Transparence, élections et vote électronique

Chantal Enguehard

▶ **To cite this version:**

Chantal Enguehard. Transparence, élections et vote électronique. 2009. hal-00435966v1

HAL Id: hal-00435966

https://hal.science/hal-00435966v1

Preprint submitted on 26 Nov 2009 (v1), last revised 28 Nov 2012 (v2)

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Enguehard, C. Transparence, élections et vote électronique. Journée d'études de l'Association Française de Droit Constitutionnel "Démocratie électronique". 13 pages. Besançon, 13 novembre 2009.

Transparence, élections et vote électronique

Chantal Enguehard
LINA - UMR CNRS 6241
2, rue de la Houssinière, BP 92208, 44322 Nantes Cedex 03 – France
chantal.enguehard@univ-nantes.fr

Une élection peut être qualifiée de démocratique si elle satisfait un certain nombre de critères comme leur régulière tenue, la possibilité pour les candidats de faire campagne sans subir de pressions, ou encore la mise en œuvre d'un scrutin à bulletins secrets. Toutefois, cet article se limite à l'expression des suffrages lors de la période de vote et au décompte des voix exprimées par les électeurs.

1 - Quelques principes associés au vote démocratique

En démocratie, le pouvoir est détenu par le peuple comme le rappelle l'article 2 de la Constitution de la République Française de 1958 : « *gouvernement du peuple, par le peuple et pour le peuple* ». Dans une démocratie représentative, le pouvoir n'est pas exercé directement, mais à travers des élus. Ainsi, à chaque élection, le peuple se défait volontairement de pouvoirs qu'il détient pour les confier à ses représentants qui l'exerceront pendant leur mandat. Cette opération concerne notamment les pouvoirs régaliens de justice, de police, ou de levée des impôts. La réussite de cette passation de pouvoir détermine la légitimité des élus. En cas de soupçons de fraude la contestation peut aller jusqu'aux émeutes[1].

L'organisation des élections a beaucoup évolué depuis la première proclamation d'un scrutin universel masculin, par la France, le 2 mars 1848. À l'époque il n'y avait ni isoloir, ni bulletins imprimés, ni enveloppes et le scrutin se déroulait sur deux jours : répondant à l'appel de son patronyme, chaque électeur devait écrire le nom de la personne à qui il accordait son suffrage sur un bulletin vierge. Les illettrés, nombreux, devaient déléguer l'écriture de leur bulletin, à cette occasion de nombreux abus étaient commis. L'électeur ne déposait pas en mains propres son bulletin dans l'urne mais le confiait au président du bureau de vote qui pouvait facilement voir ce qui y était écrit. Il arrivait aussi que le maire prépare des bulletins de vote à l'avance et les distribue à l'ensemble de ses administrés au moment de voter. Dès le premier scrutin, le 23 avril 1948, des ouvriers se sont organisés pour voter en communauté le deuxième jour afin d'éviter les intimidations, et aussi pour être certain que leurs bulletins ne seraient pas changés pendant la nuit [Offerlé 2002].

La procédure de vote a ensuite évolué afin de garantir au mieux le respect des principes associés aux élections démocratiques :

— unicité : chaque électeur dispose d'une voix.

La tenue d'une liste d'émargements permet de noter qu'un électeur a effectivement voté. Longtemps tenue par un membre du bureau de vote, depuis 1988 elle doit être signée par chaque votant.

— confidentialité : chaque électeur peut exprimer son choix à l'abri des regards afin d'éviter les pressions et les tentations de vendre son vote.

Les enveloppes protégeant les bulletins, la présence d'isoloirs dans les bureaux de vote (depuis 1913) et leur usage obligatoire contribuent à garantir le respect de la confidentialité.

A contrario, la confidentialité ne peut être garantie lorsque les électeurs s'expriment hors d'un bureau de vote, par exemple lors d'un vote par correspondance.

— sincérité : les résultats proclamés sont fidèles aux suffrages déposés par les électeurs.

La procédure de vote doit donc limiter les tentatives de fraude ou d'erreurs. Plusieurs évolutions visent à éviter les fraudes massives : la durée des élections, initialement de deux jours, est limitée à une journée, afin de ne pas laisser les urnes sans surveillance durant la nuit, et les urnes sont obligatoirement en plexiglas transparent depuis 1988. La procédure de dépouillement décrite dans le code électoral met en place un double comptage afin d'éviter les erreurs et se tient dans chaque bureau de vote, sans déplacement des urnes..

— anonymat : il n'est pas possible de relier un suffrage à l'électeur qui l'a déposé.

Les bulletins ne doivent porter aucune marque susceptible de permettre l'identification de l'électeur ; depuis 1923

1 Les émeutes pour cause d'élections contestées sont fréquentes : élection d'Ali Bongo au Cameroun en septembre 2009, élection de Mahmoud Ahmadinejad en Iran en juin 2009, élections législatives en Mongolie en juin 2008, élection de Mwai Kibaki au Kenya en décembre 2007, etc.

des bulletins pré-imprimés sont mis à disposition des électeurs. À l'ouverture de l'urne les enveloppes sont brassés, cette opération irréversible empêche de suivre du regard une enveloppe préalablement repérée dans l'urne transparente.

— transparence : le déroulement de la journée de vote, depuis l'ouverture des bureaux de vote jusqu'à l'établissement des résultats sur les procès-verbaux, se déroule sous les yeux des électeurs. Ceux-ci peuvent être mis à contribution lors du dépouillement. Pour être effective la transparence doit être directe.

La différence entre transparence directe ou indirecte est essentielle.

Par exemple, lorsque la transparence directe est de mise, n'importe quel électeur peut constater, à l'ouverture du bureau, que l'urne est vide : il peut la voir, la toucher, constater sa vacuité par ses propres sens. La transparence devient indirecte dès qu'elle s'exerce via un média humain ou logiciel privant l'électeur de sa capacité de contrôle car, dans ce cas, l'électeur doit accorder sa confiance à ce média susceptible d'erreur, de tromperie ou de malveillance, sans pouvoir vérifier lui-même l'effectivité des mesures prises, ou la réalité des informations qui lui sont transmises. Par exemple, l'urne est en bois et l'électeur n'est pas autorisé à voir et toucher l'intérieur de l'urne, mais un membre du bureau affirme qu'il l'a fait et que l'urne est vide. Dans cette situation, l'électeur peut douter de sa parole ou de sa compétence à détecter un double fond.

La transparence devient littéralement opacité lorsque l'urne est dérobée aux yeux des scrutateurs, si, à la fin de la période de vote, elle est enfermée dans une pièce de la mairie jusqu'au dépouillement, ou encore, si le dépouillement n'est pas public, mais réalisé, dans une pièce fermée, par les membres du bureau de vote qui ensuite en donnent les résultats, etc.

