L'isoloir, c'est ringard ? *

Judicaël Courant †
Judicael.Courant@free.fr

Le 12 octobre 2011

Au nom de la «modernité» et du «développement durable», on remplace les élections professionnelles, à bulletins secrets, par un «vote» électronique qui, au mieux est loin d'offrir les garanties élémentaires offertes par les scrutins classiques (secret du vote, impossibilité d'acheter ou de vendre un vote) et au pire est ouvert à toutes les erreurs et toutes les manipulations.

1. Introduction

Les élections professionnelles 2011 au sein de l'éducation nationale, processus, jusqu'ici à bulletins papiers, ont été remplacées par des élections dématérialisées, par internet, où chaque électeur peut voter d'où il le veut.

2. Des garanties du système classique

La possibilité qu'une fraude ait lieu n'implique certes pas sa réalisation. Néanmoins, l'histoire montre que les tentations voire les tentatives de fraude lors d'une élection sont fréquentes (et ce quel que soit le type d'élection, quels que soient les candidats et leurs affinités politiques). L'actualité judiciaire le démontre s'il en est encore besoin.

En conséquence, croire qu'on peut ignorer la possibilité de fraudes au motif qu'il serait moralement inacceptable de suspecter tel ou tel relève de l'angélisme. Si la sécurité absolue est illusoire il n'en reste pas moins que, dans tout processus démocratique, il est à la charge de l'organisateur d'une élection de démontrer qu'il a fait tout ce qui était possible pour diminuer les risques de fraude et augmenter la probabilité de sa détection.

Le système traditionnel de vote est le fruit d'une longue évolution démocratique.

†L'auteur, enseignant de mathématiques en classes préparatoires, est un ancien chercheur en informatique. Il a notamment travaillé sur la question de la sûreté informatique — comment produire des logiciels sans bugs — et sur la sécurité informatique — en particulier sur la certification de protocoles cryptographiques. C'est avec ce bagage scientifique qu'il s'exprime en qualité de citoyen gravement préoccupé par l'évolution de la République Française.

2.1. L'isoloir

Lors d'un processus de vote un tant soit peu démocratique, chaque électeur prend les bulletins des différents candidats et passe par l'isoloir. Il ne s'agit pas seulement d'une possibilité mais bien d'une *obligation*, quand bien même l'électeur aurait déjà son bulletin rempli sur lui, dont le but est non seulement de permettre mais de garantir le secret du vote afin que l'électeur ne soit pas tenu de céder à une éventuelle pression extérieure et ne puisse pas vendre son vote : nul ne peut savoir ce que l'électeur a mis au dernier moment dans son bulletin, il peut donc déclarer ce qu'il veut sur son vote sans que quiconque puisse vérifier que cela correspond à la réalité.

A contrario, si le passage par l'isoloir était facultatif, il serait facile de vendre son vote : il suffit de faire constater par l'acheteur que l'on a sur soi l'enveloppe de vote contenant le bulletin du «bon» candidat (et uniquement cette enveloppe), de se rendre avec lui au bureau de vote et de ne pas passer par l'isoloir pour lui prouver que l'on vote pour le «bon» candidat. L'acheteur peut alors payer le vote comme convenu. Ce cas de figure ne permet pas seulement l'achat de vote, il permet également d'exercer n'importe quel chantage auprès du votant de la même façon.

2.2. La vérification d'identité

La vérification d'identité est un élément important du processus de vote. Lors de l'affaire des faux électeurs de la mairie de Paris, il semble que des personnes se sont présentées au bureau de vote sous une fausse identité : celle d'un électeur dont ils détenaient une carte. La vérification d'identité n'ayant apparemment pas été faite correctement, nul n'a remarqué que ces votants n'étaient pas qui ils disaient être. J'ai ainsi reçu il y a quelques années le témoignage direct d'un de ces faux électeurs : mineur au moment des faits, il a été emmené au bureau de vote avec ses camarades d'un club de sport ; on leur a remis une carte d'électeur et on leur a dit pour qui voter. Comme ses camarades, il est passé dans l'isoloir et a voté. [1]

2.3. Les assesseurs

Des assesseurs désignés par les différents candidats contrôlent en permanence les opérations de vote.

