sans problème ce qui démontrerait que le système est fiable, robuste et sécurisé, et pousserait à étendre ce mode d'élection plus largement. Mais le fait qu'aucune attaque n'ait été repérée ne prouve pas qu'il n'y en ait pas eu [34] [45]. La plupart des attaques, si elles sont menées avec finesse, seraient extrêmement difficiles à détecter, même si elles avaient changé le résultat d'élections d'importance majeure. Un essai apparemment réussi de vote par internet constitue donc une pente dangereuse menant à des systèmes encore plus vulnérables.
Enfin, les menaces de fraudes externes se concrétisent avec l'accroissement continuel des attaques cybernétiques et la professionnalisation des attaquants[12].

II.3 Risques de fraudes internes

Les fraudes ou malveillances internes peuvent être menées par une ou plusieurs personnes impliquées dans l'organisation du vote. Il peut s'agir d'un programmeur, d'un technicien chargé de la maintenance et des mises à jour, ou de toute personne ayant un accès physique ou logique au serveur. Ces attaques sont les plus graves car elles sont faciles à mener, elles peuvent concerner un nombre de votes plus important que les attaques externes et rester complètement invisibles.

Il faut rappeler que le vote par internet fait partie du vote électronique et souffre des mêmes vulnérabilités et déficiences déjà constatées pour les ordinateurs de vote qui enregistrent les votes uniquement sur support électronique. En particulier, il est impossible d'être certain que les programmes s'exécutent exactement comme spécifiés. Il peut exister des autorités de certification mais elles n'ont pas la capacité de vérifier les programmes d'un serveur de vote, y compris en cours de vote, avec suffisamment de moyens et d'attention pour détecter toutes les erreurs, tentatives de

12 Par exemple, en mai 2007 des dizaines de sites du gouvernement estonien ont été mis hors service par près de 150 attaques coordonnées.

fraudes internes et failles de sécurité. En effet, en l'état de la science informatique, personne ne sait mener une telle tâche à moins d'imposer l'utilisation de méthodes développement formel qui restent très onéreuses et limitées à des composants logiciels. En effet, au-delà d'une certaine complexité, il n'existe pas encore de méthodes de développement sûres. Même les équipes de programmeurs au plus haut niveau international (qui travaillent dans le domaine de l'aérospatial) laissent passer des erreurs d'origine humaine[13]. De plus, un examen très poussé ne peut être réalisé en quelques jours et nécessiterait plusieurs mois d'études de très haut niveau. Enfin, même si un tel examen était réalisé, même si l'on disposait de méthodes de développement permettant d'éviter les erreurs humaines, il serait très difficile d'être certain que les programmes en service sont exactement ceux qui ont été certifiés ou qu'ils s'exécutent sans modification contrainte par l'environnement (détournement d'exécution par du code malveillant présent dans des logiciels périphériques ou du microcode pilotant des composants actifs).

Le risque de fraude interne est rarement mis en avant par les fabricants d'applications de vote car ils s'adressent généralement à des élus ou aux personnes qui vont effectivement mettre en place le vote, et qu'il est délicat de leur laisser entendre qu'ils sont potentiellement soupçonnés de tentative de fraude. Il serait encore plus problématique de leur laisser entendre que l'entreprise qui leur propose ces applications n'est elle-même pas à l'abri d'agissements délictueux. Pourtant, le risque de fraude interne est plus important que le risque de fraude externe car il est techniquement plus facile à mettre en place : il s'agit de personnes et de traitements automatisés ayant accès aux machines, aux mots de passe, et qui peuvent modifier furtivement l'exécution de programmes à l'insu de tous.

Nous pouvons comparer cette situation à celle du piratage informatique des entreprises. En effet, celles-ci consacrent beaucoup d'énergie à protéger leurs données informatiques et leurs programmes. Il s'avère que environ 80% des actes de piratage informatique sont perpétrés par des employés ou des ex-employés de l'entreprise [54]. Ce chiffre est sous-estimé : le secteur privé a tendance à cacher ses problèmes de sécurité car leur révélation ne donne pas une bonne image de l'entreprise touchée (surtout s'il s'agit d'une entreprise dont un des domaines d'activité est l'informatique), ce qui peut faire chuter ses cours si elle est cotée en bourse.

Il existe des processus de fraude classiques comme l'introduction d'un cheval de Troie (Trojan Horse) ou d'une porte arrière (Back Door). Ces fraudes se résument à l'introduction de quelques lignes de programme qui peuvent facilement passer inaperçues au milieu de programmes comprenant plusieurs milliers de lignes [58]. Dans des applications bancaires de telles fraudes finissent par être détectées car le système informatique ne se comporte pas comme il le devrait. Par contre, dans le cadre d'un scrutin, on ne peut connaître à l'avance les résultats. Si la fraude détourne certains votes au profit d'un candidat, personne ne peut s'en apercevoir : le fonctionnement correct prévoit que le système fournit le nombre de voix obtenues par chaque candidat, et c'est bien ce que semblerait faire un système fraudé.

Une telle fraude, implantée directement dans le serveur, représente l'éventualité la plus inquiétante puisqu'elle concernerait un nombre très important de votes (tous les votes aboutissant sur le serveur) et qu'elle pourrait être commise par très peu de personnes (une seule personne peut suffire). Les personnes au contact des systèmes de vote sont donc susceptibles de faire l'objet de tentatives de corruption ou de pression importantes. Ces éventualités ont pour l'instant été peu discutées et analysées.

Enfin, centraliser les registres d'émargement facilite le bourrage d'urnes à grande échelle : un programme frauduleux peut générer les votes de nombreux électeurs abstentionnistes dans les derniers instants de la période de vote. Ce risque ne peut être maîtrisé par une surveillance du taux

13 En voici deux exemples : lors de son vol inaugural le 4 juin 1996, Ariane 5 explose, victime d'une erreur de calcul : un programme qui fonctionnait à merveille sur Ariane 4 se révèlera être la cause de cette défaillance ; le 23 septembre 1999 la NASA perd la sonde américaine Mars Climate Orbiter à cause d'un bug.

de participation (on a observé que les sites de vote connaissent des pics de fréquentation dans les derniers instants) et il ne peut être jugulé par un contrôle des électeurs (même si quelques électeurs découvrent qu'un vote a été enregistré à leur nom, alors qu'ils n'ont pas voté, leur parole sera mise en doute car il leur sera impossible de prouver qu'ils n'ont pas voté).

Avec le vote par correspondance utilisant la voie postale, frauder implique de modifier les bulletins reçus par le bureau des élections ou d'intervenir lors du dépouillement. Ouvrir une grande quantité d'enveloppes, remplacer le bulletin qu'elles contiennent puis les refermer en toute discrétion sont des opérations physiques qui peuvent être dénoncées par un témoin imprévu ou même par une personne impliquée dans la fraude. Elles nécessitent du temps alors qu'un programme malicieux peut modifier une grande quantité de votes en un instant et de manière invisible. Remplacer un lot d'enveloppes par un autre, pratiquer le bourrage d'urnes implique également une intervention physique et visible.

Le risque de fraude interne lors des scrutins réalisés par voie postale est donc loin d'être nul. Toutefois, il est envisageable de prendre des mesures simples sécurisant le trajet des bulletins au sein du bureau de vote : stockage direct des enveloppes de vote dans un lieu fermé au fur et à mesure de leur réception, l'intégrité de ce lieux peut être garantie par la pose de plusieurs serrures dont les clefs sont conservées par plusieurs personnes (issues des partis des différents candidats et représentants des électeurs), interdisant ainsi la manipulation des enveloppes de vote. L'ouverture des enveloppes, puis le dépouillement doivent se dérouler en présence de tous les observateurs requis.

II.4 Risques de dysfonctionnement

Tout ordinateur peut connaître des pannes ou des dysfonctionnements. Il peut y avoir des défauts dans le matériel, notamment dans les cartes électroniques (soudures défaillantes), ou même dans les microprocesseurs. Ceux-ci sont de plus en plus miniaturisés ce qui les rend vulnérables aux rayons cosmiques. Ce phénomène est assez récent puisqu'il n'a été analysé et compris que dans les années 80 mais les faits sont là : les flux de particules venus du cosmos sont capables de traverser murs et blindages et de perturber le fonctionnement des microprocesseurs des ordinateurs [23]. Les ordinateurs doivent donc intégrer des mécanismes de détection d'erreurs, ce qui n'est pas réalisé systématiquement sur les ordinateurs détenus par des particuliers.

