Science & Vie - février 2007

élection piège à couac...

par Vincent Nouyrigat

En mai, plus d'un million de Français seront appelés à élire le nouveau président de la République en appuyant sur une touche ou un écran tactile. Et ce ne sera qu'un début : de plus en plus de communes s'équipent en ordinateurs de vote pour s'affranchir du dépouillement. Problème : ces machines rendent le scrutin opaque, invérifiable et vulnérable aux fraudes, affirment des chercheurs en informatique. Démonstration à l'appui.

Avec ces machines, qui peut dire si un bug ne fausse pas tout ?

Le film du dimanche électoral est un grand classique, connu de tous: l'électeur entre dans l'isoloir, choisit un bulletin, le glisse tant bien que mal dans l'enveloppe saumon, puis il se dirige vers l'urne transparente, aux dimensions codifiées depuis 1848, pour y déposer sa "voix", sous l'oeil attentif du président du bureau de vote et de ses assesseurs, citoyens lambda. Un scénario réglé comme du papier a musique... qui se voit pourtant de plus en plus réécrit sur l'air moins désuet des nouvelles technologies et de leurs promesses en termes d'efficacité. Ainsi, depuis trois ans, le ministère de l'intérieur, chargé de la bonne application des règles électorales, autorise et subventionne l'utilisation d'urnes informatiques, aux allures de bornes interactives. Avec succès. Au moment du référendum sur la constitution européenne du 29 mai 2005, une cinquantaine de municipalités avaient déjà abandonné leurs boîtes en Plexiglas. Et depuis, Mulhouse, Le Mans, Reims, Boulogne-Billancourt, Orange et bien d'autres ont opté pour l'un des trois modèles d'ordinateurs actuellement agréés, en prévision des élections présidentielles et législatives de cette année.

C'est que les avantages du "e-vote" ont de quoi séduire ! D'abord, ces municipalités n'auront plus à souffrir du manque de volontaires pour assurer le dépouillement. L'informatique s'en charge. *"Avant, nous étions obligés de payer en heures supplémentaires des fonctionnaires municipaux, au tarif du dimanche,* se souvient Alain Masson, adjoint au maire de Brest, première ville convertie. *Alors que nos rnachines, achetées 7 000 euros pièce, seront amorties avant les quatre échéances électorales à venir."* Ensuite, l'e-vote annonce la fin des quelques tours de passe passe frauduleux qui faussent un dépouillement papier. Enfin, et surtout, il contente les médias locaux et nationaux en leur donnant des résultats dès 20 heures pile. De fait, les e-urnes sont dotées d'une carte mémoire flash, semblable à celle de nos appareils photo numériques, qui livre son verdict presque immédiatement. Que rêver de mieux ?

Mais voilà: tout irait pour le mieux dans le meilleur déroulement démocratique possible si de respectés universitaires n'imploraient pas que l'on bloque sur le champ cette douce modernisation électorale. Pour trois bonnes raisons. Selon eux, l'usage de ces ordinateurs de vote rend le scrutin invérifiable, opaque et extrêmement sensible à la fraude. Rien de moins !

DES DIZAINES DE MILLIERS DE LIGNES DE CODE !

A première vue, le nouveau scénario ne parait pourtant pas mériter une telle volée de bois vert: l'électeur s'isole et appuie sur une touche; le programme interprète son choix, l'affiche à l'écran et ajoute " 1 " dans le bloc mémoire correspondant. La simplicité d'un tel logiciel, à la portée de tout bon programmeur qui se respecte, laisse même à penser qu'il fournira toujours des résultats incontestables. Rien n'est plus faux ! D'abord, parce que les fabricants n'ont pas visé la simplicité : par exemple, les urnes conçues par le constructeur néerlandais Nedap - leader en France - accomplissent pleinement leur tâche à partir de... plus de 25 000 lignes de code source ! Dans lequel il faut inclure l'algorithme de comptage, le stockage aléatoire du vote, l'interface graphique et leur propre système d'exploitation. S'il fallait trouver une analogie, que l'on imagine un dispositif

