

Ceci n'est pas une urne: À propos du vote par Internet pour l'Assemblée des Français de l'Étranger

Andrew W. Appel*

Le 14 juin 2006 à Rocquencourt, France

Résumé

Le lundi 5 juin 2006, je me suis rendu à une séance de formation destinée aux assesseurs de l'élection mondiale par Internet de l'Assemblée des Français de l'Étranger. Cette Assemblée élira à son tour 12 membres du Sénat français, ainsi la légitimité de cette élection est importante même pour les citoyens résidents en France. J'ai remarqué que de nombreux aspects du processus de cette élection rendront impossible aux assesseurs de certifier avec la moindre confiance que l'élection se soit déroulée sincèrement et sans fraude.

Un bureau de vote français normal comporte de nombreuses protections, et chacune de ces protections existe parce qu'autrefois, sans elle, il y a eu de la fraude électorale. De nombreux pays à travers le monde – pas seulement la France – ont fait l'expérience de la fraude électorale, et de nombreux pays ont des protections très similaires. En conséquence, il est important que les assesseurs puissent voir de leurs propres yeux que l'urne est vide au début de l'élection – parce que le bourrage d'urne s'est pratiqué autrefois. Ils peuvent voir de leurs propres yeux l'électeur entrer seul dans l'isoloir – parce que la vente de votes et la coercition se sont pratiquées autrefois. Les assesseurs peuvent voir l'électeur déposer un seul bulletin dans l'urne – qui est même transparente afin d'être plus facile à contrôler – parce qu'il y a eu de la fraude autrefois. Ils peuvent entendre que personne d'autre qu'un électeur ne glisse un bulletin dans l'urne, parce qu'une sonnerie se déclenche chaque fois que la fente s'ouvre. Ils peuvent voir que les votes sont comptés correctement à la fin de la journée – ils sont comptés publiquement, parce que sans cela, il y a eu de la fraude autrefois. Ce qui est compté, ce sont des bulletins réels en papier, que tout le monde peut voir et comprendre. Ainsi, lorsque les assesseurs annoncent les résultats en fin de journée, ces résultats sont considérés comme légitimes parce que tout le monde peut voir et comprendre chaque étape du processus. Ce processus comporte de nombreuses protections. Chaque protection existe parce que, sans elle, il y a eu de la fraude autrefois, et chacune implique la participation directe des assesseurs.

Par contraste, le processus d'une élection par Internet – cette élection de l'Assemblée – ne comporte aucune protection vérifiable directement par les assesseurs. L'élection est effectuée par un système conçu par EADS et mis en oeuvre par Experian dans une salle à Aix-en-Provence, et elle est contrôlée à distance par les assesseurs depuis une salle à Paris. Depuis Paris, les assesseurs voient une image vidéo provenant d'une caméra placée à Aix. Cette image est censée montrer une urne – non pas une urne physique, mais une salle informatique. Les assesseurs voient également un navigateur web censé montrer des données venant des ordinateurs d'Aix : le nombre de votes déjà dans l'urne virtuelle, le nombre d'électeurs inscrits, le nombre d'électeurs ayant déjà voté.

Il est possible de programmer un ordinateur pour simuler presque tout phénomène. Un logiciel peut tout aussi bien effectuer une élection régulière qu'une élection frauduleuse. Chaque vote exprimé par Internet est reçu et traité par un logiciel sur un serveur web à Aix. **Il est très facile d'écrire un logiciel qui, lorsqu'il reçoit un vote pour le candidat A, dépose dans l'urne un vote pour le candidat B.** Les assesseurs n'ont aucun moyen de savoir quel logiciel est installé sur les ordinateurs d'Aix, parce que EADS considère ce

* A propos de l'auteur : Andrew W. Appel est Professeur d'informatique à l'Université de Princeton dans le New Jersey, aux États-Unis. De juillet 2005 à juillet 2006, il est professeur invité à l'INRIA (Institut National de Recherche en Informatique et en Automatique) de Rocquencourt, en France. Le Professeur Appel est enseignant-chercheur en sécurité informatique et a donné à Princeton une série de cours sur l'histoire et les technologies du vote.

logiciel comme un secret industriel, et ne veut pas le montrer aux assesseurs. Même si EADS le leur montrait, les assesseurs n'auraient aucun moyen de savoir si le logiciel présenté est bien le même que celui installé sur les ordinateurs d'Aix.

