RAPPORT D'OBSERVATIONS

Établi par :

François Pellegrini, maître de conférences en informatique à l'ENSEIRB

expert mandaté par l'association représentative :

Association Démocratique des Français de l'Étranger – Français du Monde

afin d'auditer le déroulement du vote par correspondance électronique des électeurs inscrits sur les listes électorales consulaires des circonscriptions électorales d'Europe et d'Asie et Levant pour les élections de 2006 à l'Assemblée des Français de l'Étranger

---

1. Objet et déroulement de ma mission

Le mercredi 7 juin 2006, j'ai été mandaté par M. Nicoullaud, Président de l'ADFE-FdM, pour intervenir en tant qu'expert désigné par cette association pour évaluer le système de vote mis en œuvre dans le cadre du vote par Internet des Français de l'Étranger. Le rapport d'observations qu'il m'a été demandé de produire a pour finalité d'être adjoint au procès-verbal établi à la clôture du vote par Internet, constituant mes observations[1] relatives à ce dernier.

Comme les délais qui m'étaient impartis étaient assez courts, et qu'un assesseur mandaté par l'ADFE-FdM avait déjà visité le site hébergeant les matériels informatiques, j'ai décidé de concentrer mon analyse sur les aspects logiciels du système de vote. Les machines servant au vote étant pour partie scellées, et aucune intervention sur ces machines n'étant autorisée, j'ai obtenu mes informations par le biais d'échanges de courriels et d'entretiens téléphoniques auprès de personnels du Ministère des affaires étrangères ([redacted]), du Ministère de l'intérieur ([redacted]), de la DCSSI ([redacted]), ainsi que des sociétés EADS ([redacted]) et Experian ([redacted]).

1 Comme on le verra dans la suite de ce rapport, le terme d'« observation » sera très souvent à prendre de façon imagée.

2. Contexte du vote par Internet

2.1. Motivations de la procédure de vote en bureau par bulletins papier

La procédure de vote que nous connaissons est le résultat d'un processus continu d'évolution, dans lequel la procédure de vote et les moyens mis en œuvre ont été améliorés à mesure que de nouvelles techniques ont été disponibles. Par exemple, la mise à disposition d'urnes transparentes, qui offrent des garanties supplémentaires contre le bourrage (en facilitant la constatation que les urnes sont vides au début du scrutin et qu'elles ne contiennent pas de double fond, et en rendant plus difficile le remplacement d'une urne par une autre n'ayant visiblement pas le même nombre de bulletins), n'a pu se faire qu'après l'invention des matières plastiques, les urnes en verre étant trop fragiles et trop lourdes pour être déployées de façon économique. Cette procédure vise à garantir avec le plus de certitude possible un certain nombre de principes qui sont le fondement même de notre démocratie, et avec lesquels il n'est pas concevable de transiger. Ce sont :

(a) **Le secret du suffrage.** Ce principe constitutionnel[2] est garanti par l'inclusion des bulletins dans des enveloppes identiques, et par le mélange des bulletins dans l'urne, qui rompt le lien existant entre la présence du bulletin dans l'urne et l'identité de l'électeur qui l'y a placé. La mise en œuvre d'urnes transparentes augmente les risques de perte du secret, car il serait en théorie possible de suivre visuellement le cheminement d'un bulletin donné depuis son dépôt jusqu'à la table de dépouillement. Ceci n'est cependant pas censé être faisable par un être humain, et l'interdiction de tout enregistrement vidéo continu des opérations suffit à se prémunir contre ce risque.

Le secret du suffrage ne peut être garanti que si le nombre de bulletins recueillis est suffisamment grand : dans le cas hypothétique de circonscriptions unipersonnelles, on pourrait immédiatement déterminer qui a voté quoi. Il faut donc toujours garantir une « dilution » suffisante des suffrages, pour garantir un niveau d'incertitude suffisant sur chacun.

(b) **La liberté du vote**. Le fait qu'un électeur doive obligatoirement prendre un nombre significatif des bulletins qui lui sont publiquement proposés, doive passer seul par l'isoloir, doive mettre son bulletin dans une enveloppe, et que tous les bulletins marqués soient considérés comme nuls, constitue une protection efficace contre l'achat de votes et la coercition. Même si l'électeur s'engage auprès d'un acheteur, ou se voit contraint par la menace de voter pour un candidat donné, il pourra toujours prétexter l'avoir fait, tout en ayant eu la possibilité d'exprimer son libre choix[3]. **Le secret du suffrage est donc une condition nécessaire à la liberté du vote**.