mécanique constitué de 25 000 parties mobiles en interactions ! Dans ces conditions, le risque que se glisse un grain de sable est passablement démultiplié. Et de fait, après l'étape des vérifications, tout programme commercial comprend encore statistiquement entre 1 et 5 erreur(s) par millier de lignes. Cette situation est particulièrement inacceptable dans le cas d'une élection, pour une raison simple : « *un bug a, en général, des conséquences visibles*, explique Roberto di Cosmo, professeur au laboratoire "Preuves, Programmes, Systèmes" (Paris 7). *Par exemple, un avion va s'écraser ou montrer un comportement étrange, ou bien, si on vous retire à tort 50 euros de votre compte, vous pouvez le constater sur votre relevé bancaire... Ces erreurs sont ensuite rectifiées. Or, à cause du secret du vote, le logiciel des urnes informatiques peut produire des résultats faux sans que personne ne le détecte ! Ni ne le corrige...* "

QUI DIT MANQUE DE TRANSPARENCE DIT SUSPICION

Et s'il n'y avait que cela. Car à cette incertitude de fonctionnement s'ajoute le secret dont les fabricants d'urnes informatiques entourent jalousement leur programme de répartition et de comptage des voix. Concurrence industrielle oblige... Autrement dit, en lieu et place d'urnes parfaitement transparentes et au mécanisme compréhensible par tous, les électeurs auraient désormais affaire à de vraies boîtes noires informatiques ! " *Leur confier un vote revient à un pur acte de foi*, s'insurge Roberto di Cosmo. *Ne comptez pas sur moi pour le faire.* " Chantal Enguehard, maître de conférence au Laboratoire d'informatique de Nantes Atlantique, dont le vote électronique est devenu le nouveau thème de recherche, enfonce le clou: "*Il faut imaginer qu'à la place de citoyens, ce soit une entreprise privée qui emporte les bulletins pour en réaliser le dépouillement, sans que quiconque puisse avoir un droit de regard...* "

Une chose est sûre: qui dit manque de transparence, dit suspicion. Ainsi, comment savoir si les choix effectués par les électeurs sont bien comptabilisés selon leurs voeux? Un bug pourrait très bien inverser malencontreusement les résultats à l'insu de tous. Sans compter que l'informatique étant chose flexible, il suffit de quelques lignes de programme pour qu'un vote en faveur d'un candidat se reporte sur un autre. Inquiétant... D'autant qu'aux Etats-Unis, le deuxième plus grand fabricant d'e-urnes, derrière Election Systems and Software (ES&S), est... un bailleur de fonds des Républicains. Et ce n'est qu'un exemple parmi d'autres ! Depuis que le pays s'est massivement converti au vote électronique en 2002, la suspicion gangrène chaque élection, tant les résultats inexplicables et les bugs s'y multiplient. Avec, à la clé, des procès en pagaille et la réprobation officielle de l'Association for Computing Machinery (ACM), l'organisation mondiale des informaticiens professionnels.

