Qui contrôle le vote électronique ?

le déclin silencieux du contrôle citoyen[1]

Ce texte est la version longue d'une intervention faite au colloque "Le vote électronique aujourd'hui : de la machine à voter au vote par internet" organisé par l'Association des Maires de Grandes Villes de France le 6 avril 2006. L'intervention étant dans une table ronde sur les machines à voter actuelles, ce texte ne traite pas des machines à voter en réseau, ni du vote par internet[2].

Souligner des expressions n'indique pas leur importance, mais qu'elles renvoient vers des pages internet : la version électronique de ce document vous permet d'accéder à ces pages par simple clic.

Ce texte est susceptible d'évoluer pour répondre à des demandes d'éclaircissement ou à des informations nouvelles. ***Plutôt que de le photocopier****, imprimez sa version la plus récente depuis le site Internet, à l'adresse www.recul-democratique.org/article.php3?id_article=135. Ce que vous avez devant les yeux date du 6 avril 2006.*

Qui sommes-nous ? Pour la plupart d'entre nous, des citoyens réunis par notre inquiétude face à l'arrivée des machines à voter dans nos villes respectives, sans le moindre débat[3], comme si il s'agissait de renouveler le parc de micro-ordinateurs. Je suis pour ma part informaticien, comme environ la moitié d'entre nous[4] : ce texte est donc le double point de vue d'un citoyen et d'un informaticien. Notre première réaction a été d'interroger nos mairies. Elles nous ont parlé meilleure organisation et économies, sans prendre au sérieux nos interrogations. Cela nous a incités à nous documenter sur Internet. Nous avons rapidement découvert le moratoire de fait de la Belgique[5], le refus de l'Irlande[6] d'utiliser des machines Nedap pourtant achetées massivement, l'année même où la France autorisait leur usage, ainsi que les innombrables difficultés des États-Unis[7]. Quelques mois après notre création, nous avons observé de près la catastrophique élection municipale du Québec[8]. Il nous est apparu que de la communauté des informaticiens avait exprimé de nombreuses réserves, comme en

---

1 Titre inspiré par Ulrich Wiesel, informaticien allemand qui conteste en justice les dernières élections législatives réalisées avec des machines Nedap.

2 A ce sujet, nous avons publié une traduction du rapport sur SERVE, rapport qui a conduit l'armée américaine à abandonner ce projet de vote par internet. Egalement une traduction de l'audition de l'expert en sécurité informatique Bruce Schneier devant la Chambre des Représentants des États-Unis, qui explique pourquoi Internet n'est pas sécurisé, et que ce n'est pas qu'une affaire de technologie.

3 Sans le moindre débat, et parfois sans même une délibération du Conseil Municipal. Ceux qui ne lisent pas les bulletins municipaux, ni la presse locale, découvrent l'existence des machines à voter au moment de l'élection.

4 Nous nous sentons obligés de le préciser régulièrement, sous peine d'être traités de passéistes, comme l'a fait le maire de Brest: « Franchement, je crois que contester la fiabilité de ces machines, c'est aussi contester à la fin du 19 ème siècle que le train pouvait être un outil performant et qu'il rendait malade ceux qui rentraient à l'intérieur. ». Passéiste est finalement un qualificatif plutôt banal : un jour, au parlement irlandais, le ministre responsable de l'introduction des machines à voter a traité d'altermondialistes les membres de l'Irish Computer Society, association professionnelle d'informaticiens.

5 La Belgique a démarré les expériences de vote électronique en 1991, et cela concerne actuellement 44% des électeurs, proportion stagnant depuis 1999. Plusieurs incidents techniques: notamment Anvers et Schaerbeek (resté sans autre explication que les rayons cosmiques). Une association citoyenne combat ce système depuis 1992 ("Pour une éthique du vote automatisé" www.poureva.be), 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 coût est triple.

6 L'Irlande devait voter électroniquement dès 2004 avec des machines Nedap. Suite à une contestation citoyenne croissante (que l'opposition politique n'a relayée que tout à la fin), il a été formé une commission indépendante (la CEV, "Commission on Electronic Voting") qui a déconseillé leur utilisation. 7300 machines sont donc restées dans des entrepôts depuis. Cf. Irish Citizens for Trustworthy Evoting (http://evoting.cs.may.ie).

7 Les difficultés ne proviennent pas uniquement du vote électronique : les listes électorales comptent également. Le feuilleton de la présidentielle 2000 n'était pas dû au vote électronique, mais à une technologie plus ancienne : les cartes perforées. Celles-ci, mal dessinées, ont été difficiles à recompter. Au moins y avait-il quelque chose à recompter... En réaction, la législation HAVA a été votée. Elle a incité à remplacer les technologies anciennes : en 2004, environ 30% des électeurs ont utilisé des machines tout-électronique, et environ 30% des tabulatrices optiques. La multiplication des bugs dans les machines tout-électronique, la prise de conscience qu'elles étaient des "boites noires" (noires au sens d'opaques), ainsi que la suspicion entourant la présidentielle 2004, ont popularisé le concept de bulletin papier vérifié par l'électeur . 26 des États ont incorporé ce principe à leur législation, et 13 autres y songent. Pour l'instant, les fabricants trainent les pieds pour modifier leurs machines, se contentant d'ajouter une imprimante sans réfléchir à l'ergonomie de l'électeur, ni à la facilité de recompte. Beaucoup de législations sur le recompte sont trop contraignantes. (www.VerifiedVoting.org, www.BlackBoxVoting.org, www.VotersUnite.org)

8 "Les ratés des élections municipales", Direction informatique.

témoignent la prise de position de l'ACM[9], ou la "Resolution on Electronic Voting"[10], de David Dill (professeur d'informatique à Stanford). Nous avons rapidement compris l'immense potentiel des informations disponibles à l'étranger. Tout cela contrastait fortement avec l'absence d'inquiétudes en France. Nous avons par la suite interrogé les divers acteurs du vote électronique : les mairies équipées ou non, le Ministère de l'Intérieur, les organisme d'inspection (Bureau Veritas et Ceten-Apave), et les importateurs.

