.be

Pour une Ethique du Vote Automatisé
http://www.poureva.be/

.fr

Citoyens et informaticiens pour un vote vérifié
http://www.recul-democratique.org

Le vote électronique nuit gravement à la démocratie

Le logiciel libre *n'est pas* la solution magique.

Avertissement ! Ceci est un tract. Sa brièveté fait que c'est forcément réducteur. Pour des explications plus subtiles, consultez nos sites internet.

Dans Le vote électronique est un terme général qui englobe deux familles de systèmes :

- les **machines à voter,** placées dans les bureaux de vote. Le terme de machine est trompeur: ce sont de véritables ordinateurs. Elles enregistrent les votes et les dépouillent, en général sans s'occuper de l'identification de l'électeur ni de son émargement. Utilisées à grande échelle par la Belgique, les Pays-Bas, les États-Unis, le Brésil, l'Inde, le Canada et le Venezuela.
- le **vote par internet** s'effectue depuis n'importe quel ordinateur, par exemple à son domicile. Identification et émargement sont gérés. Contrairement aux machines à voter, il reste expérimental, et certains pays l'ont même abandonné : États-Unis, Grande-Bretagne, Finlande, Espagne.

Les systèmes de vote électronique actuels ont **une particularité les différenciant des autres systèmes informatiques**, venant du secret du vote. Des comparaisons infondées sont souvent faites avec les transactions bancaires : leur exactitude est contrôlable a posteriori, par exemple en vérifiant ses relevés de compte, imprimés sur du papier bien tangible. Tous les systèmes informatiques ont des conséquences **vérifiables** dans le monde réel. Presque tous... Si la machine modifie des votes, qui s'en apercevra ?

Puisque l'utilisateur du système informatique - l'électeur - ne peut pas vérifier son bon fonctionnement, cela oblige à s'en remettre à des informaticiens. Selon nous, c'est déjà un problème en soi : **les électeurs et les assesseurs devraient être en mesure de comprendre tout ce qui se passe dans un bureau de vote.** Tout le monde ne sait pas lire un code source. Quoi qu'il en soit, les informaticiens sont-ils en mesure de garantir ce bon fonctionnement ?

Un logiciel se vérifie soit par des tests, soit par inspection de son code source. **Les tests sont inopérants** : un comportement frauduleux peut se déclencher seulement le jour de l'élection. **L'inspection du source se heurte à la complexité**, complexité accrue si on inspecte également le système d'exploitation, le compilateur... Il reste des bugs dans tous les logiciels du monde, libres ou propriétaires. Un comportement malveillant bien dissimulé est bien plus difficile à trouver qu'un bug. Certains bugs, en créant des failles de sécurité, permettent des attaques extérieures.

Même si l'on était satisfait de l'inspection du code source, **il serait difficile de savoir si le logiciel examiné est bien celui qui tourne dans tous les systèmes de vote le jour de l'élection.** Comme lors d'une expertise judiciaire, il faudrait extraire le medium (ROM, disque dur, disquette, carte flash...) contenant le logiciel pour l'examiner dans un autre ordinateur, par exemple le soir de

l'élection. Si le medium est modifiable, c'est insuffisant : le logiciel frauduleux a pu se remplacer par sa version officielle juste avant la clôture de l'élection. Cela serait quand même incomplet : il faut également examiner le matériel. Par exemple, certains microprocesseurs existent en deux versions : l'une utilisant une mémoire externe que l'on aura inspectée, l'autre intégrant sa propre mémoire. Les cartes mémoires stockant les votes peuvent être passives, ou bien équipées d'un microcontrôleur.