2.4. L'urne

L'urne est transparente. Chacun peut vérifier qu'elle ne possède aucun double fond.

Elle est fermée avec deux serrures différentes : le président possède la clé de l'une d'elle, la clé de l'autre est remise à un assesseur tiré au sort.

Seule une fente permet de placer un bulletin dans l'urne. Chaque ouverture de la fente incrémente un compteur mécanique, lisible à tout moment par tous (on vérifie à la fin

1. Il est à noter que la personne en question, même si elle n'était pas en mesure de protester, avait compris quel était l'enjeu et que l'isoloir — et lui seul — lui a cependant permis de ne pas voter pour le candidat qu'on lui avait désigné.

qu'il y a eu autant de bulletins qu'indiqué par le compteur) et déclenche une sonnette. L'électeur ne lâche son bulletin que lorsque la fente est ouverte, ce qui lui permet d'être certain qu'un illusionniste ne substitue pas un autre bulletin au dernier moment.

2.5. Le dépouillement

Il se fait sous le contrôle des assesseurs. Chaque bulletin est vu par quatre personnes, deux notent le nom indiqué sur le bulletin et vérifient régulièrement qu'ils ont le même compte. Les bulletins peuvent être recomptés au besoin.

3. Le système imposé pour les élections 2011

3.1. Pas d'isoloir

L'élection est remplacée par une élection par correspondance, donc sans isoloir. Il est donc possible de vendre son vote ou de faire pression sur quelqu'un pour découvrir la teneur de son vote et le forcer à voter pour le «bon» candidat.

3.2. Pas de vérification d'identité

La vérification d'identité ne peut plus avoir lieu : elle est remplacée par l'attribution d'un identifiant de vote (envoyé par la poste) qui permet ensuite de recevoir, par courrier électronique, un mot de passe pour voter.

3.3. L'envoi de l'identifiant n'est pas sécurisé

L'envoi est fait par simple courrier. Il contient deux des trois informations nécessaires pour voter : un identifiant de vote, et l'identifiant Éducation Nationale du votant (appelé NUMEN). La troisième information est le département de naissance de l'électeur (qui est loin d'être une information secrète).

Aucune information à ce stade ne permet de savoir qui a vu l'identifiant lorsqu'il a été imprimé, ni s'il est stocké de façon sécurisée.

Sur le courrier envoyé aux électeurs, l'identifiant est recouvert d'une pellicule dorée, ce qui donne l'illusion que personne n'a pu lire l'identifiant avant que la pellicule ne soit enlevée. J'ai pourtant constaté qu'il suffisait de placer la feuille au-dessus d'une simple lampe de chevet pour lire le NUMEN et l'identifiant par transparence. Il m'aurait été aisé de faire de même sur le courrier reçu par mon épouse.

3.4. L'envoi du mot de passe n'est pas sécurisé

Pour obtenir le mot de passe, il convient de se connecter sur un site via une connexion sécurisée par le protocole https (protocole utilisé pour effectuer des paiements sur Internet). Là encore, on donne à l'utilisateur une illusion de sécurité : l'envoi du message est

fait par simple courrier électronique, qui n'est pas sécurisé. [2]

L'envoi du mot de passe par mail pourrait répondre à deux impératifs :

1. Être sûr que le mot de passe est envoyé à la bonne personne
2. Être en mesure de trouver qui a détourné le mot de passe dans le cas d'une fraude.