---

2 Article 3 de la Constitution : « *Le suffrage* [...] *est toujours universel, égal et secret* ». Voir par exemple : `http://www.conseil-constitutionnel.fr/textes/constit.htm`.

3 À titre d'exemple du processus de co-évolution entre l'état de la technique et la procédure électorale, on peut citer la nécessaire interdiction des téléphones mobiles et autres appareils de prise de séquences vidéo dans les isoloirs, car ceux-ci peuvent permettre à l'électeur de filmer ses actions dans l'isoloir, et donc être requis comme preuve de bonne exécution par les acheteurs ou racketteurs éventuels. Une telle mesure d'interdiction a d'ailleurs déjà été prise en Italie :

Un grand nombre d'électeurs ne se décidant que dans les derniers jours, voire les dernières minutes précédant leur vote, il est tout aussi essentiel de garantir à l'électeur l'autonomie de son choix en le protégeant des influences extérieures. C'est pour cette raison que des règles très strictes s'appliquent au niveau des bureaux de vote ainsi que des média, afin de laisser l'électeur libre de ses pensées.

(c) **La prise en compte du suffrage**. Le fait que l'électeur conserve toujours lui-même son bulletin en main depuis la sortie de l'isoloir jusqu'au dépôt dans l'urne, qu'il puisse attester par ses propres yeux de la présence de celui-ci parmi les autres bulletins, voire rester jusqu'au dépouillement public et participer à celui-ci, est un élément essentiel de la confiance que les citoyens peuvent mettre en leur système démocratique. La destruction de cette confiance serait, à bien des égards, beaucoup plus dommageable que la découverte des fraudes perpétrées dans quelques bureaux. **Le rôle des assesseurs est à ce titre essentiel**. Tout électeur ne pouvant assister à l'intégralité du processus de vote fait confiance à un assesseur, désigné par le parti pour lequel il compte voter, pour représenter ses intérêts, à savoir la bonne prise en compte de son suffrage. Tout comme l'électeur, l'assesseur peut, grâce à ses propres sens et sans aucun intermédiaire, constater le bon fonctionnement du processus de vote. **La simplicité du processus de vote est donc un élément essentiel de la confiance que les citoyens peuvent y apporter**. Plus le nombre d'intermédiaires est important entre la personne constatant la réalité d'une opération et celle qui en est informée, et moins l'information peut être considérée comme fiable, à moins que ces personnes ne soient liées par une communauté d'intérêts, comme par exemple le désir de voir son candidat gagner qui lie implicitement l'électeur votant pour un candidat et l'assesseur nommé par le parti de ce candidat.

(d) **La sincérité du processus électoral**. La période de calme institutionnel que nous connaissons actuellement n'est qu'un bref moment de répit en comparaison de l'histoire politique agitée de notre pays. Les règles ci-dessus préservent la sincérité du vote contre des attaques extérieures, mais il est également essentiel que le processus de vote puisse résister à des tentatives d'attaques internes, c'est-à-dire de la part des personnes en charge d'assurer l'organisation de l'élection. En particulier, il faut que les cas de fraudes internes puissent être, sinon empêchées, du moins détectées, afin que le droit du peuple Français à disposer de lui-même, liberté constitutionnelle, puisse s'exercer pleinement, y compris en dehors du processus électoral si celui-ci est manifestement empêché. **La possibilité pour tout citoyen de déterminer par lui-même s'il peut faire globalement confiance au processus de vote auquel il est convié est donc essentielle**.

2.2. Vote par correspondance et vote par procuration

C'est pour les raisons énumérées ci-dessus que le vote par correspondance est interdit en France. En

`http://news.bbc.co.uk/1/hi/technology/3033551.stm` .

effet, il ne répond pas, par nature, aux critères (a) et (c), l'électeur pouvant être sous contrainte lors de son vote, ou avoir décidé de monnayer celui-ci sous l'œil d'un acheteur qui pourra contrôler la nature du vote effectué, voire lui-même glisser le bulletin dans l'enveloppe et l'expédier.
Le vote par procuration est cependant de nature différente : s'il ne garantit pas la liberté du suffrage, le nombre limité de procurations dont peut se prévaloir un électeur se rendant aux urnes circonscrit la portée de la fraude, qui se réduit à quelques suffrages par fraudeur. En revanche, avec un vote par correspondance, une officine d'achat de votes tenue par un unique fraudeur peut conduire à la manipulation d'un très grand nombre de suffrages. Cette notion de **portée potentielle de la fraude**, mesurée par le **nombre de suffrages pouvant être altérés par un fraudeur donné**, est essentielle. Il en découle que **tout système qui ne peut offrir de garanties contre la fraude massive ne peut être accepté**.