La transparence est un concept clef des élections car, non seulement elle fonde la confiance des électeurs, mais elle est indispensable au constat du respect d'autres concepts fondamentaux des élections démocratiques : unicité, sincérité et anonymat.

Le vote électronique, apparu en France avec le nouveau millénaire, a modifié la pratique des élections. Urnes, enveloppes et bulletins ont disparu en même temps que le dépouillement public et les scrutateurs. Cette brutale évolution a suscité des méfiances et une controverse est apparue lors de l'élection présidentielle de 2007.

La question la plus fréquemment évoquée au sujet du vote électronique concerne la sécurité et la fiabilité des procédures.

Cet article vise à démontrer que

(1) En l'absence de transparence directe, des atteintes à la sécurité et/ou à la fiabilité et affectant la sincérité des élections peuvent rester invisibles.

(2) Par conséquent, la transparence directe est indispensable à la tenue d'élections démocratiques.

2 -Vote électronique

2.1 - Brève typologie

En France, deux types de systèmes électroniques sont susceptibles d'être utilisés lors d'élections politiques :

— Ordinateurs de Vote avec Bulletin Dématérialisé (OdV-BD)[2]

Il s'agit de systèmes informatiques autonomes placés dans des bureaux de vote en remplacement du matériel habituel (urne, bulletins, enveloppes, isoloir). L'ordinateur présente les alternatives (candidats, listes, ou réponses en cas de référendum), l'électeur fait son choix à l'aide de l'ordinateur de vote, en appuyant sur un bouton, ou en utilisant une souris, ou bien encore en mettant ses doigts directement sur l'écran tactile, selon les modèles ; l'électeur peut confirmer son choix, ou bien revenir en arrière pour éventuellement en changer. Une fois son choix confirmé, il peut quitter l'isoloir et émarger.

Les ordinateurs de vote ne contrôlent pas les identités des électeurs. Ce sont les membres du bureau de vote qui effectuent cette tâche et font signer le registre des émargements par les électeurs, comme dans la procédure de vote traditionnelle.

Quelques dizaines de communes ont mis en service des OdV-BD, à leur initiative, depuis 2007. Dans ces communes, il s'agit du seul mode de vote autorisé[3].

2 Improprement nommés "machines à voter" dans le code électoral

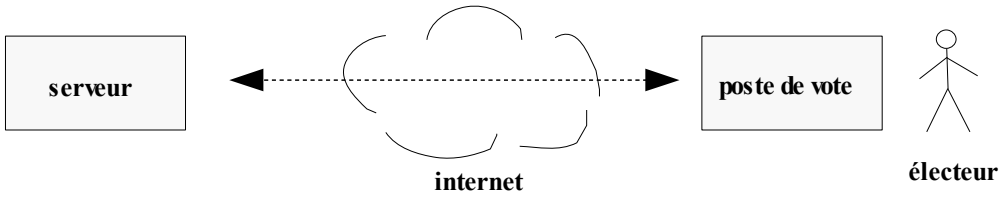
3 Il concernait 1,3 million d'électeurs inscrits lors des élections européennes de juin 2009.

OdV-BD « iVotronic » de la société ES&S Datamatique
(photographie Benoît Sibaud - licences LAL/CC BY/GFDL)

— Vote par internet

Le vote par internet est assimilé à un mode de vote par correspondance. Les électeurs procèdent depuis n'importe quel ordinateur connecté à internet, que cet ordinateur soit chez eux, au travail, dans un lieu public ou un cybercafé. Il faut se connecter sur le site officiel de vote hébergé sur l'ordinateur du bureau centralisateur (le serveur). Après les phases d'identification et d'authentification (à l'aide d'un identifiant et d'un mot de passe généralement reçus au préalable par courrier postal), l'électeur peut faire son choix. Après confirmation, il reçoit un accusé de réception de son vote (cet accusé de réception ne mentionne pas le sens du suffrage). Les échanges d'informations empruntent le réseau internet.

L'ordinateur qui fait office de serveur se charge de la tenue de la liste des émargements, de la collecte des votes au fur et à mesure de leur réception, et du dépouillement à la fin de la période de vote.



Vote par internet

Depuis 2003 les électeurs pour les membres de l'Assemblée des Français de l'Etranger (AFE) peuvent choisir de voter par internet, par correspondance postale, ou à l'urne en se déplaçant dans un bureau de vote.

2.2 - Dématérialisation, anonymat, opacité

OdV-BD et Vote par internet sont des systèmes de traitement de l'information présentant plusieurs points communs.

2.2.1 - Les objets du vote sont dématérialisés.

Il n'y a plus de bulletins, ou d'urne ou d'enveloppes réels mais une représentation de ces objets.

La différence entre objets réels et représentation a été exprimée avec brio par René Magritte dans son œuvre intitulée fort à propos "La trahison des images". Elle représente une pipe de manière très réaliste et est sous-titrée par la phrase "Ceci n'est pas une pipe". Effectivement, il est impossible de fumer du tabac avec un tableau qui représente une pipe.

Il apparaît que la transformation des objets réels en une représentation a pour conséquences (1) la modification des

propriétés des objets en question (une représentation d'une pipe n'est pas creuse et ne peut être bourrée de tabac) (2) l'inadéquation des gestes usuels associés à ces objets (bourrer la pipe, allumer, fumer).

On observe la même mutation des propriétés physiques en ce qui concerne les objets du vote. Ainsi, La forme de l'urne (quand elle est fermée, seule une petite fente permet de glisser des bulletins) et son matériau (plexiglas transparent) visent à garantir que les suffrages décomptés sont bien les bulletins déposés par les électeurs. La vigilance du contrôle exercé autour de l'urne conditionne le constat d'éventuelles atteintes à la sincérité du scrutin que ce soit par substitution de l'urne pendant la journée ou de paquets de bulletins lors du dépouillement, etc. Il faut noter que cette surveillance n'a de sens que parce que les objets ont pour propriété la persistance physique : les mots imprimés ou écrits sur les bulletins déposés dans l'urne ne peuvent être modifiés sans intervention extérieure.

Ces propriétés ne sont pas conservées dans les représentations virtuelles de ces objets au sein du vote électronique. L'urne est représentée par un fichier informatique qui peut être altéré (par erreur ou par malveillance) sans que ces modifications soient directement perceptibles par les personnes présentes autour du dispositif de vote. Les choix exprimés par les électeurs sont transformés : la pression de quelques joules exercée sur un bouton lors du vote est traduite en une impulsion électrique qui va ensuite modifier la valeur de quelques bits d'un fichier informatique. Ces transformations invisibles peuvent aboutir à la modification du choix initialement exprimé. La volatilité de l'information ainsi numérisée contraste avec la continuité physique des bulletins de vote en papier.