Une élection doit être **vérifiée par le citoyen et transparente**. La première de ces qualités est la plus importante : le consensus scientifique est qu'on ne peut l'assurer qu'au moyen de l'impression d'un bulletin vérifié par l'électeur (VVAT), et cela ne marche que dans le cas des machines à voter. Le logiciel libre ne peut apporter qu'une certaine transparence, ce qui serait déjà mieux respecter l'électeur. Il pourrait inciter à une meilleure qualité : il est toutefois difficile de tirer des conclusions des différentes publications de code source, faites dans des conditions très variables : eVacs (australien, GPL provisoire), KOA (néerlandais, GPL à 90%), machines belges (obtenue juridiquement) ou Diebold (américain, fuites).

Ce qu'en disent des militants du libre

Richard Stallman :

« I think that computerized voting is dangerous, and that the danger cannot be prevented by using only free software.
The danger is that someone could fiddle the software so that it cheats on the vote. You cannot prevent this by studying the source code of the program that conducts the election, because the program that actually runs during the election may be different. Someone could substitute another program to misrecord the votes or miscount the votes, and put the right program back afterwards; nobody would ever be able to prove this had occurred. There would be no way to do a recount.

So I am with those who say there should be paper ballots so that a manual recount is possible. »

David Glaude, membre de PourEva.be et de l'AEL (Association Electronique Libre) :

« En Belgique, des citoyens ont gagné une bataille juridique pour obtenir la transparence de l'administration et consulter le code des logiciels de vote utilisés. A la différence de la France ou de l'Irlande, au moins nous avons le code, mais nous ne sommes pas plus avancés. L'analyse indépendante (http://www.afront.be/lib/vote.html) que nous avons pu voir ne nous a pas rassurés ! »

En France

Trois fabricants de machines à voter sont autorisés depuis 2004 : Nedap (néerlandais), ES&S (américain) et Indra (espagnol). Une cinquantaine de villes utilisent leurs machines, dont deux grandes villes : Brest et le Havre (Reims, Le Mans et Grenoble le projettent). Cela concerne presque un million d'électeurs. Le vote par internet n'est autorisé que pour les expatriés, et seulement pour élire l'AFE (Assemblée des Français de l'Étranger), comme au mois de juin 2006 : outre que cette élection fut caractérisée par une grande désorganisation, elle a été l'occasion de prendre conscience de l'impossibilité de son contrôle, tant par les assesseurs que par les informaticiens. Tous les logiciels sont propriétaires et leur inspection n'est pas requise par la loi. Même les rapports d'agrément sont secrets.Aucun mécanisme de vérification de l'intégrité des machines à voter n'existe.

En Belgique

Les expériences de machines à voter (appelé vote automatisé) ont démarré en 1991, et concernent actuellement 44% des électeurs, proportion stagnant depuis 1999. Plusieurs incidents techniques: notamment Anvers et Schaerbeek (resté sans autre explication que les rayons cosmiques). Le coût est triple. PourEVA combat ce système depuis 1994, et trois des quatre partis francophones se sont maintenant prononcés contre. Un projet de loi imagine d'abandonner le vote électronique et de s'en tenir à l'automatisation du dépouillement (Nyssens 3-120). Le code source est publié le lendemain des élections (licence inconnue).

En Irlande

La totalité de ce pays devait utiliser des machines à voter Nedap dès 2004. Suite à une contestation citoyenne croissante, initiée dans une université, relayée par l'opposition politique tout à la fin, il a été formé une commission indépendante : la CEV (“Commission on Electronic Voting”). Elle s'est déclarée être “incapable de recommander” l'utilisation de ces machines. 7500 machines sont donc restées dans des entrepôts depuis, et leur abandon définitif est maintenant clairement envisagé.

En tant qu'informaticiens conscients de nos responsabilités, nous avons le devoir d'affirmer clairement que, dans l'état actuel de nos connaissances, on ne peut pas faire confiance au vote purement électronique.

Il ne faut surtout pas vous méprendre en croyant que le logiciel libre serait la solution miracle.

Contact - France : Pierre Muller, http://www.recul-democratique.org, 06 63 72 63 56, les références de son intervention de jeudi seront aussi disponibles sur le site des RMLL.

Contact - Belgique : Association PourEVA, http://www.poureva.be, email@poureva.be