Qui sommes-nous ? Nous sommes aussi des porteurs de mauvaises nouvelles. Nous tenons à rappeler :

- que le vote électronique, tel que proposé, entraîne inévitablement **la disparition du contrôle citoyen des élections au profit de techniciens**[11]. Qu'il s'agit de changer de système politique : de la démocratie (le pouvoir au peuple) vers la technocratie (le pouvoir aux techniciens), en revenant à l'étymologie de ce mot. Ce changement, que l'on nous présente comme inéluctable, mérite un véritable débat national.
- qu'en pratique, ce contrôle que le citoyen est contraint de transmettre aux techniciens s'est **largement perdu en route**. La suite de ce texte vise à démontrer cela.
- que les systèmes de vote électronique actuels ont **une particularité les différenciant des autres systèmes informatiques** : l'impossibilité de garantir leur bon fonctionnement. La cause est le secret du vote. Des comparaisons infondées sont souvent faites avec les procédures bancaires. Vous pouvez contrôler l'exactitude d'une transaction bancaire a posteriori, par exemple en vérifiant vos relevés de compte, imprimés sur du papier bien tangible. Toutes les informations nécessaires à l'intégrité des données peuvent être mémorisées : il n'y a pas de secret entre vous et votre banque. Si votre réservation aérienne se perd dans l'éther informatique, on ne vous laissera pas monter dans l'avion, et vous pourrez protester, preuve de débit bancaire à l'appui. Tous les systèmes informatiques ont des conséquences vérifiables dans le monde réel. Presque tous... Si la machine avale votre vote, qui s'en apercevra ?
- que **les machines à voter sont des ordinateurs**, même si le marketing d'un fabricant[12] cherche à faire croire le contraire, peut-être pour éviter des comparaisons désagréables avec nos micro-ordinateurs capricieux. C'est totalement fallacieux[13], et comme tous les ordinateurs, les machines à voter contiennent un logiciel qui va déterminer l'essentiel de son comportement. Connaître le comportement de ce logiciel intégré est donc crucial.
- que la sécurité informatique ne se résume pas à éviter de connecter ces machines à Internet. Que la sécurité informatique, c'est compliqué, coûteux et incompréhensible par l'électeur lambda[14]. Qu'il faut **éviter de confondre fiabilité et sécurité** : une machine qui ne tombe pas en panne, ne garantit par pour autant un résultat authentique.
- que **l'accessibilité[15] par tous les électeurs n'a pas été étudiée scientifiquement** sous l'angle de l'interaction

---

9 L'ACM (Association for Computer Machinery), association d'informaticiens fondée en 1947, comptant 80 000 membres, demande des machines à voter conçues plus rigoureusement et avec impression d'un bulletin vérifié par l'électeur. Détails de cette résolution.

10 Signée par des universitaires américains spécialistes du vote électronique, tels David Jefferson, Douglas W. Jones, Rebecca Mercuri, Avi Rubin, Barbara Simons, Dan Wallach... ou des experts en sécurité informatique tel Bruce Schneier. Un autre appel est "the free e-democracy project", dont le sens est très proche de la "Resolution on Electronic Voting", mais dont les signataires sont plutôt européens.

11 Lire également "L'exigence de transparence", Rapport CNIL 2003, page 93.

12 La communication municipale nous semble influencée par Nedap/France-Élection. Quelques exemples :
« La technologie employée fait appel à des solutions mécaniques » Service élections de Brest.
« Contrairement à d'autres systèmes de vote électronique, la machine à voter ne contient pas d'éléments informatiques. » Mairie de Suresnes.

13 La machine de conception la plus ancienne, la Nedap, contient le même processeur 68000 que les Apple MacIntosh des années 80. Son logiciel intégré est constitué d'environ 25 000 lignes écrites en langage "C". Imprimer son code source nécessiterait donc environ 400 pages (cf rapport du PTB "Test report 2 - Voting machine ESI2" du 17/9/2003 sur les Nedap destinées à l'Irlande, page 7). Il faut se garder des apparences : ce sont des ordinateurs avec un boitier et un écran inhabituels. L'ES&S iVotronic est de conception semblable mais plus moderne : elle utilise un écran tactile. L'Indra est plus complexe, car elle contient Windows XP.

14 Encore faudrait-il systématiquement évaluer les machines sous l'angle de la sécurité : cela n'est jamais prévu lors de leur autorisation. Des heureux hasards font que des études de sécurité sont parfois conduites a posteriori : en Irlande, ou dans certains états des USA.
Selon les mairies, le coût est le principal frein à l'équipement. On nous annonce maintenant des machines à voter en réseau, telle e-Poll, nécessitant donc une sécurité accrue. **Où sera placé le compromis entre coût et sécurité ?**

15 L'accessibilité est la capacité à être utilisable par le maximum d'électeurs. Ne pas confondre avec la facilité d'utilisation ou l'ergonomie.

homme-machine[16]. Une enquête de satisfaction ne saurait répondre à cette question. A force de s'entendre seriner que voter sur une machine, c'est très facile, quel électeur osera avouer qu'il n'est pas à l'aise ?

