Avertissement
Élections municipales et cantonales, 9 mars 2008

Les observations techniques et juridiques faites durant près de trois ans par des experts (informaticiens, juristes et ergonomes travaillant en France et à l'étranger) avec l'association Ordinateurs-de-vote.org ont permis de dévoiler les principaux problèmes du vote électronique en France.

A l'occasion des élections Municipales et Cantonales 2008, quelques 75 villes s'obstinent à utiliser des machines à voter malgré le coup d'arrêt à leur déploiement imposé par la Ministre de l'Intérieur en janvier 2008 et en dépit des réserves et mises en garde du président de l'association des maires de France (A.M.F.).

Des milliers d'électeurs nous ont contactés pour nous faire part de leur opposition au vote électronique et de leurs craintes concernant la sincérité du vote. Des dizaines de candidats de villes équipées nous ont demandé de leur communiquer les points à surveiller particulièrement afin d'éviter toute triche, erreur ou rupture du contrat de confiance « citoyen » .

Ils trouveront ci-dessous la liste des problèmes de sécurité recensés pour lesquels ils devront être particulièrement vigilants lors des opérations électorales. L'ensemble des problèmes juridiques et de transparence ont déjà été largement couverts par Ordinateurs-de-Vote.org et ont fait l'objet d'une prise de conscience institutionnelle (Conseil Constitutionnel, Sénat, ...)

A la moindre dérive ou erreur constatée sur les points signalés, les électeurs sont encouragés à déposer – sur les procès-verbaux de leur bureau de vote – leur témoignage précis et motivé (date et heure, description précise du fait, description des pièces, indication du nom des témoins ou des électeurs, indication de l'article du code électoral en cause, durée du problème, attitude des personnes présentes, numéro de la machine, nombre d'électeurs ayant émargé, nombre d'électeurs enregistrés sur la machine….).

Les candidats, les présidents de bureaux, les assesseurs et les délégués noteront précisément leurs observations sur les procès-verbaux avant de se pourvoir devant le tribunal administratif (ou correctionnel en cas de délit flagrant visé par le code pénal).

Dans tous les cas, rappelez-vous que le maire de votre commune peut être aussi la cible d'un dysfonctionnement ou d'une fraude électronique. Les ordinateurs de vote électroniques rendent les processus électoraux opaques pour tous, quoiqu'en disent certains technocrates relayant les discours des vendeurs. Restez vigilants.

Nb : Les faiblesses de sécurité visées dans le texte qui suit sont dues à des aléas industriels ou réglementaires quelquefois rédhibitoires. Au-delà de cet aspect, il faut rappeler plus fondamentalement qu'il n'existe à ce jour dans le monde aucun dispositif de vote électronique garantissant à la fois le respect du secret du vote et le réel contrôle de la justesse des résultats par les électeurs.

(I) Problèmes de sécurité observables les plus importants concernant les ordinateurs de vote de type NEDAP et intéressant le déroulement des opérations de vote

CLES DE LA MACHINE A VOTER :

Statut de l'information : *Point expérimenté en mairie, Témoignage disponible pour production en justice.*
Risque : *Bourrage d'urne, non prise en compte de vote, substitution d'urne.*

Chaque machine à voter est munie de deux clés physiques, à l'image d'une véritable urne. Ces deux clés sont destinées à réaliser différentes fonctions très importantes dont le contrôle de la machine, l'édition des résultats, l'invalidation d'une erreur de manipulation ou les retraits/insertions de la mémoire faisant office d'urne électronique.

L'usage simultané des deux clés est réservé au président du bureau de vote qui doit en garder une sous son contrôle, l'autre étant sous le contrôle d'un assesseur.

Tout porteur d'un jeu de clés identique à celle du président et de l'assesseur pourrait avoir accès à l'urne électronique, à la machine et réaliser des opérations frauduleuses

Une expérimentation faite par des élus et des citoyens (ordinateurs-de-vote.org) a permis d'établir qu'un seul jeu de clés ouvrait plusieurs machines.

BOITIER AUDIO :

Statut de l'information : *Constat d'huissier disponible en mairie n'intégrant pas le scellement des boitiers audio.*
Risque : *Détournement de vote, fausse affectation de bulletin.*

Les boîtiers pour déficients visuels sont amovibles. Il devrait y en avoir un par machine à voter mais cette disposition légale (accessibilité et non discrimination) n'est que rarement appliquée.