Il peut également y avoir des erreurs dans les programmes qui équipent un ordinateur. Ces erreurs peuvent intervenir à tous les niveaux : système, logiciels, compilateurs, failles de sécurité, etc., tout simplement parce que ces programmes sont conçus par des humains et que les humains ne sont pas infaillibles.

En l'état actuel de la science, il est impossible d'étudier le fonctionnement d'une application informatique sans en observer le déroulement pas à pas. Or, introduire des sondes logicielles dans des programmes pour en suivre l'exécution pose la question de l'objectivité et de la neutralité de ces sondes et des programmes chargés d'analyser les données d'observation. Dans le cadre d'une application de vote, suivre le le traitement d'une opération de vote implique la tenue d'un journal de bord dans lequel sont notés et horodatés tous les événements : arrivée d'un bulletin, émargement du votant, dépouillement, etc. Mais la lecture de ce journal permettrait de connaître le vote de chacun et viole donc le secret du vote. Si les informations du journal ne sont pas complètes (pour protéger le secret du vote), le procédé devient alors complètement inutile puisqu'il ne permettrait plus de suivre pas à pas le traitement des informations reçues, un dysfonctionnement (ou une fraude), même majeur, pourrait passer inaperçu. Nous constatons ici qu'une mesure efficace dans le cadre des utilisations habituelles d'internet (comme les transactions bancaires) ne peut être mise en œuvre du fait des caractéristiques très particulières des scrutins démocratiques.

La démarche de tests est impraticable car il n'est pas possible de simuler le déroulement d'une vraie

élection impliquant des millions de personnes, avec tous les aléas qui peuvent subvenir. Par ailleurs, tester une application avec succès ne permet pas de prédire avec certitude son comportement lors d'une autre utilisation.

Il s'avère donc qu'un système de vote à distance pourrait présenter des dysfonctionnements sans que quiconque ne s'en rende compte, sauf si les résultats des élections sont manifestement étranges. On peut d'ailleurs se demander quelles seraient les actions légales susceptibles d'intervenir dans ce cas, les preuves de malfonctionnement ou de fraude ayant certainement disparu.

Pour le vote par correspondance postale, les dysfonctionnements concernent essentiellement les problèmes, déjà évoqués, d'acheminement de courriers. Ces difficultés sont bien identifiées selon les pays. Le vote par internet est également concerné par ce sujet dans la mesure où, dans la plupart des mises en œuvres observées, les informations nécessaires au vote sont envoyées par la voie postale.

III. Carences démocratiques du vote par internet

III.1 Confidentialité

Comme on peut voter depuis n'importe quel ordinateur, la question de la confidentialité est épineuse. S'assurer qu'il n'y a pas d'usurpation d'identité, que l'électeur est seul devant l'ordinateur et qu'il n'est soumis à aucune pression (qu'il s'agisse de pressions familiales ou d'achat/vente de vote) reste un problème insoluble [2].

Pour tenter de lutter contre cette possibilité de pression, les estoniens ont mis en place la possibilité de voter à plusieurs reprises, seul le dernier vote est finalement compté. Les électeurs peuvent aussi voter de manière traditionnelle pendant quelques jours avant le jour officiel des élections ce qui annule leur éventuel vote par internet. Cet aménagement semble répondre aux problèmes de pression mais a plusieurs conséquences fâcheuses. Pour pouvoir être annulés, les votes doivent être stockés sur le serveur en conservant le lien entre le vote et l'identifiant de la personne qui l'a envoyé ce qui met à mal le principe d'anonymat. Curieusement, des études proposent que les électeurs aient la possibilité de signaler un vote comme ultime, alors que cette possibilité ruinerait les avantages apportés par le vote multiple puisque, en cas de pression, on forcerait évidemment la victime à déclarer qu'il s'agit de son dernier vote [59].

De nombreuses personnes pourraient être tentées de voter à partir de leur lieu de travail sans toujours se rendre compte que les entreprises exercent un contrôle de plus en plus serré sur l'utilisation du réseau internet [12], et qu'elles seraient donc en mesure d'espionner les votes de leurs employés.

Enfin, l'usage d'une unique carte d'identité électronique[14] pour effectuer différentes opérations (voter, payer ses impôts, etc.) rend les citoyens particulièrement vulnérables aux agissements abusifs d'un État qui pourrait être tenté de croiser toutes ces données. Ce risque important ne doit pas être négligé, d'autant plus que l'État tenté par ces pratiques ne serait certainement pas le plus désireux d'en informer la population [19].

Le vote à distance par voie postale, présente également des vulnérabilités, mais celles-ci sont réduites à l'environnement proche des électeurs proche puisque le vote ne se déroule pas dans un bureau de vote. Un électeur peut être soumis à des pressions, quelqu'un peut voter à sa place en lui dérobant le courrier comportant le matériel de vote.

III.2 Anonymat

Coté serveur, il est délicat de garantir l'anonymat puisque chaque bulletin voyage accompagné de

14 Effective en Estonie.

l'identité du votant et que ces informations parviennent ensemble sur un premier serveur de vote. Il faut être capable de garder le lien entre l'identité de l'électeur et son vote lorsque les votes multiples sont autorisés (comme en Estonie). Ce point est particulièrement délicat et a fait l'objet de nombreuses publications montrant comment crypter les votes de manière à décoder l'identité du votant indépendamment de son vote ([22] par exemple). Les solutions proposées ont tendance à être de plus en plus compliquées mais elles présentent toujours des failles : on ne peut mettre en place des mesures techniques qui rendraient impossible la violation du secret du vote par une personne ayant des intentions malveillante et bénéficiant d'accès aux serveurs.
En France, pour plus de sécurité, la Commission Nationale Informatique et Libertés (CNIL) exige des gestions séparées des émargements et des votes qui doivent être mises en œuvre sur des serveurs séparés, mais il n'existe aucun moyen pour que les électeurs puissent vérifier que la séparation entre identité et bulletin est effective. Des spécialistes observant le programme de l'application peuvent difficilement certifier que la reconstitution des votes est impossible car cette reconstitution peut emprunter différents moyens selon les données disponibles : il est envisageable que les fichiers horodatant les événements permettent de reconstituer les votes, des données peuvent être mal effacées, les votes peuvent être stockés en mémoire dans l'ordre de leur arrivée, puis brassés dans un second temps, etc...

Avec le vote par correspondance, il faut s'assurer que les enveloppes contenant les bulletins sont correctement brassées après avoir été ôtées des enveloppes de correspondance, il est alors certain que les votes ne peuvent être reliés avec les identités et qu'il est impossible de connaître leur date et heure d'émission. Les enveloppes de correspondance devraient être inviolables pour être sécurisées durant le trajet. Leur délivrance devrait être certifiée par l'envoi d'un reçu.

III.3 Transparence vs confiance

Le lien entre légitimité et transparence directe est crucial.

> « La régularité[15] de la procédure de vote, et le contrôle de cette régularité, sont ainsi des éléments décisifs et irremplaçables de la légitimité démocratique. » [3]
>
> « Mais la légitimité dépend avant tout du *contrôle* du déroulement et du dépouillement du scrutin. » [3]

Comme pour les ordinateurs de vote, la transparence directe ne peut être effectivement mise en place car les bulletins de vote sont dématérialisés. L'urne, les bulletins, le cahier d'émargement sont remplacés par un dispositif qui "mime" l'existence de ces objets. Le processus de vote est ainsi déplacé du monde réel, dont l'expérience est à la portée de la majorité des citoyens, vers un monde virtuel où les constats effectués directement au travers nos perceptions (la vue, le toucher, etc.) ne s'appliquent pas. Des possibles sans précédent apparaissent. Alors que dans le monde réel il est impossible de modifier ce qui est inscrit sur un bulletin enfermé dans une enveloppe scellée, dans le monde virtuel cette opération est faisable et même facile, elle peut porter sur un nombre important de votes, se dérouler en un instant et rester dissimulée lors des tests ou des expertises. Alors que dans le monde réel la vacuité de l'urne peut être vérifiée visuellement (car l'urne est obligatoirement transparente) et même tactilement, il apparaît peu vraisemblable de prétendre vérifier qu'une "urne électronique" est vide en se fiant au seul affichage produit par un ordinateur. Pire, une "urne électronique" n'est en réalité qu'une mémoire électronique, et une mémoire électronique n'est jamais vide : elle est toujours absolument remplie de bits ayant la valeur 0 ou 1.

