

COMMENT ÇA MARCHE ?

La machine à voter

Lors des prochaines élections présidentielles et législatives, quelques millions de Français voteront à l'aide d'appareils électroniques. La simplicité de fonctionnement semble encore la meilleure façon de prévenir les tentatives de piratage.

Des puces dans l'isoloir

Piratage, escroqueries et autres détournements d'informations confidentielles font régulièrement la une des journaux. Les machines à voter, déjà utilisées dans certains bureaux de vote en France depuis quelques années suscitent donc des craintes bien compréhensibles. Sont-elles justifiées ?

En France, trois modèles sont homologués : l'un est néerlandais, le deuxième espagnol et le dernier américain [1]. Le premier modèle, produit par la société Nedap, est le plus répandu. Assez sommaire, certains lui reprochent de ne pas posséder les dernières avancées technologiques. Mais compter des bulletins de vote et attribuer des voix à un candidat ou à un autre sans faire de calcul statistique, ni même de pourcentage ne requiert pas une puissance de calcul gigantesque. De simples compteurs suffisent. Par ailleurs, plus une machine est complexe, et plus il est aisé de lui faire réaliser une tâche

Henri-Pierre Penel et Renaud de la Taille,
journalistes scientifiques.

différente de celle pour laquelle elle a été conçue, ce qui est justement à la base du piratage.

La partie supérieure de l'appareil se résume à un petit écran à cristaux liquides encadré de deux grosses touches : correction et validation. La partie inférieure est une zone sensitive comportant 1044 zones tactiles de 2 centimètres sur 1,4 réparties en 29 lignes de 36 cases chacune. Lors du scrutin, cette surface est recouverte d'un fac-similé qui porte le nom de chaque candidat et délimite la zone à presser si l'on vote pour lui : difficile de faire plus simple. Lors de la préparation du scrutin, parallèlement à l'impression de ce fac-similé, les machines sont programmées sur deux mémoires électroniques.

Celles-ci contiennent strictement les mêmes données, et durant son fonctionnement la machine contrôle en permanence leur similitude. On a, en effet, parfois parlé de rayons cosmiques pouvant altérer le fonctionnement d'appareils informatiques. Ici la probabilité que les deux mémoires soient affectées en même temps par la même erreur est quasi nulle. En revanche, si l'appareil détecte une divergence dans le contenu des mémoires, il s'interrompt et signale la panne.

Enfin, le logiciel contenu par ces mémoires reste simple. Pour l'essentiel, il affecte une zone sensitive à un candidat, vérifie que l'électeur a le droit de voter, associe l'affichage d'un nom à une zone frappée, puis stocke la voix, une fois la validation réalisée, dans un second jeu de mémoires. Chacune de ces étapes est réalisée sous contrôle

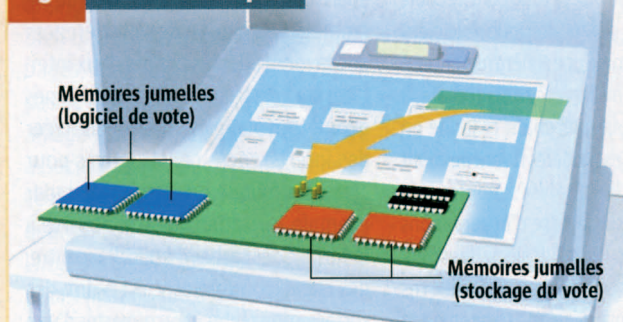
humain et, de l'ouverture du scrutin à sa clôture, un jeu de serrures vient bloquer l'accès aux mémoires.

Lors de la mise en route de la machine, la petite imprimante qu'elle contient imprime un rapport qui permet de vérifier, d'une part, l'absence d'anomalie dans les mémoires de programmation et, d'autre part, le fait qu'aucun vote n'est déjà enregistré. Lorsque l'électeur se présente, il effectue le même parcours que lors d'un vote manuel. Il présente sa carte d'électeur au président du bureau et à ses assesseurs, qui vérifient son identité et son droit au vote. Le président active alors la machine, pour un vote unique, grâce à la télécommande filaire.

L'électeur choisit son candidat, et la machine affiche son choix sur le petit écran pour vérification. L'électeur peut alors le corriger ou le valider. Après la validation, la machine se verrouille de nouveau, jusqu'à la prochaine autorisation de vote, donnée par le président du bureau. La voix est alors stockée dans deux mémoires, totalement dissociées de celles de programmation, et qui exploitent le même principe de redondance des données. Toute divergence entre les contenus conduit à l'arrêt de la machine.

À l'issue du vote, l'imprimante édite un nouveau rapport. Cette fois-ci il précise le bon déroulement du scrutin, le nombre de suffrages exprimés et, bien évidemment, le décompte des voix obtenues par chaque candidat. Ce rapport, signé par le président du bureau et ses assesseurs, est le seul document faisant foi. Légalement, le contenu des mémoires n'a aucune