Pour les Français résidant à l'Étranger, un régime dérogatoire a été instauré, permettant le vote par correspondance. La motivation de cette dérogation est que, ces électeurs se trouvant parfois très éloignés des lieux de vote mis en place, il ne peut leur être matériellement possible de se déplacer pour aller voter à un coût acceptable. Cette dérogation découle donc d'un compromis entre le droit qu'a tout citoyen de pouvoir voter, que la Nation doit honorer, et le risque de fraude potentielle. Un argument en faveur de cette dérogation concerne la portée de la fraude possible : dans le cas d'électeurs répartis sur un territoire vaste et difficile d'accès, un fraudeur potentiel devrait déployer des moyens considérables afin de s'assurer du vote de chacun des électeurs qu'il chaperonne, rendant ainsi insupportable le coût économique de la fraude. En revanche, l'existence d'une concentration d'électeurs diminue le coût économique d'une telle fraude et rend possible un scénario d'achat de votes.

2.3. Vote par Internet

Le vote par Internet, qui a été expérimenté en 2003 lors de l'élection des représentants pour les deux circonscriptions des États-Unis d'Amérique[4], et mis en œuvre de façon systématique pour l'élection actuelle, peut sembler s'apparenter, vu de l'extérieur, au vote par correspondance : il est demandé à l'électeur d'effectuer son vote à distance, l'Internet étant utilisé pour l'acheminement du suffrage depuis l'endroit d'où l'électeur a rempli son bulletin jusqu'au bureau destinataire. Cependant, **la dématérialisation du bulletin constitue en fait une rupture radicale, aux conséquences considérables sur le processus de vote, et dont les risques ne doivent pas être sous-estimés**.

3. Le système de vote

3.1. Descriptif

Le système mis en œuvre pour le vote des Français de l'Étranger appartient à la classe des systèmes de

4 Décret n°2003-396 du 29 avril 2003, n° NOR : MAEF0310019D.

vote électronique à distance (VED). Voici le descriptif du système tel qu'il m'a été présenté par téléphone.

3.1.1. Architecture matérielle

Sur un site informatique central sécurisé situé à Aix-en-Provence sont localisés plusieurs ordinateurs : le premier est le serveur Web sur lequel se connectent les électeurs[5], le deuxième gère la liste d'émargement, le troisième héberge l'« urne électronique », et le quatrième a un rôle de supervision. Ces machines sont interconnectées, mais des équipements informatiques spécifiques (routeurs et systèmes de détection d'intrusions) veillent à ce que les ordinateurs hébergeant la liste d'émargement et l'« urne électronique » ne soient ni accessibles de l'extérieur, ni entre elles ; les seules communications possibles se font entre l'extérieur et le serveur Web (connexions entrantes des électeurs), entre le serveur Web et l'ordinateur gérant la liste d'émargement (pour la mise à jour de celle-ci lorsque l'électeur a transmis son bulletin de vote), et entre le serveur Web et l'ordinateur gérant l'« urne électronique » (pour la prise en compte du suffrage de l'électeur). L'hébergement de la liste d'émargement et de l'« urne électronique » sur deux ordinateurs distincts fait partie des recommandations de la CNIL[6]. Le superviseur interagit avec les deux machines hébergeant l'« urne électronique » et la liste d'émargement, pour en vérifier la cohérence à intervalles réguliers.
Le bureau du vote électronique, dans lequel se trouvent les assesseurs, est pour sa part situé à Paris. Un système de surveillance vidéo renvoie aux assesseurs l'image de la salle des ordinateurs, et un écran de contrôle affiche en temps réel le nombre total de suffrages recueillis dans l'« urne électronique ». Il est également possible grâce à ce système d'interroger à distance, par l'intermédiaire du superviseur, l'ordinateur hébergeant la liste d'émargement, et d'afficher la liste complète des électeurs, par nom d'électeur, par bureau, etc.