2.2.2 - Les suffrages doivent rester anonymes

Il doit être impossible de relier un suffrage à l'électeur qui l'a exprimé.

Les OdV-BD n'ont pas communication des identités des électeurs mais l'ordre avec lequel les suffrages ont été enregistrés peut constituer un lien permettant de retrouver l'auteur de chaque suffrage (il n'est pas illégal de noter l'ordre de vote des électeurs et ces pratiques ont été constatées dans certains bureaux de vote). L'enregistrement des suffrages en mémoire de manière aléatoire constitue un problème non trivial : la génération de nombres aléatoires est toujours un sujet de recherche[4]. En ce qui concerne la procédure de vote classique à l'urne, ces difficultés sont définitivement résolues par le brassage des bulletins à l'ouverture de l'urne.

Les systèmes de vote par internet reçoivent en même temps l'identité de l'électeur et le vote que celui-ci a exprimé. Il est possible d'organiser l'application informatique de gestion des élections afin qu'elle ne dévoile pas en même temps identité et vote. Mais il est difficile d'être certain qu'une telle organisation est effectivement suivie et il est impossible de prouver que d'autres traitements informatiques visant à dévoiler les auteurs des votes ne sont pas mis en œuvre en parallèle.

2.2.3 - Opacité

Les systèmes de vote informatiques sont, par essence, opaques : le codage et le traitement d'informations sur des supports informatiques procédant par déplacements d'électrons au sein de composants électroniques ou de microprocesseurs, ne peuvent s'observer directement.

Ainsi, la procédure de vérification de la vacuité de l'urne ne procède plus par observation directe, mais par consultation d'informations délivrées par un média : affichage sur un écran d'un message indiquant "l'urne est vide" ou "les compteurs sont à zéro", ou l'impression de ces informations sur un ticket.

2.2.4 - Conséquences

La sincérité des élections organisées à l'aide d'objets réels dépend de la vigilance exercée lors de la période de vote : électeurs, scrutateurs, délégués, membres du bureaux de vote exercent conjointement leur surveillance afin d'éviter toute atteinte à l'intégrité de l'urne ou à l'un des principes à respecter (unicité, anonymat, confidentialité).

Avec le vote électronique, les objets du vote étant dématérialisés, ils ont perdu la propriété de continuité physique, la vigilance ne peut plus s'exercer de manière efficace.

Il peut sembler qu'une solution serait de suppléer à la disparition de la continuité physique par un suivi logique des transformations appliquées aux suffrages. Il est classique en informatique de déployer des procédures de suivi permettant de vérifier pas à pas le bon fonctionnements de programmes. Elles consistent à noter les étapes du déroulement des programmes dans un ou plusieurs fichiers collectant l'historique des événements et permettant de vérifier que le résultat obtenu est en adéquation avec les entrées du système[5].

4 Les ordinateurs sont des dispositifs déterministes. Les algorithmique de génération de nombres aléatoires les plus courants produisent des nombres pseudo-aléatoires dont la suite exacte peut être reconstituée *a posteriori*.

5 Les systèmes informatiques embarqués nécessitant un haut degré de fiabilité (aéronautique par exemple) sont fondés sur la redondance des traitements effectués sur des matériels différents et sur la vérification croisée des calculs (un ordinateur vérifiant

Mais, déployé pendant la période de vote, un tel suivi dévoilerait le sens des suffrages exprimés, violant ainsi le secret du vote (anonymat et confidentialité), tandis qu'un suivi partiel, faisant abstraction des suffrages, serait inutile puisqu'il ne permettrait pas de détecter si des votes ont été altérés ou mal comptabilisés. En ce qui concerne le vote par internet, le suivi est *de facto* limité aux traitements réalisés par le serveur depuis la réception des suffrages jusqu'à leur décompte. Une transformation de suffrages sur des postes d'électeurs (et à leur insu) ne peut être décelée.

Cette situation est originale et ne se présente dans aucune autre activité humaine informatisée. Ainsi, pour les exemples ci-dessous, nous constatons que l'utilisateur est en mesure de discerner un éventuel dysfonctionnement car les échanges ne sont pas anonymes (exemples 1, 2 ou 3) ou parce qu'il existe une boucle de rétroaction (exemple 4).

(1) Lors d'achats sur internet, acheteurs et vendeurs sont identifiés, les échanges d'argent sont communiqués à leurs banques respectives et seront inscrits dans leurs relevés de comptes bancaires respectifs.

(2) L'acquisition d'un billet de train à l'aide d'une borne libre service sncf donne lieu à la délivrance d'un billet matérialisé et à des échanges bancaires dont les débiteurs et créditeurs sont identifiés.

(3) Les parlementaires utilisent des boîtiers de vote électronique pour exprimer leurs voix, mais ces votes ne sont pas anonymes. Comme l'auteur de chaque vote est connu, et que l'assemblée est de taille réduite, une erreur de transmission ou de comptage d'une ou plusieurs voix est facilement dénoncée et réparée.

(4) L'envoi d'un commentaire anonyme sur un site web est suivi de sa publication sur ce site ou de la réception d'un message de rejet. Si aucune de ces prévisibles conséquences ne se produit, il est impossible de savoir si le commentaire a été reçu par le site destinataire.

La conjonction de l'obligatoire respect de l'anonymat, de la perte des propriétés physiques attachés aux objets réels du vote et de l'opacité inhérentes aux traitements informatiques a donc pour conséquence, quand le nombre de voix décomptés correspond toujours à peu près au nombre des émargements, l'impossibilité de déceler d'éventuelles erreurs dans les résultats énoncés par un système de vote électronique.

2.3 - Évaluation de la justesse des résultats [Enguehard 2007c]

Il est donc nécessaire de disposer d'une procédure d'évaluation de la justesse des résultats énoncés par un système de vote électronique, d'une manière indépendante de celui-ci.

Nous explorons trois voies d'évaluation :

— la vérification par approximation,

— les garanties apportées par les traitements,

— la preuve de résultat.

2.3.1 - Vérification par approximation

Il s'agit de mesurer l'écart entre les résultats fournis par le système de vote évalué et des estimations statistiques.

Il existe deux types d'estimations statistiques :

— les estimations statistiques concurrentes au vote : elles sont établies en même temps que les opérations électorales. Il s'agit des sondages de sorties d'urnes.

— les estimations statistiques antérieures au vote : elles sont fondées sur des données recueillies avant les opérations électorales. Il s'agit des résultats aux précédentes élections et/ou des intentions de votes pondérées (sondages).

