HAL
archives-ouvertes.fr

Le vote électronique en France : opaque & invérifiable

Chantal Enguehard

▶ **To cite this version:**

Chantal Enguehard. Le vote électronique en France : opaque & invérifiable. Terminal. Technologie de l'information, culture & société, L'Harmattan / CREIS, 2007, pp.199-214. halshs-00085071

HAL Id: halshs-00085071
https://halshs.archives-ouvertes.fr/halshs-00085071

Submitted on 7 Aug 2009

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Enguehard, C. Le vote électronique en France : opaque & invérifiable ! Terminal, p.199-214, #99-100, printemps 2007.

Le vote électronique en France : opaque & invérifiable

Chantal Enguehard, LINA, Université de Nantes, France
chantal.enguehard@univ-nantes.fr

Introduction

Cet article se limite au vote politique (élections de représentants, référendum) et ne traite donc pas des autres types d'élections (élections professionnelles, étudiantes, etc.).

L'utilisation d'ordinateurs de vote dans la procédure électorale en France est très récente. Elle n'a pas fait l'objet d'une information auprès des citoyens au niveau national[1] et encore moins de débats. Pourtant, l'introduction de cette technologie modifie profondément le procédé par lequel le peuple délègue son pouvoir aux élus qui le représentent.

Il faut souligner que l'utilisation d'ordinateurs de vote peut participer à l'amélioration de la procédure électorale en permettant, par exemple, à tous les candidats d'être effectivement présentés aux électeurs, ce qui n'est pas le cas actuellement puisque certains "petits candidats" ne peuvent remettre des bulletins à leur nom dans tous les bureaux de vote. Mais les ordinateurs de vote représentent également un marché émergent, au développement prometteur, sur lequel se pressent de nombreuses entreprises désireuses d'équiper nos bureaux de vote. Il s'agit d'examiner comment s'articulent trois réalités du vote électronique : le discours marchand des entreprises, les textes issus du monde politique et les exigences de sécurité informatique que doivent remplir ces dispositifs.

Évolution de la procédure de vote en France

Les lois

L'article 3 de la Constitution de la République Française de 1958 précise : « *La souveraineté nationale appartient au peuple qui l'exerce par ses représentants et par la voie du référendum*. » tandis que l'article 2 rappelle le principe de la République Française : « *gouvernement du peuple, par le peuple et pour le peuple* » [Conseil constitutionnel 1958]. Les élections représentent le transfert de la souveraineté du peuple à ses représentants, il est donc essentiel que le processus de désignation des représentants (les élections politiques) soit transparent et honnête, comme le précise le code électoral[2].

Un décret (n ❑ 64-1086 du 27 octobre 1964) puis 3 lois (n ❑ 88-1262 du 30 décembre 1988 art. 3, 4 et 5, n ❑ 2004-1343 du 9 décembre 2004 art. 14 1 ❑, n ❑ 2005-102 du 11 février 2005 art. 72) fixent le cadre légal du vote à l'aide d'ordinateurs de vote en France [Légifrance 2005]. Celui-ci est réservé aux communes de plus de 3500 habitants. Il doit se dérouler sur un ordinateur d'un modèle agréé par arrêté du ministre de l'Intérieur et doit vérifier huit critères que l'on peut qualifier de bons sens commun (le vote doit se dérouler dans un isoloir, doit être possible pour les personnes handicapées, doit permettre le vote blanc, etc.).

---

1 Le site du Ministère de l'Intérieur ne présente que les élections selon la procédure traditionnelle http://www.interieur.gouv.fr/rubriques/ (cliquer sur "les élections" dans le menu "A votre service") (consulté le 16 mai 2006)

2 Le code électoral énonce cinq critères que doit respecter une élection : transparence, confidentialité, anonymat, sincérité (le bulletin dans l'urne est-il celui que j'ai choisi ? Sera-t-il compté ?), unicité (un vote par personne).

Le vote

vote électronique

Le vote électronique désigne trois types de systèmes informatiques : les ordinateurs de vote (dénommés "machines à voter" par le code électoral[3]), le vote par internet et les kiosques électroniques.
Les ordinateurs de vote enregistrent les votes des électeurs pendant le scrutin puis les additionnent lors du dépouillement.
Le vote d'un citoyen se déroule ainsi :

- le citoyen entre dans l'isoloir
- il consulte les choix présentés sur l'écran
- il choisit en pressant un bouton
- son choix est affiché sur l'écran
- il confirme son choix
- il sort de l'isoloir
- il émarge.

Nous remarquons qu'à aucun moment l'électeur ne peut vérifier que son vote a été effectivement bien noté.

Trois modèles d'ordinateurs de vote ont été agréés par le Ministère de l'Intérieur : la version "2.07" de l'ordinateur de vote de la société NEDAP, le modèle "iVotronic" de la société ES&S[4] Datamatique et le modèle "Point & Vote" de la société Indra Sistemas SA [Intérieur 01].

Le vote par Internet a pour objectif d'autoriser le vote à l'aide de n'importe quel ordinateur connecté à Internet. La procédure comprend l'authentification de l'électeur, le vote lui-même, et l'émargement. Les kiosques électroniques sont des terminaux placés dans les bureaux de vote et reliés à un ordinateur central (serveur). Ils se chargent de l'authentification, de l'émargement et du vote, les choix des électeurs sont transmis au serveur pour enregistrement. C'est le serveur qui se charge du dépouillement.

Cet article traite de problèmes qui sont communs à ces trois dispositifs mais ne détaille pas les spécificités du vote par Internet ou à l'aide de kiosques électroniques.

vote traditionnel avec bulletin papier

La procédure actuelle de vote, qui utilise des bulletins en papier, n'utilise aucun dispositif informatique.