En 2003, l'armée américaine a passé commande du développement d'un système de vote par Internet, afin de permettre aux soldats américains loin de chez eux de voter à l'élection présidentielle de 2004. Préalablement à l'élection, l'armée a composé une commission d'experts pour évaluer le système avant de l'utiliser. Ces experts ont produit un rapport, le "rapport SERVE" (www.servesecurityreport.org) concluant qu'il y a trop de problèmes avec le vote par Internet : en particulier la vulnérabilité des machines clientes au détournement de vote par des virus, la vulnérabilité des serveurs et l'impossibilité globale pour les assesseurs de savoir ce que le logiciel est en train de faire. Sur la base du rapport SERVE, l'armée américaine a décidé d'abandonner le vote par Internet. En tant qu'expert en sécurité informatique et en technologies du vote, j'estime que ce fut une sage décision.

Lorsque que l'élection se terminera le 18 juin 2006, le peuple français et les assesseurs qui le représentent n'auront aucun moyen d'être sûrs que l'élection se soit déroulée sincèrement et sans fraude. Il n'existe pas de manière d'effectuer une élection par Internet qui puisse assurer sa légitimité.

Introduction

Le lundi 5 juin 2006, je me suis rendu à une séance de formation à Paris au Ministère des Affaires étrangères, non loin de l'Arc de Triomphe. L'objectif de la réunion était de former les assesseurs officiels du "bureau du vote par voie électronique" d'une élection effectuée par Internet. Du 6 au 18 juin, les citoyens français vivant à l'étranger (en Europe, Asie et Moyen-Orient) votent pour leurs représentants à une Assemblée de 155 conseillers, l'Assemblée des Français de l'Etranger. Les conseillers d'Afrique et d'Amérique ont été élus en 2003, la prochaine élection aura lieu en 2009.

L'Assemblée représente les intérêts des citoyens français à l'étranger auprès du gouvernement français, et elle élit également 12 sénateurs au Sénat français, lequel est influent sur les lois et le gouvernement français.

Déroulement normal d'élections en France

Comme la plupart des démocraties, la France possède des lois spécifiques régulant le fonctionnement des bureaux de vote. Des assesseurs (correspondant aux *pollworkers* ou aux *election judges* des différents Etats américains) sont présents physiquement dans le bureau de vote durant toute la journée de l'élection. Ils supervisent le scrutin afin de s'assurer qu'il a lieu conformément aux lois et sans fraude.

Dans la plupart des élections en France, on utilise des bulletins de vote. Contrairement aux Etats-Unis, où les électeurs cochent au crayon un bulletin unique pré-imprimé, les électeurs français doivent choisir parmi plusieurs bulletins pré-imprimés, préparés par chaque parti politique. L'électeur prend au moins deux de ces bulletins pour se rendre dans l'isoloir, met un seul bulletin dans l'enveloppe officielle, sort de l'isoloir et dépose l'enveloppe contenant le bulletin dans une urne. Le mot français *urne* vient du latin *urna* qui veut dire pot, récipient. Les Romains votaient en jetant des billes dans des récipients en terre. En France, l'urne est une boîte verrouillée, pourvue d'une fente sur le dessus.

L'électeur ne coche rien sur le bulletin ; d'ailleurs, une marque, quelle qu'elle soit, invaliderait le bulletin. Ceci peut surprendre l'électeur américain : comment les Français peuvent-ils à la fois voter pour le Président, les députés, les sénateurs, les maires, les gouverneurs, les shériffs et les *dogcatchers*¹ avec un tel système ? Il faut préciser que la France n'a pas de système fédéral comme les Etats-Unis, et les Français votent pour une

¹ NdT : Aux Etats-Unis, employé municipal chargé d'attraper les chiens errants. Autrefois, dans certains endroits, ils étaient réellement élus. De nos jours, c'est une expression condescendante désignant tout poste de "faible" importance soumis à élection.

seule chose à la fois : il y a un scrutin pour les élections présidentielles, un autre pour les élections parlementaires, et encore un autre pour les élections municipales. Ainsi, puisqu'il s'agit d'une seule élection à la fois, la méthode consistant à choisir un bulletin parmi plusieurs autres fonctionne parfaitement bien.