Estimations statistiques concurrentes au vote

Les évaluations statistiques sont calculées sur un échantillon des électeurs auxquels il est demandé de révéler leur vote. Leur précision dépend de la qualité de l'échantillon sur lequel elles sont établies ainsi que du savoir-faire des personnes qui procèdent au sondage. Il existe plusieurs facteurs de biais :

- l'échantillon, de taille réduite, ne représente pas certains segments de la population.
- le vote étant révélé, les sondés ont la possibilité de ne pas répondre à la question qui leur est posée.
- il n'existe aucune contrainte garantissant le fait que chaque personne sondée exprime son vote réel.

les résultats de l'autre) via les fichiers de collecte des événements.

- les personnes procédant au sondage peuvent, consciemment ou inconsciemment, favoriser la représentativité de certaines catégories de la population au détriment d'autres catégories de la population.

Néanmoins, un sondage de sorties d'urnes peut être considéré comme le résultat d'un système de vote dont les modalités sont :

- votes révélés,

- échantillon partiel,

- absence de contrainte validante.

Nous disposons donc de deux systèmes de vote dont les modalités sont différentes : l'un procède par vote anonyme et l'autre par vote révélé ; l'un concerne tous les électeurs, l'autre n'opère que sur un échantillon.

Supposons que les deux systèmes fournissent des résultats différents, il faut déterminer lequel de ces deux systèmes de vote doit être considéré comme susceptible de fournir les résultats ayant la plus grande exactitude.

● *Première possibilité* : c'est le sondage de sorties d'urnes

La conséquence immédiate est qu'il devient inutile de déployer des élections concernant l'ensemble des électeurs, puisque, quels que soient les résultats de la consultation électorale, leur validité sera déterminée en fonction de leur conformité avec les sondages de sorties d'urnes.

● *Deuxième possibilité* : c'est le système de vote anonyme

Dans ce cas, les sondages de sorties d'urnes ne peuvent être utilisés comme une référence pour évaluer l'exactitude des résultats fournis par le système de vote.

Estimations statistiques antérieures au vote

Les estimations statistiques antérieures au vote sont établies principalement par l'analyse d'élections précédentes et/ou des intentions de votes pondérées, intentions exprimées avant le déroulement des opérations électorales.

● *Analyse d'élections précédentes*

En démocratie, la tenue d'élections à intervalles réguliers consacre la possibilité d'avoir des alternances politiques. D'une élection à l'autre, les électeurs peuvent progresser dans leur culture et leur analyse politique, changer d'avis et exprimer, par leur vote, une opinion en rupture avec les opinions qui étaient les leurs dans le passé.

● *Analyse des intentions de votes pondérées*

Les accidents de prédictions sont toujours possibles. L'évolution des résultats électoraux est un phénomène dynamique complexe faisant intervenir de multiples paramètres. Il n'existe pas d'approche scientifique valide qui permette de prédire avec justesse les résultats de tels phénomènes en se fondant sur l'analyse du passé.

Les informations apportées par les élections précédentes ou les sondages ne présentent donc pas la fiabilité et la pertinence nécessaires pour valider les résultats d'un système de vote.

2.3.2 - Garanties apportées par les traitements

Il s'agit de prouver que les traitements mis en œuvre dans le système de vote à évaluer transforment les entrées du système pour produire des résultats qui correspondent aux votes effectivement émis.

Il faut prouver que le système de vote est (1) immune de faute et (2) qu'il ne peut être altéré[6].

Système immune de fautes

Pour prouver qu'un système informatique est immune de fautes deux approches peuvent être envisagées : les tests et la preuve formelle.

● Tests

Les tests, s'ils peuvent valider un dispositif à un instant donné et pour un ensemble restreint d'interactions avec les utilisateurs, ne valident pas ce dispositif pour l'ensemble des interactions possibles car il n'est pas économiquement possible de tester tous les ordinateurs et toutes les interactions possibles (dont le nombre est potentiellement infini).

En ce qui concerne les OdV-BD, seuls quelques exemplaires sont soumis à des tests d'ampleur limitée. Dans le cas du vote par internet, les ordinateurs à partir desquels votent les électeurs ne peuvent être soumis à des tests préalables. En plus de présenter une grande diversité, ils sont susceptibles d'être infectés par des virus inconnus.

6 Le système de vote à l'urne, en se restreignant à manipuler des objets inertes (urne, bulletins) peut être considéré comme immune de faute et non altérable dans la mesure où le matériel est conforme et qu'il est soumis à une surveillance constante durant la journée d'élection et le dépouillement. Les atteintes à son intégrité sont matérielles (substitution d'urnes, d'enveloppes, etc.) et des preuves matérielles ainsi que des témoignages peuvent en être produits devant un juge.

● *Preuve formelle*

Établir une preuve formelle permet de tester virtuellement toutes les entrées possibles d'un programme et de vérifier que les sorties seront conformes à ce qui est attendu.

Un système de vote électronique comprend un programme de réception et de comptabilité des suffrages, mais aussi d'autres programmes (drivers, micro-code, compilateurs, etc.), dont le fonctionnement implique des interactions entre le matériel, les logiciels et l'environnement extérieur. La démarche de preuve, concluante pour un programme particulier de taille réduite, reste impuissante face à un système complexe.

Enfin, les comportements inattendus et erreurs inopportunes que rencontre tout utilisateur de logiciels de bureautique nous rappellent qu'il semble toujours extrêmement difficile de produire des programmes sans erreur.

Altération du système

Un système de vote électronique peut être altéré sans que cette altération puisse être détectée de manière certaine par une procédure indépendante du système lui-même.

- le logiciel de vote, ou un autre programme présent sur le système, n'est pas identique à l'ensemble des logiciels initialement validés.

- le logiciel de vote produit une erreur d'exécution, sans tomber en panne, à cause d'un défaut du matériel électronique (hardware). Cette erreur peut modifier des votes.

De plus, en ce qui concerne le vote par internet, les interactions ayant lieu sur le poste de l'électeur se déroulent dans un environnement non stable, échappant au contrôle et susceptibles de subir des modifications à l'insu de l'utilisateur.

Il est donc à la fois impossible de prouver que les traitements sont immunes de faute et qu'ils ne peuvent être altérés.

2.3.3. Preuve de résultat

La preuve de résultat consiste à confronter les résultats d'un système aux résultats établis indépendamment de celui-ci en procédant sur les données reçues en entrée.

En ce qui concerne le vote, les données sont les suffrages. Ces données sont inconnues du fait de l'anonymat (les votes ne sont pas révélés au moment où ils sont exprimés).

Il n'est donc pas possible de procéder à une preuve de résultat[7].

Il apparaît donc qu'il n'y a aucune procédure valide d'évaluation de la justesse des résultats issus de dispositifs de vote OdV-BD ou de vote par internet.

3 - Sécurité

3.1 - Définitions

La **sureté** englobe l'ensemble des moyens matériels, humains, organisationnels visant à éviter ou contrer toute attaque malveillante. Le niveau de sureté est total si aucune attaque ne peut réussir.