Les électeurs n'ont donc aucun moyen de contrôler directement la procédure de vote et d'évaluer dans quelle mesure elle se déroule correctement. Les scrutateurs, délégués des partis et membres des bureaux de vote n'ont pas d'avantage accès au fonctionnement intime de l'application, ils doivent se contenter d'observer des processus qui sont censés refléter le fonctionnement de

15 Il s'agit ici de la régularité dans le sens sincérité du vote, et non dans le sens temporel.

l'ordinateur, mais qui peuvent aussi en donner une vision déformée.

Paradoxalement, la publication des programmes, souhaitable pour en accroître la sécurité[16], n'accroît pas la transparence de la procédure car il faut prouver que le programme en service est exactement identique à celui qui a été publié, et qu'il n'y a pas d'intrusion d'autres programmes. Or, dans tous les cas, le serveur utilise un système d'exploitation, éventuellement un compilateur ou un interpréteur de code qu'il faudrait également examiner, etc. Cette démarche devient rapidement titanesque et donc impraticable.

La surveillance de l'application de vote est, dans le meilleur des cas, confiée à des tiers, ce qui amoindrit la confiance des électeurs.

> « (...) les citoyens n'auraient aucune possibilité de constater les défaillances du système informatique. Ils en seraient réduits à faire confiance aux dires et aux informations émanant des entreprises qui ont mis en place l'infrastructure du e-voting, éventuellement de l'autorité étatique qui certifie et contrôle les résultats de la votation. » [3]

Il n'y a alors d'autre choix que de confier cette tâche de contrôle à des experts tributaires de leurs relations à l'industrie de l'informatique et des télécommunication, tout en restant conscient des limites de cette délégation et de la perte de transparence (et donc de confiance) qui en résultent.

> « Le contrôle par des experts enlève certainement un élément "démocratique" au contrôle des opérations électorales pour le remplacer par un aspect "technocratique". Mais il peut permettre que les citoyens puissent être informés d'éventuelles pannes techniques ou d'irrégularités. Mais là aussi, il faut se méfier: les experts ne contrôlent que ce qu'ils veulent, ou ce qu'ils peuvent. » [3]

La confiance ne peut être uniquement fondée sur l'honnêteté supposée des gestionnaires des élections et des experts censés les contrôler. Les informations détenues par les experts mandatés en raison de leurs compétences doivent également être accessibles aux citoyens qui le souhaitent[17].

Enfin il faut se garder de surévaluer les capacités des experts. D'une part, ni les tests, ni les expertises ne peuvent détecter toutes les erreurs, d'autre part la confidentialité interdit de suivre toutes les étapes du traitement des votes. Enfin, les experts sont aussi confrontés aux problèmes de la preuve de l'identité entre les programmes observés et ceux qui sont utilisés pendant les scrutins, et aux limites de leur investigation qui ne peut être complète du fait de l'ampleur de la tâche.

Cette impossible transparence pourrait être partiellement compensée par une information honnête et complète concernant les détails techniques et les risques ainsi que sur les mesures prévues pour lutter contre ces risques et garantir la sincérité des élections, laissant les électeurs décider en toute connaissance si le système mérite leur confiance ou s'ils préfèrent voter selon une autre modalité.

De plus, la perte de transparence doit impérativement être compensée par la possibilité de vérifier les résultats des scrutins. Des outils cryptographiques sont nécessaires pour que chaque électeur puisse vérifier son vote [37] et il est indispensable d'inciter fortement les électeurs à effectuer ces vérifications. En effet, cette procédure peut permettre de détecter certaines fraudes qui, sinon, passeraient inaperçues. Les personnes n'ayant pas voté doivent être également être encouragées à procéder à des vérifications afin de détecter les usurpations d'identité. Cette incitation peut être acceptée sans saper la confiance des citoyens si les électeurs ont été correctement informés des risques du vote par internet et qu'ils comprennent l'objectif poursuivi. Le nombre de personnes déclarant constater une anomalie doit être public.

---

16 La publication des programmes autorise leur examen par de nombreuses personnes, et donc la détection de failles de sécurité ayant échappé aux développeurs. Ce principe s'oppose à celui de sécurité par l'obscurité dans lequel les programmes restent secrets : un individu y ayant accès peut alors facilement se glisser dans les failles de sécurité qui n'ont pas été décelées par l'équipe de développeurs.

17 « La confiance ne peut venir que des procédures et de leur transparence, et non des acteurs qui les gèrent, quels que soient leurs mandats : en période troublée, chacun est suspect pour une partie ou une autre. » B. Lang [31]

Toutefois, cette démarche de vérification connaît des limites qui affaiblissent sérieusement son efficacité. Si les électeurs détiennent une preuve de leur vote, ils deviennent vulnérables à la coercition. Si les électeurs ne détiennent aucune preuve de leur vote, ils doivent être crus sur parole, ce qui laisse le champ libre aux affabulateurs.

III.4 Unicité

L'unicité est contrôlée par la tenue du registre d'émargement et dépend en grande partie de l'identification de la personne qui envoie son vote.

Une première difficulté réside dans la sécurisation des informations durant la phase de génération des identifiants et lors de la transmission des données aux imprimeurs chargés de les faire figurer sur le matériel de vote. Ensuite les identifiants et mots de passe sont envoyés au domicile des électeurs par courrier non recommandé, ce qui ne garantit pas que les informations nécessaires à la connexion sont délivrées à leur destinataire car plusieurs personnes peuvent habiter le même domicile. Il est donc courant de demander en sus des informations personnelles comme la date ou la commune de naissance[18]. L'identification par une carte d'identité électronique, comme en Estonie ne fait que repousser le problème : en cas de pressions familiales, utiliser la carte d'identité d'autrui pour voter à sa place, lui usurper son mot de passe, avoir connaissance de quelques informations personnelles ne présente pas de difficultés.

Les processus biométriques, parfois envisagés, ne résolvent pas ces problèmes car leur mise en œuvre contredit plusieurs principes de sécurité comme le fait qu'un mot de passe doit toujours être stocké dans un fichier unique et de manière cryptée, qu'il doit être possible d'en changer et que les étapes d'identification et d'authentification, généralement réalisées par la reconnaissance d'un nom utilisateur et d'un mot de passe, doivent être distinctes. Lorsque des procédés biométriques sont mis en œuvre, on observe que ce sont les mêmes données qui servent à s'identifier et à s'authentifier, qu'il s'agisse de la paume de la main, de l'iris de l'œil, ou des empreintes digitales. Ces données ne sont pas secrètes et il est impossible d'en changer. Or, il a été démontré à plusieurs reprises qu'il est facile de tromper les systèmes biométriques en usage fondés sur la vérification des empreintes digitales, des vaisseaux sanguins ou de l'iris de l'œil en fabriquant un faux doigt portant des empreintes digitales volées ou une photo trompant la reconnaissance d'iris, etc. [36]. En France, ces faiblesses ont amené la direction de la protection et de la sécurité de l'État du Secrétariat Général de la Défense Nationale (SGDN) à formellement déconseiller l'usage de la biométrie en ce qui concerne la sécurisation des systèmes informatiques de l'État [61].

IV. La pratique du vote par internet

Les systèmes mis en œuvre sont très divers, les approches des États aussi, mais, dans tous les cas, les informations sont rares et la plupart du temps très partielles. Nous n'avons trouvé aucun document public permettant d'avoir une description précise d'une des applications de vote sur internet en service. De nombreuses informations restent donc inconnues comme, par exemple, les langages de programmation et les systèmes de gestion de bases de données utilisés, la structure des programmes et du stockage des données, les systèmes de contrôle des communications par internet, etc. Dresser un tableau synoptique des expériences en les comparant sur un ensemble de critères s'est révélé irréalisable. Le panorama ci-dessous réalise la synthèse et l'analyse des informations qui ont pu être collectées.