- le citoyen prend des bulletins (d'au moins deux candidats différents) et une enveloppe
- il entre dans l'isoloir
- il met le bulletin de son choix dans l'enveloppe
- il sort de l'isoloir et glisse l'enveloppe dans l'urne transparente et visible de tous
- il émarge.

Le dépouillement

Dans tous les cas le dépouillement se déroule après la clôture du vote.

ordinateurs de vote

Dans la procédure électronique, le président du bureau de vote (en présence d'assesseurs) appuie sur un bouton, l'ordinateur donne les résultats sous la forme d'un ticket imprimé qui est agrafé au procès-verbal et dont les résultats sont recopiés sur ce même procès-verbal. Ces résultats sont également inscrits dans la carte mémoire de l'ordinateur de vote qui peut être éventuellement transmise à la mairie pour totalisation (mais c'est le procès-verbal qui fait foi).

Nous remarquons immédiatement que la procédure électronique ne permet pas aux citoyens de participer au dépouillement puisque l'ordinateur le réalise en toute opacité sans qu'il soit possible de vérifier ses résultats.

---

3 Le terme de "machines à voter" a été introduit dans le code électoral en 1969, époque où il ne s'agissait pas d'informatique. Il n'est plus approprié aux ordinateurs actuellement utilisés.

4 Election Systems and Software

Le contrôle du vote échappe aux citoyens qui doivent faire "confiance" à un ordinateur.

vote traditionnel avec bulletin papier

Dans la procédure classique, le dépouillement est effectué par des scrutateurs (quatre par bureau de vote) aidés du président du bureau de vote et de un ou plusieurs assesseurs. N'importe quel citoyen peut assister au dépouillement et en contrôler l'honnêteté.

Les spécialistes de l'informatique

Recommandations et risques

Les chercheurs en informatique se sont intéressés au vote électronique depuis son apparition et ont produit des critères visant à garantir que l'ordinateur de vote fonctionne effectivement comme il doit fonctionner [Neumann 1993]. Ces critères sont largement inspirés des critères de sécurité actuellement en vigueur en informatique. En voici quelques-uns (légèrement adaptés à la situation française). Cette liste n'est pas exhaustive et si un seul de ces critères n'est pas respecté, le système informatique ne peut être considéré comme sécurisé, autrement dit, la procédure de vote ne peut se dérouler dans des conditions satisfaisantes.

Un ordinateur non sécurisé présente des risques importants de dysfonctionnement majeur, il est susceptible, en particulier, de donner des résultats qui ne reflètent pas la réalité du vote. Comme nous le verrons plus loin, des cas de dysfonctionnement se sont déjà produits dans d'autres pays utilisant des systèmes de vote électronique depuis plusieurs années.

Intégrité : le système (matériel et logiciel ainsi que les paramètres initiaux et la configuration générale), une fois certifié, ne doit pas être modifié, et ne doit pas pouvoir être modifié. Les informaticiens savent qu'il est facile de modifier un programme avec une intention malveillante par l'insertion d'un cheval de Troie[5], ou d'une porte arrière. Ces mécanismes sont particulièrement discrets et quasi impossibles à détecter car ils ne sont pas forcément statiques. Ils peuvent être générés par le programme et n'apparaître que pendant de brefs instants pour rester totalement invisibles le reste du temps [Thompson 1984]. Il faut souligner que la présence d'un checksum censé vérifier l'intégrité d'un système n'empêche nullement la présence de tels procédés malveillants[6]. La présence d'un mécanisme de super-utilisateur peut aussi faciliter la corruption du système.

Ouverture : le système (matériel, programmes, circuits intégrés supplémentaires, documentation) doivent pouvoir être inspectés à n'importe quel moment, même s'ils sont protégés par le secret industriel. Les systèmes propriétaires que l'on ne peut pas vérifier sont fortement suspects. Même en présence d'un système ouvert il est possible qu'une inspection détaillée ne détecte pas un procédé malveillant comme un cheval de Troie ou des lignes de programmes qui se modifient elles-mêmes, ou une partie du programme qui ne correspond pas à la documentation afférente.

Disponibilité : le système doit être protégé contre toute tentative, frauduleuse ou non, de corrompre son fonctionnement. Un système en état de marche doit pouvoir être utilisé à n'importe quel moment.

---

5 Un "**Cheval de Troie**" (en anglais *trojan horse*) est un programme informatique limité à quelque lignes et qui effectue des opérations malveillantes et à l'insu de l'utilisateur. Généralement il donne un accès à l'ordinateur sur laquelle il est exécuté en ouvrant une **porte dérobée** (en anglais *backdoor*). Il est extrêmement difficile de détecter un tel programme.

« 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 . » [Thompson 1984]

6 Le checksum d'un fichier est une séquence de chiffres et de lettres obtenue de manière précise (mais non unique) à partir d'un fichier afin de savoir s'il a été altéré. Un checksum permet de détecter quasiment toute modification *accidentelle* mais ne protège pas des modifications *intentionnelles.*

Sûreté : la méthode de développement du système (architecture, implémentation, maintenance, etc.) doit minimiser les erreurs (bugs) et l'insertion malveillante de lignes de programme ayant pour intention d'en corrompre le fonctionnement. Il existe différentes techniques visant à accroître la sûreté d'un système, mais aucune de ces méthodes n'est infaillible. Tester un programme avec succès ne prouve en rien son intégrité.

Documentation et tests : l'architecture du système, son implémentation, les pratiques de développement, les procédures à suivre pour l'utiliser et les procédures de tests doivent être suffisamment documentées. La documentation doit également décrire quelles mesures de sécurité ont été prises concernant chacune de ces étapes.