Malheureusement :

1. Une fois qu'on possède l'identifiant et le département de naissance d'un électeur, on peut faire envoyer le mot de passe à n'importe quel destinataire. Cela n'a rien de difficile : le site sur lequel on doit se connecter pour recevoir le mot de passe demande à quelle adresse il doit l'envoyer. J'ai ainsi pu faire parvenir mon mot de passe à une adresse située aux États-Unis qui n'a (en apparence) rien à voir avec l'adresse avec laquelle je communique avec ma hiérarchie.
2. L'adresse à laquelle j'ai fait parvenir mon mot de passe est une adresse temporaire, qui disparaît 24h après sa création (`http://spambox.us`). Dans le cas d'une fraude, retrouver le destinataire final est donc quasi impossible. [3]

3.5. Absence de contrôle démocratique sur les opérations de vote

Les assesseurs n'auront aucun contrôle sur le déroulement des opérations. En effet, celles-ci auront lieu sur un serveur, centralisant les votes et comptant les résultats. Or tous les ingénieurs systèmes le savent : Lorsqu'un ordinateur fonctionne, il est difficile, même pour celui qui l'a programmé et/ou configuré, d'être certain qu'il n'a pas été modifié. [4] A fortiori, les assesseurs qui n'ont ni programmé ni configuré les serveurs de vote n'auront aucune idée de ce qui peut se passer sur le serveur.

3.6. Difficulté du recomptage

En cas de problème lors d'un vote papier, on peut souvent le déceler grâce à l'existence de comptages indépendants : le compteur mécanique de l'urne qui compte le nombre de votes et ceux des deux personnes effectuant le compte à une table de dépouillement.

Il semble que cela ait été prévu ici. Mais bien sûr, il est difficile d'avoir foi en un compteur de vote électronique qui serait géré par la machine qui enregistre les votes. Le site du ministère sous-entend que pour augmenter cette confiance dans le compteur, on associera à chaque bulletin de vote un identifiant unique [5] et que cet identifiant sera associé au votant dans une base de donnée. Autrement dit, le système aura toutes les informations permettant de savoir qui a voté quoi. Mais qu'on se rassure : «Deux systèmes

2. Un courrier électronique est l'équivalent d'une carte postale, à la différence près que votre facteur n'a pas le temps de lire les cartes postales qui passent entre ses mains, alors que les outils d'analyse du trafic réseau n'ont aucun problème de ce type.

3. Certes, il existe d'autres méthodes (adresse IP) pour repérer d'où le mot de passe a été demandé. Dans mon cas, une recherche permettrait de savoir que j'ai demandé l'envoi du mot de passe depuis mon domicile. Mais le ministère indique lui-même qu'il est possible de voter depuis un cybercafé.

4. C'est pourquoi, lorsqu'on suspecte qu'un ordinateur est compromis, on le réinstalle complètement.

5. Cet identifiant peut être par exemple l'heure précise d'envoi du vote ainsi que l'adresse Internet (adresse IP) de la machine d'où il a été émis.

informatiques différents et cloisonnés recueillent, l'un l'émargement de l'électeur, l'autre ses votes. Il est ainsi impossible de faire un lien entre l'identité de l'électeur et son choix de vote.»

Le ministère semble avoir oublié que les deux systèmes informatiques en question sont tous deux reliés à Internet. Et que l'assertion selon laquelle le cloisonnement garantit l'impossibilité de faire un lien entre électeur et vote n'est pas une assertion scientifique. Dans le meilleur des cas, un scientifique aurait dit que cela était improbable.

On peut également se demander ce qu'on fera de ces informations sensibles à la fin du vote : Va-t-on les utiliser et violer le secret du vote en cas de contestation ? Ou les détruire ? À quoi sert-il de garder une trace des liens entre votes et votants si celle-ci n'est pas utilisée ?

Dans le cas d'un vote papier, on peut effectuer un recomptage des bulletins. Or ici, seul l'ordinateur qui les a comptés pourra les recompter. Et le plus grand risque n'est certainement pas qu'un bulletin soit mal compté mais tout simplement qu'il ne soit pas mis dans l'urne. Dans le cas d'un vote papier, il est rare qu'un bulletin se volatilise ; dans le cas d'un vote électronique, si le serveur de vote ignore le bulletin de vote qu'on lui envoie, tout se passera comme s'il s'était volatilisé. Pour peu que le problème ait lieu en amont de la séparation entre enregistrement du bulletin de vote et enregistrement de l'«émargement» de l'électeur, on considérera tout simplement que l'électeur n'a pas voté.