Le vote à distance par internet a été peu utilisé. Seul l'Estonie l'a généralisé à l'ensemble de ses votants, sans en rendre toutefois l'utilisation obligatoire. D'autres pays l'ont testé sur de petits effectifs d'électeurs.

18 Informations qui ne peuvent pourtant être qualifiées de secrètes et sont souvent connues de l'entourage familial.

Estonie

L'Estonie est le seul pays à avoir autorisé l'ensemble de ses électeurs à voter par internet, sans en rendre toutefois l'utilisation obligatoire [34]. Depuis, deux élections ont eu lieu, en 2005 et 2007. Le vote par internet reste encore marginal puisqu'il représente moins de 6% des votes exprimés.

Le système de vote, développé par le National Election Committee (NEC) qui est en charge des élections, suit le schéma général décrit précédemment, sauf en ce qui concerne le processus d'identification réalisé grâce à la carte d'identité électronique dont la presque totalité de la population est équipée. Lors du vote, la carte, glissée dans un lecteur, joue le rôle d'identifiant, l'authentification est réalisée par la saisie d'un code à quatre chiffres. La saisie d'un second code à quatre chiffres autorise la carte à apposer la signature électronique sur le vote. Il n'y a donc pas d'envoi de matériel de vote par courrier postal. La législation autorise les votes multiples : un électeur peut voter plusieurs fois, annulant à chaque fois le vote précédent. Il peut procéder par internet, ou bien à l'urne, quatre à six jours avant la journée officielle des élections (le vote par internet est alors clos).

Les élections de 2007 ont été observées par une mission de l'Organisation pour la Sécurité et la Coopération en Europe (OSCE) [48]. Concernant la transparence, cette mission constate que toute observation directe du processus de comptage des voix réalisé par le serveur est impossible. Les possibilités offertes pour examiner le système de vote se révèlent peu réalistes : bien que de nombreux partis, associations et organisations aient eu la possibilité d'assister à toutes les opérations de gestion des votes, de consulter la documentation et le code source, aucun n'a exercé ce droit par défaut de compétences et manque de financement pour mandater des experts. Le système de vote est donc resté complètement opaque.

Par ailleurs, plusieurs failles de sécurité ont été mentionnées. Ainsi, le National Election Committee (NEC) a reconnu son incapacité à sécuriser les ordinateurs des électeurs, en particulier contre les virus qui pourraient intervenir dans le processus de vote.

Mais de nombreuses autres failles, sous-estimées par le NEC, ont été relevées. Par exemple, l'ordinateur qui effectue la lecture des CD (Compact Disc) contenant les résultats est resté connecté à internet alors que le processus de comptage était lancé. De plus cet ordinateur ne semble pas sécurisé, ce qui peut constituer une entrée pour une attaque extérieure vis-à-vis du serveur. Comme les textes légaux ne spécifient ni les prérequis, ni les obligations de certification et de tests que doit vérifier le système de vote, ces étapes ont été franchies de manière informelle, et les résultats n'en sont pas publics. Un audit a bien été réalisé avec des procédures suivies à la lettre, mais qui paraissent inadéquates pour détecter des divergences entre le fonctionnement constaté et les objectifs ultimes du système. Le système de vote peut donc héberger des erreurs qui n'ont pas été détectées. L'identité du programme de vote du serveur est vérifiée à l'aide d'un calcul de checksum, ce qui est une procédure insuffisante : ce calcul est prévu pour détecter les erreurs de copie mais pas pour révéler les modifications volontaires. Même si la salle des serveurs est constamment filmée et gardée par un policier il n'y a aucune procédure pour vérifier qu'il n'y a eu aucun accès non autorisé par internet. Le programme a été implémenté sans que les différentes tâches soient formellement réparties entre les programmeurs, une personne seule peut intervenir sur n'importe quelle portion du code. Il apparaît donc que le programme peut être subrepticement modifié sans que cette modification ne soit décelée.

Enfin la procédure de vote multiple, imaginée pour lutter contre les pressions, est matérialisée par l'enregistrement des dates et heures précises de votes dans les journaux d'événements qui sont ensuite accessibles aux observateurs et partis. Il est donc possible de savoir si une personne a décidé de voter de nouveau. Ces informations peuvent favoriser les pressions sur les votants pour les empêcher de corriger un vote réalisé en situation de coercition.

Suisse

La Suisse expérimente le vote par internet avec prudence en n'autorisant que trois cantons (Genève, Neufchâtel et Zurich) à procéder à des expériences menées à l'aide de systèmes différents, choisis en toute autonomie [6]. Ces expériences sont ouvertes à un nombre réduit d'électeurs.

Le **canton de Genève** est propriétaire du système de vote électronique qui a été développé par le service informatique cantonal (le Centre des Technologies de l'Information de l'Etat - CTI), en collaboration avec les entreprises privées Hewlett Packard Suisse (matériel et logiciel), Wisekey (technologie de cryptage) et Blue-Infinity (sécurité).

De nombreuses études portant sur les questions juridiques et techniques ont précédé et accompagnent ce développement.

Dans le domaine des sciences politiques [3], il a été rappelé que « la légitimité dépend avant tout du *contrôle* du déroulement et du dépouillement du scrutin. » et que la publication des programmes de vote[19] ou, à défaut, son examen par des experts est recommandée, tout en pointant les limites de cette démarche.

Les rapports consacrés à la sécurité [60] [45] [18] [32] confirment l'existence de nombreuses vulnérabilités qu'il semble difficile de réduire « Il n'y a aucune protection contre des chevaux de Troie [...] qui permettraient d'intercepter, de modifier ou de détourner le vote car l'Etat n'a aucun contrôle sur le contenu du poste de travail de l'électeur. », « une fraude de grande ampleur peut s'envisager avec la participation d'une personne au service de l'Etat participant à l'exploitation du serveur. » et soulignent qu'une telle fraude peut passer inaperçue. L'impossibilité de mener un examen de l'ensemble des programmes est également exprimée[20]. Ces rapports proposent des solutions pour lutter contre le vote sur un site web usurpateur (spoofing), ou les agissements de virus, mais ces propositions ne seront pas retenues pour des raisons techniques ou ergonomiques (ne pas compliquer la procédure de vote).

Huit votes ont eu lieu depuis la première utilisation de l'application de vote en 2003, le nombre d'utilisateurs potentiels passant d'un millier à près de 90 000. Après une flambée initiale due à l'attrait de la nouveauté, le taux de vote par internet semble stagner autour de 9% [16].

Malgré les recommandations des études de sécurité, il n'y a pas d'experts à l'œuvre durant les scrutins, les seuls contrôles étant effectués par les représentants des partis mis en place initialement pour le vote par correspondance. Deux rapports récents mentionnent des expertises et même des tests de hacking, mais ces rapports ne sont pas publics[21] [17] [32].

Il semble que les gestionnaires de l'application, conscients des risques, renouvellent constamment les systèmes et les procédures mais certaines menaces sont oubliées. Par exemple, l'affirmation que le système de surveillance assure que les tentatives de fraudes ne passeront pas inaperçues est faussement rassurante. Ce système de surveillance est inopérant contre les vers et virus opérant sur le poste de l'électeur et pourrait être neutralisé en cas de fraude interne. Dans le même esprit, la mise en œuvre d'une nouvelle procédure de cryptage est trompeusement présentée comme capable de détecter l'intervention d'un virus sur le poste de l'électeur [24].

L'application de vote du canton de **Neuchâtel** s'inscrit dans un projet de guichet virtuel unique développé par les sociétés Computer Associates et Lanexpert.

Six votes ont eu lieu depuis septembre 2005, étendant la possibilité de voter par internet de 1700 à 4200 personnes. Les taux de vote par internet y sont nettement plus élevés que dans le canton de

19 Sans toutefois mesurer qu'une telle disposition reste insuffisante s'il est impossible de prouver que le programme en service est identique à celui qui a été publié

20 « La diversité des postes de travail des électeurs et la complexité des couches de logiciels rend en effet impraticable un audit exhaustif de l'application dans sa forme actuelle. »

21 Ils sont accessibles aux représentants des électeurs.

Genève mais suivent le même processus d'érosion, décroissant régulièrement de 68% à 36% [16].