Intégrité des personnes : l'intégrité de toutes les personnes impliquées dans le développement, l'utilisation ou l'administration d'ordinateurs de vote doit être vérifiée. Les personnes ayant été condamnées pour des crimes ou des fraudes doivent être écartées.

Vérification : il doit être possible de recompter les votes manuellement, et les procédures de recomptage manuel doivent faire partie des connaissances détenues par le président du bureau de vote.

Mémoires : les mémoires sur lesquelles sont inscrits le programme et les paramètres ne doivent être accessibles qu'en lecture pour éviter toute modification ultérieure, tandis que les mémoires recueillant les votes doivent être non réinscriptibles (once-writable memories).

Fiabilité : Aucun ordinateur n'est complètement fiable. Dans le cas de systèmes de vote la moindre inversion de la valeur d'un bit peut provoquer une erreur de une, 1024 ou encore 65 536 voix.

Il faut souligner que respecter les critères de sécurité entraîne un surcoût important : plus le développement du système a été réalisé en limitant les coûts, plus ce système sera susceptible de ne pas fonctionner comme il le devrait.

Analyse

Nombre de ces critères ne peuvent être respectés avec un coût de développement raisonnable, et il faut bien admettre que l'action d'une seule personne peut corrompre le fonctionnement d'un ordinateur de vote. L'ordinateur peut également simplement dysfonctionner à cause d'une erreur dans son programme. Prenons l'exemple de la NASA ; cet institut développe les programmes les plus sûrs du monde car des vies humaines et des sommes considérables d'argent dépendent de leur bon fonctionnement. Bien que les ingénieurs de la NASA utilisent des techniques très avancées pour s'assurer que leurs programmes comportent aussi peu d'erreurs que possible, ils savent également qu'il en subsiste toujours [Fishman 1996].

Il faut accepter que **les ordinateurs ne sont pas infaillibles**, et que toute affirmation du contraire tient davantage de la croyance que de la logique.

La fragilité des systèmes informatiques d'une manière générale, qu'il s'agisse d'une fragilité due à des erreurs involontaires ou à l'intrusion de lignes de programme malveillantes, est largement admise dans la communauté des informaticiens professionnels, que ceux-ci évoluent dans le monde industriel ou dans celui de la recherche. Aussi, les programmes sont-ils toujours assujettis au contrôle de leur fonctionnement dans le monde réel. Si le programme pilote une fusée, celle-ci atteindra son objectif, ou bien déviera de sa route et explosera[7], s'il y a une erreur de calcul dans votre compte en banque, vous vous en apercevrez en vérifiant votre relevé de comptes, si le robot qui réalise une pièce mécanique dévie du plan prévu, la pièce sera défectueuse.

Dans le cas d'ordinateurs de vote, seuls les résultats manifestement erronés parce qu'invraisemblables peuvent être détectés. Si un candidat obtient davantage de voix qu'il n'y a d'électeurs, il est évident qu'il s'est passé quelque chose d'anormal et une enquête peut être diligentée. C'est d'ailleurs exactement ce qui s'est passé lors de l'incident de Schaerbeek (relaté plus loin). Mais le problème peut être plus discret et n'affecter qu'un faible pourcentage des votes cependant suffisant pour faire basculer le résultat, ou bien échanger les

7 Ariane 5 explose lors de son vol inaugural le 4 juin 1996, victime d'une erreur de calcul : un programme qui fonctionnait à merveille sur Ariane 4 se révèlera être la cause de cette défaillance [Ariane 1997] .

suffrages obtenus par deux candidats.

> Nous constatons que s'il n'y a aucun support physique gardant une trace de chaque vote, il est impossible de détecter les dysfonctionnements non aberrants.
>
> Il est donc crucial qu'un ordinateur de vote garde une trace physique des votes (un bulletin imprimé portant le nom du candidat choisi, par exemple), et que cette trace ait été vérifiée par chaque électeur au moment de son vote pour prouver la sincérité du vote.
>
> Il est essentiel également que cette trace physique fasse foi s'il y a désaccord entre le dépouillement manuel et le dépouillement informatique.

Ce principe a été clairement affirmé dans la thèse de Rebecca Mercuri [Mercuri 2000], puis rappelé à de nombreuses reprises par différents informaticiens au plus haut niveau. La prestigieuse association américaine ACM (Association for Computing Machinery)[8] a nettement pris position dans le même sens le 27 septembre 2004 :

> << Virtually all voting systems in use today (punch-cards, lever machines, hand counted paper ballots, etc.) are subject to fraud and error, including electronic voting systems, which are not without their own risks and vulnerabilities. (...) In addition, voting systems should enable each voter to inspect a physical (e.g., paper) record to verify that his or her vote has been accurately cast and to serve as an independent check on the result produced and stored by the system.
> (...)
> **Ensuring the reliability, security, and verifiability of public elections is fundamental to a stable democracy**. Convenience and speed of vote counting are no substitute for accuracy of results and trust in the process by the electorate. >>

Les industriels

Le vote électronique est devenu un marché potentiel important et concerne de nombreux États. Logiquement, différentes entreprises se sont emparées de ce nouveau marché en utilisant les techniques habituelles de promotion et de marketing. Le discours de type managérial a progressivement remplacé les réflexions de type politique ou administratif. On use de l'argument de « modernisation » de la vie politique, on vante la rentabilité (le coût des élections serait diminué), l'augmentation assurée du taux de participation, et la fiabilité des systèmes de vote électronique (la fraude serait quasi impossible) sans qu'**aucun** de ces critères ne soit prouvé.