Les marques de crayon sur un bulletin pourraient être utilisées par un électeur pour s'identifier, et dans l'hypothèse d'un chef politique local corrompu, prouver comment il a voté. La France (tout comme les Etats-Unis) a probablement connu dans son histoire des problèmes de corruption et de coercition, et a ainsi institué des procédures pour éviter ces fraudes : le bulletin secret, qui ne permet à personne de savoir pour qui l'on a voté, ni même de prouver quel a été son vote.



Ceci n'est pas une urne

Comme dans toute élection par bulletins de vote se déroulant en bonne et due forme, les assesseurs surveillent l'urne toute la journée afin de s'assurer que personne ne dépose de bulletin frauduleusement. Ils vérifient que l'urne est vide au début de la journée. Dans la plupart des pays, on vérifie cela en ouvrant l'urne, mais en France, cette dernière est transparente. Cet exemple de procédure électorale est très frappant : les assesseurs peuvent ainsi contrôler le contenu de l'urne du début à la fin. Ceci est dû au fait que la France (tout comme les Etats-Unis) a vraisemblablement connu dans le passé des problèmes de bourrage d'urne ou d'autres formes similaires de fraude (les Américains peuvent alors se demander « Mais les assesseurs peuvent pourtant voir ce qui est inscrit sur les bulletins puisque l'urne est transparente ? », mais rappelons le fait que l'électeur met son bulletin dans une enveloppe avant de la déposer dans l'urne.).

A la fin de la journée, les voix sont comptées. Ce sont les citoyens qui dépouillent les votes, devant les assesseurs, lesquels représentent les différents partis politiques. L'un de mes collègues en France (je suis cette année chercheur invité à l'INRIA, le laboratoire de recherche français en informatique) m'a raconté qu'une fois, alors qu'il allait voter en fin de journée, on lui a proposé de rester pour le dépouillement. On a ouvert l'urne et étalé son contenu sur la table, on a ouvert les enveloppes une par une puis compté les bulletins. Pour de telles élections, le comptage à la main est une bonne solution puisque le bulletin correspond à un seul scrutin. Je ne recommanderais pas cette méthode pour une élection américaine où le même bulletin est utilisé pour plusieurs scrutins ; je pense que la lecture optique des bulletins de vote, suivie du recomptage à la main de bulletins venant de circonscriptions sélectionnées au hasard, reste ici la meilleure solution.

Le comptage des voix avec la présence de représentants de tous les partis correspond à la façon dont les recomptages à la main sont effectués aux Etats-Unis. Il paraît évident que les deux pays ont connu des problèmes de corruption dans le comptage des voix.

Contrairement aux Etats-Unis, la France n'admet pas les votes par correspondance dans une élection normale. Apparemment, dans le passé, ces derniers ont été associés à des problèmes de fraude (corruption ou coercition).

En fin de journée, les assesseurs rédigent et signent un procès-verbal, c'est-à-dire un rapport écrit concernant d'une part les résultats de l'élection de ce bureau de vote et d'autre part leur jugement sur le bon déroulement du vote, sans fraude et conformément aux procédures.

J'ai fait cette longue digression sur le déroulement normal d'élections en France afin de bien illustrer le fait que la loi française possède de nombreuses règles spécifiques quant au déroulement des scrutins à bulletin secret et au rôle des assesseurs. Cependant, la réunion à laquelle je me suis rendu ce lundi concernait la formation des assesseurs d'une élection effectuée par Internet. Comme vous pouvez l'imaginer, les procédures sont quelque peu différentes.

Le vote par Internet pour l'Assemblée

Il y a plus de 500 000 électeurs inscrits pour cette élection. Pour l'élection 2006 de l'Assemblée, chaque citoyen a le choix de voter en personne dans un consulat français à l'étranger, par courrier physique ou par Internet. Au 6 juin, environ 28 000 électeurs avaient choisi de voter par Internet, ce qui représente à peu près le tiers de la participation habituelle pour cette élection. Chaque pays ou région du monde a ses propres représentants; par exemple, les électeurs français des pays scandinaves choisiront parmi plusieurs listes de candidats spécifiques à ce groupe de pays.