- qu'il faut se faire à l'idée que certaines technologies puissent se révéler inapplicables. De vieux romans de science-fiction nous imaginaient tous nous déplacer dans des voitures volantes. Pourquoi cela ne s'est-il jamais réalisé ? Ce n'est pas un problème technique. Ce serait tout simplement très dangereux[17].
- que répéter mécaniquement "notre situation est différente de celle des États-Unis" élude la question de savoir si nous suivons la même direction. Tout le monde connait le dicton "la France fait la même chose que les États-Unis avec dix ans de retard". Tant notre organisation[18] que nos machines[19] ne sont guère différentes.
- que la simplification de l'organisation matérielle des élections qu'apportent ces machines est bien réelle, mais qu'elle ne pèse pas lourd face à toutes ces questions. Il ne s'agit après tout que d'informatiser un processus rare : rien de comparable à l'automatisation du tri du courrier qui concerne des millions de lettres chaque jour. On sort une coûteuse[20] machine de son placard environ une fois par an.

Les machines à voter sont donc des ordinateurs. Nous ne sommes pas tous conscients de **l'infinie flexibilité de comportement d'un ordinateur**. Quand nous tournons à droite le volant d'une voiture, nous savons qu'elle se dirigera vers la droite. Il en est ainsi parce qu'il y a une liaison mécanique entre le volant et les roues.

Imaginez maintenant que l'on remplace cette liaison par un système informatique : le volant devient alors semblable à une manette de jeu, dont les capteurs sont connectés à l'entrée d'un ordinateur, et la sortie de ce dernier commande des moteurs électriques agissant sur l'orientation des roues. Sur autoroute, on peut imaginer un genre de pilote automatique : l'ordinateur ignore les signaux venant du volant, et dirige la voiture en fonction d'autres informations (cartographie de l'autoroute et position des autres véhicules). Le logiciel contenu dans cet ordinateur a toute liberté d'orienter les roues à sa guise.

En quittant l'autoroute, on débranchera ce pilote automatique. Le terme "débrancher" est trompeur : on ne coupe pas un tel système comme on éteint une lampe, sinon les roues deviendraient inertes. On se contente de basculer vers une autre partie du logiciel, dans laquelle il est censé transcrire fidèlement les mouvements du conducteur.

Une conception malveillante pourrait tout aussi bien envoyer la voiture dans le décor chaque premier janvier entre minuit et quatre heures du matin. Voire se comporter ainsi seulement une fois sur dix. Définir un comportement conditionné par une date précise est l'enfance de l'art pour un programmeur informatique[21]. Pour cette raison, **simuler quelques votes peu avant l'élection, ou le matin même, n'apporte aucune garantie**[22].

Donc, qui contrôle le vote électronique ? Il est beaucoup plus aisé de répondre à la question "Qui contrôle le vote papier ?". L'électeur peut vérifier l'essentiel par lui-même, et exercer son esprit critique, car il comprend le fonctionnement des objets en jeu (bulletin, urne...) dépourvus de technologie. Il doit seulement faire confiance à ses concitoyens assesseurs pour ne pas ouvrir l'urne avant le dépouillement, lequel est une opération publique et compréhensible par tous. Le grand nombre de personnes impliquées dans une élection (en France : entre 200 000 et 300 000 assesseurs, plus les scrutateurs), chacune faisant une petite part du contrôle, ne permet que des fraudes sporadiques et de portée limitée.

Mais qui contrôle le vote électronique ?

- L'électeur ? Il n'a pas de preuve tangible de l'enregistrement de son vote : un ordinateur peut afficher une chose sur son écran, et en mémoriser une autre. Il n'est pas non plus assuré que son vote soit compté, faute de dépouillement dont le

16 Une étude scientifique de la machine à voter brésilienne a montré qu'elle constituait une barrière à l'expression de leur vote pour une importante proportion de gens âgés, handicapés ou non familiers des ordinateurs (G.Michel-W.Cybis-M.Pimenta-J.M.Robert : "Electronic voting for all : the experience of the Brazilian computerized voting system").

17 Nous peinons déjà à réduire les accidents de la route, dus pour l'essentiel à des erreurs humaines. Imaginez des milliers de voiture se croisant dans le ciel, sans même la ressource de simplement s'arrêter sur le bord de la route en cas de problème...

18 Principe d'un certificateur indépendant se prononçant sur un référentiel défini par l'État. Machines protégées par le secret industriel.

19 L'iVotronic est fabriquée par ES&S, l'un des deux principaux fabricants américains. Nedap essaye de s'implanter sur le marché américain, notamment dans l'état de New-York.

20 Les machines Nedap sont vendues environ 6000 € TTC pièce.

21 Cette infinie flexibilité s'accompagne de la possibilité d'agir à l'avance, sans devoir être présent quand le comportement programmé se produit.