L'activité de lobbying est particulièrement intense.

Les industriels publient de nombreux articles dans lesquels les auteurs ne manquent jamais de défendre avant tout les intérêts de leur société[9]. Les dangers inhérents à l'utilisation de cette technologie sont toujours minimisés. Lorsque l'article semble souligner un quelconque problème, en fait il s'attache souvent à un problème déjà plus ou moins résolu comme la menace d'intrusions extérieures, ainsi le lecteur a l'impression que les seuls problèmes qui subsistent seront facilement réglés. On met en exergue les risques de la méthode traditionnelle de vote avec bulletin papier même si ceux-ci sont absolument minimes[10]. La

8 L'Association for Computing Machinery existe depuis 1947. Elle possède une dimension internationale avec plus de 80 000 membres institutionnels, universitaires et industriels issus de plus de 100 pays. http://www.acm.org/

9 Ainsi, Marin Ledun et Patrick Paniez de France Télécom présentent l'ensemble des projets financés par la Commission Européenne. Ils soulignent que « le projet E-POLL, de loin le plus important et le plus abouti, (...) » . Parmi les participants à ce projet on trouve naturellement ... France Télécom. [Ledun et al. 2005]

10 On donne cet exemple de coercition : un jour une personne a codé son numéro de passeport en forme binaire en participant à un scrutin de listes avec des listes particulièrement longues [Van Acker 2004] (Bernard Van Acker est employé par IBM). Il ne semble pas que cet exemple soit réellement probant quant à la coercition puisque le problème réside dans la perte d'anonymat. Cette anecdote figure pourtant sous le titre évocateur "Practical risks

question de l'honnêteté du dépouillement n'est jamais posée, cette opération apparaît donc comme réglée et non discutable alors qu'elle est non transparente et qu'elle échappe au contrôle des citoyens.

Des conférences et séminaires sont également organisés, dans lesquels sont invitées les personnalités du monde politique. Ainsi un séminaire officiellement organisé par l' "Association des Maires de Grandes Villes"[11] est-il principalement organisé (choix des intervenants) et financé par l'entreprise NEDAP qui a fourni 80 % des ordinateurs de vote déjà installés en France.

Plus grave, les commissions émanant du pouvoir politique et qui étudient la question du vote électronique sont fortement composées d'industriels alors que les universitaires spécialistes en informatique sont absents ou très minoritaires. Ainsi, en France, le Groupe E-démocratie du Club.sénat.fr (dont 16 membres sur 18 sont issus de sociétés privées, les deux derniers membres étant le sénateur présidant la commission et un membre de la présidence du sénat) a remis un rapport [Trégouët 2002] à M. le Président du Sénat le 27 novembre 2002. Une partie de ce rapport concerne le vote électronique, elle est intitulée « Le e-vote - Ferment de la e-démocratie » et reprend des arguments des industriels en faveur du vote électronique, en particulier la lutte contre la fraude, en omettant le fait que les ordinateurs peuvent faciliter les fraudes massives et indétectables. De manière identique, aux États-Unis, la commission Project P1583 de l'IEEE (Institute of Electrical and Electronics Engineers), chargée de produire des critères visant à garantir la qualité des ordinateurs de vote, a été largement noyautée par des représentants des industriels [Oostveen et al. 2004]. Les critères émis se sont révélés particulièrement faibles puisqu'ils peuvent être vérifiés par des ordinateurs peu sûrs.

Enfin, des décisions importantes ont été prises en se fondant sur des critères de minimisation des coûts et donc de maximalisation des risques : l'impression d'un bulletin papier vérifié par l'électeur lors de son vote est apparue non essentielle aux fabricants d'ordinateurs de vote car ce processus "double" le comptage informatique effectué dans l'ordinateur, et peut être source de pannes (bourrage de papier, manque d'encre, de papier, etc.). Les ordinateurs de vote ne produisent donc aucune trace physique prouvant la sincérité du vote et permettant un recomptage manuel des voix. Par conséquent, ces ordinateurs sont totalement invérifiables.

Récemment, aux États-Unis, devant la multiplication des problèmes survenus lors des votes utilisant des ordinateurs de vote, les autorités de 26 États (dont le New-Jersey et l'État de New-York) ont décidé d'imposer aux fabricants l'ajout d'un dispositif d'impression d'un bulletin papier vérifié par l'électeur. Ces preuves physiques du vote pouvant être recomptées, y compris manuellement, les ordinateurs deviennent alors vérifiables.

Le pouvoir politique

Les décisions politiques ont été largement influencées par le lobbying des industriels.

En France, le règlement [Intérieur 2003] qui fixe les critères que doit remplir un ordinateur de vote pour être autorisé est particulièrement superficiel et ne tient aucun compte des recommandations des spécialistes du domaine, il fixe quelques règles qu'il est facile et peu coûteux de respecter mais qui ne garantissent aucunement que les ordinateurs de vote soient sûrs. Ce règlement précise que les ordinateurs doivent recevoir un agrément avant d'être autorisés, mais cet agrément ne vise pas à détecter des failles de sécurité, en particulier il n'impose pas d'examiner leur programme.

Il admet que le programme utilisé dans les ordinateurs de vote soit secret. Il est donc impossible aux simples citoyens de l'examiner : la protection du secret industriel a été jugée plus importante que la transparence de la procédure de vote. Il n'y a aucun examen approfondi du programme ou des documents, aucune vérification de l'intégrité des personnes intervenant sur ces ordinateurs, seuls quelques ordinateurs sont sommairement examinés par l'entreprise délivrant l'agrément, les ordinateurs installés dans les bureaux de vote étant censés être identiques aux ordinateurs examinés, mais il est impossible de vérifier cette identité. De plus, il n'est pas prévu de procédure spéciale de scellement ou de surveillance des ordinateurs

with traditionnal voting methods".