3.1.2. Schéma fonctionnel

Tout électeur ayant émis le souhait de voter par Internet doit s'inscrire à l'avance auprès des services consulaires, en fournissant un certain nombre d'identifiants personnels. Par la suite, à la confirmation de son inscription, il reçoit, par courrier postal, un identifiant de connexion ainsi qu'un mot de passe protégé par des moyens physico-chimiques garantissant à l'électeur qu'il puisse savoir s'il est le premier à le lire ou non (il saurait alors que son courrier a été intercepté et que son vote peut avoir été usurpé, mais seulement à la condition que l'intercepteur connaisse l'ensemble des autres identifiants personnels).

Pour voter, l'électeur se connecte, au moyen de tout ordinateur suffisamment récent à sa disposition, au site Web dédié, en utilisant ici encore un navigateur Web suffisamment récent. L'accès au site Web de

5 Afin de garantir la plus grande disponibilité possible du service de vote électronique à distance, plusieurs ordinateurs sont en fait dédiés au rôle de serveur Web (principe de redondance).

6 Point n° I.2 de la Délibération n° 03-036 du 1er juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique : `http://www.cnil.fr/index.php?id=1356` .

vote proprement dit se fait au moyen d'une connexion cryptée (utilisation du protocole HTTP sécurisé par cryptage SSL). Une fois ses identifiants personnels tapés, une « applet » (fragment de programme destiné à s'exécuter au sein du navigateur Web de l'électeur) est téléchargée[7], qui vérifie localement la conformité de son suffrage avec les règles de procédure électorale (nombre de candidats choisis, etc.). Une fois l'électeur sûr de son choix, il valide son vote au moyen de son mot de passe. L'applet utilise alors une clé de chiffrement pour crypter le bulletin électronique, avant de le transmettre au serveur.

Cette clé de chiffrement est la clé publique d'une paire de clés, générée sur un ordinateur dédié peu avant l'ouverture du scrutin, et dont la clé privée, qui servira au déverrouillage de l'urne, a été tronçonnée en fragments conservés sur des supports numériques individuels remis au président et aux assesseurs du bureau de vote.

Lorsque le bulletin de vote crypté arrive sur le serveur Web, le programme de réception effectue deux requêtes auprès des deux autres ordinateurs. D'une part, en se basant sur les identifiants de l'électeur transmis par celui-ci, il demande à l'ordinateur gérant la liste d'émargement de mettre à jour celle-ci. À partir de ce moment, toute nouvelle tentative de connexion de la part du même électeur sera refusée par le système, pour éviter les doubles votes. D'autre part, le bulletin crypté, après une nouvelle vérification de sa conformité, opérée sur sa forme cryptée, est transmis au serveur chargé d'héberger l'« urne électronique ».

Après la clôture du scrutin, le président et ses assesseurs joignent leurs fragments de clé privée pour reconstituer la clé privée complète, qui est utilisée pour décrypter le contenu de l'« urne électronique » et fournir les résultats de l'élection.

4. Observations

4.1. Sur l'organisation du scrutin

Force m'est de constater que **le déroulement de ce scrutin pose un problème grave de violation du secret du vote de certains électeurs**. En effet, en vertu des Articles 9 et 10 de l'Arrêté du 6 avril 2006[8] pris en application du décret n° 2006-285 du 13 mars 2006[9], le président et les assesseurs de chaque bureau de vote recevront d'une part les listes d'émargement sur lesquelles les électeurs du bureau qui ont voté par Internet ont été signalés, et d'autre part la somme des suffrages exprimés par Internet par l'ensemble de ces mêmes électeurs.
Or, vu les faibles nombres d'électeurs s'étant engagés à voter par Internet dans certains bureaux, et qui représentent eux-mêmes des bornes supérieures des nombres de suffrages effectivement exprimés à la

7 C'est justement pour pouvoir disposer des fonctionnalités nécessaires à la bonne exécution de cette applet que le navigateur Web de l'électeur doit être récent.