Lors du paramétrage de la machine en vue d'une élection, avant mise sous scellés, des informations décrivant les candidats (bulletins de vote sonores) sont enregistrées sur le boîtier. A chaque touche désignant une candidature sur la machine, doit correspondre exactement un message audio nommant le candidat ou la liste, ceci afin de permettre une « navigation et un choix audio » pour des déficients visuels.

Après le paramétrage fait en mairie, les machines sont enfermées sous scellés afin que les données de candidature affichées ou enregistrées ne puissent être reprogrammées par accident ou malveillance.

Dans les nombreuses mairies qui ne possèdent que quelques boîtiers audio, ceux-ci ne sont pas scellés dans les machines après paramétrage : des modifications ultérieures pourraient donc être frauduleusement apportées aux messages, induisant en erreur les électeurs déficients visuels.

Seule une simulation-test de vote faite à chaque branchement du boîtier audio par le président du bureau et un témoin (test à coucher sur le procès-verbal), permet de s'assurer de la correspondance entre messages sonores et choix. Si cette opération n'est pas réalisée à chaque fois qu'un déficient visuel réclame que soit mis à sa disposition le boîtier audio stocké en mairie, aucune garantie de sincérité ne peut être apportée.

CONFIGURATION ET CONTENU DU BOITIER « URNE ELECTRONIQUE »

Statut de l'information : *Logiciels et matériels non soumis à l'agrément/contrôle de l'Etat Français*.
Risque : *Contenu initial de l'urne électronique hors contrôle normatif et sécuritaire, fraudes, erreurs.*

Malgré l'inadaptation aux enjeux de sécurité contemporains du Règlement Technique d'Agrément mis en place par le Code Electoral, il apparaît nécessaire de se conformer au minimum à ce dernier lorsqu'il prévoit que les logiciels et modules qui interviennent dans les fonctionnalités des machines soient audités et agréés.

Une telle obligation, requise par le Code Electoral, vise à apporter quelques garanties (ndlr : certes insuffisantes) aux électeurs et à l'Etat quant au fonctionnement des machines à voter. Elle oblige les fournisseurs de systèmes à déposer auprès d'un tiers un exemplaire des matériels et logiciels qui seront vendus et utilisés par les mairies. Ce dépôt, en cas de recherche de fraude, permet au tribunal et aux experts de disposer d'une version de référence, labellisée par un agrément à valeur légale et accessible auprès d'un tiers de confiance ; la détection de modifications frauduleuses est ainsi permise.

De plus, cette obligation apporte un premier niveau de garantie quant à la conformité au code électoral des configurations et données internes aux machines.

Or, avant chaque élection, les machines voient leur configuration de vote mise à jour par un logiciel NEDAP fonctionnant sur un simple PC de bureau, sous Windows, et modifiant le contenu de l'urne électronique utilisée comme mémoire de configuration.

Seul un test intensif, par un expert judiciaire, permettrait de constater que les données informatiques mises dans l'urne au moment de la configuration sont strictement conformes au code électoral, ne comportent aucune information malicieuse et ne font courir aucun risque d'exécution au programme de la machine à voter utilisée dans le bureau de vote.

CONFUSION/MULTIPLICITE D'URNES :

Statut de l'information : *Documentation NEDAP et communication des mairies.*
Risque : *Fraude, erreurs, incohérences de données d'émargement et de vote.*

Villes ayant choisi de procéder à un double scrutin par machine à voter (les votes pour les municipales et les cantonales sont enregistrés par la même machine et par un passage unique de l'électeur).

Les votes sont placés dans une seule urne électronique (boîtier amovible) impliquant la coexistence des bulletins virtuels de deux élections dans le même dispositif de rétention.

Il faut noter que dans le cas des urnes physiques transparentes, le Conseil d'Etat avait précisé que l'apparition d'un bulletin d'un scrutin dans une urne destinée à une autre élection était de nature à interdire la lecture du sens du vote des électeurs.

(II) Problèmes de sécurité observables les plus importants, concernant à la fois les ordinateurs de vote de type ES&S et de type NEDAP, et intéressant le déroulement des opérations de vote

CODE INFORMATIQUE DES MACHINES :

Statut de l'information :
- Nedap : *Démonstration réalisée par des hackers hollandais et présentée aux parlementaires des Pays-Bas.*
- ES&S : *rapport "Security and Reliability of Webb County's ES&S Voting System and the March '06 Primary Election", analyse du code source commandée par l'Etat de Floride "Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware", document diffusé par l'importateur français.*

Risque : *Fraude, erreurs, fonctionnement erratique, pertes de données.*

Nedap : Des informaticiens hollandais ont cloné en quelques jours les puces d'une machine à voter en y introduisant deux types de logiciels. Le remplacement des éléments « modifiées » dans la machine a pu être fait en quelques minutes.