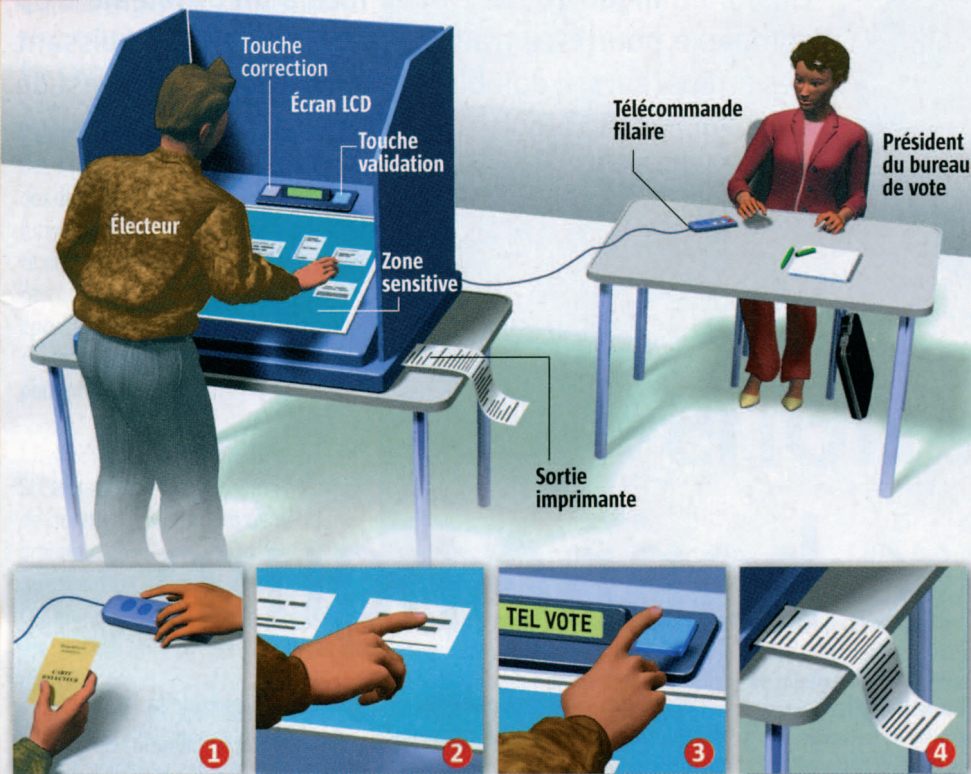
Fig.1 L'électronique



LES COMPOSANTS DE BASE sont doublés, afin de réduire les risques de panne. Ainsi, deux mémoires programmables contiennent le même logiciel, qui attribue les zones de l'écran aux différents candidats et enregistre les votes, dans deux autres mémoires.

COMMENT ÇA MARCHE ? La machine à voter

Fig.2 Les étapes du vote



L'ÉLECTEUR COMMENCE PAR SE PRÉSENTER au président du bureau de vote, qui lui accorde l'autorisation de voter (1). Dans l'isoloir (non figuré ici), il presse la zone tactile correspondant à son choix (2). Son vote s'affiche alors sur un écran à cristaux liquides : il peut encore corriger, ou valider (3). À la fin du scrutin, le président du bureau active l'imprimante de la machine, qui produit un rapport comptabilisant les voix (4).

valeur *a posteriori*. Enfin, un procès-verbal traditionnel, auquel est joint le bordereau imprimé, est établi. Les points d'entrée pour un éventuel piratage sont donc peu nombreux : pas de mise en réseau, identification manuelle de l'électeur, ouverture

[1] <http://tinyurl.com/2r387p>

de l'urne électronique également manuelle par télécommande à fil. Il n'y a guère qu'au niveau des mémoires qu'il puisse y avoir intrusion ou piratage. Mais pour la machine Nedap, bien que le fabricant refuse, en invoquant des raisons de sécurité, de donner le

détail complet de sa programmation interne, il semble que son fonctionnement soit plus proche de celui d'un automate programmable que d'un ordinateur. Un point qui ne permet guère de lui faire réaliser des calculs assez subtils pour affecter le vote tout en passant inaperçu des électeurs ou du président du bureau.

Les machines concurrentes peuvent paraître nettement plus évoluées. Plus proches d'un ordinateur, elles disposent d'un écran tactile, parfois en couleurs, et peuvent, éventuellement, se charger de l'identification de l'électeur par insertion d'une carte à puce. Leur cœur se fonde même sur un système informatique assez traditionnel. Actuellement, en France, elles sont utilisées avec la même procédure que celle décrite précédemment.

Certaines personnes estiment qu'en raison même de leur capacité de calcul plus élevée de telles machines seraient plus faciles à pirater que les précédentes. Ce n'est pas prouvé : ces appareils ne sont jamais mis en réseau, et les contrôles humains, du début à la fin du scrutin, sont omniprésents. Dès qu'il est question de systèmes totalement isolés, il est nettement plus simple de garantir la sécurité. Dans un autre domaine, comparable, les machines à sous électroniques exploitent des logiciels destinés à plumer leurs utilisateurs dans les règles de l'art et n'ont jamais, à notre connaissance, été piratées. ■■

ET DEMAIN Voter de chez soi, mais sans anonymat

■ **ON PEUT S'INTERROGER SUR L'INTÉRÊT** de l'informatique dans le domaine électoral. En effet, son unique atout serait de pouvoir fournir des tendances en temps réel durant le scrutin. Or, en France, une telle pratique est prohibée. Au mieux, le journal télévisé de 20 heures pourrait-il annoncer un résultat définitif dès ses premières minutes, mais les sondeurs font déjà presque aussi bien. L'exactitude du décompte

des voix est primordiale, mais sa rapidité est secondaire.

■ **LE TÉLÉSCRUTIN EST POSSIBLE, VIA INTERNET.** Il est même utilisé pour certaines élections professionnelles : on attribue à chaque électeur un code d'identification unique, qu'il doit introduire dans l'ordinateur pour pouvoir voter. Cela permettrait-il de réduire les abstentions pour cause de vacances, voire de belle journée prin-

tanière ? Il est certain en tout cas que les problèmes sécuritaires prendraient une tout autre dimension. La mise en ligne d'une urne électronique la met en effet à la portée de pirates du monde entier. En outre, sécuriser des transactions, pourtant simples puisqu'il ne s'agit que d'associer une voix à un électeur, tout en conservant l'anonymat qu'impose le scrutin, semble extrêmement délicat.