La **fiabilité** désigne la capacité d'un système à fonctionner sans erreur et sans tomber en panne. Le niveau de fiabilité est total si aucune panne, aucun dysfonctionnement ne peut subvenir.

Nous définissons la **sécurité** comme la conjonction de la sureté et de la fiabilité. La sécurité totale correspond à une situation ou aucune attaque ne peut réussir, aucun dysfonctionnement ne peut subvenir.

7 Il est fréquent qu'une procédure de tests avec votes révélés soit mise en œuvre immédiatement avant chaque opération de vote réelle dans le but d'établir une preuve de résultat : quelques suffrages, soigneusement notés par ailleurs, sont entrés dans le système de vote, puis le dépouillement est effectué. Le résultat fourni par le système de vote est alors confronté à la liste des votes notés.
Cette procédure est inopérante car :
- elle s'appuie sur l'assertion qu'une performance passée réussie vaut garantie de réussite pour la performance à venir.
- elle repose sur un jeu de données en entrée excessivement réduit.

La **transparence directe** est l'exercice du contrôle du déroulement des élections directement par les électeurs, sans média (logiciel, expert autorisé ou membre du bureau de vote).

3.2 - Sécurité du vote électronique

3.2.1 - Atteintes à la fiabilité

Un système de vote électronique peut connaître des dysfonctionnements causés par des défaillances matérielles, des erreurs de conception (bug) ou des erreurs de manipulation. En l'absence de vérification de la justesse des résultats, les incidents de ce type peuvent être repérés lorsque le système de vote ne fonctionne pas, présente un comportement inattendu, ou émet des résultats électoraux absurdes (par exemple, un candidat recueille plus de voix qu'il n'y a d'électeurs) ou bizarres (par exemple, taux anormalement élevé d'abstentions).

En ce qui concerne les OdV-BD, des exemples de tels dysfonctionnements ont été enregistrés et rendus publics dans les pays où leur utilisation est massive ([VotersUnite.org 2007], [Enguehard 2007]). En France, l'examen des remarques portées sur les procès-verbaux fait apparaître des retards à l'ouverture de bureaux de vote (à Reims en 2007 par exemple), des pannes ayant quelquefois nécessité de changer d'ordinateur de vote (Arcueil, Boulogne-Billancourt, Le Mans en 2007, Sèvres en 2008, etc.), l'absence de dispositif pour les non voyants ou leur inadéquation (dans quasiment tous les bureaux de vote). Une étude a porté sur le nombre de votes et le nombre d'émargements enregistrés dans plusieurs milliers de vote. Alors que, idéalement, ces nombres devraient toujours être identiques, il a été constaté que la proportion de bureaux de vote pour lesquels ces nombres ne sont pas identiques est plus importante quand les bureaux de vote sont équipés d'OdV-BD par rapport aux bureaux de vote équipés d'urnes[8] [Enguehard 2008].

Les votes par internet se déroulent généralement sur une période de plusieurs jours. Une assistance téléphonique est mise en place par la société prestataire chargée de l'organisation afin d'aider les électeurs rencontrant des difficultés. Comme il n'existe aucune obligation de publication des interactions se déroulant dans ce cadre privé (nombre d'appels, problèmes rencontrés, conseils apportés, etc.), il n'est pas possible de connaître les obstacles que peut rencontrer un électeur particulier, ce qui empêche la collecte des incidents concernant la fiabilité. En revanche, des constats portant sur des systèmes de vote ont pu être réalisés par des candidats ou des experts. En voici quelques exemples : tous les candidats ne sont pas présentés sur les écrans (élections prud'homales 2008 à Paris), il est impossible de faire apparaître le bouton permettant de voter (élections prud'homales 2008 à Paris), le secret du vote de certains électeurs est violé (élections AFE 2006) [Pellegrini 2006], le calcul des résultats est très lent (élections prud'homales 2008 à Paris), un dysfonctionnement nécessite l'intervention d'un technicien durant la période de vote (élections prud'homales 2008 à Paris, élections AFE 2006), les résultats électoraux ne sont pas édités dans les délais prévus et nécessitent une intervention technique spéciale (élections prud'homales 2008 à Paris).

3.2.2 - Atteintes à la sûreté

L'histoire des élections est émaillée de fraudes, parfois réussies, et de tentatives de fraude qui ont été dénoncées et ont donc échouées, les fraudes réussies restant, par nature, inconnues.

Nous distinguons deux types de fraudes en fonction de leur origine :

— fraude interne

Les fraudes ou malveillances internes peuvent être menées par une ou plusieurs personnes impliquées dans l'organisation du vote. Il peut s'agir d'un programmeur, d'un technicien chargé de la maintenance et des mises à jour, ou de toute personne ayant un accès physique ou logique au système de vote avant ou pendant la période de vote.

En l'absence de possibilité de vérifier la justesse des résultats des élections indépendamment des dispositifs de vote, il n'existe aucun moyen de détecter les manipulations (contrairement aux domaines comme l'informatique bancaire).

Le ministère de l'intérieur, de l'outre-mer et des collectivités territoriales a publié des instructions à mettre en œuvre en cas d'utilisation de "machines à voter" [MinInt 2008]. Une page détaille des mesures de sécurisation des dispositifs de vote hors des périodes de vote :

- stockage sécurisé, dès réception des "machines" en mairie, avec accès limité à des personnes autorisées,
- pas d'intervention de personnes seules,
- suivi de chaque machine à l'aide d'un "livret d'intervention",
- etc.

8 Sur un échantillonn de référence de 1600 bureaux de vote équipés en OdV-BD et 2400 pratiquant le vote à l'urne, 30% des bureaux de vote équipés en OdV-BD présentent un nombre de votes différent du nombre d'émargements, cette proportion est de 5% pour le vote à l'urne.

Mais les dispositifs de vote en service sont livrés dans les mairies utilisatrices depuis plusieurs années sans suivi particulier ; même si les techniciens ne sont plus laissés seuls en présence des ordinateurs de vote, les personnels de mairie ne sont pas compétents pour apprécier la nature de leurs interventions. Ces mesures sont donc inaptes à empêcher ou détecter les fraudes internes (d'ailleurs, la circulaire annonce, en préambule, que ces instructions sont "destinées à créer un climat de confiance accru" et non à sécuriser les dispositifs de vote).

— fraude externe

Les fraudes externes sont le fait de personnes non impliquées dans l'organisation du vote.