11 « Le vote électronique aujourd'hui : de la machine à voter au vote par internet » . Le 6 avril 2006 – Maison de la chimie – Paris.

entre les scrutins.

Surtout, il est impossible de vérifier si l'ordinateur a bien fonctionné puisque le règlement n'impose PAS aux ordinateurs de vote d'imprimer un bulletin papier vérifié par l'électeur. Celui-ci doit faire confiance à l'informatique qui est censée fonctionner correctement. Les nombreux incidents qui sont déjà survenus sur des ordinateurs analogues n'incitent pourtant pas à la confiance !

La procédure de vote à l'aide d'un ordinateur dont le résultat est invérifiable, et qui est entièrement contrôlé par une entreprise privée peut être représentée par une analogie : il faut imaginer que le vote se déroule selon la procédure habituelle à l'aide de bulletins papier, mais que le dépouillement des bulletins soit réalisé par une entreprise privée qui emporterait les bulletins, sans que quiconque puisse contrôler ce dépouillement, et qu'il soit impossible d'obtenir les bulletins afin d'effectuer une vérification. Il s'agit bien d'une confiscation du contrôle du vote qui échappe alors aux citoyens pour être confié (par le pouvoir politique) à une entreprise privée.

Aux États-Unis, le dernier document fixant les règles de certification (2002 Federal Election Commission guidelines[12]) a également été sévèrement critiqué par les scientifiques [Mercuri 2003].

La réalité

Les ordinateurs de vote sont très récents en France (2004). Il y a donc peu de faits qui peuvent être relatés concernant leur utilisation dans ce pays. En revanche, leur introduction est plus ancienne dans de nombreux autres pays (début des années 1990 aux États-Unis par exemple). Cette période de temps assez longue a permis une observation pertinente de leur comportement.

Il faut souligner que les ordinateurs de vote peuvent être différents d'un pays à l'autre (par exemple, quelques-uns impriment un bulletin papier), néanmoins ils ont plusieurs points communs : ce sont des systèmes informatiques (qui présentent donc potentiellement toutes les fragilités déjà citées) et ils effectuent un dépouillement automatique.

De nombreux incidents

Nous avons constaté que le discours des spécialistes de la sécurité informatique a été largement occulté par celui des industriels qui ont réussi à largement influencer la rédaction des textes officiels régentant l'utilisation des ordinateurs de vote.

Cette situation n'est pas propre à la France, une dizaine de pays[13] utilisent largement le vote électronique malgré les mises en garde des informaticiens. De nombreux incidents ont été relevés, en voici quelques-uns à titre d'exemples, mais cette liste n'est pas exhaustive.

- États-Unis : en novembre 2003, dans le comté de Boone (Indiana), un ordinateur de vote a enregistré plus de 144 000 votes alors qu'il n'y avait que 19 000 électeurs [Simons 2004]
- États-Unis : en mars 2002, dans la ville de Wellington, une élection visant à départager deux candidats se déroule sur des ordinateurs de vote. Les résultats sont de 1263 voix pour un candidat contre 1259 voix pour l'autre, mais 78 voix n'ont pas été enregistrées alors que les électeurs ont émargé. La directrice des élections a conclu que ces personnes n'ont simplement pas voté lorsqu'ils étaient en présence de l'ordinateur, ce qui n'est vraiment pas prouvé. Il est bien plus probable que ces votes n'ont pas été enregistrés par l'ordinateur. Des incidents similaires ont eu lieu à Palm Beach, et Miami [Mercuri 2002].
- États-Unis : le 10 septembre 2002, les ordinateurs fournis par Election Systems and Software (ES&S) ont présenté des délais de démarrage particulièrement longs le jour des élections : entre 10 et 23 minutes au lieu des 2 minutes annoncées par le constructeur. Ces systèmes avaient pourtant été préalablement examinés et jugés corrects par les observateurs de l'État et des agences de contrôle

12 http://www.eac.gov/election_resources/vss.html (consulté le 18 mai 2006)

13 Belgique, Brésil, Canada, États-Unis, Inde, Pays-Bas, Vénézuéla, etc..

(qui ont été réprimandées par la très officielle NASED[14] pour leur manque de perspicacité) [Mercuri 2002].

- En Belgique chaque vote sur un ordinateur de vote est enregistré sur une carte magnétique anonyme. Lors du vote, il faut insérer la carte dans l'ordinateur puis procéder au choix. Celui-ci est mémorisé dans la carte que l'on dépose ensuite dans une urne électronique qui décomptera les voix. Ce système a le mérite de prendre en compte la nécessité absolue de mémoriser le vote sur un support qui permette un dépouillement indépendant de celui de l'ordinateur. Il présente cependant le défaut majeur d'utiliser un support qui n'est pas directement lisible par un humain (comme un bulletin imprimé avec le nom du candidat) : il n'est pas possible de voir ce qui est inscrit sur sa carte magnétique (est-ce bien mon vote ?[15]). Lors des élections du 18 mai 2003, à Schaerbeek, un candidat d'une liste obtient plus de voix qu'il n'est possible d'en obtenir. Le recomptage manuel à partir des cartes magnétiques a montré une erreur de 4096 voix, erreur qu'il a été impossible d'expliquer ou de reproduire lors de nombreux tests menés sur le même ordinateur [Rapport Chambre et Sénat belge 2004, page 21].
- Toujours en Belgique lors des élections du 18 mai 2003, des pannes d'ordinateurs de vote et le fait que les électeurs prennent le temps de vérifier que leur vote est bien inscrit sur leur carte magnétique ont entraîné des files d'attente pouvant dépasser 2 h dans plusieurs bureaux de vote. Il faut souligner que le vote étant obligatoire en Belgique sous peine d'amende, la plupart des électeurs ont patienté, ce qui ne serait sûrement pas le cas en France.
- Au Québec les élections municipales du 6 novembre 2005 se sont déroulées à 95% à l'aide d'ordinateurs[16], les incidents ont été massifs : des résultats sont arrivés avec plusieurs heures de retard, des équipements sont tombés en panne, des connexions Internet ont été coupées, des votes ont été comptabilisés deux fois, etc. [Beaulieu 2006].
- etc.