Comme pour chaque élection, le travail des assesseurs est de surveiller l'élection et de s'assurer de leurs propres yeux que chaque électeur est légitime, que chaque électeur légitime a la possibilité de voter, que chaque électeur dépose un vote – et pas plus d'un – dans l'urne, que l'urne est vide au début de l'élection, qu'il n'y a aucune interférence avec l'urne pendant l'élection, et que le contenu de l'urne est compté correctement à la fin de l'élection. Le 5 juin, le jour précédant le début de l'élection, il y avait une séance de formation pour les assesseurs. Les formateurs étaient trois ingénieurs d'EADS, la société qui a conçu le logiciel, et un d'Experian, la société engagée pour organiser en pratique l'élection. EADS est un grand fabricant européen dans les domaines aérospatial et militaire; Experian est la filiale d'une grande société britannique de “solutions informatiques”.

J'ai assisté à cette séance de formation en tant qu'observateur, et non pas en qualité officielle. Lors de cette séance, plusieurs choses nous ont été expliquées : comment les électeurs s'étaient déjà inscrits pour le vote par Internet; comment les électeurs allaient interagir avec le système; l'architecture générale de l'installation à Aix-en-Provence (dans le sud de la France); et l'interface utilisateur qui permettrait aux assesseurs de contrôler depuis Paris l'élection se déroulant à Aix. En fait, le premier objectif était d'expliquer l'interface utilisateur, par des diapos Powerpoint.

Comme cela nous a été expliqué, avant l'élection, chaque électeur visite un site web afin de télécharger une applet Java, qui sera l'interface utilisateur pour voter. Cette étape permet de tester la compatibilité de la machine de l'utilisateur, du système d'exploitation et de la machine virtuelle Java. Le téléchargement de la machine virtuelle Java peut être conseillé à l'utilisateur, ou bien il peut lui être expliqué que son système n'est pas compatible : il devra alors soit trouver un autre ordinateur pour voter, soit revenir à l'une des deux autres méthodes de vote (en personne, ou par courrier physique).

Une applet Java est utilisée au lieu de HTTP ordinaire, afin que le vote soit encrypté puis signé avant d'être envoyé par le canal SHTTP. Le fait d'encrypter et signer le bulletin sur la machine cliente est censé assurer le secret et l'authenticité du bulletin. J'expliquerai plus loin pourquoi il n'est pas possible pour les assesseurs d'évaluer si l'applet Java apporte réellement secret et authenticité.

L'applet Java tournant sur l'ordinateur de l'utilisateur transmet le bulletin à un serveur web tournant à Aix-en-Provence. Plusieurs de ces serveurs fonctionnent en parallèle, tous dans la même salle sécurisée. Il y a aussi dans cette salle un ordinateur avec une base de données contenant la liste des électeurs inscrits (l'ordinateur Liste), un autre ordinateur avec une base de données contenant les votes déjà exprimés (l'ordinateur Urne) et un troisième ordinateur contenant un logiciel pour gérer l'élection et faire des requêtes sur les deux bases de données (l'ordinateur Supervision).

Dans une salle distante de 760 km, dans un immeuble du Ministère des Affaires Étrangères dans un très beau quartier de Paris, il y a quelques machines supplémentaires. C'est la salle utilisée par les assesseurs. Une de ces machines est connectée par un VPN (Virtual Private Network - réseau privé virtuel) à la machine Supervision à Aix, et ainsi d'autres PCs de cette salle parisienne sont mis en réseau avec les machines d'Aix (moyennant divers routeurs et firewalls).

La séance de formation s'est tenue dans la même salle que les assesseurs allaient réellement utiliser, j'ai donc pu voir par moi-même les machines et les câbles à Paris. Je n'ai pas vu la salle d'Aix, mais les ingénieurs d'EADS et d'Experian m'en ont parlé. Il y avait environ 8 assesseurs à la séance de formation de ce lundi; la plupart d'entre eux ne semblaient pas s'y connaître en informatique. Ils ont été invités à visiter la salle d'Aix, mais il était assez clair qu'aucun d'entre eux ne le ferait.

Une interface utilisateur, tournant dans le navigateur Microsoft Internet Explorer sur les PCs de Paris, est censée montrer des données transmises par la machine Supervision d'Aix. J'écris “censée” parce que, comme les assesseurs et moi sommes assis dans une salle à Paris, il nous est impossible de savoir quelle est l'origine des nombres affichés sur l'écran. Nous ne pouvons nous fier qu'aux dires des quatre ingénieurs de la séance

de formation.

De même que je n'ai aucun moyen d'être sûr que les données viennent d'Aix-en-Provence, je n'ai aucune base pour soupçonner qu'elles *ne* viennent *pas* d'Aix. Je continuerai à écrire “censé” pour indiquer “c'est ce qu'on nous a dit”.