22 Il y a toutefois une utilité. Avant l'élection, le personnel municipal doit programmer la machine : notamment indiquer les noms des candidats, et à quel bouton de la machine ils correspondent. "Programmer" s'entend ici dans le sens de programmer un magnétoscope, et non pas dans le sens d'écrire un logiciel. Le matin de l'élection, les assesseurs doivent s'assurer par eux-mêmes (puisqu'ils s'engagent par leur signature sur le ticket d'ouverture du scrutin) qu'il n'y ait pas d'erreur dans la programmation : deux candidats inversés, par exemple.

mécanisme soit compréhensible. Même si cet électeur était informaticien, il ne pourrait en savoir plus, **le code source[23] du logiciel intégré à la machine à voter étant gardé secret par son fabricant**. Voudrait-il connaître dans quelles conditions cette machine a été autorisée ? C'est impossible : lui communiquer le rapport de l'organisme d'inspection violerait le “secret industriel et commercial” et “pourrait compromettre le bon déroulement des élections”[24]. Ce dernier point est totalement surréaliste : l’intégrité de nos élections dépend-elle maintenant de la qualité de la serrure du placard dans lequel ces rapports sont enfermés ?

- Les assesseurs[25] ? Ils n'ont pas plus de compétences en informatique. Ils certifient l’honnêteté des élections en signant le P.V. des résultats, mais **peuvent-ils garantir autre chose que d’avoir respecté des procédures techniques** énumérées dans un mode d’emploi ? Par exemple, à la place d’une urne transparente dont ils vérifieraient la vacuité de leurs propres yeux, un ordinateur imprime un ticket affirmant que sa mémoire est vide. Que peuvent-ils réellement en savoir ?
  Ils surveillent physiquement la machine tout au long de la journée de l'élection, évitant ainsi que son logiciel soit modifié, mais n'ont aucune garantie qu'il soit authentique le matin de l'élection. Comment le pourraient-ils sinon en débutant leur journée par le désossage de la machine par un expert en sécurité informatique[26] ? Ce qui serait de toute façon transmettre leur rôle de contrôle à un tiers.
  Pire, une vérification de “checksum”[27], dont le nom même est obscur, leur donne l'**illusion d'avoir contrôlé quelque chose**. Tout en étant parfaitement inefficace puisque imprimé par le logiciel même qu'il est supposé garantir[28].
  Comment peuvent-ils certifier que la machine compte les votes exprimés par les électeurs, puisqu'ils ne peuvent surveiller les électrons d’une mémoire informatique comme ils le faisaient du contenu d’une urne : ils savaient que l’encre d’un bulletin en papier placé dans une urne verrouillée, était incapable de se modifier.
- Les scrutateurs[29] ? Ils ne peuvent qu'assister à la magie de l'impression instantanée des résultats. Le Conseil de l'Europe recommande la "possibilité de second dépouillement"[30], mais un scrutateur peut-il obtenir autre chose que la réimpression d'un ticket ?
- Les délégués des partis ? A nouveau, leur manque de connaissances informatiques les laisse démunis. Ils devraient alors se résoudre à se faire accompagner d'un expert en sécurité informatique. Ce n'est pas le cas, probablement parce que personne n'en a compris la nécessité, et que de toute façon, rien n'est organisé techniquement pour permettre le travail de cet expert[31].
- La mairie ? Elle se fie à l'agrément donné par l'Etat aux machines à voter. Quand les machines sont achetées, comment sont-elles stockées entre deux élections ? Certainement sous clef, eu égard à leur coût, mais a-t-on conscience de l'**extrême facilité de modification du logiciel intégré**[32], facilité qui n'est compensée par aucune procédure sérieuse de

---

23 Ce qu'est le code source est expliqué en annexe de ce texte.

24 Avis de la CADA (Commission d'Accès aux Documents Administratifs) du 26 janvier 2006. Un recours devant le Conseil d'Etat est en préparation.

25 Les assesseurs sont les quatre citoyens qui entourent le président du bureau de vote. Ils doivent tous être là à l'ouverture et la clôture du scrutin, et au moins deux d'entre eux doivent être présent à tout moment de la journée. Ils proviennent de partis politiques différents. Le président est généralement un conseiller municipal.

26 Dans cet ordre d'idées, Michael Scott (Dublin City University) recommande qu'une autorité indépendante examine des machines sélectionnées aléatoirement, le soir de l'élection, dans le but de vérifier l'authenticité du logiciel intégré (rapport CEV, app. 2B, page 140).

27 Opération demandée aux assesseurs utilisant les machines Nedap/France-Élection. Le matin de l'élection, la machine imprime un ticket indiquant ces checksums : ce sont deux séries de 8 chiffres ou lettres (i.e. deux nombres 32 bits exprimés en hexadécimal). Les assesseurs vérifient qu'ils soient identiques à ce qu'indique le manuel d'utilisation. "Checksum" se traduit par "somme de contrôle" : on se demande pourquoi le terme anglais a été conservé. Pour rajouter un peu de "magie technologique" ?

28 Voir en annexe notre document détaillé : "la vérification de checksums est une duperie".

29 Les scrutateurs sont les électeurs qui participent au dépouillement, ou le surveille.

30 Recommandation Rec(2004)11 "sur les normes juridiques, opérationnelles et techniques relatives au vote électronique", point 26.

31 Le défunt projet de loi sur les machines à voter en réseau (kiosques) allait dans cette direction : il prévoyait une "Cellule de veille technique composée des membres du bureau de vote centralisateur et d’experts désignés par le maire et les candidats." (selon l’exposé du représentant du ministère de l’Intérieur au Forum e-democratie 2005).