Il faut souligner que seules les situations de dysfonctionnement manifestes ont pu être détectées lors de l'utilisation d'ordinateurs invérifiables (n'imprimant pas de bulletin papier vérifié par l'électeur). Il est très probable que des dysfonctionnements sont passés inaperçus car les résultats énoncés par l'ordinateur n'étaient pas aberrants. Imaginons une inversion du nombre de suffrages obtenus par deux candidats, les nombreux incidents qui se sont déjà produits montrent que cette erreur peut arriver, et que rien ne prouve qu'elle ne soit pas arrivée.

Promesses non tenues

Rapidité

Non seulement le moindre incident entraîne des retards colossaux pour la publication des résultats, mais en plus des files d'attentes parfois impressionnantes se forment devant les bureaux de vote : soit un seul ordinateur a été installé là où il y avait trois ou quatre isoloirs[17], soit des pannes de matériel ont réduit le nombre d'ordinateurs en état de fonctionner.

---

14 National Association of State Election Directors http://www.nased.org/board.htm

15 Il est théoriquement possible de vérifier ce qui est inscrit sur la carte en la repassant sa carte dans le lecteur de l'ordinateur sur lequel on vient de voter, ce qui ne constitue manifestement pas une preuve du bon enregistrement du vote sur la carte magnétique. Des citoyens pugnaces ont insisté pour procéder à cette vérification en lisant leur carte à l'aide d'un autre ordinateur de vote (ce qui est théoriquement absolument interdit par la loi) et ont déniché quelques erreurs (les votes pour les derniers candidats d'une liste très longue n'étaient pas enregistrés).

16 Les incidents relatés concernent les ordinateurs de la Société PG election http://www.pgelections.com/

17 Cet inconvénient a déjà été relevé en France et a été expressément mentionné par le chef du bureau des élections et des études politiques au Ministère de l'Intérieur le 6 avril 2006 lors du séminaire « Le vote électronique aujourd'hui : de la machine à voter au vote par internet » organisé par l'"Association des Maires de Grandes Villes"

Sûreté

Aux États-Unis, en 2004, un quart du corps électoral a voté sur des ordinateurs de vote. Ceux-ci sont principalement produits par les sociétés Diebold et Election Systems and Software (ES&S).

Diebold ayant malencontreusement rendu public le programme de ses ordinateurs sur Internet[18], des chercheurs de l'Université John Hopkins de Baltimore ont pu l'étudier pendant plusieurs mois. Ils ont publié un rapport soulignant l'absence totale de garantie des ordinateurs vendus par Diebold et la très grande facilité avec laquelle il est possible de fausser les résultats et même de les modifier à distance [Kohno and al. 2004].

Malheureusement, la diffusion publique des défauts relevés dans les programmes de Diebold n'a pas eu pour effet la remise en compte du vote électronique mais a au contraire poussé les autorités politiques du Maryland à décidé d'un plan d'action dans le but de rendre ces ordinateurs plus sûrs. Il s'agit d'une fuite en avant qui ne résoudra pas les problèmes : les ordinateurs resteront peu fiables quelle que soit la somme investie dans l'amélioration de leurs programmes.

L'acharnement de certaines entreprises à éviter de rendre ces ordinateurs vérifiables (en les dotant de l'impression d'un bulletin papier vérifié par l'électeur)[19] devient suspect : cette vérification systématique pourrait démontrer de nombreux cas de résultats erronés et discréditer complètement cette technologie pour cet usage très particulier qu'est le vote. L'entreprise NEDAP utilise d'ailleurs ce curieux argument : le dépouillement des bulletins papier pourrait mener à la découverte d'anomalies dans le fonctionnement des ordinateurs de vote le jour des élections, ce qui ébranlerait la confiance des électeurs.

> <<An audit trail could only show that the event, identified as a risk occurs on Election Day, but that is too late!! In our opinion every voting machine should be designed, built and tested in accordance to the highest standards. Lowering the standards cannot be compensated by any audit trail. Errors or flaws detected during the election would shake voter's confidence and are unacceptable.>> [CEV 2004] Appendix 4, Part 1, page 419[20].

Coût

Malgré les promesses quant à la réduction du coût des élections et comme nous l'avons déjà vu, il apparaît que des sommes considérables ont été investies dans les ordinateurs de vote. Entre autres, le coût annoncé par les fabricants ne prend pas en compte les nécessaires frais de maintenance et de sécurisation des ordinateurs entre les scrutins.