Elles sont rares dans le cadre de vote en environnement contrôlé (bureaux de vote). En revanche, le vote par correspondance reste très vulnérable dans son déroulement hors d'un environnement contrôlé (acheminement et réception du matériel de vote, expression des choix, acheminement des suffrages), qu'il s'agisse de vote par internet ou par voie postale. Toutefois, il apparaît que le vote par internet est le mode de vote par correspondance le plus susceptible d'abriter des actions malveillantes de grande ampleur et restant invisibles : virus modifiant les choix des électeurs à leur insu, phishing (hameçonnage), rupture de service, man-in-the-middle (homme au milieu), etc. [Enguehard 2009].

3.2.3 - Constats et garanties

Nous observons que des atteintes à la sécurité peuvent rester inconnues, et qu'il n'existe pas de mesures techniques ou organisationnelles capables de prévenir ces atteintes, ou simplement de les constater, de manière certaine, même si elles sont de grande ampleur.

Par conséquent, il est impossible de garantir l'absence d'atteinte à la sécurité et d'en apporter des preuves en ce qui concerne le vote électronique utilisant des OdV-BD ou le vote par internet.

4 - Sécurité versus transparence

Nous détaillons les différentes situations correspondant aux valences des deux paramètres sécurité et transparence.

Pour cette démonstration, nous considérons que la sécurité peut être totale, même si cette possibilité est théorique : la sécurité totale serait atteinte s'il était certain que le système de vote ne pouvait rencontrer aucune panne, aucune défaillance technique et qu'aucune fraude ne pouvait être commise avec succès. Cet objectif est hypothétique et hors de portée de l'industrie informatique. Les efforts de sécurisation portent sur la redondance des calculs et des informations (voir note 5), voie qui ne peut être empruntée en ce qui concerne le vote (voir 2.2.4).

La transparence peut être directe (exercée sans intermédiaire humain ou logiciel) ou indirecte (exercée via un intermédiaire.

Quatre cas théoriques se présentent :

	sécurité totale	sécurité non totale
transparence directe	cas 1	cas 2
"transparence" indirecte	cas 3	cas 4

cas 1 : sécurité totale et transparence directe

La transparence permet aux électeurs de constater le bon déroulement des élections.

cas 2 : sécurité non totale et transparence directe

La procédure de vote est susceptible de connaître des défaillances, qu'il s'agisse d'erreurs ou de fraudes. L'exercice de la transparence permet de constater les atteintes importantes à la sincérité du vote. Les constats, portés devant la juridiction compétente, permettent l'exercice du droit.

cas 3 : sécurité totale et "transparence" indirecte

L'absence de transparence directe empêche les électeurs de constater le déroulement sans faille de la journée électorale et de fonder leur confiance. Cette situation est propice à l'apparition et à la propagation de rumeurs infondées.

cas 4 : sécurité non totale et "transparence" indirecte

L'absence de transparence directe empêche les électeurs de faire le constat de fraudes ou de dysfonctionnements même dans le cas d'atteinte à la sincérité du vote. Sans preuve, les juridictions compétentes ne peuvent exercer le droit.

Analyse

Dans deux cas la sécurité est réputée totale. Toutefois, en cas de transparence non directe (cas 3) il est impossible d'apporter des garanties que la sécurité totale est effective, le système électoral n'est alors pas en mesure de susciter la confiance chez les électeurs.

Dans deux cas la transparence est directe. Même quand la sécurité n'est pas réputée totale (cas 2), les électeurs peuvent exercer leur contrôle et faire valoir leur droit au contentieux électoral.

Nous constatons que la promesse de sécurité n'est pas en mesure de compenser la disparition de la transparence directe.

5 - Transparence et textes légaux

Nous examinons des textes régissant les élections organisées avec des dispositifs de vote électronique afin de mettre en lumière (sans exhaustivité) quelques extraits concernant la notion de transparence.

5.1 - Ordinateurs de Vote avec Bulletin Dématérialisé (OdV-BD)

5.1.1 - Code électoral

Il n'existe aucune occurrence des mots "transparence" ou "transparent" dans le code électoral.

Néanmoins, la transparence directe, sans être nommée, s'incarne dans la procédure de vote à l'urne : les opérations de vote et de dépouillement sont effectuées sans média humain ou logiciel privant les électeurs de leur capacité de contrôle.

> L'article 62 dispose que l'électeur « prend, lui-même, une enveloppe », se soustrait aux regards pour y mettre son bulletin et introduit lui-même son bulletin dans l'urne.
> L'article 63 dispose que « L'urne électorale est transparente » n'a « qu'une ouverture destinée à laisser passer l'enveloppe contenant le bulletin de vote »
> L'article 65 détaille la procédure de dépouillement : « l'urne est ouverte et le nombre des enveloppes est vérifié. » « Le bureau désigne parmi les électeurs présents un certain nombre de scrutateurs sachant lire et écrire, lesquels se divisent par tables de quatre au moins. Si plusieurs candidats ou plusieurs listes sont en présence, il leur est permis de désigner respectivement les scrutateurs, lesquels doivent être répartis également autant que possible par chaque table de dépouillement. » « Les enveloppes contenant les bulletins sont regroupées par paquet de 100. Ces paquets sont introduits dans des enveloppes spécialement réservées à cet effet. Dès l'introduction d'un paquet de 100 bulletins, l'enveloppe est cachetée et y sont apposées les signatures du président du bureau de vote et d'au moins deux assesseurs représentant, sauf liste ou candidat unique, des listes ou des candidats différents. » « A chaque table, l'un des scrutateurs extrait le bulletin de chaque enveloppe et le passe déplié à un autre scrutateur ; celui-ci le lit à haute voix ; les noms portés sur les bulletins sont relevés par deux scrutateurs au moins sur des listes préparées à cet effet. »

La procédure de vote électronique à l'aide d'OdV-BD fait apparaître l'utilisation systématique de médias, quelquefois de manière inappropriée (il n'y a pas de compteurs sur les OdV-BD, il n'existe pas de procédure valide permettant de vérifier le fonctionnement normal d'un dispositif de vote électronique). Les opérations de vote (enregistrement des suffrages, vacuité de l'urne, dépouillement) ne sont plus sous le contrôle des membres du bureau, des scrutateurs et des candidats, mais sont entièrement gérées par la "machine à voter".

> L'article 62 dispose que l'électeur « fait enregistrer son suffrage par la machine à voter. »
> L'article 63 « le bureau de vote s'assure publiquement, avant le commencement du scrutin, que la machine fonctionne normalement et que tous les compteurs sont à la graduation zéro. »
> L'article 65 détaille la procédure de dépouillement : « le président, à la fin des opérations de vote, rend visibles les compteurs totalisant les suffrages obtenus par chaque liste ou chaque candidat ainsi que les votes blancs, de manière à en permettre la lecture par les membres du bureau, les délégués des candidats et les électeurs présents. »

5.1.2 - Règlement technique fixant les conditions d'agrément des machines à voter

Le règlement technique énumère 18 principes à respecter et 114 exigences que doivent satisfaire les dispositifs de vote, il détaille l'organisation de la procédure d'agrément : chaque modèle fait l'objet d'une inspection par un organisme de certification [MinInt 2003].