Comme il est demandé aux assesseurs de signer un procès-verbal établissant qu'ils ont vu une urne vide, un des écrans disponibles à travers l'interface utilisateur est censé montrer le nombre de bulletins enregistrés dans la base de données Urne. Au début de l'élection, les assesseurs doivent vérifier que l'urne est vide; cela les intéresse donc de voir que cet écran de l'interface indique 0 vote dans l'Urne. Il y a également une caméra vidéo censée montrer la salle d'Aix sur les écrans des PCs de Paris, parce que l'une des choses que l'on demande aux assesseurs de vérifier, c'est “qui a accès à l'urne ?”.

On nous a été expliqué l'utilité de plusieurs autres écrans de l'interface utilisateur web. Les assesseurs ont la possibilité d'interroger la base de données des électeurs inscrits pour voir lesquels ont l'intention de voter par Internet. Ils peuvent aussi voir le format des bulletins présentés aux électeurs dans chaque circonscription (chaque pays ou région).

Il y a également un écran appelé Supervision destiné à “contrôler le bon déroulement de l'élection”. Apparemment, cela comprend des tests de cohérence sur la base de données Liste, des tests de cohérence sur la base de données Urne, entre la liste des électeurs ayant formellement exprimé leur vote (émargement) et le nombre de votes dans l'Urne, etc... Cet écran, comme les autres, est censé montrer le fonctionnement de programmes informatiques à Aix.

Il semble “évident” que le serveur web a pour travail d’“ouvrir les enveloppes” et de “déposer les votes dans la base de données Urne”. Un ordinateur peut faire toutes sortes de choses dès lors qu'on l'a programmé pour cela : un programme informatique, écrit par un employé d'EADS, et tournant sur un serveur web, a pour tâche de décrypter les messages reçus de l'électeur, et ensuite, de transmettre des messages à l'ordinateur Urne. Le message transmis à l'Urne peut correspondre ou non au vote reçu de l'électeur – cela dépend comment le programme est écrit. Ce programme fait-il un travail d'interprétation des bulletins fidèle et précis ? On ne peut le dire en faisant seulement des tests avant l'élection, car il est facile d'écrire un programme qui se comporte d'une façon avant le 6 juin, et d'une autre après.

On pourrait penser qu'examiner le programme informatique permettrait de s'assurer qu'il interprète fidèlement les votes. Mais on ne donne pas aux assesseurs la possibilité d'examiner ces programmes informatiques, au motif que ce sont des secrets de fabrication. Même si ils pouvaient examiner ces programmes, il est extrêmement difficile de comprendre ce que fait un programme informatique dans toutes les circonstances possibles : en particulier en cas de bugs introduites par mégarde ou de fraude délibérée qui altérerait les votes reçus par Internet en provenance de l'applet Java tournant sur les ordinateurs des électeurs.

Même si les assesseurs pouvaient examiner les programmes et les comprendre, il serait extrêmement difficile de savoir quel est le programme qui tourne réellement sur l'ordinateur Urne. Si vous avez un ordinateur juste en face de vous, vous pouvez lui demander d'imprimer tous les programmes installés sur son disque dur – mais c'est en fait demander à un programme informatique installé sur la machine de lire le disque dur, et vous ne saurez pas si ce programme informatique dit la vérité. Vous pouvez ouvrir la machine et enlever son disque dur afin de le lire depuis un autre ordinateur en lequel vous avez confiance : de cette façon, vous saurez ce qu'il y a sur le disque dur. Par contre, vous ne saurez pas si le logiciel dans le BIOS de l'ordinateur (qui se situe ailleurs que le disque dur) fait réellement tourner le programme depuis le disque dur, ou bien un tout autre programme. Et, inutile de le dire, les assesseurs ne sont invités pas à venir à Aix avec un tournevis pour démonter le disque dur de l'ordinateur Urne afin de l'examiner.