32 Machines Nedap/France-Élection : deux minutes suffisent à remplacer le logiciel intégré, selon Michael Scott (Dublin City University) (rapport CEV, app. 2B, page 139).
Machines Indra : le logiciel est placé sur un disque dur. Selon Ceten-Apave, organisme qui a produit le rapport pour agrément, il y a seulement un contrôle de l'usine de fabrication, et aucun mécanisme de signature du logiciel.
L'exigence n° 45 du Règlement technique fixant les conditions d’agrément est : “Les programmes [...] doivent être [...] stockés sous forme inaltérable.”. Les machines Nedap/France-Élection nous paraissent en violer l'esprit : leurs mémoires peuvent être considérées comme inaltérables (bien que ce soient des EPROMs, on ne peut pas les reprogrammer par le biais

contrôle ?
Quand les machines sont louées, la responsabilité du stockage revient au prestataire de services (en pratique, c'est la société importatrice des machines).

- L'Etat ?
  i. Le Ministère de l'Intérieur est à l'origine du cadre de fonctionnement de ces machines, et partage avec les mairies l'organisation pratique des élections. Pour chaque modèle de machine, il délivre un agrément en se basant entièrement sur le rapport rendu par l'organisme d'inspection (Bureau Veritas ou Ceten-Apave). Son rôle est donc mineur.
  ii. La DCSSI[33], habituellement en charge des questions de sécurité informatique, s'est penchée à deux reprises[34] sur les machines à voter, mais **sans rendre de rapport public**.
  iii. La CNIL (Commission nationale de l'informatique et des libertés) a fixé un cadre théorique pour le vote électronique en 2003[35], et s'est ensuite prononcée à plusieurs reprises sur les élections par Internet[36], mais jamais spécifiquement sur les machines à voter. La logique de sa mission semble de se concentrer avant tout sur les menaces envers la liberté et la vie privée, c'est à dire le respect du secret du vote. Avec les machines à voter actuelles[37], l'identification et l'émargement de l'électeur se fait selon les procédures traditionnelles : le secret du vote paraît[38] naturellement préservé par la séparation physique du vote et l'identification. Dans son rapport d'activité 2004[39], la CNIL recommande une "évaluation globale des dispositifs de vote électronique", **recommandation qui n'a pas été suivie d'effet à ce jour**.
  iv. La justice : elle a été saisie par un candidat à l'élection au Barreau de Paris, concernant un vote par internet, et l'a débouté[40], au motif qu'il se "contentait d'énumérer des risques"[41]. Elle n'a jamais eu à se prononcer sur une élection politique effectuée sur des machines à voter.
- L'organisme d'inspection (Bureau Veritas ou Ceten-Apave) ? Il examine une machine à un moment donné : **l'agrément est accordé sur un modèle de machine, et non pas pour chaque exemplaire fabriqué de cette machine.** Il n'accède parfois pas au code source de son logiciel : la CNIL le recommande[42], mais le "Règlement technique" ne l'impose pas. Il n'est pas clair si ce logiciel peut évoluer par la suite sans nécessiter une nouvelle procédure d'agrément[43]. On ne demande pas à cet organisme d'évaluer globalement la sécurité, mais seulement de vérifier la conformité à **un cahier des charges[44] qui a ses limites**. Ce dernier répond avant tout aux besoins des municipalités : fiabilité de l'électronique, longévité et facilité d'utilisation. En résumé, on pose à ces organismes une question très précise : comme cette question (le "Règlement technique") est mal posée, la réponse (le rapport rendu)

---

de la machine), mais elles sont amovibles. Les machines Indra nous semblent n'en respecter ni l'esprit ni la lettre : un disque dur permet par principe de changer facilement son contenu.

33 La DCSSI est une des cinq directions du SGDN (Secrétariat Général de la Défense Nationale), qui dépend du Premier Ministre. Elle est en charge des questions de sécurité informatique. Présentation.

34 Une première fois il y a plusieurs années, ainsi qu'à l'automne 2005. Le vote par internet a également été étudié récemment.

35 Délibération n°03-036 du 1er juillet 2003. Voir également le rapport 2003, page 92 et suivantes.

36 Français de l'Etranger (CSFE) 2003 (03-019). CCI (04-073). Barreaux de Paris (2005-272), Lyon et Nanterre.

37 Ce ne sera plus le cas avec les machines à voter en réseau du type e-Poll. Elles intègrent en un seul dispositif l'identification de l'électeur, l'enregistrement de son vote et de son émargement.

38 Mais faute de transparence, l'électeur ne peut intuitivement exclure que la machine enregistre l'ordre de passage des votants, ou encore que le boitier de contrôle des machines Nedap/France-Élection (dans les mains du président du bureau) affiche le vote que l'électeur est en train de composer. Cela amène également à réfléchir aux usages détournés de caméras miniaturisées (interdites en Italie), qui seraient moins facilement détectées dans l'environnement déjà technologique d'un bureau de vote informatisé : un câble de plus pourrait passer inaperçu (rapport CEV, app. 2B, page143).

39 CNIL, rapport d'activité 2004 (paru début 2005), page 70.

40 Une première fois à Paris le 27 janvier 2005, jugement annulé par la Cour de Cassation le 7 juin 2005, et une deuxième fois à Lyon le 3 octobre 2005.

41 Etablir une preuve informatique n'est pas simple, et suppose d'avoir accès au système de vote au minimum le soir de l'élection (mais cela ne suffit pas concernant les manipulations qui effacent leurs traces une fois leur forfait accompli, ou qui n'en laissent pas de significatives). Cet accès n'est pas facilité par le secret industriel ajouté aux légitimes exigences de sécurité entourant le scrutin.