Le paramétrage de l'urne électronique est un processus présenté comme hautement sécurisé par la présence de personnalités politiques et d'un juriste, pourtant a priori dénués de compétences en sécurité informatique. La procédure de comparaison des accusés de réception reçus et stockés dans l'urne n'est pas adéquate pour détecter une manipulation des votes. Le serveur de vote a résisté avec succès à des des tests d'intrusion mais il n'est pour autant pas à l'abri de toutes les attaques. De la même façon, des failles repérées au niveau du processus d'authentification lors d'un audit ont pu être comblées, mais il peut en subsister d'autres [17] [32].

Enfin, les votes sont stockés dans l'urne électronique dans leur ordre d'arrivée, ce qui peut permettre de lever le secret du vote, ils ne sont brassés qu'après décryptage.

Dans le canton de **Zurich**, le vote à distance peut être réalisé par internet mais aussi par l'envoi de messages SMS. Ici encore, le taux de participation tend à baisser régulièrement. Alors que la première expérience, sur la commune de Bülach avait vu plus d'un tiers des 4000 votants s'exprimer par internet, cette proportion est tombée autour de 8% puis 5% lorsque le vote a été étendu à environ 17 000 votants [16].

Dans les trois cantons, la carte comportant les informations nécessaires au vote par internet (identifiant et mot de passe) est envoyée à chaque électeur par simple courrier postal. Selon les systèmes, il faut fournir sa date et parfois sa commune de naissance pour parfaire l'authentification.

D'une manière générale, la faisabilité d'une fraude à grande échelle est sous-estimée, puisqu'elle est considérée comme équivalente, que l'on procède par internet ou correspondance.

Parmi les mesures envisagées pour améliorer ces applications pilotes, la conservation de tous les fichiers des événements afin de reconstituer l'urne électronique en cas de panne, ou la sauvegarde du contenu de l'urne électronique afin d'améliorer les possibilités de recours, présentent des inconvénients en ce qui concerne la préservation de l'anonymat des votes. Même si ces fichiers sont cryptés, leur divulgation permettrait à un informaticien de les décrypter et d'en révéler le contenu. Cette opération est simplifiée si les fichiers des événements contiennent le détail des messages ou des paquets transmis par le réseau. Disposer de données en quantité suffisante et de temps pour les étudier sont des facteurs facilitant ce type de fraude. La conservation de ces fichiers constitue donc une fragilité supplémentaire.

Malgré des rapports officiels trop optimistes, la Confédération Helvétique semble rester très prudente : le Conseil fédéral a décidé de ne pas autoriser le vote électronique lors des élections fédérales de 2007.

Pays-Bas

Aux Pays-Bas, lors des élections législatives du 22 novembre 2006, 20 000 expatriés ont voté avec le système de vote par internet Rijnland Internet Election System (RIES), développé par la société TTPI en collaboration avec le bureau des élections du district de Rijnland. Ce système présente la particularité de permettre aux électeurs de vérifier leur vote, et même la totalisation de l'ensemble des votes, par le calcul de différentes clés. Malheureusement offrir cette possibilité a nécessité de sacrifier le secret du vote. Celui-ci est préservé si chaque électeur détruit ses clés et si la société en charge de gérer l'application de vote détruit aussi ses clés, ce qu'il est impossible de certifier. De plus, il s'est avéré que la démarche de vérification est trop compliquée pour les simples votants qui, pour la plupart, n'ont pas su l'utiliser, tandis que la vérification de la totalisation est une procédure encore plus complexe. Par ailleurs le système apparaît aussi très vulnérable à des attaques de virus sur le poste de l'électeur et à la fraude interne [26]. D'une part les développeurs eux-mêmes ont jugé qu'il ne pourrait convenir à l'ensemble de la population, d'autre part, la commission d'observation de l'OSCE a noté que la transparence reste insuffisante pour répondre au scepticisme des électeurs [47].

Royaume-Uni

Les premières expériences, portant sur plusieurs systèmes, ont eu lieu en 2002 et se sont poursuivies en 2003 et 2004, puis 2007 mais il semble qu'elles aient toujours été menées dans l'urgence.

Lors des élections de mai 2007, des essais ont été autorisés avec trois partenaires[22]. La Commission Électorale a noté que tous les pilotes présentaient de grands risques dus à l'insuffisance des tests (tant en quantité que dans leurs modalités) en ce qui concerne la sécurité et le contrôle qualité. Le manque de transparence et de documentation détaillée a également été noté. Les programmes n'ont pas été évalués par des experts, les tests d'attaques sont restés d'un niveau insuffisant. Ces faiblesses ont été jugées comme inacceptables et la Commission Électorale a recommandé de ne pas faire d'autres expérimentations tant qu'une stratégie globale ne sera pas définie, rappelant qu'elle avait déjà émis les mêmes objections en 2003 sans être entendue [57].

Les informations permettant de voter (identifiant et mot de passe) ont été envoyées par courrier postal aux seules personnes qui s'étaient préalablement inscrites. 34% à 58% des personnes enregistrées ont effectivement voté.

La Commission Électorale souligne les risques induits par les virus que peuvent héberger les ordinateurs des électeurs, ainsi que la possibilité de fraude interne.

France

Plusieurs expériences de vote par internet ont eu lieu depuis le 21 avril 2002 (premier tour de l'élection présidentielle), date d'un vote par internet mené en parallèle du vote officiel, à Vandœuvre-lès-Nancy. La Commission Nationale Informatique et Liberté (CNIL) avait donné un avis défavorable à cette expérience relevant, entre autres, des défauts dans le cryptage des votes, et le fait que les serveurs de vote, situés à New York, échappaient à tout contrôle des autorités françaises [10]. Suite à cette expérience, la CNIL a publié des recommandations précises sur le vote électronique [11] afin de guider les futures applications. Elle a notamment précisé la nécessité de recourir à des experts extérieurs, la séparation entre les données nominatives et les bulletins de votes (stockage sur deux serveurs différents), l'attention particulière qu'il est nécessaire de porter à l'authentification de l'électeur. Elle souligne l'extrême fragilité des systèmes quant à leur sécurité et réclame des traces de fonctionnement permettant de vérifier les résultats.

L'Assemblée des Français de l'Étranger est composée de 155 conseillers[23] élus par plus de 800 000 électeurs expatriés. C'est le seul scrutin politique qui peut être par mené par correspondance en France. Dans ce cadre, le vote par internet a été proposé aux français vivant en États-Unis en juin 2003, puis a été généralisé à tous les français de l'étranger en juin 2006.

Le logiciel de vote a été conçu par la European Aeronautic Defence and Space company (EADS) et mis en pratique par Experian. Les électeurs recevaient leurs identifiant et mot de passe par courrier postal et devaient télécharger l'interface.

La CNIL a officiellement constaté l'inobservation de ses recommandations (il est impossible d'attester que les enregistrements des votes et des identités sont séparés, que les bulletins sont chiffrés sur le poste de l'électeur, que les codes personnels envoyé par courrier ont bien été délivrés à son destinataire), ainsi que l'absence d'expertise indépendante pendant le scrutin [13]. Trois experts en sécurité informatique, dont deux mandatés par des candidats, ont fourni des rapports sévères

22 Consortium mené par Election Systems and Software avec le Rushmoor Borough Council et le South Bucks District Council ; Opt2Vote avec Sheffield City et Shrewsbury & Atcham Borough Council ; consortium mené par Tata Consultancy Services avec le Swindon Borough Council.

23 Les 155 conseillers élisent douze sénateurs représentant les Français établis hors de France.

soulignant en particulier le manque de transparence[24], l'inadéquation des tests[25], la difficulté à vérifier l'authenticité du programme[26], la possibilité d'une fraude massive[27], les éventuelles conséquences d'erreurs informatiques[28] ou d'agissements de virus, l'incapacité à détecter des atteintes à la sincérité du scrutin[29]. Ces expertises externes contredisent le Forum des Droits sur l'Internet (FDI) qui affirme que la fraude électorale peut être limitée par le recours au vote électronique. Le FDI semble ignorer l'éventualité des fraudes internes et n'a paradoxalement pas tiré les conclusions qui auraient dû découler de son analyse des risques liés à la mise en place du vote électronique [21].