UN CODE SOURCE INACCESSIBLE

A première vue, la France semble s'être prémunie contre de tels dérapages: le ministère de l'Intérieur n'a-t-il pas rédigé à l'attention des fabricants d'urnes électroniques un cahier des charges fort de 114 exigences ! D'où il ressort que nos organismes de certification doivent se concentrer sur la résistance de ces ordinateurs aux chocs pendant le transport, aux températures caniculaires, aux embruns, aux sautes de courant, éventuellement aux agressions électromagnétiques, etc. Autant d'exigences belles et bonnes... mais *quid* du code source qui régit le logiciel sur lequel repose exclusivement le résultat des élections ? Eh bien... rien, ou le strict minimum! *"Par acquit de conscience, nous avons demandé et obtenu un accès aux morceaux de code les plus sensibles, notamment pour analyser les risques d'intrusions dans le programme susceptibles de changer les votes ",* tempère Eric Blanc, directeur du pôle Procédés au bureau Veritas, certificateur du modèle de la société ES&S et de celui conçu par Nedap. Le bureau de conformité concurrent Ceten-Apave s'est, lui, reposé *"sur la présentation des tests menés par le fabricant espagnol Indra Sistemas ",* le troisième opérateur en France. Ces analyses, non-obligatoires, et dont le détail est lui aussi soumis au secret, manquent singulièrement d'ambition ! '«*Au vu des enjeux politiques, sociaux et économiques, il faudrait certifier le code des ordinateurs de vote comme un logiciel ' mission critique', type logiciel de contrôle du trafic aérien",* propose Bruce Schneier, grand gourou de la sécurité informatique outre-Atlantique et fondateur de Counterpane, société de protection des réseaux.

L’extrême rigueur imposée en aéronautique s'applique d'ailleurs dès l'écriture. Principaux mots d'ordre: épurer la rédaction, décrire scrupuleusement chaque opération dans une documentation afférente, éviter les techniques de programmation à risques (récursivité, allocation dynamique de mémoire ...). Beaucoup se contenteraient d'une approche plus transparente, en mettant fin au secret industriel. Cela n'a rien d'une utopie: la Belgique publie sur Internet le code source de ses ordinateurs de vote ! Les bénéfices à en tirer sont nombreux- D'abord, les programmeurs, sachant qu'ils seront lus, ont tendance à écrire plus proprement. Ensuite, le programme peut être évalué de façon contradictoire par quantité d'informaticiens. La découverte de failles s'en trouve accélérée. Et l'urne informatique regagne un peu de crédit, au moins aux yeux des familiers de son langage de programmation...

LA CONFIDENTIALITÉ N'EST QU'UN ALIBI

Les trois opérateurs exerçant dans l'Hexagone (ES&S, Nedap et Indra) ont pris l'exact contre-pied de cette démarche. Hormis les questions relatives à la propriété intellectuelle, *"peut-être ont-ils peur qu'un examen public révèle nombre de failles et de bugs, synonymes de mauvaise publicité ",* ose Andrew Appel, chercheur en sécurité informatique à l'université de Princeton et nommé expert dans un procès portant sur les ordinateurs de vote du New Jersey. Ce moment de vérité a déjà eu lieu, en 2003, lorsqu'un échange de fichiers entre des employés de Diebold a transité par un serveur Internet public. Cette fuite assez cocasse permit soudain à de nombreux chercheurs indépendants d'étudier les 49 609 lignes de son code. Les informaticiens de l'université Johns Hopkins de Baltimore en étaient ressortis consternés : ".*Nous ne voyons aucun indice de développement logiciel discipliné !",* écrivent-ils dans leur rapport. Au moins 328 failles seront découvertes, dont 26 susceptibles d'être exploitées pour produire de faux résultats. Hélas, les supputations d’Andrew Appel ne se vérifient pas uniquement dans le cas Diebold. La société ES&S, par exemple, montre un zèle dans la protection de ses archives qui ne trompe pas Dan Wallach. Cet éminent spécialiste en sécurité logicielle de l'université de Rice (Texas) a été nommé expert dans un procès intenté cette fois par des électeurs du Colorado à cette firme du Nebraska. Certes, il a pu avoir accès aux dossiers de certification et à de minuscules bouts de code, mais dans des conditions de confidentialité hallucinantes, bien plus drastiques, selon lui, que lors de ses travaux sur le code ultrasensible de Microsoft ! Son explication ? "Si *chacun des documents que j'ai lus devait être rendu public, ce serait seulement préjudiciable pour la réputation des fournisseurs (pour la mauvaise qualité de leurs systèmes) et pour les organismes de certification (pour la mauvaise qualité de leurs analyses) ",* écrit-il dans son expertise, rendue partiellement publique en septembre dernier. Le peu d'informations consultables suffit à montrer que les programmeurs auraient une furieuse tendance à masquer les problèmes et à ne rien expliquer de ce qu'ils font. De quoi rendre la tâche impossible aux organismes d'audit, de toute façon fort peu curieux. Stupéfiant ! Comme la lecture du logiciel, chargé notamment du comptage des voix, vendu, en 2003, au gouvernement irlandais par la société Nedap - l'équipementier d'une cinquantaine de villes en France. La Commission indépendante qui l'a analysé n'a pas compris grand-chose: "*Il ne semble avoir suivi aucun standard de développement industriel des logiciels ",* concluait-elle, à l'été 2006. Ces observateurs irlandais ont aussi trouvé quantité de codes *a priori* sans aucune utilité, offrant un camouflage idéal aux bugs voire aux sabotages. L'éditeur du programme, Groenendaal, plaidera le manque de dialogue entre ses ingénieurs et les membres de la Commission. Sans vraiment convaincre : les 7 500 urnes Nedap achetées il y a quatre ans par l’Irlande, pour la bagatelle de 52 millions d'euros, n'ont toujours pas été sorties de leurs hangars de stockage...