8 N° NOR : MAEF0610023A.

9 N° NOR : MAEF0610015D.

clôture du vote Internet, il existe une très forte probabilité que les membres de l'organisation des bureaux de vote puissent savoir quel sera le suffrage de certains de leurs électeurs.
Ainsi, à la date du samedi 10 juin 2006, à 23h45, le seul électeur inscrit au bureau de Kaboul n'avait pas voté, mais s'il le fait, son suffrage sera connu avec certitude ; de même pour les bureaux de Riga et de Skopje. Pour le bureau de Colombo, les deux électeurs inscrits ont déjà voté, et la probabilité qu'ils votent de la même manière, et donc que leurs deux suffrages soient connus des membres de l'organisation, est de 50 % si leurs votes sont indépendants ; il en est de même pour d'autres bureaux, comme Bandar Seri, Erevan et Tbilissi. Si les seuls électeurs d'Oulan Bator et Suva à avoir voté pour le moment ne sont pas rejoints, leurs suffrages seront connus avec certitude, et si un autre électeur les rejoint, à 50 %, et ainsi de suite.
Puisque ce système est utilisé de façon expérimentale, il aurait été préférable de prévoir un seuil de nombre d'inscrits par bureaux au dessous duquel le vote par Internet n'aurait pas été activé (cela aurait été possible, puisque par exemple le scrutin électronique n'a pas été ouvert pour le bureau de Hambourg en raison d'un problème de saisie). Maintenant que le scrutin est ouvert et que des suffrages ont été exprimés, la situation est plus délicate. En tout état de cause, si le secret du suffrage était effectivement violé, le scrutin pourrait être annulé[10], le système perdrait toute crédibilité, et le nombre de volontaires pour d'éventuelles expériences ultérieures serait encore plus faible, aggravant le problème.
On se trouve en fait en présence d'un cercle vicieux : parce que le vote par Internet ne peut garantir les critères de liberté de vote, de prise en compte du suffrage et de sincérité du processus électoral, on le met en œuvre sur une petite échelle, mais la petitesse de cette échelle pose alors un problème de secret.

4.2. Sur le système informatique mis en place

À la lumière des explications fournies, il apparaît que les réalisateurs de ce système de vote par Internet semblent avoir fait tout ce qui était en leur mesure pour que ce système *simule* le fonctionnement d'un bureau de vote traditionnel, et je ne mets en doute ni leur compétence, ni l'énergie qu'ils ont déployée pour mener à bien ce projet. Cependant, **le système mis en œuvre n'offre aucune des garanties que l'on doit attendre d'un processus de vote**. Ce n'est pas une question de moyens, mais de principe, comme il sera détaillé dans les sections suivantes.

Je ne peux également que regretter le refus qui m'a été opposé de pouvoir accéder au code objet de l'applet téléchargée sur l'ordinateur de l'électeur, qui ne m'a pas été motivé malgré ma demande et n'est pas dans l'esprit des recommandations de la CNIL[11].

4.3. Sur la dématérialisation du processus de vote

La rupture fondamentale provient de la dématérialisation du bulletin de vote, qui oblige à recourir à un

10 Voir par exemple : `http://www.conseil-constitutionnel.fr/cahiers/ccc13/scrutin2.htm` .

11 Point n° I.1 de la Délibération n° 03-036 du 1er juillet 2003 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique : `http://www.cnil.fr/index.php?id=1356` .

intermédiaire technique pour mener à bien le processus de vote. La dématérialisation de l'information place de fait l'ensemble des participants au processus de vote dans la situation de la caverne de Platon : personne ne peut plus faire confiance à ses sens pour attester de la réalité d'actions immatérielles, se produisant au sein d'équipements informatiques dont seule l'existence peut être attestée, et dont les effets ne sont perceptibles qu'à travers d'autres dispositifs techniques.

Les différents logiciels mis œuvre dans le cadre du processus de vote s'appuient sur des bibliothèques logicielles tierces, des systèmes d'exploitation, et des pilotes de périphériques dont le comportement n'est pas parfaitement connu. C'est pour cela que, alors qu'un logiciel a semblé bien fonctionner pendant des semaines, on peut parfois se placer dans une configuration d'utilisation exceptionnelle, qui n'a pas ou a été mal traitée par le programmeur, et qui conduit à un comportement erroné du programme. La complexité de ces composants logiciels (constitués pour certains de plusieurs centaines de milliers de lignes de code source) les rend extrêmement difficiles à valider par des méthodes mathématiques de preuve de programmes, et de toute manière le fait que code source de ces composants tiers ne soit pas disponible empêche de mener à bien cette tâche. Quel que soit le processus de validation mené sur ces logiciels, son périmètre est de toute façon incomplet.