Québec : M. Gautrin, député de Verdun et adjoint parlementaire au premier ministre du Québec, remet en question l'argument de réduction des coûts, découlant de l'élimination des tâches manuelles, avancé par les défenseurs du vote électronique : « Les économies liées au recours au vote électronique sont loin d'être prouvées : il faut compter la maintenance des systèmes informatiques, qui ne sont utilisés qu'une fois aux quatre ans. » [Beaulieu 2006]>>

États-Unis : en Floride, le gouvernement a dépensé 125 millions de dollars pour remettre à niveau le

---

18 Ce qui est particulièrement cocasse de la part d'une entreprise de haute sécurité.

19 Lors des élections du 18 mai 2003 en Belgique, quelques ordinateurs ont été dotés d'une extension permettant d'imprimer un ticket que l'électeur visualisait à travers une vitre (en fait une loupe grossissante). Après vérification et confirmation de la sincérité du vote, le ticket était automatiquement détaché et déposé dans une urne pour qu'à aucun moment l'électeur ne puisse modifier ou emporter ce ticket. Les tickets ont ensuite été dépouillés pour vérifier les résultats de l'ordinateur. Ce dépouillement n'a pas été achevé car le papier était de mauvaise qualité et ne permettait pas de faire des piles avec les votes, les caractères imprimés étaient si petits et si peu lisibles que les assesseurs n'ont pu mener l'opération à bien. La commission d'évaluation en a donc conclu que l'impression d'un bulletin vérifié par l'électeur n'était pas possible [Rapport chambre et sénat belge 2004]. Il est consternant de constater que tout a été fait pour que cette expérience se déroule aussi mal que possible et que cette mise en œuvre calamiteuse n'ait pas été relevée par la commission d'évaluation.

20 http://www.cev.ie/htm/report/first_report/pdf/Appendix%204-Part1.pdf

système de vote électronique [Mercuri 2002]. Malgré cet effort les élections du 10 septembre 2002 ont vu le Gouverneur Jeb Bush déclarer l'état d'urgence et prolonger l'ouverture des bureaux de vote de deux heures. Il faut noter que les deux tiers des équipements fournis par Election Systems and Software (ES&S) avaient des défauts et ont dû être réparés quelques mois avant les élections.

Votée par le Congrès américain fin 2002, la loi fédérale baptisée *"Help American Vote Act"* (HAVA)[21] prévoit le remplacement des anciens systèmes à cartes perforées par le vote électronique d'ici à 2006 et alloue 3,9 milliards de dollars à cette opération.
Le rapport accablant de l'Information Security Institute de l'Université Johns Hopkins de Baltimore (Maryland) sur les ordinateurs de Diebold a été confirmé par un audit du Science Applications International Corporation [SAIC 2003] mais n'a pourtant pas eu les conséquences attendues : le contrat de 55,6 millions de dollars qui venait d'être signé entre cette entreprise et l'État du Maryland n'a pas été dénoncé, et l'État du Maryland a déclenché un plan d'action visant à sécuriser le système électoral pourtant censé être déjà sûr...

Irlande : 50 millions d'euros ont été investis pour acquérir 7500 ordinateurs de vote. La commission du Parlement chargée de contrôler les dépenses a contesté les prévisions d'économies que devait permettre le vote électronique, et a pointé les grandes variations des coûts de stockage et d'assurances selon les endroits. Leur coût total est de 700 000 \ par an [O'Brien 2005].

Conclusion

Malgré la forte opposition des scientifiques spécialistes de la sécurité informatique et la mobilisation croissante des citoyens, il apparaît extrêmement difficile de remettre en cause le vote électronique que le pouvoir politique continue à soutenir.

Nous constatons qu'après plus d'une décennie d'errements certains États ont quand même commencé à prendre conscience des problèmes posés par ces ordinateurs. L'État de Californie a décidé de rendre obligatoire l'impression d'un bulletin papier vérifié par l'électeur à partir de juillet 2006. En Irlande, suite aux protestations de la population et des spécialistes en informatique de la Irish Computer Society, la commission indépendante nommée par le gouvernement (Commission on Electronic voting[22]) a déclaré en décembre 2004 être incapable de recommander l'utilisation des ordinateurs de vote NEDAP pour les prochaines élections (il s'agissait d'élections locales, européennes et d'un référendum). Dick Roche, ministre en charge du dossier, a confirmé officiellement que ces ordinateurs de vote ne seront pas utilisés pour les élections de 2007. Cette commission a finalement conclu en juillet 2006 que l'équipement de vote et de comptage pourrait être utilisé à condition de mettre en œuvre des mesures supplémentaires comme : permettre aux opérateurs et aux observateurs de vérifier indépendamment l'authenticité des composants logiciels et matériels (R5), l'amélioration des contrôles d'accès aux fonctionnalités réservées (R6), le cryptage des votes (R10), la mise en place de tests rigoureux et contrôlés (R20), ou encore la nécessité de procéder à un examen indépendant des fonctionnalités et des spécifications (R19). L'Irlande continue donc à ne pas utiliser les ordinateurs de vote achetés.

Il serait douloureux que les erreurs relevées à l'étranger soient commises en France alors même que des élections majeures (présidentielles et législatives) vont avoir lieu en 2007, d'autant plus que la remise en cause a posteriori du bon déroulement de ces votes de première importance pourrait menacer la stabilité politique de ce pays. Il apparaît donc urgent de suspendre l'utilisation des 900 ordinateurs de vote équipant déjà des bureaux de vote.

Enfin, il est regrettable que la mise en œuvre d'ordinateurs de vote ait eu lieu sans qu'une commission indépendante à la fois du pouvoir politique et des tentations commerciales ne soit mise en place. L'utilisation de l'informatique peut contribuer à améliorer le fonctionnement de la démocratie, par exemple en ce qui concerne l'accès des handicapés, ou la possibilité effective de voter pour tous les candidats, si la mise en œuvre de ces systèmes ne dégrade pas la qualité de la procédure de vote dans son ensemble.