LE CITOYEN PERD ICI TOUT ESPOIR DE CONTRÔLE

L'INFORMATIQUE PERMET TOUS LES SUBTERFUGES

Mais quand bien même un logiciel de vote serait rendu aussi sûr que les quatre millions de lignes de code d'un Boeing 777, tout ne serait pas réglé pour autant. *"Les membres du bureau de vote ne pourront jamais être certains que c'est bien le programme expertisé qui tourne effectivement dans l'urne ! ",* lance Andrew Appel. Alors qu'un simple regard suffit à vérifier qu'une urne transparente n'a pas de double-fond, les assesseurs n'ont aucun moyen de contrôle aussi fiable sur ces ordinateurs. Pis, *"certains fabricants offrent une parodie de vérification",* dénonce Pierre Muller, informaticien de profession, qui a vu sa commune, Mandelieu (Alpes-Maritimes), s'équiper en ordinateurs de vote en 2005. Depuis, il anime un site Internet pour dénoncer les méfaits du vote électronique (www.ordinateurs-de-vote.org). " Nedap *demande d'imprimer la somme de contrôle* [addition des binaires] *de son logiciel,* poursuit-il. *Cela revient à demander à un programme, possiblement malveillant, s'il est authentique. Celui-ci se débrouillera pour répondre: oui !, ce qui, convenez-en, n'est pas une preuve d'honnêteté."* De même, la dématérialisation du vote enlève tout espoir de contrôle aux citoyens venus assister au dépouillement. *"Ils doivent croire le ticket de caisse sorti par l'ordinateur,* regrette Chantal Enguehard. *Tandis que la validité du résultat du vote papier repose sur l'examen croisé des citoyens, de toutes sensibilités politiques: ceux qui palpent et lisent les bulletins, ceux qui tiennent les comptes et ceux qui regardent par dessus l'épaule. " "Rien n'empêche les assesseurs de simuler, avant ou après chaque élection, un scrutin sur l'ordinateur pour juger de son honnêteté",* se rebiffe Hervé Palisson de France Election, l'importateur français des ordinateurs conçus par Nedap. Certes. Mais c'est oublier un peu vite la gamme immense des subterfuges permis par l'informatique !