42 « La Commission estime que dans le cas d'une élection organisée par une collectivité publique, **le code source des logiciels utilisés par le système de vote électronique devrait être accessible sans restriction**, afin de permettre la réalisation de toutes les expertises jugées nécessaires. », délibération 03-036 du 1er juillet 2003.

43 Par exemple, aux Etats-Unis, la NASED indique quel numéro de version du logiciel intégré de l'ES&S iVotronic est certifié. Rien n'apparait dans l'arrêté d'agrément français. Le paragraphe 2.2.1 du "règlement technique", concernant les "modifications à l'initiative du fabricant" ne dit rien sur le logiciel.

44 C'est à dire toujours ce même "règlement technique fixant les conditions d'agrément des machines à voter".

ne présente guère d'intérêt[45].

- A l'extrémité de la chaine, se situent le fabricant et son importateur[46]. Une organisation bien conçue devrait avoir pour but d'éviter de se poser des questions à son sujet. **Le contrôle devrait être exercé par les premiers maillons de la chaine : en démocratie représentative, les seuls légitimes sont les électeurs, les assesseurs, les délégués et les scrutateurs.** Ce maillon-ci est en effet hautement critique. Nul besoin d'imaginer la collusion de toute une entreprise avec un parti politique. Un petit nombre (peut-être même un seul) de programmeurs ou de techniciens de la chaîne de fabrication peuvent, d'une action unique, compromettre des centaines de machines, et donc une élection entière. Ce cas de figure est celui permettant la fraude la plus efficace. Il illustre une règle générale de l'informatique : **celle-ci permet de faire ce qui était auparavant manuel, à plus grande échelle, parfois longtemps à l'avance, sans se déplacer, sans laisser de traces[47] et avec moins de personnel (parfois tout seul)[48]**. D'autre part, le modèle économique de ces entreprises est la cause du secret qui entoure les machines à voter[49].

A quelle conclusion cela nous amène-t-il ? Elle pourrait s'articuler autour des mots suivants : **le contrôle et la transparence. Ils manquent tous les deux cruellement.** La confiance, pour être fondée, doit s'appuyer sur son corollaire : le contrôle. Pour que cette confiance ne soit pas aveugle, la transparence doit être totale.

Quelle solution préconisons-nous, j'entends déjà certains se demander. Soyons clairs : nous n'avons pas créé le problème, nous avons déjà bien du mal à alerter à son sujet, alors nous ne nous sentons pas tenus d'apporter une solution. **La charge de la preuve ne devrait pas nous incomber**. Aux promoteurs du vote électronique de démontrer son innocuité. Le **principe de précaution** doit s'appliquer également dans ce domaine. Toutefois, quelques pistes existent.

Concernant le manque de contrôle, la solution généralement préconisée[50] par les universitaires et les spécialistes en sécurité informatique, est l'**impression d'un bulletin vérifié par l'électeur (VVAT)**[51]. La machine, une fois le vote composé, imprime un bulletin reprenant les choix effectués. Ce bulletin est montré à l'électeur, derrière une vitre. Il le compare avec l'écran, et le valide. Le bulletin est ensuite conservé dans la machine. Le soir de l'élection, une proportion statistiquement significative des bulletins est dépouillée. Les suffrages sont ainsi vérifiables au moyen d'un circuit indépendant de l'informatique: bulletins papier conservés dans une urne et dépouillement manuel.

Concernant le manque de transparence, la solution réside dans des systèmes de conception totalement ouverte, tant au niveau matériel que logiciel. Comme les clients des systèmes de vote sont des collectivités publiques, le modèle du Logiciel Libre est ici particulièrement pertinent[52]. La sécurité, actuellement basée sur le concept douteux de "sécurité par l'obscurité"[53], en serait renforcée. **Il faut toutefois garder à l'esprit qu'obtenir la transparence sans garantir le contrôle est quasiment inutile.** Le code source d'un logiciel a beau être publié sur Internet, si vous ne pouvez garantir que ce même logiciel est présent dans toutes les machines le jour de l'élection, vous n'avez guère progressé.

Notre système politique est la démocratie représentative. La plupart d'entre nous ne participent pas aux décisions politiques. Néanmoins **détenteurs de la "souveraineté populaire"**, nous déléguons temporairement notre pouvoir à nos maires, à nos députés, à notre président... pour cinq ou six années. Nous ne détenons réellement le pouvoir que le jour des élections. Durant ce jour précis, pourquoi nous demande-t-on une **confiance aveugle** en un système informatique dont l'intégrité est vaguement contrôlée par une poignée de techniciens mal identifiés ?

---

45 Notre interlocuteur chez l'un des organismes concernés nous a confié qu'il aurait apprécié que son entreprise ait pu jouer un rôle dans la rédaction du "règlement technique". Chez un autre organisme, il espérait que le "règlement technique" soit amélioré d'ici les élections de 2007.

46 France-Élection importe Nedap des Pays-Bas, Datamatique importe ES&S des États-Unis, Berger-Levrault importe Indra d'Espagne.

47 Ou alors des traces sans valeur judiciaire, ou plus simplement un résultat électoral plausible n'incitera pas à faire l'effort de les rechercher.

48 Le Pr Roberto Di Cosmo, auteur de l'article "E-duquons l'e-citoyen !", emploie l'analogie suivante : votre facteur ouvre peut-être votre courrier à la vapeur, pour le lire à votre insu. Ce serait désagréable, mais ce ne serait que quelques lettres à un endroit précis. L'équivalent électronique est un ordinateur qui analyse les emails de tout le monde. Rien de bien irréaliste...