Il énonce, parmi les principes à respecter,

> « transparence : le processus doit pouvoir être examiné et vérifié ; »

Outre, le fait qu'il n'est pas possible de prouver qu'un système est immune de faute, que ce soit en procédant par examen ou par des tests (voir 2.3.2) et qu'un règlement ne peut décréter la validité de nouvelles lois scientifiques, il apparaît que seuls les organismes de certification sont autorisés à procéder à des examens et vérifications et que leurs rapports ne sont pas rendus publics : "Dans un avis du 26 janvier 2006, la CADA a estimé que ces rapports comportaient des informations couvertes par le secret industriel et commercial, protégé par les dispositions du II de l'article 6 de la loi du 17 juillet 1978. Par ailleurs, selon la CADA, l'utilisation des rapports d'agrément pourrait compromettre le bon déroulement des élections et contreviendrait par là même au I de l'article susvisé." [MinInt 2006]

Non seulement, les votes se déroulent dans l'opacité, mais en plus, les électeurs ne sont autorisés ni à observer les dispositifs de vote, ni à avoir communication des rapports de ceux qui les ont observés. Or, une procédure juridique [Graton 2007] a révélé que, pour au moins un des modèles agréés en France, le respect des critères a été évalué de manière très approximative. Ces informations ont conduit l'Organisation pour la Sécurité et la Coopération en Europe à relever : « il est préoccupant que les organismes agréés de vérification aient un pouvoir discrétionnaire aussi important pour apprécier la marge de variation acceptable pour la validation de chaque critère et pour déterminer si certains critères sont pertinents ou non. » [OSCE 2007].

5.2 - Vote par internet

5.2.1 - Commission Nationale de l'Informatique et des Libertés (CNIL)

Sortant de sa compétence qui est de veiller au respect de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, La CNIL a produit une recommandation au sujet de la sécurité des systèmes de vote électronique [CNIL 2003], contribuant ainsi à organiser le déploiement de ces systèmes de vote.

Ses préconisations ne visent pas à rétablir la transparence directe mais, au contraire, laissent à penser qu'il serait possible de compenser la perte de la transparence directe par la mise en œuvre de mesures de sécurité. De plus elles consacrent l'usage d'experts dont les rapports restent protégés par le secret.

5.2.2 - Décret n° 2007-1130 du 23 juillet 2007 relatif à l'expérimentation du vote électronique pour les élections prud'homales de 2008 à Paris

> Article 16
> « Avant l'ouverture du vote, le bureau du vote par voie électronique constate la présence du scellement du système de vote, son bon fonctionnement, la remise à zéro du compteur des suffrages et le fait que l'urne électronique est vide. Il déclare alors le vote ouvert. »

La procédure de vote par internet fait apparaître l'utilisation systématique de médias, quelquefois de manière inappropriée : il n'y a pas de compteur sur les serveurs de vote, mais une représentation virtuelle d'un compteur, les systèmes de vote en service n'offrent aucune procédure valide permettant de vérifier le bon fonctionnement normal du dispositif de vote, il n'y a pas d'urne mais une représentation virtuelle d'une urne. En aucun cas, celle-ci ne peut être vide.

6 - Recherche de nouvelles procédures de contrôle par les électeurs

Il existe des variantes de méthodes de vote électronique visant à établir des procédures de contrôle par les électeurs : contrôle des programmes avant les opérations de vote, ou contrôle des résultats énoncés par les dispositifs de vote après les opérations de vote. Sans en faire une présentation complète, nous en expliquons les principes.

6.1 - Contrôle des programmes *a priori*

Dans le cadre de l'approche "logiciels libres" les programmes de gestion des élections sont publics, c'est-à-dire qu'ils peuvent être consultés, téléchargés, testés, et éventuellement modifiés, par les personnes qui le souhaitent. Cette démarche serait susceptible de faciliter la détection et la correction d'erreurs.

Toutefois elle fait l'hypothèse que de nombreuses personnes mèneront des expertises poussées, or la proportion d'électeurs disposant des connaissances nécessaires pour mener efficacement de telles expertises, et ayant la volonté et la possibilité de les mener à bien, est infime. De plus, elle rencontre les problèmes déjà signalés (voir 2.3.2) : un système de vote est un assemblage complexe qu'il est difficile d'expertiser[9], et prouver que le système en usage le jour de l'élection est identique au système expertisé (qu'il n'a pas été altéré) reste un problème non trivial. Enfin, il faut

9 En ce qui concerne le vote par internet, les ordinateurs à partir desquels votent les électeurs restent hors de portée des investigations.

remarquer qu'un tel système utilisé pour des élections délivrerait des résultats même si les démarches censées vérifier la correction des programmes n'ont pas été menées : la vérification reste optionnelle.

6.2 - Contrôle des résultats *a posteriori*

Il existe deux concepts de systèmes de vote produisant des traces utilisables (à considérer avec d'importantes précautions) pour vérifier les résultats *a posteriori*.

6.2.1 - Ordinateurs-de-Vote avec Bulletin Matérialisé (OdV-BM)

Les Ordinateurs-de-Vote avec Bulletin Matérialisé (OdV-BM) sont des dispositifs destinés à être installés au sein d'un environnement contrôlé (bureaux de vote). Lorsqu'un électeur exprime son choix, le dispositif, en sus de l'enregistrer, imprime un bulletin de vote portant mention de ce choix ; ce bulletin de vote est présenté à l'électeur pour vérification puis est stocké dans une urne à des fins d'éventuels recomptages [Mercuri 2002].

Ce système, déployé au Vénézuela et dans une partie des États-Unis, présente plusieurs inconvénients juridiques et organisationnels [Enguehard 2007b] :

- il apparaît que de nombreux électeurs ne détectent pas les modifications apportées à leur vote [Campbell & al. 2009] et que l'électeur qui a détecté une disparité entre son choix et le bulletin imprimé ne dispose d'aucune preuve pour faire valoir ses dires devant la juridiction compétente.

- les procédures de choix des urnes qui seront recomptées sont variables, certaines s'avèrent mal encadrées (par exemple, la désignation des urnes peut obéir à des règles dont l'application n'est pas contrôlée).

- les urnes doivent être déplacées puis stockées dans l'attente d'une éventuelle vérification, elles échappent alors à la surveillance des scrutateurs ; les procédures de vérification ne sont pas systématiquement publiques.