Car définir un comportement conditionné par une date et une tranche horaire - le 22 avril 2007, entre 8 heures et 20 heures, par exemple - est le B.A.ba de la programmation. Et si la date de l'échéance n'est pas connue au moment du piratage ? Pas de problème: un électeur complice (ou le pirate lui-même) peut très bien activer le programme voleur de voix le jour du scrutin, à l'abri dans l'isoloir, en appuyant sur une combinaison improbable de touches. La seule difficulté ici consistant dans le détournement d'un nombre suffisant mais raisonnable de voix pour ne pas éveiller les soupçons. A plus grande échelle, le code malhonnête pourrait aussi s'enclencher sur plusieurs urnes au bout d'une centaine de votes ou sur la base de comportements de vote «naturels", très différents des tests élémentaires et rapides des assesseurs. A *posteriori,* aucun outil ne distinguera quels ont été les votes volés, puisque rien ne permet de les identifier et qu'ils sont stockés aléatoirement afin de garantir l'anonymat ! Duper un organisme de certification de programme n'est pas plus compliqué: " *Contrairement à l'encre des bulletins, les codes ont le pouvoir de se modifier par eux-mêmes sur quelques lignes ou de s'effacer pour réécrire dessus le logiciel certifié conforme ",* rappelle Andrew Appel. L'aigrefin peut aussi éparpiller ses instructions sur les centaines de pages du programme.

GARE AU VIRUS VOLEUR DE "VOIX"

Bref, les moyens de renverser plus d'une élection majeure ne manquent pas pour un programmeur d'urnes malhonnête, qui aurait des idées politiques bien arrêtées. D'autant plus que, selon nos informations, le passé de ces informaticiens n'est pas étudié. Et que dire des sous-traitants ! Eux pourraient glisser un cheval de Troie au sein d'un patch censé résorber un bug, sachant que ces petits programmes sont très rarement contrôlés. " *Le fait que ces équipes soient toutes installées à l'étranger les rend moins sensibles aux pressions politiques françaises ",* veut croire Marc Pichon de Vendeuil, adjoint au chef du bureau des élections, au ministère de l'Intérieur. Devant tant de facéties informatiques, la méthode Coué n'est pas forcément la mieux indiquée...

A preuve, l'épais rapport sur l'e-vote publié en juin dernier par le Centre Brennan pour la justice - un pôle de l'université de droit de New York. Ses conclusions, validées par la fine fleur de la sécurité informatique et des pratiques électorales, donnent le frisson: en clair, un pirate informatique pourrait inverser le cours d'un scrutin d'envergure, et les possibilités qui lui sont offertes vont largement au-delà de ce qui avait été envisagé en deux siècles de vote papier ! Au final, les rapporteurs recensent plus de 120 types d'assauts informatiques tout à fait réalisables. Et nul doute que cette contribution théorique n'est que le hors-d'oeuvre des fraudes possibles. C'est en tout cas ce que suggère l'histoire survenue au Centre de politique des technologies de l'information de l'université de Princeton (CITP). *"Dernièrement,* raconte son directeur Edward Felten, *nous avons eu la grande chance de*

recevoir un modèle à écran tactile Diebold Accuvote TS [utilisée par 10 % des électeurs américains], *d'une source dont nous voulons garder l'anonymat, En moins de quatre mois d'analyse, nous avons pu mettre au point un système viral de vol de vote. Son intérêt: il ne nécessite d'avoir accès qu'une petite minute à une seule urne !* " Reproduit devant les caméras de CNN et de Fox News quelques semaines avant les élections de mi-mandat en 2006, ce piratage a fait grand bruit outre-Atlantique. Il ouvre surtout une nouvelle ère, celle du virus voleur de voix, dont les mémoires amovibles des urnes, facilement accessibles, sont de parfaits vecteurs de transmission. Car celles-ci sont utilisées la veille des élections pour entrer la liste des candidats, puis le soir du jour J afin de centraliser les résultats sur une même machine. Le virus se propage alors d'urne en urne, en profitant des largesses de leur logiciel de démarrage, qui n'authentifie pas le code qu'il exécute. *"C'est un problème difficile à résoudre,* admettent d'ailleurs les chercheurs du CITP dans leur publication. *Mais il est quelque peu décourageant de voir les fabricants de machines à voter faire beaucoup moins d'effort sur ce thème que les concepteurs de consoles de jeu. "*