États-Unis

Les premières expérimentations ont eu lieu en Alaska et en Arizona durant les élections primaires de 2000. Ensuite le système Secure Electronic Registration and Voting Experiment (SERVE) a été développé afin de permettre aux militaires américains expatriés de voter par internet pour les élections présidentielles de 2004. Une commission indépendante formée de plusieurs spécialistes universitaires en sécurité informatique a été chargée d'évaluer ce système. Leur rapport témoigne d'une étude très poussée de ce système en particulier et des systèmes de vote par internet en général [28]. Cette étude a eu pour conséquence l'abandon de toute idée de vote par internet par les États-Unis.

Bahreïn

Après avoir observé avec enthousiasme les expériences de vote par internet en Estonie en 2005, le Bahreïn avait envisagé ce mode de vote pour les élections de novembre 2006. Le Central Informatics Organization (CIO) a même développé un système électronique de vote dont les programmes ont été examinés par les experts de Microsoft [4]. Ce projet a été finalement abandonné

24 « La dématérialisation de l'information place de fait l'ensemble des participants au processus de vote dans la situation de la caverne de Platon : personne 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. » OSCE [48]

« L'observation directe du déroulement d'un processus électronique n'est pas possible. Comment dans ce cas garantir la transparence des opérations pour établir la confiance ? » « qu'est-ce qui prouve que l'urne est vide quand l'écran affiche zéro » B. Lang [31]

« Il ressort de cette analyse que *le système informatique sur lequel repose la sincérité et donc la confiance du scrutin* n'est auditable que par des représentants du maître d'œuvre et du maître d'ouvrage, mais aucunement par le bureau (président et assesseurs) pourtant en charge du "*bon déroulement des opérations électorales"* et notamment "*de la mise en œuvre des dispositifs de sécurité."* Rien n'indique par ailleurs que les délégués des associations représentatives, c'est-à-dire en fait des candidats, soient logés à meilleure enseigne. » B. Lang [31]

25 « Does this program do an accurate and faithful job of interpreting the ballots? One cannot tell just by running tests before the election, because it's easy to write computer programs that behave one way before the 12th of June and another way after. » W. Appel [2]

26 « Even if the *assesseurs* could examine the programs and understand them, it is extremely difficult to know whether that is the program actually running on the *Urne* computer. » W. Appel [2]

27 « Si la fraude est plus difficile, plus technique, dans le cas du vote électronique, elle peut aussi être plus efficace, plus massive, en étant automatisée. Intercepter les courriers des votes par correspondance est une tâche considérable à grande échelle, alors qu'il est concevable que la violation des communications électroniques vers une adresse donnée soit automatisée. » B. Lang [31]

28 « Ceci est d'autant plus inquiétant que, dans l'état actuel des techniques, un système de cette complexité contient nécessairement des bogues. Celles-ci ont peu de chance d'être identifiées dans de telles conditions de secret. » B. Lang [31]

29 « De même rien ne permet de penser, ni là encore de penser le contraire, que le résultat de l'élection qui sera effectivement affiché sur l'écran au moment du dépouillement numérique correspondra bien à la réalité des suffrages que voulaient exprimer les électeurs devant leurs ordinateurs. » F. Pellegrini [50]

« La dématérialisation du processus de vote vide le rôle d'assesseur de sa substance, et par là même enlève toute possibilité d'attester de la sincérité du processus de vote. » F. Pellegrini [50]

en septembre 2006 lorsque des soupçons concernant une conspiration visant la procédure de vote ont été révélés.

Autres

D'autres pays ont testé ponctuellement le vote par internet.

Des tests officieux dans le secteur public ou privé ont été mené en Italie (élections administratives du 17 novembre 2002 à Crémone), en Catalogne, en Espagne[30], en Allemagne, au Canada (élections locales en Ontario en 2003) et au Portugal. [32].

Le Japon a vu les élections communales par internet annulées par une cour de justice et a maintenant abandonné cette procédure de vote.

D'autres pays, comme l'Autriche, la Suède, la Norvège, le Luxembourg ou la Bulgarie ont lancé des commissions politiques qui étudient la question du vote électronique [32]. La Corée du Sud prévoit des expérimentations en 2012.

Bilan

Il est difficile de dresser un bilan de toutes ces expériences. Cependant, quelques éléments récurrents peuvent être mis en évidence.

Les commissions qui définissent les spécifications des systèmes de vote par internet méconnaissent le domaine de l'informatique et ses spécificités. Par exemple, les procédures prévoient souvent que toutes les données soient détruites après l'expiration des délais de contentieux, sans que l'étendue de cette opération ne soit précisée. Or l'effacement simple de fichiers par les commandes informatiques usuelles ne suffit pas à effectivement effacer toutes les données, seul le registre contenant la liste des fichiers est mis à jour, mais la zone de la mémoire où sont inscrites les données reste intacte jusqu'à ce que d'autres données y soient inscrites. Localiser leur lieu de stockage en mémoire et y inscrire, par exemple, la valeur zéro, autant de fois que nécessaire serait déjà une procédure plus efficace, mais elle ne suffirait pas à garantir que les données ne peuvent être retrouvées. Finalement, la seule manière de détruire avec efficacité des informations écrites sur un support électronique est de détruire, physiquement, ce support.

D'une manière générale, on constate une dégradation systématique des informations techniques et éthiques, au fur et à mesure de leur migration depuis les spécialistes (en sciences politiques ou en informatique) vers les structures institutionnelles puis les électeurs. Les failles de sécurité, les carences éthiques, clairement énoncées par les spécialistes, sont passées sous silence lorsque les systèmes de vote sont l'objet d'opérations de communication.

Voici quelques exemple extraits de documents de communication visant les électeurs :

> « The e-voting system described in the document enables, provided that sufficient organisational, physical and technical security measures are implemented, a basis for conducting e-voting at least as securely as traditional voting. » [40]
>
> « Le vote par Internet est plus sûr que le vote postal [...]. » [56]
>
> « Il va de soit que toutes les mesures de sécurité en termes d'authentification du votant, d'intégrité des données transmises, de confidentialité du vote et d'inviolabilité du vote sont prises afin de garantir la validité du scrutin. » [42]

Comme toute transparence directe est exclue, les membres des bureaux de vote ainsi que les

30 Le test, sans valeur légale, a été mené parallèlement à l'élection parlementaire du 14 mars 2004 à Lugo, à Zamora et à Toro, puis du 1er au 18 février 2005. Il a potentiellement concerné 2 millions de votants . La dernière expérience avait suscité de vives critiques de la part des universitaires de l'Observatoire du Vote Électronique du fait des nombreuses failles de sécurité.

délégués des candidats sont dépossédés de leur pouvoir de contrôle[31]. Des processus de transparence indirecte fondés sur les travaux d'experts sont donc déployés pour remédier à cette absence (même si ce principe est largement discutable). Les systèmes de vote que nous avons étudiés montrent que la transparence indirecte est constamment contrariée : les expertises ne sont pas réalisées ou les rapports d'expertises ne sont pas publics. Enfin, lorsque les rapports sont publics, leur contenu est si inquiétant que les expériences sont stoppées.

V - Perspectives

Dans le domaine de la vérification des résultats, des cryptographes ont produit d'audacieuses propositions adaptées aux ordinateurs de vote dématérialisant les bulletins [9] mais il reste plusieurs inconvénients. D'abord, ces innovations sont incompréhensibles pour des personnes n'ayant pas des connaissances pointues dans le domaine, ensuite, le cryptage peut permettre d'encoder des informations supplémentaires (il peut s'agir de l'identité du votant, ou de dévoiler le vote alors même qu'il est crypté) [51]. Enfin, la correction de la totalisation est vérifiée par des audits portant sur les processus de construction des bulletins, de mélange des votes, etc. et n'est donc pas accessible à tous. Les cryptographes reconnaissent volontiers que si les protocoles qu'ils établissent peuvent être théoriquement sûrs, leur implémentation et leur utilisation font apparaître des vulnérabilités non prévues, notamment dans les interactions avec l'environnement : matériel, logiciels, électeurs, gestionnaires des élections.