49 La sécurité est un prétexte : il s'agit du concept discutable de "sécurité par l'obscurité" (cf note n°53). La véritable raison est que l'investissement fait par ces sociétés est en grande part le développement du logiciel intégré.

50 Afin de ne pas insulter l'avenir, les pétitions, telles celle de David Dill, ou celle de "the free e-democracy project", utilisent l'expression "trace d'audit vérifiée par l'électeur". Elles précisent ensuite qu'en l'état actuel des connaissances, seul le papier permet de réaliser cette trace d'audit.

51 Sur notre site : le bulletin papier vérifié par l'électeur (VVPB/VVAT), détails de ce concept, difficultés de mise en oeuvre, et réalisations (bâclées) à l'étranger.

52 "L'argent public ne doit payer qu'une fois", comme le dit l'ADULLACT.

53 Cf Wikipedia (en anglais) : "Security through obscurity".Un usage raisonnable du secret est possible, en s'inspirant de la cryptographie : les logiciels et méthodes de calculs (algorithmes) sont publics, seule la clef étant secrète. Dans le cas du vote électronique, voir le rapport CEV, app. 2B, page145, Appendix B.

La confiance envers les hommes politiques ou leur possibilité d'action est déjà entamée. Il serait dangereux d'y ajouter une méfiance vis à vis de l'honnêteté des élections.

Voici maintenant quelques questions précises :

Comment rendre au citoyen le contrôle de l'élection, comme le commandent les principes de la démocratie représentative[54] ?

Quel mécanisme garantit le contenu des machines à voter, notamment l'authenticité de leur logiciel ? Nous n'en voyons aucun de sérieux, et nous estimons ce problème insoluble.

Si une élection est contestée, qui apparaîtra responsable de l'incertitude créée par le vote électronique[55] ? A qui sera reprochée une insuffisance de contrôle ?

Quelle est l'explication du marketing invraisemblable pratiqué par France-Élection/Nedap[56], qui cherche à faire croire que ses machines ne sont pas des ordinateurs ? Aucun informaticien ne peut prendre au sérieux de telles affirmations.

Pourquoi une telle opacité entoure le vote électronique, allant même jusqu'aux rapports d'agrément ?

La CNIL a recommandé une "évaluation globale des dispositifs de vote électronique", quand sera-t-elle réalisée ? Ne devrait-on pas également prendre l'avis de la DCSSI[57] ? Voire aller plus loin, et suivre l'exemple de l'Irlande, en créant une commission indépendante pour enquêter sur le vote électronique ?

La démocratie électronique est porteuse de nombreuses promesses. Pourtant, il faut prendre conscience qu'une de ses composantes, **le vote électronique, soulève des problèmes très spécifiques**. S'agirait-il d'un...

www.recul-democratique.org

Machines Nedap/France-Élection :la vérification de checksums est une duperie

L'explication qui suit est un peu technique. Il est tout à fait naturel que vous ne la compreniez pas. Nous vous invitons alors à la soumettre à quelqu'un de votre entourage ayant quelques bases en informatique. ***Que vous ne compreniez pas est néanmoins significatif.*** *Si vous étiez assesseur, vous auriez l'illusion d'effectuer un contrôle de la machine, mais la présence de technologie vous empêcherait d'exercer votre sens critique, et de comprendre que ce contrôle est inopérant.*

Lors de la procédure d'agrément, une seule machine (ou tout au plus quelques unes), sont examinées par l'organisme d'inspection. L'agrément est accordé sur un modèle de machine, et non pas pour chaque exemplaire fabriqué de cette machine. Il est donc crucial de garantir que toutes les machines présentes dans les bureaux de vote soient identiques à celle examinée. Un point essentiel est le logiciel intégré, car l'essentiel de l'intelligence de la machine à voter y réside.

France-Élection, importateur des machines Nedap, prétend contrôler l'authenticité de ce logiciel au moyen de la vérification des checksums. De quoi s'agit-il ? La machine à voter sait calculer un nombre appelé checksum (en français : somme de contrôle) à partir de tous les 0 et 1 qui constituent son logiciel intégré. Si le moindre de ces 0 ou 1 est modifié, ce checksum va changer de valeur. En pratique, deux checksums sont calculés, chacun concernant la moitié de la mémoire. Leur valeur est indiquée dans le manuel d'utilisation de la machine. Le matin de l'élection, les assesseurs doivent donc demander à la machine d'imprimer ces checksums et vérifier qu'ils soient identiques à ce qu'indique le manuel.

Cette procédure est recommandée et considérée comme efficace par le rapport du PTB (Physikalisch-Technische Bundesanstalt), organisme indépendant en charge de certifier le logiciel intégré. A l'exigence[58] *"Dans le cas d'une machine à microprocesseur, toute altération du logiciel intégré par une personne non autorisée sera détectée."*, PTB répond que l'exigence est satisfaite, et se justifie ainsi:

"Les numéros de version des programmes et les checksums du logiciel intégré, pour la carte principale de contrôle, la

---

54 Selon la CNIL, "le recours à des techniques informatiques sophistiquées ne doit pas conduire à faire échapper les systèmes de vote au contrôle démocratique des membres du bureau de vote, des scrutateurs et des électeurs au profit de techniciens informatiques.". Malheureusement, la transition avec le paragraphe suivant est "schizophrénique" Rapport 2003, page 94.