Que dire alors du degré de protection des ordinateurs iVotronic d'ES&S, utilisés à Saint-Malo et à Meylan (Isère) ! *"Leur mode 'superviseur 'est seulement protégé par un mot de passe de trois caractères - celui de la sortie d'usine – largement connu: par ce biais, n'importe qui pourrait effacer tous les votes pendant l'élection !,* avertit Dan Wallach, qui a pu les étudier au cours d'une expertise judiciaire dans le comté de Webb (Texas). *Avant le scrutin, un employé du bureau des élections malhonnête pourrait aussi 'mettre à jour' le logiciel stocké en mémoire, en installant, pourquoi pas, un code hostile.* " Et cela, d'après ce chercheur, en seulement quelques opérations à la portée du tout-venant. Car, là encore, aucun mécanisme ne permet de déceler la présence d'un programme ennemi!

UN ORDINATEUR DÉTOURNÉ EN ... DEUX MINUTES!

Plus généralement, les urnes d'ES&S offriraient un concentré de chiffrement indigent ou inopportun. Illustrations : les fichiers de vote sont rendus illisibles, sans présenter d'autre intérêt que de rendre un audit indépendant plus difficile. Alors que " la *clé de cryptage (Blowfish) est stockée à côté des données qu'elle est censée protéger - une erreur de sécurité fondamentale".* Commentaire acerbe de Dan Wallach: " *Leur manque évident de compétences s'étend bien au-delà de leur manque de compréhension de la sécurité informatique."* Sans que cela ne trouble, visiblement les bureaux de certification américain et français qui ont apposé leur tampon !

LA SOLUTION ? ASSOCIER LA MACHINE ... AU PAPIER

Fort de ses trente années d'expérience aux Pays-Bas, le constructeur néerlandais Nedap, leader des urnes électroniques en France, veut afficher sa différence: "*Nos machines ne contiennent pas d'élément informatique programmable,* clame Hervé Pâlisson. *Elles sont donc beaucoup plus difficiles à trafiquer. "* C'est juste : il aura fallu cette fois deux minutes aux Hollandais de l'association "Wij vertroinven steincomputers niet" (en français, "nous ne faisons pas confiance aux ordinateurs de vote"), savant mélange de hackers et d'universitaires, pour en reprogrammer une. *"Ils ont fait un travail impeccable! ",* apprécie, en connaisseur, Edward Felten. En moins d'un mois d'étude - ce qui est peu pour un projet de piratage - et sans la moindre documentation du fabricant, ces activistes ont pu comprendre puis détourner le fonctionnement du modèle ES3B, très proche de celui utilisé en France. Voilà qui sape à la base cette "sécurité par l'obscurité" à laquelle s'accrochent ces industriels et que résume ainsi Ludovic Viornay, de la société Datamatique, importateur des Votronic en France: *"Si nous ne voulons rien révéler de notre code, c'est pour ne donner aucune indication à d'éventuels pirates."* Sauf que, face à un ordinateur protégé sur ce seul principe, il suffit à un assaillant d'accéder au code binaire, exécutable par la machine, puis de remonter vers la structure du code source (lisible par les humains) par "ingénierie inverse": c'est-à-dire l'enfance dans l'art du piratage ! Dans le cas du Nedap, les hackers se sont aperçus que si les puces contenant la version binaire du logiciel ne sont effectivement pas programmables par l'ordinateur, elles peuvent être aisément... remplacées, d'autant qu'elles ne sont pas même soudées ! Après avoir surmonté ses dispositifs de sécurité électroniques, pourtant plus exigeants ici que chez Diebold, ils sont ainsi