---

21 http://www.fec.gov/hava/hava.htm

22 http://www.cev.ie/

Bibliographie

[Ariane 1997] Ariane 501, "Rapport de la commission d'enquête", 1997.[23]

http://www.capcomespace.net/dossiers/espace_europeen/ariane/ariane5/AR501/AR501_rapport_denquete.htm (consulté le 16 mai 2006).

[Beaulieu 2006] Alain Beaulieu, "Les ratés des élections municipales", magazine Direction informatique, décembre 2005-janvier 2006.

http://www.directioninformatique.com/di/client/fr/DirectionInformatique/Nouvelles.asp?id=37916 (consulté le 17 mai 2006).

[CEV 2004] Commission on Electronic Voting, First Report, "Secrecy, Accuracy and Testing of the Chosen Electronic System, December 2004.
(consulté le 13 mai 2006).

[CEV 2006] Commission on Electronic Voting (Irlande), "Secrecy, Accuracy and Testing of the Chosen Electronic Voting System, juillet 2006.

http://www.cev.ie/htm/report/download_second.htm (consulté le 1er septembre 2006).

[Conseil constitutionnel 1958] http://www.conseil-constitutionnel.fr/textes/constit.htm (consulté le 13 mai 2006).

[Fishman 1996] Charles Fishman, "They write the right stuff", FastCompany, 06, Dec 1996.

http://www.fastcompany.com/online/06/writestuff.html

[Intérieur 01] "Machines à voter"

http://www.interieur.gouv.fr/rubriques/b/b3_elections/b31_actualites/2003_07_04_machines_voter

(consulté le 13 mai 2006)

[Intérieur 2003] "Arrêté du 17 novembre 2003 portant approbation du règlement technique fixant les conditions d'agrément des machines à voter". Auteur(s) inconnus(s).

http://www.interieur.gouv.fr/rubriques/b/b3_elections/b31_actualites/2003_07_04_machines_voter/mav2.pdf (consulté le 16 mai 2006)

[Kohno and al. 2004] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, Dan S. Wallach, "Analysis of an Electronic Voting System", IEEE Symposium on Security and Privacy, Oakland, CA, May, 2004.

[Ledun et al. 2005] Marin Ledun, Patrick Paniez, "Le vote électronique en France :des préconisations aux usages de la e-Démocratie", colloque DEL, « Démocratie électronique, Paris, 7 décembre 2005.
http://loiseaugerard.free.fr/DELcolloque/ (consulté le 2 mai 2006)

[Légifrance 2005] article L57-1 du code électoral, http://www.legifrance.gouv.fr/WAspad/ (consulté le 13 mai 2006).

[Mercuri 2000] Rebecca Mercuri, "Electronic Vote Tabulation Checks & Balances", Ph.D. dissertation, School of Engineering and Applied Science of the University of Pennsylvania, Philadelphia, PA , October 27, 2000.

[Mercuri 2002] Rebecca Mercuri, "Florida 2002: Sluggish Systems, Vanishing Votes",

23 http://www.capcomespace.net/dossiers/espace_europeen/ariane/ariane5/AR501/AR501_rapport_denquete.htm (consulté le 16 mai 2006).

Communications of the Association for Computing Machinery, Volume 45, No. 11, November 2002.

[Mercuri 2003] Rebecca Mercuri, "Rebecca Mercuri on HAVA and Electronic Voting", 2003. http://www.notablesoftware.com/Papers/RMonHAVA04.htm (consulté le 18 mai 2006)

[Neumann 1993] Peter G. Neumann, "Security Criteria for Electronic Voting", 16th National Computer Security Conference Baltimore, Maryland, September 20-23, 1993.

[O'Brien 2005] Carl O'Brien "Electronic Voting Unlikely to be used in Next Election", The Irish Times, Dublin, Ireland, September 27, 2005.

[Oostveen et al. 2004] Anne-Marie Oostveen, Peter van der Besselaar, "Security as Belief User's Perceptions on the Security of Electronic Voting Systems", « Electronic Voting in Europe – Technology, Law, Politics and Society » , workshop of the ESF TED Programme together with GI and OCG, p.72-82, July, 7th-9th, 2004, Austria.

[Rapport chambre et sénat belge 2003] Sénat et chambre des représentants de Belgique, "Rapport concernant les élections du 18 mai 2003", numéro 3-7/1 (Sénat) Doc 51 0001/2 (Chambre), juin 2003.

[SAIC 2003] "Risk Assessment Report Diebol AccuVote-TS Voting System and Processes", September, 2, 2003.

http://www.dbm.maryland.gov/dbm_publishing/public_content/dbm_search/technology/toc_voting_system_report/votingsystemreportfinal.pdf (consulté le 22 mai 2005).

[Simons 2004] Barbara Simons, "Electronic Voting Systems: the Good, the Bad, and the Stupid", ACM Queue vol. 2, no. 7 - October 2004 .

[Thompson 1984] Ken Thompson, "Reflections on Trusting Trust", Communication of the ACM, p. 761-763, Vol. 27, No. 8, August 1984.

[Trégouët 2002] René Trégouët , "La e-démocratie, enjeux et perspectives". club.senat.fr/admin/dir_files/Rapport_e_democratie_en_ligne.doc (consulté le 16 mai 2006).

[Van Acker 2004] Bernard Van Acker, "Remote e-Voting and Corcion : a Risk-Assessment Model and Solutions", « Electronic Voting in Europe – Technology, Law, Politics and Society » , workshop of the ESF TED Programme together with GI and OCG, p.53-62, July, 7th-9th, 2004, Austria.

Je remercie Pierre Muller pour sa relecture attentive de cet article et ses conseils toujours avisés.

Article révisé le 8 décembre 2006.