55 "Aucun des systèmes de vote connus de la CNIL ne prévoient de produire des éléments de preuve en cas de contentieux électoral. Ces éléments de preuve s'entendent sur le fonctionnement du système de vote lui-même lors du déroulement du scrutin, de manière à démontrer de façon convaincante qu'il n'a pas donné lieu à un fonctionnement anormal, que celui-ci soit involontaire ou délibéré." Rapport CNIL 2003, page 93.

56 Cf note n°12.

57 Cf note n°33.

58 "Type testing of a voting machine for elections/referenda in Ireland...", page 7, exigence (4).

carte de connexion (communication), et les cinq cartes d'affichage peuvent être affichés, et imprimés, par la machine à voter.
Cela permet au personnel électoral de comparer ces numéros de version des programmes et ces checksums avec les valeurs indiquées par le fabricant dans la documentation (manuel d'utilisateur), ou par exemple inscrits sur un certificat agréé."

Qu'est-ce qui ne va pas ? C'est déjà se tromper de technologie. Un checksum a pour vocation de détecter des modifications ***accidentelles*** : par exemple si l'un des 0 ou 1 s'est modifié à cause d'une défaillance physique de la puce électronique qui le stocke. Par contre, cela ne protège pas des modifications ***intentionnelles***: à cet effet, on utilisera la technique du hash cryptographique.

Soyons charitables, et plaçons ce choix en perspective avec l'époque de conception de cette machine. Parce que finalement, tout cela n'a guère d'importance : ***le principe même de cette vérification est inepte***, quelle que soit la technique employée. En effet, on demande d'imprimer cette checksum au logiciel que l'on cherche à contrôler. L'alternative se présente ainsi : soit il est authentique, et il va réellement le calculer et le résultat sera conforme, sauf défaillance de l'électronique ; soit il a été modifié frauduleusement, et il se gardera de faire le moindre calcul, et se contentera d'imprimer la valeur indiquée dans le manuel d'utilisateur. L'infinité flexibilité d'un logiciel fait que cela ne pose aucune difficulté de réalisation.

Faire confiance à cette vérification de checksum est comme d'arrêter un inconnu dans la rue, de lui demander si il est honnête, et en cas de réponse affirmative, de le charger de faire un retrait d'argent en lui confiant notre carte bleue.

L'ineptie de cette vérification de checksum a été pointée par le rapport[59] de la Commission on Electronic Voting, commission indépendante qui a déconseillé l'utilisation des machines Nedap en Irlande.

Par quel bout que l'on prenne cette procédure de vérification de checksum, on n'en comprend pas la mise en oeuvre. En effet, si l'objectif se réduisait à vérifier le bon fonctionnement de l'électronique, une procédure bien plus simple suffirait : si tout va bien, la machine démarre sans rien dire, sinon elle s'arrête en affichant un message d'erreur. Tous les PC du monde vérifient ainsi leur mémoire lorsqu'on les allume[60], sans pour autant vous demander d'aller consulter leur manuel d'utilisation. La machine Nedap utilise d'ailleurs à cet usage un troisième checksum interne.

La difficulté de contrôle de l'authenticité du logiciel intégré est générale à toutes les machines à voter. La machine concurrente Indra[61] ne fait pas mieux. Elle ne tente même pas de réaliser cette vérification du logiciel intégré. On peut toutefois lui reconnaître le mérite de la franchise.

Le code source, définition

L'essentiel de l'intelligence d'un système informatique est dans son logiciel (en anglais : "software"). Celui-ci existe sous deux formes :

- le "code source" : écrit et lisible par des humains, plus précisément une peuplade appelée programmeurs ou développeurs. C'est la description méthodique, et dans les moindres détails, de tout ce que fait le logiciel. Cette description est tapée comme vous taperiez une lettre, mais au lieu du français, dans un langage informatique. Il en existe des centaines, les plus connus ont pour nom : C, C++, Pascal, Basic, Java... Ces langages ont comme particularité de ne permettre aucune ambiguïté, contrairement aux langages naturels où un mot peut avoir plusieurs sens.
- le "code binaire" ou "exécutable" formé de 0 et de 1, donc uniquement exploitable par l'ordinateur. Il est produit automatiquement à partir du "code source" au moyen d'une moulinette appelée compilateur. Il va faire s'animer l'ordinateur, au départ simple assemblage électronique inerte (en anglais : "hardware", traduit par "matériel").

A l'exception notable des Logiciels Libres, vous n'achetez qu'un droit d'utilisation de l'exécutable. Le code source reste secret et propriété de son concepteur. Sans lui, vous ne pourrez qu'observer le comportement apparent de l'exécutable. Des fonctionnalités cachées (oeuf de Pâques, cheat codes, backdoor...) ne se révéleront pas si on ne connaît pas l'astuce pour les déclencher.

---

59 «Le programme intégré à la machine à voter pourrait être modifié pour altérer les votes. Le programme a un checksum, qui le protège contre des modifications accidentelles, mais qui ne protège pas contre des manipulations délibérées.»
En V.O. « The controlling program inside the voting machine could be modified to affect the vote. The program has a "checksum" which protects it against accidental changes, but does not protect against deliberate tampering. » Michael Scott (Dublin City University), rapport de la CEV, app. 2B, page 139.

60 Pour être précis, il s'agit de vérifier la mémoire vive (RAM), et non pas la mémoire morte (ROM ou EPROM).

61 Seule la chaîne de fabrication est contrôlée par l'organisme d'inspection indépendant Ceten-Apave. Pas d'information sur la ES&S iVotronic.