Dans un cas, la machine à voter a permis de simuler un jeu d'échec ! Dans un autre cas, la machine s'est comportée comme une machine normale mais a délivré des résultats faux.

ES&S : Sur la version américaine (même numéro majeur de version que le modèle français : 8.X), sans même ouvrir l'ordinateur, son logiciel interne peut être changé : c'est une procédure prévue pour la mise à jour, mais susceptible de permettre le chargement d'une version délivrant des résultats faux. Cette procédure n'est protégée que par deux mots de passe de trois caractères, qui sont de plus figés à la fabrication. Un transfert de type viral d'une machine à l'autre serait théoriquement possible.

Pour les deux ordinateurs : Jusqu'à ce que le ministère de l'intérieur (décision de Janvier 2008) exige que des précautions renforcées de sécurité soient prises pour les machines à voter, certains maires confiants dans les dires des promoteurs des ordinateurs de vote, n'appliquaient que des mesures de contrôle très faibles. En conséquence, pendant longtemps les machines n'ont pas été mises à l'abri de modifications intentionnellement frauduleuses ou réalisées de bonne foi mais en fraude des agréments. Seuls deux niveaux d'inspection, réalisés par des experts-contrôleurs (assermentés, indépendants et sous contrôle de magistrats), permettraient de confirmer d'une part que les machines n'ont subi aucune modification matérielle et d'autre part que les logiciels embarqués par ces dernières sont conformes – octet par octet (et non par l'intermédiaire d'une « somme de contrôle ») aux modèles ayant reçu l'agrément du ministère.

Problème, la modification d'une portion de programme peut être indétectable sauf comportement visiblement aberrant de la machine :

- Lenteur excessive inhabituelle.
- Impression de tickets présentés de manière incohérente.
- Affichage vacillant.
- Difficultés de prise en compte de commandes.
- Score impossible (ex : 800 votes par rapport à un cahier d'émargement de 730 électeurs ou le contraire),
- Indique « a voté » même en cas d'absence de validation d'un électeur ou le contraire.
- Allumage/extinction difficile de la machine.

Ces comportements peuvent avoir d'autre causes (bugs informatiques recensés sur la documentation obligatoire fournie par le constructeur, problèmes électriques, problèmes mécaniques).

La conjugaison de plusieurs de ces dysfonctionnements apparents est de nature à indiquer si ce n'est à coup sûr une modification du logiciel, du moins un comportement matériel et logiciel pouvant perturber l'élection. Comme le doute ne pourrait être levé que par le biais d'une expertise non partisane, notre recommandation est de faire mettre immédiatement l'urne et la machine sous scellés par les membres du bureau de vote, après avis et autorisation du maire, sans la débrancher ou réaliser la moindre opération

dessus. Quelle que soit la position du maire ou du préfet, il serait sage de saisir immédiatement les services du procureur et d'attendre ses instructions ; demander, le cas échéant, au maire la fourniture immédiate d'une autre machine ou d'une urne trrnasparente et de bulletins papier ; ne pas oublier d'informer la préfecture et le bureau de vote centralisateur. L'ensemble des faits observés et des comportements/dires des acteurs devront être soigneusement notés dans le procès-verbal du bureau.

(III) Problèmes de sécurité observables les plus importants concernant les ordinateurs de vote de type ES&S et intéressant le déroulement des opérations de vote

OBSERVABILITÉ DE LA PARTICIPATION :

Statut de l'information : *Observation visuelle de la machine et communication des mairies.*

Risque : *Bourrage d'urne, non prise en compte de vote, erreurs, incohérences de données d'émargement et de vote.*

L'article L57-1 du Code électoral demande : « Les machines à voter doivent être d'un modèle agréé par arrêté du ministre de l'Intérieur et satisfaire aux conditions suivantes : (...)
- totaliser le nombre des votants sur un compteur qui peut être lu pendant les opérations de vote ; »

Cette demande est traduite dans le Réglement technique par l'exigence 15 : « La machine à voter doit indiquer à tout moment aux membres du bureau de vote le nombre de votes effectués depuis l'ouverture du scrutin. »

Il est impossible aux assesseurs de connaître à tout moment le nombre de votants. Cela nécessite un accès à la machine lorsqu'aucun électeur ne l'utilise, ainsi que l'utilisation du boitier interactif portable (BIP) détenu par le président.