parvenus à subtiliser finement les votes en faveur du candidat voulu, ciblé par une reconnaissance du motif de son parti. Dès lors, les faux résultats peuvent s'enchaîner sur les dix prochaines années, soit la durée de vie estimée de ces ordinateurs, sans susciter la moindre protestation. Bien obligés de réagir, Nedap, ES&S et Indra ont décidé d'installer, les jours précédant chaque élection, des scellés numérotés sur leurs machines. Elles-mêmes placées sous clé, en mairie. Objectif: parer les attaques au cœur de l'électronique ou sur leurs mémoires amovibles. Mais, à bien y réfléchir, la meilleure protection de ces ordinateurs de vote réside peut-être dans la facilité même d'en prendre le contrôle - un pirate digne de ce nom ne serait même pas tenté de relever le défi. A preuve, les urnes produites par l'espagnol Indra Sistemas, en qui Vandoeuvre-lès-Nancy (Lorraine) et Reims font confiance, n'ont pas encore attisé la curiosité des bidouilleurs. Or, *«elles sont sûrement les plus faciles à pirater du marché!»*, évalue Pierre Muller.

La bonne vieille urne garde plus d'un atout

Un constat s'impose à beaucoup: *"Je ne vois aucune solution de vote purement informatique digne de foi,* confie David Dill, professeur d'informatique à l'université de Stanford et fondateur de la Verified Voting Foundation (association pour un vote vérifié), très active aux Etats-Unis. *En revanche, nous pourrions associer à ces machines un outil que nous connaissons bien : le papier !"* Voici comment: l'électeur fait son choix sur l'ordinateur. Un bulletin, reproduisant son vote (si tout se passe bien), est imprimé et s'affiche derrière une vitre. Puis, le votant valide, ou pas. Le bulletin tombe ensuite dans une urne, brassée de temps en temps pour garantir l'anonymat. Les suffrages suivent alors deux circuits indépendants. L'un, électronique, pourra servir immédiatement des résultats aux médias. L'autre, papier, permettra un second dépouillement tangible. Cette idée recueille presque tous les suffrages ! Vingt-six Etats américains ont déjà intégré ce principe à leur législation. En France, aucune loi ne l'impose et aucune machine ne le fait. "*Nous n'y sommes pas opposés, mais il s'agirait d'un geste purement psychologique ",* répond Marc Pichon de Vendeuil, du ministère de l'Intérieur. La position officielle de Nedap est plus embarrassée: *"les erreurs ou les imperfections détectées pendant l'élection pourraient ébranler la confiance des votants ".* Sous-entendu, dans leur technologie. Le début d'un aveu ? Pas vraiment: "Nous *craignons surtout que l'imprimante ne s'enclenche pas à tous les coups ",* rétablit Hervé Palisson. De fait, le recours au papier est encore balbutiant et les modalités exactes du recomptage des voix restent à définir. Même son efficacité n'a rien de sûr ! Après avoir tant critiqué, certains universitaires, tel Dan Wallach, ont toutefois décidé de s'atteler eux-mêmes à la construction de l'e-urne de leurs rêves, dotée d'à peine 4000 lignes de code ! Les premiers résultats sont attendus avec impatience, vers 2008, dans les pays où tout dépouillement manuel parait rédhibitoire: "Aux *dernières élections, j'ai été amené à faire près de 40 choix (choix du shérif, du juge, du directeur d'école, référendums divers*...)", témoigne Bruce Schneier. En France, où la nécessité se fait nettement moins sentir, quelques politiques - essentiellement Patrick Bloche, député de Paris (PS) et des élus locaux Verts - réclament un moratoire sur les machines à voter actuelles. L'acte de résistance de Grenoble, berceau français de l'informatique, pourrait les y aider. Fin octobre, ES&S avait tenté d'y placer 96 ordinateurs - un lot évalué à 400 000 euros. Ses VRP se sont fait rabrouer. Il faut dire qu'ils ont joué de malchance : l'adjoint au maire de la ville, Gilles Kuntz, est aussi maître de conférence à l'Institut national de recherche en informatique et en automatique (Inria) ! Et, très vite, il avait été secoué par le doute. *"Tant de systèmes informatiques tiennent par des bouts de ficelle: la moindre des éducations informatiques serait de refuser de leur faire une confiance aveugle ",* soutient le professeur Roberto di Cosmo, qui a écrit une lettre aux maires sur le point de s'équiper. En espérant qu'à sa lecture, les édiles soient pris d'une violente crise de foi informatique et reconsidèrent les excellentes propriétés d'un certain réceptacle en plexiglas…

QUE DIT LA LOI ?