Il existe certes des systèmes qui permettent un recomptage indépendant des bulletins. Cependant leur mise en œuvre est délicate et ne résout pas les problèmes du secret du vote.[6] Mais avoir confiance dans un tel système, cela demande un niveau de l'ordre du master en informatique théorique et la foi en quelques conjectures mathématiques, certes non réfutées depuis une quarantaine d'années, mais non démontrées non plus. Est-il bien raisonnable que le processus démocratique ne puisse être contrôlé que par une infime fraction de la population ?

3.7. Impossibilité de détecter les erreurs

À l'exception d'exemples théoriques, tous les logiciels comportent des erreurs de programmations (communément appelées bugs). Y compris des logiciels dont l'échec coûte des sommes astronomiques : un exemple célèbre est celui de l'échec du premier lancement d'Ariane 5.

Sans parler de fraude, il est illusoire d'espérer que le logiciel de vote électronique mis en place par le ministère sera exempt de bugs. La question n'est donc pas de savoir si ce logiciel a des bugs, mais de savoir après l'élection si ces bugs ont ou non affecté le résultat du vote.

Dans la plupart des programmes, l'erreur peut être détectée par ses conséquences : on détecte l'explosion d'une fusée, on peut constater qu'il est anormal que la sécurité sociale demande à un centenaire de se faire vacciner contre les maladies infantiles, ou constater un débit indu sur son compte bancaire.

6. Le projet Debian, une association d'informaticiens à but non lucratif utilise un tel système. Mais les votes sont publics et non secrets.

Le cas du vote est tout autre : les conséquences d'une erreur seraient la sur-représentation ou la sous-représentation de certaines listes. Mais personne ne pouvant prétendre connaître précisément le résultat que le vote aurait dû donner, personne n'est en mesure, au vu du résultat, d'affirmer qu'il y a une erreur.

3.8. Impossibilité de sécuriser la machine de l'utilisateur

Nombreux sont les ordinateurs affectés par des logiciels malveillants, créant parfois un véritable réseau de machines zombies, contrôlées à distance. Ces ordinateurs sont en général infectés à l'insu de leurs utilisateurs. On estimait en février 2010 que le nombre de réseaux botnets actifs était compris entre 4000 et 5000. En 2009, le plus gros connu comportait 30 millions de machines.

Certains sont notamment utilisés pour espionner les données rentrées par les utilisateurs (notamment les numéros de carte bancaire). Il est illusoire de croire que le vote puisse avoir lieu de façon sécurisée sans sécuriser d'abord les machines utilisées par les votants.

4. Conclusion

Imaginez qu'on vous propose un scrutin classique (avec bulletin papier) mais où :

1. Votre carte d'électeur vous est envoyée par simple courrier électronique.
2. Pour voter, il suffit d'une carte d'électeur (donc pas de vérification d'identité), avec même la possibilité de voter plusieurs fois pour ceux qui détiennent plusieurs cartes.
3. Il n'y a pas d'isoloir.
4. L'urne n'est pas dans le bureau de vote.
5. Vous ne mettez pas votre bulletin sous enveloppe vous-mêmes : vous le confiez à un technicien qui effectue la mise sous enveloppe. On vous assure qu'il ne communiquera à personne votre vote et l'oubliera aussitôt. Le technicien écrit sur l'enveloppe le lieu de vote et l'heure précise du vote et fait de même sur un formulaire sur lequel il inscrit également votre nom.
6. Les bulletins ainsi remplis sont transférés par un coursier dans une société extérieure : les bulletins sont stockés dans une urne dans une pièce, les formulaires dans une autre urne, dans une autre pièce.
7. Les urnes sont opaques.
8. Pour le dépouillement, un «expert» vient, s'isole dans la pièce où se trouvent les bulletins et fait le compte sans aucun témoin.
9. Sur chaque enveloppe l'expert peut constater l'horaire et le lieu du vote. S'il pouvait avoir accès aux formulaires stockés dans l'autre pièce, il pourrait savoir précisément qui a voté quoi.
10. Pour éviter cela, un deuxième expert va dans la pièce où sont stockés les formulaires. Les deux experts sont tous les deux connectés à Internet mais on vous explique qu'il

n'y a aucun risque qu'ils croisent leurs informations car les experts sont dans des pièces «différentes et cloisonnées».