Concernant les vers et virus, l'idée de complexifier la reconnaissance de leurs cibles, qu'il s'agisse de logiciels ou de communications, constitue un nouvel axe de recherche. Plusieurs procédés comme l'"offuscation", la génération automatique de différentes versions des logiciels ou la dissimulation des adresses des destinataires lors de communications peuvent être envisagés [29]. Cette approche présente l'inconvénient d'introduire des processus complexes ouvrant de nouvelles failles de sécurité qu'il sera plus difficile d'identifier et de sécuriser. Au contraire, une démarche globale de sécurité s'appuie avant tout sur des procédés simples. Ces nouvelles idées, exploitables dans le domaine du commerce en ligne[32], ne sont donc pas adaptées aux contraintes des scrutins démocratiques.

La lutte contre la fraude interne reste également un sujet extrêmement préoccupant. Un programme malveillant peut être dissimulé sur le serveur de vote et modifier les résultats en toute discrétion. Alors que ces risques sont attestés, il est difficile de mettre en place des mesures efficaces. Les méthodes de développement formelles visent à éviter les erreurs involontaires, il n'existe pas, à notre connaissance, de recherches spécifiques sur la détection de portions de programmes volontairement erronées (par rapport aux spécifications).

Actuellement, la seule démarche consisterait à écrire les spécifications précises des logiciels, puis à effectuer une construction systématique des programmes par des opérateurs mathématiques, sans intervention manuelle. Théorique, cette approche est rarement suivie de bout en bout du fait de la difficulté à écrire des spécifications assez précises et du coût de la démarche pour des projets de grande taille. En pratique, des modules indépendants sont produits de cette manière, tandis que des programmeurs humains écrivent encore une partie des programmes. Dans ce cas, il faut mettre en œuvre des revues croisées des programmes manuellement écrits en faisant intervenir plusieurs spécialistes. Les spécifications formelles devraient également faire l'objet de revues croisées.

---

31 « Il ressort de cette analyse que *le système informatique sur lequel repose la sincérité et donc la confiance du scrutin* n'est auditable que par des représentants du maître d'œuvre et du maître d'ouvrage, mais aucunement par le bureau (président et assesseurs) pourtant en charge du "*bon déroulement des opérations électorales"* et notamment "*de la mise en œuvre des dispositifs de sécurité."* Rien n'indique par ailleurs que les délégués des associations représentatives, c'est-à-dire en fait des candidats, soient logés à meilleure enseigne. » B. Lang [31]

32 Dans le domaine du commerce en ligne les transactions sont observées, puis vérifiées a posteriori : l'acheteur et le vendeur, le bien échangé ainsi que sa valeur sont connus, les archives des transactions sont conservées.

Les coûts d'un projet mené selon ces principes sont très élevés, le développement d'applications de vote est loin de suivre de tels standards. De plus, bien que rigoureuses et contraignantes, ces méthodes ne peuvent garantir que les risques de fraude internes seraient complètement annihilés : une portion de code malicieux pourrait être dissimulée dans le compilateur ou l'interpréteur de code.

Il apparaît finalement que l'informatique est démunie face à ce problème. Écrire un programme de taille importante ne comportant plus d'erreurs reste considéré comme un exploit. Or, garantir qu'un programme n'héberge aucune "erreur" volontairement dissimulée est une tâche bien plus complexe. Ni les tests[33], ni les expertises des programmes ne sont suffisants, comme nous le rappelle Ken Thompson, co-concepteur du système UNIX.

> « You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.) No amount of source-level verification or scrutiny will protect you from using untrusted code. (...) As the level of program gets lower, these bugs will be harder and harder to detect. A well installed microcode bug will be almost impossible to detect. » [58]

Conclusion

Cette étude a présenté les failles du vote par internet dans les domaines technique et démocratique. Elle a montré que si le transfert des votes de l'électeur vers le bureau centralisateur (point faible du vote par correspondance postale) peut prétendre être sécurisé par des procédés cryptographiques, l'utilisation de l'informatique introduit de nouvelles fragilités compromettant la sécurité du processus dans sa globalité : les votes peuvent être modifiés lors de leur émission sur le poste de l'électeur, il n'y a aucun moyen efficace de se prémunir contre la fraude interne alors que celle-ci peut être massive et invisible.
Plus fondamentalement, l'opacité des traitements informatiques interdit, par nature, toute transparence directe et les processus de transparence indirecte censés compenser cette carence démocratique se révèlent loin d'être satisfaisants.
Il semble donc que le vote par internet rompt avec le mouvement d'amélioration des qualités démocratiques des élections qui prévalait depuis l'introduction du scrutin universel.

Loin des mises en garde des scientifiques, les entreprises exploitant ce nouveau marché n'hésitent pas à promettre l'impossible à des autorités séduites par l'image de modernité dont ils peuvent bénéficier et les économies induites en cas de généralisation (diminution du nombre de bureaux de vote traditionnels), n'hésitant pas à sacrifier au passage la transparence, et donc la sincérité des élections et la confiance des électeurs.

> « The clear consensus of computer-science experts around the world who have studied these issues is that Internet elections cannot be trusted, for all the reasons that I have explained: the voters and political parties cannot audit the operation of the software and hardware that serves as the real *bureau de vote*. Therefore it is not clear to me how the *assesseurs* can sign anything but a surrealist image of a true *procès-verbal*.. » [2]

Bibliographie

[1] ACM. ACM Recommends Integrity, Security, Usability in E-voting, (2004).

[2] APPEL (W.) Ceci n'est pas une urne: On the Internet vote for the Assemblée des Français de l'étranger, (juin 2006).

[3] AUER (A.), VON ARX (N.) La légitimité des procédures de vote : les défis du e-voting, *faculté de droit de l'Université de Genève,* Suisse, (décembre 2001).

33 « Il existe en outre un théorème fondamental de la théorie de l'informatique selon lequel il ne peut y avoir de test général pour décider si un système et ses logiciels hébergent ou non un code malveillant. » R. Oppliger [45]

[4] BAHRAIN NEWS AGENCY. King briefed on new e-voting system, (26 juin 2006).

[5] BIRDSALL (S.) The democratic divide, *first monday, peer-reviewed journal on the internet*, (2005).

[6] BRAUN (N.), BRÄNDLI (D.) Swiss E-Voting Pilot Projects: Evaluation, Situation Analysis and How to Proceed. *Electronic Voting 2006, 2nd International Workshop*, GI-Edition, Lecture Notes in Informatics, Robert Krimmer (Ed.), p.27-36, Bregenz, Austria, (August, 2nd-4th 2006).

[7] CEV. Commission on Electronic Voting, Secrecy, Accuracy and Testing of the Chosen Electronic System", first report, (December 2004).

[8] CEV. Commission on Electronic voting. Secrecy, Accuracy and Testing of the Chosen Electronic Voting System. second report, (July 2006).

[9] CHAUM (D.) Secret-ballot receipts: True voter-verifiable elections. *IEEE Security and Privacy*, 2(1), p.38-47, (January-February 2004).

[10] CNIL. Un avis défavorable de la CNIL à une expérimentation de vote électronique par internet aux élections présidentielles des 21 avril et 5 mai 2002. communiqué (10 avril 2002).

[11] CNIL. Délibération n° 03-036 du 1er juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique, (1er juillet 2003)

[12] CNIL. La cybersurveillance des salariés. rapport de la Commission Nationale Informatique et Libertés, (2003).

[13] CNIL. Le vote électronique pour les élections des Français de l'étranger, (2006).

[14] COLEMAN (S.) Internet voting and democratic politics in an age of crisis. in Trechsel A. (ed.) *The European Union and E-Voting: Addressing The European Parliament's Internet Voting Challenge,* Londres: Routledge, p.223-237, (2005)

[15] COMMISSION EUROPÉENNE POUR LA DÉMOCRATIE PAR LE DROIT (COMMISSION DE VENISE). Code de bonne conduite en matière électorale, (juillet 2002).