La même chose est vraie pour l'applet Java qui tourne sur la machine de l'électeur. On n'a pas montré aux assesseurs le code source de ce programme. Les assesseurs n'ont aucun moyen direct de savoir si ce programme tourne réellement sur la machine de l'électeur. En fait, même les ingénieurs d'EADS et d'Experian ne savent pas ce qui tourne sur la machine de l'électeur. Au mieux, ils peuvent savoir quelle applet Java est envoyée à l'électeur. Mais ils ne peuvent pas savoir si la machine virtuelle Java (le programme informatique intégré au navigateur de l'électeur qui interprète l'applet Java) n'est pas corrompue par un virus. N'importe quelle faille de sécurité dans le système d'exploitation ou le navigateur de l'électeur – c'est à dire, n'importe quel virus ou spyware ayant pu infecter la machine de l'électeur – peut altérer le comportement de l'applet Java. Cela signifierait que l'électeur verrait sur son écran que les cases sont cochées pour une certaine liste de candidats, mais que le vote réellement envoyé pourrait être assez différent.

Les assesseurs ne peuvent pas voir l'électeur entrer dans l'isoloir parce qu'il n'y a pas d'isoloir. En fait, l'électeur peut facilement vendre son vote – ou être soumis à des pressions – parce qu'une autre personne peut le voir exprimer son vote.

De fait, en 2003, l'armée américaine a passé commande du développement d'un système de vote par Internet, le “Secure Electronic Registration and Voting Experiment (SERVE)”, afin de permettre aux soldats américains loin de leur État de résidence de voter à l'élection présidentielle de 2004. Préalablement à l'élection, l'armée a composé une commission d'experts pour évaluer le système avant de l'utiliser. Ces experts ont produit un rapport, le “rapport SERVE” (www.servesecurityreport.org) concluant qu'il y a trop de problèmes avec le vote par Internet : en particulier la vulnérabilité des machines clientes au détournement de vote par des virus, la vulnérabilité des serveurs et l'impossibilité globale pour les assesseurs de savoir ce que le logiciel est en train de faire. Sur la base du rapport SERVE, l'armée américaine a décidé d'abandonner le vote par Internet et elle n'a pas utilisé le système SERVE lors de l'élection présidentielle de 2004. En tant qu'expert en sécurité informatique et en technologies du vote, j'estime que ce fut une sage décision.

Les Français cultivés comprennent la différence entre un objet et l'image d'un objet, telle que la démontre le célèbre tableau de l'artiste belge René Magritte, “La trahison des images”. Il s'agit de la peinture réaliste d'une pipe, accompagnée des mots en écriture scripte “Ceci n'est pas une pipe”. La représentation d'un objet n'est pas l'objet – ou peut-être voulait-il dire, les noms que nous attribuons aux objets sont arbitraires.

Les assesseurs d'une élection française normale voient une urne physique de leurs propres yeux. Ils peuvent la toucher de leurs propres mains pour s'assurer qu'il ne s'agit pas d'un mirage. Ils peuvent voir et entendre chaque électeur s'approcher de l'urne et y déposer une seule enveloppe. La photo de l'urne française que j'ai montrée est, à ce qu'on m'a dit, ce à quoi l'urne ressemble vraiment. Mais la photo n'est pas l'objet.

Lorsque les assesseurs de l'élection des Conseillers à l'Assemblée des Français de l'Étranger voient un écran d'ordinateur à Paris disant “0 vote dans l'urne”, ils ne sont pas en train de voir une urne. Ils en voient une représentation, à Paris, censée être une communication avec une machine Supervision à Aix censée, elle, être connectée à une machine Urne à Aix censée, à son tour, faire tourner un certain logiciel. Les assesseurs ne voient même pas une représentation ou une image de ce logiciel, car celui-ci est considéré comme un secret industriel. Les assesseurs ne voient pas l'électeur s'approcher de l'urne; en fait, il n'y a pas de moyen particulier de savoir si le vote enregistré par l'électeur est réellement transmis au serveur web à Aix, ou si le serveur web à Aix transmet fidèlement le vote vers l'Urne.

Les experts en informatique du monde entier qui ont étudié cette question, ont abouti au consensus clair qu'on ne peut pas faire confiance aux élections par Internet, pour toutes les raisons que je viens d'expliquer : les électeurs et les partis politiques ne peuvent pas auditer le fonctionnement du logiciel et du matériel qui sont en fait le véritable bureau de vote. En conséquence, je ne vois pas comment les assesseurs pourraient signer autre chose que l'image surréaliste d'un véritable procès-verbal.

Traduction et relecture : John Johnson, Sabine Monin, Philippe Muller, Pierre Muller, Christine Winter.

Original du texte (en anglais) : <http://www.cs.princeton.edu/~appel/policy.html>.