De plus, même les programmeurs experts, ayant certifié et audité tous leurs logiciels, ne peuvent être sûrs du résultat de leurs programmes. Le célèbre « bogue de la division du processeur Pentium™ », qui n'est pas un cas isolé, en est l'exemple le plus représentatif. Des milliers de personnes ont utilisé ces processeurs, y compris pour des calculs de bureaux d'études, avant qu'un utilisateur, spécialiste de l'arithmétique des ordinateurs, ne débusque ce vice de conception[12]. Le matériel devrait donc lui aussi faire l'objet d'audits poussés, mais le schéma de câblage interne des différents circuits électroniques et composants est lui aussi secret.

Qui plus est, au cours d'un suffrage électronique ayant eu lieu en Belgique, il a été constaté au bureau de Schaerbeek une erreur de décompte de 4096 voix. Après analyse du système, et aucune cause directe n'ayant pu être mise en évidence, la conclusion de la commission d'enquête a été que cette erreur « *pouvait probablement être attribuée à une inversion spontanée d'une position binaire dans la mémoire vive du PC* »[13]. Ceci est extraordinaire, les unités mémoire étant dotées de dispositifs d'auto-correction rendant la probabilité de triple erreur mémoire[14] excessivement faible. Cependant, si cette explication est la bonne, elle illustre de façon exemplaire que la miniaturisation de l'information, désirable en terme de performances, la rend plus fragile. Alors qu'une gerbe de rayons cosmiques est

12 Voir par exemple : `http://fr.wikipedia.org/wiki/Bogue_de_la_division_ du_Pentium` .

13 `http://www.senate.be/www/?MIval=/publications/viewPubDoc&TID=50332887&LANG=fr#3-7/1_38` .

14 Les codes auto-correcteurs d'erreurs ECC incorporés dans les mémoires RAM peuvent détecter et corriger une erreur unique se produisant sur une valeur binaire, détecter deux erreurs sans pouvoir les corriger, et ne pas détecter trois erreurs, car la configuration binaire obtenue en changeant trois bits à une configuration valide peut elle aussi être une configuration valide. Par exemple, en Français, si « POMME » est la configuration valide, « PIMME » et « PISME » sont des configurations modifiées reconnues comme invalides, mais « PISTE » ne sera pas reconnue comme une erreur. Voir par exemple : `http://en.wikipedia.org/wiki/Error-correcting_code` .

suffisante pour changer un scrutin de 4096 voix, la probabilité d'occurence des transmutations atomiques ou sauts quantiques nécessaires au changement du nom porté par un bulletin papier est incommensurablement plus faible, car la disparition d'une molécule d'encre ne rendra pas le bulletin illisible. Si l'explication de l'inversion binaire spontanée n'est en fait pas la bonne, alors cet exemple prouve que le degré de complexité du système mis en œuvre dépasse la compétence des personnes les plus à même de le comprendre, ce qui n'est pas moins inquiétant.

La fiabilité d'un système est celle de son maillon le plus faible[15]. **Remplacer un processus simple, robuste et perceptible par un processus plus complexe, plus fragile, et invisible n'a de sens que si les avantages qu'on en retire sont supérieurs aux inconvénients**. Or, **la simplicité, la robustesse et la perceptibilité sont justement les principes essentiels qui doivent caractériser un processus électoral, et qui ne peuvent être négociés**[16]**.**

4.4. Sur le rôle des assesseurs

Comme on l'a vu en introduction, le rôle des assesseurs est de témoigner en personne du bon déroulement du scrutin et du respect des principes fondamentaux auquel il doit répondre. Mais alors, sur quoi exactement les assesseurs peuvent-ils témoigner ? Tout ce qu'ils peuvent dire avec certitude, c'est par exemple qu'ils ont pu voir en permanence, sur un écran, l'image d'une salle informatique dans laquelle des ordinateurs fonctionnaient. Que l'un au moins des assesseurs a pu visiter une salle informatique correspondant à l'image montrée à l'écran (peut-être même ses collègues de Paris l'ont-ils vu apparaître sur l'image), où ces ordinateurs étaient en fonctionnement.

Pour autant, rien ne peut permettre aux assesseurs de penser, ni tout autant de penser le contraire d'ailleurs, que l'image qu'ils ont vue en permanence est celle de la salle informatique d'Aix, et qu'elle reproduisait fidèlement ce qu'il s'y passait. Il est tout à fait possible qu'ait été inséré, dans la chaîne de transmission, un dispositif de mémoire d'images permettant à certains moments de rediffuser des images déjà acquises pendant que des manipulations physiques avaient lieu dans la salle informatique.