6.2.2 - Cryptographie

Les recherches en cryptographie permettent de définir des protocoles de vote par internet qui, sous certaines hypothèses[10], fournissent une forme de vérification autorisant les électeurs à constater que leur vote est compté sans avoir été modifié (un électeur constatant une modification pourrait en apporter la preuve), et que les résultats énoncés correspondent bien à l'aggrégation des votes exprimés. Ainsi, il serait par exemple possible de découvrir partiellement les effets d'un virus silencieux installé sur des postes d'électeurs et modifiant leur vote, à leur insu, avant cryptage.

Cette approche fait l'hypothèse que suffisamment d'électeurs, en sus de voter, vérifieront que leur vote a bien été pris en compte, même si les procédures à suivre sont complexes [Hubbers et al. 2005] et qu'un électeur constatant un désaccord signalerait l'incident à l'autorité juridique compétente dans les formes établies par le droit.

Cependant, même si la quantité de suffrages ayant fait l'objet de vérifications était insuffisante, les résultats seraient réputés sincères : il apparaitrait juridiquement, politiquement et socialement inacceptable de remettre en cause les résultats d'une élection pour ce seul motif.

6.2.3 - Points communs

Ces deux approches nécessitent d'établir des procédures de calcul qui prennent en compte les écarts éventuellement constatés par les vérifications partielles pour les extrapoler à l'ensemble des suffrages. Ces procédures doivent être intégrées aux textes légaux et aux pratiques juridiques afin que leurs résultats aient de réelles conséquences en ce qui concerne l'évaluation de la sincérité des élections par les juges électoraux. Par conséquent, les vérifications effectivement menées doivent faire l'objet d'un comptage précis, ce qui reste délicat dans le cas de la cryptographie.

Des résultats d'élection sont automatiquement émis immédiatement après la clôture de la période de vote, même si les vérifications à venir ne concernent qu'un nombre très faible de suffrages. Or, avec le temps, il est probable que les efforts qu'il est nécessaire de fournir pour mener à bien les vérifications verront l'ampleur de celles-ci se réduire, surtout si celles qui ont été menées sur des élections antérieures n'ont révélé aucun incident d'importance. Paradoxalement, le succès de l'approche de vérification *a posterori* pourrait donc mener à une annihilation des bénéfices qui en sont attendus.

Conclusion

Nous avons démontré que les promesses de sécurité ne sont pas en mesure de remédier à la disparition de la transparence directe. Pourtant le thème de la sécurité reste privilégié par les industriels, certains n'hésitant pas à vanter

10 Ces hypothèses, ainsi que les détails d'implémentation des protocoles, doivent être observés avec soin car ils sont susceptibles d'introduire des failles touchant, par exemple, au respect de l'anonymat.

la sécurité totale tout en niant les conséquences logiques découlant de l'opacité propre aux systèmes de vote électronique.

« *Les résultats fournis par la machine à voter NEDAP sont sûrs à 100 % [...]. Ils n'ont donc pas besoin d'être vérifiés[...].* » page web "Foire Aux Questions", site NEDAP France Election.

Il existe des procédures de vote électronique visant à suppléer la perte de transparence directe par la possibilité offerte aux électeurs d'exercer des formes de contrôle. Dans tous les cas, ces systèmes de vote sont conçus pour fournir des résultats de vote même en l'absence de contrôle effectif, ils ne sont donc pas en mesure de garantir l'exercice des contrôles censés compenser l'opacité.

Bibliographie

[Campbell & al. 2009] Campbell, B. A. & Byrne, M. D. Now Do Voters Notice Review Screen Anomalies? A Look at Voting System Usability. EVT/WOTE'09, Electronic Voting Technology Workshop / Workshop on Trustworthy Elections, Montreal, Canada, August 10-11, 2009.

[CNIL 2003] Commission Nationale de l'Informatique et des Libertés. Délibération n°03-036 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique. 1er juillet 2003.

[Enguehard 2007] Enguehard, C. Le vote électronique en France : opaque & invérifiable ! Terminal, p.199-214, #99-100, printemps 2007.

[Enguehard 2007b] Enguehard, C. Vote électronique et preuve papier. Actes du 14 ème Colloque international De l'insécurité numérique à la vulnérabilité de la société. Paris, 14 et 15 Juin 2007.

[Enguehard 2007c] Enguehard, C. Éléments de réflexion à destination du groupe de travail sur les machines à voter du Ministère de l'intérieur, de la sécurité intérieure et des libertés locales. Document communiqué lors de la réunion 30 novembre 2007.

[Enguehard 2008] Enguehard, C. Vote électronique - Élections présidentielle et législatives 2007 municipales et cantonales 2008 - Rapport exploratoire. Observatoire du vote, 8 juillet 2008.

[Enguehard 2009] Enguehard, C. Vote par internet : failles techniques et recul démocratique. Jus Politicum, n°2, mars 2009.

[Graton 2007] Graton, J.-D. Référé-liberté de Géraldine Carayol. Vaucresson, 21 avril 2007.

[Hubbers et al. 2005] Hubbers, E., Jacobs, B., Pieters, W. RIES - Internet Voting in Action. In R. Bilof, editor. Proceedings of the 29th Annual International Computer Software and Applications Conference, COMPSAC'05, pages 417-424. IEEE Computer Society. July 26-28, 2005.

[Mercuri 2002] Mercuri, R. A Better Ballot Box? IEEE Spectrum Online. vol.39, n°10, p.46-50. October 2002.

[MinInt 2003] Ministère de l'intérieur, de la sécurité intérieure et des libertés locales. Règlement technique fixant les conditions d'agrément des machines à voter. Annexe à l'arrêté du 17 novembre 2003. NOR : INTX0306924A, 17 novembre 2003.

[MinInt 2006] Ministère de l'intérieur et de l'aménagement du territoire, Lettre du chef de service chargé de la sous-direction des affaires politiques et de la vie associative à Monsieur Pierre Müller, 3 février 2006.

[MinInt 2008] Ministère de l'intérieur, de l'outre-mer et des collectivités territoriales. Utilisation des machines à voter à l'occasion des élections municipales et cantonales des 9 et 16 mars 2008. Circulaire NORINTA080002C. 1er février 2008.

[Offerlé 2002] Offerlé, M. Un homme, une voix ? Histoire du suffrage universel. Gallimard, Collection Découvertes Gallimard, ISBN : 2-07-076406-0 (br.), 2002.

[OSCE 2007] Organisation pour la Sécurité et la Coopération en Europe / Bureau des Institutions Démocratiques et des Droits de l'Homme. France - élection présidentielle 22 avril et 6 mai 2007. Rapport de la Mission d'évaluation électorale, 4 October 2007.

[Pellegrini 2006] Pellegrini, F. Rapport d'observations. juin 2006.

[VotersUnite.org 2007] VotersUnite.org. E-Voting Failures in the 2006 Mid-Term Elections - A sampling of problems across the nation, 2007.