En France, l'entrée de machines à voter dans les bureaux de vote des communes de plus de 3 500 habitants est prévue depuis la loi **69-419** du 10 mai **1969.** Il s'agissait à l'époque, de lutter contre la fraude à travers des dispositifs mécaniques et électromécaniques. Aujourd'hui, ce sont des ordinateurs, toujours désignés sous l'appellation générique de "machines à voter". Leurs caractéristiques techniques, ayant trait à l'informatique, ont été remises au goût du jour par l'arrêté du 17 novembre **2003.** Le code électoral, lui, n'a pas changé: son article L 57-1 exige, entre autres, qu'une telle machine comporte "un dispositif qui soustrait l'électeur aux regards pendant le vote", n'autorise naturellement "pas plus d'un seul suffrage par électeur et par scrutin", "permette l'enregistrement du vote blanc " (un bouton est prévu à cet effet), comporte des "compteurs qui ne peuvent être lus qu'après la clôture du scrutin", et aussi qu'elle permette "plusieurs élections de type différent le même jour", comme des élections municipales et cantonales. Par ailleurs, l'article L 63 intime au président du bureau de vote de s'assurer "publiquement, avant le commencement du scrutin, que la machine fonctionne normalement et que tous les compteurs sont à la graduation zéro ". Enfin, le dépouillement sur un ordinateur de vote s'opère, selon l'article L 65, en rendant "visibles les compteurs totalisant les suffrages obtenus par chaque liste ou chaque candidat ainsi que les votes blancs, de manière à en permettre la lecture par les membres du bureau, les délégués des candidats et les électeurs présents. Le président donne lecture à haute voix des résultats qui sont aussitôt enregistrés par le secrétaire."

LES PRÉSIDENTIELLES SE JOUERONT AUSSI PAR ÉLECTRONIQUE

Une soixantaine de communes françaises ont déjà troqué leurs boîtes transparentes pour des ordinateurs de vote. Au total, plus d'un million d'inscrits seront appelés aux urnes informatiques pour les prochaines présidentielles, puis pour les législatives. Et le nombre de mairies converties pourrait évoluer d'ici là, car aucune date limite n'est fixée. A ceci près que la décision de s'affranchir des bulletins papier passe normalement par des délibérations en Conseil municipal, parfois houleuses comme à Arniens, Saint-Denis (93) ou Kingersheim (68). La commune doit aussi demander une autorisation préfectorale. Simple formalité: la seule restriction porte sur le fait qu'elle compte plus de 3 500 habitants. En dessous de ce seuil, il est en effet autorisé pour les municipales d'ajouter un nom sur une liste, ce que ne permettent pas ces ordinateurs. Pas plus qu'ils n'autorisent un vote accompagné d'un message, donc jugé nul. Hormis ce détail, les e-urnes ne devraient pas trop bouleverser les habitudes ; l'identification de l'électeur et son émargement se font toujours de la même manière. De plus, le public peut généralement s'exercer avant le jour J: Les bornes Nedap ont ainsi fait le tour des maisons de retraites et des centres commerciaux de Brest, dès 2004. Soit, mais les plus curieux auront du mal à en savoir plus: la Commission d'accès aux documents administratifs, dans son avis du 26 janvier 2006, a indiqué qu'il était impossible de consulter les dossiers de certification de ces ordinateurs pour cause de secret industriel mais aussi... parce que cela pourrait nuire au bon déroulement des élections ! A l'inverse, ceux qui ne lisent pas les gazettes municipales risquent d'être surpris en arrivant au bureau de vote. Tant pis pour eux : si un électeur mis devant le fait accompli "*proteste et exclut de voter sur ordinateur cela sera tout simplement assimilé à un refus de vote* " précise-t-on, serein, au ministère de l'intérieur.