De même, rien ne permet de penser, ni là encore de penser le contraire, que le résultat de l'élection qui sera effectivement affiché sur l'écran au moment du dépouillement numérique correspondra bien à la réalité des suffrages que voulaient exprimer les électeurs devant leurs ordinateurs. De quels outils les assesseurs peuvent-ils disposer pour attester qu'aucune manipulation informatique à distance n'a pu avoir lieu sur les équipements, qui sont interconnectés en permanence, en profitant de failles de sécurité délibérées ou non dans les différents sous-systèmes, ou bien que les logiciels qui s'exécutent sont bien ceux qui ont été validés ?

Il faut pour cela faire confiance aux intermédiaires techniques qui ont réalisé les logiciels et installé les matériels, qui ont conçu ces matériels et les logiciels qu'ils embarquent, etc, toutes personnes qui n'ont

15 Il suffit pour s'en convaincre de repenser au fait qu'une navette spatiale, dispositif technique le plus complexe jamais construit par l'homme, a été perdue à cause du givrage d'un joint d'étanchéité.

16 C'est ce qui différencie un système de vote électronique d'un système de transactions bancaires, par exemple.

pas les mêmes intérêts que les assesseurs et donc auxquels ces derniers ne peuvent justement, par définition, faire confiance puisque leur rôle est d'être critique vis-à-vis du déroulement du processus électoral.
Qu'il me soit permis d'illustrer ce discours par une anecdote : il a été constaté que, lorsqu'on effectue, sur le système d'interrogation basé à Paris, la recherche d'un électeur par son nom et son prénom, le système indique que l'électeur n'existe pas sur la liste d'émargement, alors que lorsqu'on effectue cette recherche uniquement sur le nom, l'électeur est bien trouvé. Ceci montre que les assesseurs n'ont en fait accès qu'à l'ombre de l'ombre, le logiciel d'interrogation de la liste d'émargement pouvant lui aussi se révéler faillible[17].
La dématérialisation du processus de vote vide le rôle d'assesseur de sa substance, et par là même enlève toute possibilité d'attester de la sincérité du processus de vote.

4.5. Sur le vote par Internet

L'utilisation d'Internet comme moyen de communication, ainsi que l'usage de l'ordinateur banalisé de l'électeur, constituent un changement radical par rapport aux envois par correspondance, en terme de portée de nuisance d'un fraudeur potentiel. En effet, avec le système actuel d'envoi postal aux bureaux de vote, un fraudeur ne peut s'interposer physiquement que sur le cheminement d'un nombre réduit de suffrages, que ce soit pour les détruire ou les falsifier. Il en va bien autrement avec l'Internet.

La littérature anglo-saxonne abonde sur les moyens permettant à un petit groupe d'individus décidés, voire à une personne unique, de perturber le fonctionnement global d'un système de vote utilisant l'Internet comme vecteur de communication[18]. Rien ne peut par exemple empêcher une attaque massive du serveur, par saturation de sa connexion à l'Internet (attaques dites de type « déni de service »[19], ou DDoS : « *Distributed Denial of Service* »), qui serait du plus mauvais effet médiatique si elle s'inscrivait dans le contexte d'une attaque de groupuscule. Mais le plus grave concerne en fait la machine de l'utilisateur. Grâce à l'Internet, il peut être très facile de diffuser sur grande échelle des virus capables d'infecter les machines des électeurs, et qui auront pour fonction d'intercepter les frappes des identifiants qu'ils effectuent au clavier, puis d'empêcher la connexion finale au serveur, en redémarrant l'ordinateur de l'électeur ou en bloquant son navigateur, après avoir transmis les informations recueillies à une machine relais piratée pour l'occasion et affiché, comme leurre, une fenêtre indiquant que le vote a bien été pris en compte. Dès lors, le fraudeur pourra, en quelques secondes, effectuer le vote de son choix au nom de l'électeur. Celui-ci, s'il recommence le processus de vote par acquis de conscience, recevra du serveur le message disant que son vote a déjà été pris en compte, et supposera alors que son navigateur ne s'est bien arrêté qu'après la validation de son suffrage. De même, en falsifiant à distance les informations réseau permettant la communication entre

17 De façon amusante, le système n'accepte pas non plus les noms et prénoms contenant la lettre « o », cette dernière devant être remplacée par le symbole « % » afin que la requête puisse aboutir.