[16] CONFÉDÉRATION SUISSE. Tableau synoptique des essais de vote électronique ayant eu lieu en Suisse de 2003 à 2007, (15 août 2007).

[17] CONSEIL D'ETAT. Rapport du Conseil d'Etat au Grand Conseil sur le projet genevois de vote électronique", RD639, Confédération Suisse, (24 mai 2006).

[18] CONSEIL FÉDÉRAL. Rapport sur le vote électronique Chances, risques et faisabilité, n°02.009, Confédération Suisse, (9 janvier 2002).

[19] DESWARTE (Y.), MALCHOR (C. A.) Current and future privacy enhancing technologies for the Internet. Ann. Télécommun., 61, n°3-4, p.399-417, (2005).

[20] DILL (D.), DOHERTY (W.) Electronic Voting Systems. *Report for the National Research Council*, (November 22, 2004).

[21] LE FORUM DES DROITS SUR L'INTERNET. Recommandation - Quel avenir pour le vote électronique en France ?, (26 septembre 2003).

[22] GÓMEZ OLIVA (A.), SÁNCHEZ GARCIA (S.), PÉREZ BELLEBONI (E.) Contributions to traditional electronic systems in order to reinforce citizen confidence. *Electronic Voting 2006, 2nd International Workshop*, GI-Edition, Lecture Notes in Informatics, Robert Krimmer (Ed.), p.39-49, Bregenz, Austria, (August, 2nd-4th 2006).

[23] GORMAN (O.) The Effect of Cosmic Rays on the Soft Error Rate of a DRAM at Ground Level, *IEEE Transactions on Electron Devices*, vol.41, issue 4, p.553-557, (April 1994).

[24] HENSLER (R.) Le vote par Internet, la forme la plus sûre de vote à distance, *1er Geneva Security Forum*, (21 juin 2007).

[25] HOFF (J.) Towards a theory of Democracy for the information age. Discussion paper for the Democracy Platform UK-Nordic Meeting, (16-17 septembre 1999).

[26] HUBBERS (E.), JACOBS (B.), PIETERS (W.) RIES - Internet Voting in Action. In R. Bilof*, Proceedings of the 29th Annual International Computer Software and Applications Conference, COMPSAC'05*, pages 417-424. IEEE Computer Society, (July 26-28, 2005).

[27] JEFFERSON (D.R.), RUBIN (A.D.), SIMON (B.), WAGNER (D.) Analyzing Internet Voting Security. *Communications of the ACM*, vol.47, n°10, p.59-64, (October 2004).

[28] JEFFERSON (D.R.), RUBIN (A.D.), SIMON (B.), WAGNER (D.) A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE), (January 2004).

[29] JONES (D.W.) Trustworthy Systems on Untrusted Machines. *Workshop on the Future of Voting Technology in a Networked Environment*, Georgia Tech. Research Institute, Atlanta, (June 4-5, 2002).

[30] KOHNO (T.), STUBBLEFIELD (A.), RUBIN (A.D.), WALLACH (D.S.) Analysis of an Electronic Voting System. *IEEE Symposium on Security and Privacy*, Oakland, CA, (May, 2004).

[31] LANG (B.) Rapport sur l'usage du vote électronique par l'Internet pour les élections à l'Assemblée des Français

de l'Étranger de juin 2006, (23 juin 2006).

[32] LEUENBERGER (M.), HUBER-HOTZ (A.) Rapport sur les projets pilotes en matière de vote électronique. *Conseil fédéral suisse*, rapport n°06.056, (31 mai 2006).

[33] LOI n°75-1329 du 31 décembre 1975. codifiée sous l'article L72-1 du code électoral, (1975).

[34] MADISE (Ü.), MARTENS (T.) E-voting in Estonia 2005. The first pratice of country-wide binding Internet voting in the world. *Electronic Voting 2006, 2nd International Workshop*, GI-Edition, Lecture Notes in Informatics, Robert Krimmer (Ed.), p.15-26, Bregenz, Austria, (August, 2nd-4th, 2006).

[35] MANIN (B) Principes du gouvernement représentatif, Champs, Flammarion, (1996).

[36] MATSUMOTO (T.), MATSUMOTO (H.), K. YAMADA (K.), HOSHINO (S.) Impact of artificial "gummy" fingers on fingerprint systems, *Proceedings of SPIE*, Optical Security and Counterfeit Deterrence Techniques IV, vol.4677, (2002).

[37] MEISSNER (N.), HARTMANN (V.), RICHTER (D.) Verifiability and Other Technical Requirements for Online Voting Systems. *« Electronic Voting in Europe – Technology, Law, Politics and Society », workshop of the ESF TED Programme together with GI and OCG*, July, 7th-9th, 2004, Austria, (2004).

[38] MERCURI (R.) A Better Ballot Box?. *IEEE Spectrum Online*, (October 2002).

[39] MOORE (D.), PAXSON (V.), SAVAGE (S.), SHANNON (C.), STANIFORD (S.), WEAVER (N.) Inside the Slammer worm. *IEEE Security and Privacy*, (2003).

[40] THE NATIONAL ELECTION COMMITTEE. E-Voting System Overview, Tallinn, Estonia, (2005).

[41] NATIONS UNIES. Déclaration universelle des droits de l'homme, (1948).

[42] NEUFCHÂTEL. page "E-démocratie" du site de la ville de Neufchâtel.

[43] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC, (November 2006).

[44] OFFERLÉ (M.) Un homme, une voix ? Histoire du suffrage universel. *Gallimard, Collection Découvertes Gallimard*, ISBN : 2-07-076406-0 (br.), (2002).

[45] OPPLIGER (R.) Traitement du problème de la sécurité des plates-formes pour le vote par Internet à Genève, (3 mai 2002).

[46] OSCE/ODIHR. USA 2 November 2004 Elections - OSCE/ODIHR Needs Assement Mission Report. 7-10 September 2004, Warsaw, (28 September 2004).

[47] OSCE/ODIHR. The Netherlands Parliamentary Elections 22 November 2006 OSCE/ODIHR Election Assessment Mission Report, (12 March 2007).

[48] OSCE/ODIHR. Republic of Estonia parliamentary elections 4 March 2007 OSCE/ODIHR Election Assessment Mission Report, (28 June 2007).

[49] OSCE, Manuel d'observation des élections, cinquième édition, ISBN 83-60190-02-X, (2005).

[50] PELLEGRINI (F.) Rapport d'observations, (juin 2006).

[51] RYAN (P.Y.A.), PEACOK (T.) Prêt à Voter: Systems Perspective, (September 20, 2005).

[52] RUBIN (A.D.) Security considerations for remote electronic voting over the internet. *The magazine of Usenix & Sage*, vol.26, number1, p.20-28, (February 2001).

[53] SCHNEIER (B.) The Trojan Horse Race. *Inside Risks 111, Communications of the ACM*, vol.42, n°9, (September 1999).

[54] SERVICE CENTRAL DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION. Délégation Interministérielle pour la Sécurité des Systèmes d'Information, La menace et les attaques informatiques, *rapport n° 650/DISSI/SCSSI*, (28 mars 1994).

[55] SIMONS (B.) Electronic Voting Systems: the Good, the Bad, and the Stupid. *ACM Queue* vol.2, no.7, (October 2004).

[56] SITE WEB DU CANTON DE GENÈVE. Foire aux Questions.

[57] THE ELECTORAL COMMISSION. Electronic voting - May 2007 electoral pilot schemes, (August 2007).

[58] THOMPSON (K.) Reflections on Trusting Trust. *Communication of the ACM*, vol.27, n°8, p.761-763, (August 1984).

[59] VOLKAMER (M.), GRIMM (R.) Multiple Casts in Online Voting: Analyzing Chances. *Electronic Voting 2006, 2nd International Workshop*, GI-Edition, Lecture Notes in Informatics, Robert Krimmer (Ed.), p.97-106, Bregenz, Austria, (August, 2nd-4th, 2006).

[60] WENGER (M.) Rapport du Comité Sécurité sur l'application de vote par Internet, (28 janvier 2002).

[61] WOLF (P.) de l'authentification biométrique", Sécurité Informatique, n° 46, p.1-6, (octobre 2003).