11. Une fois les bulletins comptés, l'expert note les résultats et brûle les bulletins. Le deuxième expert note de même le nombre de formulaire dont il dispose avant de les brûler. Puis ils annoncent leur résultats. En cas de différence, aucun recomptage n'est de toute façon possible. En cas de contestation, aucun élément matériel ne permettra de vérifier quoi que ce soit.

Une telle organisation paraît incroyable. C'est pourtant bien de cela qu'il s'agit sur le plan électronique. Bien sûr, on vous expliquera que le vote est sécurisé parce que, suite aux recommandations de la CNIL, le technicien scelle votre enveloppe de vote à la cire inviolable, et que le coursier transporte l'urne dans un véhicule blindé. Cela ne résout aucun des problèmes fondamentaux de ce scrutin folklorique mais ça donne à ceux qui pensent ne pas y connaître grand-chose l'illusion que «c'est sécurisé».

Il est donc manifeste que le vote par Internet pour les élections professionnelles dans l'Éducation Nationale en 2011 ne remplit pas les exigences élémentaires requises pour un vote démocratique.

J'appelle chacun à se renseigner de façon indépendante sur les enjeux et les risques du vote électronique. Je ne connais aucune étude indépendante qui y soit favorable. Pour ma part, je n'irai pas voter.

A. Ressources intéressantes

En 2006, Andrew W. Appel, professeur d'informatique à l'université de Princeton, à écrit un rapport intitulé «Ceci n'est pas une urne. À propos du vote par Internet pour l'Assemblée des Français de l'Étranger», `http://www.cs.princeton.edu/~appel/urne.html`

Une pétition existe pour demander le retour au vote papier : `http://www.ordinateurs-de-vote.org/Actions-Petition.html`

Le site http ://www.ordinateurs-de-vote.org est très intéressant, notamment en ce qui concerne l'Éducation Nationale : `http://www.ordinateurs-de-vote.org/FAQ-Foire-Aux-Questions,447.html`

Avec quelques collègues, j'ai rédigé une lettre à notre ministre, à signer et envoyer par voie hiérarchique. Voir `http://judicael.courant.free.fr/2011/10`.

L'ouvrage *Vote électronique : les boîtes noires de la démocratie* paraît très intéressant. Il est disponible sur `http://www.ilv-bibliotheca.net/librairie/vote_electronique__les_boites_noires_de_la_democratie.html` — on peut gratuitement télécharger la version électronique.

B. L'argument du «développement durable»

L'efficacité en terme de «développement durable» du passage au vote électronique n'est qu'un aspect mineur de la question : la démocratie vaut, me semble-t-il plus que le coût

de quelques feuilles de papier tous les trois ans. C'est cependant un des arguments mis en avant par le ministère. Pourtant le caractère écologique du vote électronique reste largement à démontrer.

Alors qu'un bulletin papier ne demande que d'imprimer quelques feuilles, le processus de vote mis en œuvre demande plusieurs connexions à la suite et de longueur relativement importante. Il est douteux que, même dans le cas où tout se passe bien, il faille moins d'un quart d'heure pour voter. Il n'est pas clair qu'écologiquement, un quart d'heure d'ordinateur (plus le fonctionnement des serveurs à l'autre bout) soit plus écologique que l'impression de quelques bulletins papier.

Pour mémoire, selon l'ADEME, l'impression de 4 pages de texte recto engendre la même quantité de CO_2 que 12 minutes de temps d'ordinateur.

De plus le passage au vote électronique ne dispense pas d'envoyer une lettre à chaque votant, lettre comportant de plus une pellicule dorée, probablement difficile à recycler.