18 Voir par exemple : `http://avirubin.com/vote/` .

19 Voir par exemple : `http://fr.wikipedia.org/wiki/Déni_de_service` .

l'ordinateur de l'électeur et le serveur du système de vote (techniques dites de « *DNS poisoning* »[20]), il est possible de faire croire à l'utilisateur qu'il se connecte sur le bon serveur alors qu'il interagit avec un serveur pirate qui, une fois ses identifiants obtenus, effectuera à sa place le vote, mais pour un autre candidat. Ces quelques exemples d'attaques sont indétectables par le site serveur, mais surtout peuvent être menées à grande échelle depuis n'importe quel point du globe.

5. Recommandations

À la lumière de ce qui précède, voici les recommandations que je peux formuler.

5.1. Sur la violation du secret du scrutin

Afin de ne pas contrevenir aux recommandations de la CNIL, ni surtout à l'Article 3 de la Constitution, il est à mon sens nécessaire d'annuler les élections pour les bureaux dont le nombre de votes reçus par Internet sera inférieur à un seuil donné. Idéalement, il faudrait que ces résultats ne soient même pas dépouillés. Ceci implique la reprise individuelle de chaque bulletin, dont on m'a dit qu'ils étaient individuellement archivés sur la machine hébergeant l'« urne électronique », au moyen d'une application dédiée écartant les bulletins étiquetés comme relatifs aux bureaux en question.

5.2. Sur le vote électronique à distance

L'utilisation de tout système conduisant à une dématérialisation de l'information du suffrage est à proscrire.

Dans les cas où il est nécessaire de mettre en œuvre un mécanisme de vote à distance, comme par exemple pour les Français de l'Étranger, **le mécanisme le plus fiable reste le vote par correspondance papier**. Comme montré plus haut, le vote dématérialisé n'offre aucun contrôle, et permet une portée de fraude considérable.

Ces arguments ne sont d'ailleurs pas nouveaux. Au début de l'année 2004, le FVAP (« *Federal Voting Assistance Program* »), l'agence étasunienne en charge du vote des personnels militaires et des citoyens résidant à l'Étranger, avait commandé un rapport d'audit sur le système de vote électronique SERVE qui devait être déployé dans le courant de l'année 2004. Sur la base de ce rapport[21], bien plus détaillé techniquement que le mien et dont je recommande la lecture[22], le FVAP a définitivement arrêté son programme. Ici encore, il ne s'agissait pas d'une question de moyens (les États-Unis n'en manquent

20 Voir par exemple : `http://en.wikipedia.org/wiki/DNS_poisoning` .

21 Disponible sur : `http://www.servesecurityreport.org/` .

22 Le site : `http://www.recul-democratique.org/article.php3?id_article=136` offre une traduction en Français de ce rapport, et précise qu'elle émanerait de services de l'État. Je trouve surprenant que puisse être mis en œuvre en 2006, en toute connaissance de cause puisque ce rapport est effectivement connu des acteurs du projet, un système dont le principe de conception a été rejeté de façon aussi argumentée deux ans plus tôt.

assurément pas) ou de faiblesse cryptographique, mais bien de principe.

Le manque de sécurité de l'Internet n'est pas seul en cause. Même dans le cas de systèmes de vote utilisant un réseau plus contrôlé et sécurisé, comme par exemple le vote par SMS ou téléphone mobile, de graves problèmes se poseraient pour des élections de grande ampleur : il serait facile à des fraudeurs de racoler des quartiers entiers, proposant des sommes en liquide contre le fait que l'électeur effectue devant le fraudeur l'opération de vote pour le candidat désigné. L'impact qu'aurait ce genre de pratique, même circonscrite, sur l'image du processus électoral et de ses représentants, serait désastreuse. Ce ne serait pas un service à rendre à la démocratie.

5.3. Sur le rôle des assesseurs

Je ne peux que recommander aux assesseurs de ne s'engager que sur ce qu'ils ont effectivement pu constater de leurs propres sens ; une image affichée sur un écran, qu'elle figure un paysage ou des colonnes de chiffres, ne représente qu'elle-même. En tout état de cause, **je ne pense pas que la sincérité d'un scrutin dématérialisé tel que celui-ci puisse être garantie**, ni par eux, ni par moi, ni par quiconque.

Rédigé à Bègles le 12 juin 2006.

François Pellegrini