Lettre aux Québécois sur les dangers du vote électronique

Chers et lointains cousins,

Je suis le fondateur du collectif de citoyens français recul-democratique.org, critiques envers le vote électronique. Je suis pour ma part informaticien, et nombreux sont ceux dans cette profession[1] qui partagent mes inquiétudes, que ce soit en France[2] ou à l'étranger[3].

Nous vous écrivons d'une part pour vous alerter au sujet de la **généralisation massive**[4] du vote électronique dans votre Province. Des citoyens québécois s'inquiètent[5] et s'étonnent d'avoir appris par les médias que leur ville vient de s'équiper, sans grand bruit, de machines à voter électroniques, comme si il s'agissait d'une modernisation anodine. Pas de véritables débats. Nous connaissons ce même phénomène en France. Néanmoins, des journaux commencent à publier des articles très critiques[6]. Et des Québécois nous ont rejoint et ont participé à la rédaction de cette lettre.

D'autre part, nous vous alertons sur les vulnérabilités d'une urne électronique précise : la Diebold Accuvote utilisée au Québec (liste des villes concernées à la fin). Le rapport à l'origine de cette alerte est maintenant référencé par le GAO (Government Accountability Office, agence d'audit du Congrès des États-Unis).

Ce texte est à la fois une lettre ouverte et une pétition (en huit points, voir à la fin) que vous pouvez signer sur Internet. Il est destiné à vivre **au-delà des élections municipales**.

Vu son délai très court de parution avant les élections, ce texte est susceptible d'évoluer pour répondre à des demandes d'éclaircissement ou à des informations nouvelles. Par contre, les huit points sur lesquels s'engagent les signataires de la pétition ne seront évidemment pas modifiés. Le site Internet[7] est donc l'endroit où trouver sa version la plus récente. Ce que vous avez devant les yeux a été produit le 9 novembre 2005 à 18h.

Au Québec, deux types de machines

- L'urne électronique ou compilateur de bulletins. Vous remplissez votre bulletin comme avant, puis vous le glissez dans la fente d'une sorte de scanner. Exemple : PERFAS-TAB ou Accu-Vote ES 2000.
- Le terminal de votation : tout-électronique. Vous faites votre choix directement sur l'appareil, et il est enregistré dans une mémoire électronique. Exemple : PERFAS-MV ou Votex.

Indépendamment de cela, vous entendrez peut-être le terme de "bureau de vote informatisé". Il s'agit d'ordinateurs pour gérer la liste électorale. Ils servent à identifier l'électeur, et à imprimer la liste de ceux ayant voté.

Quels problèmes voyons-nous ?

Le vote électronique nous semble retirer des mains du citoyen le contrôle de l'élection pour le confier à une poignée de techniciens, certainement bien intentionnés, mais peu nombreux et peu contrôlés (il faudrait des spécialistes tout à fait neutres pour les surveiller).

Un électeur peut légitimement se demander si son vote est bien enregistré et compté. Dans un scrutin traditionnel, il le vérifie par lui-même, car il comprend le fonctionnement des objets en jeu (bulletin, stylo, urne,...) dépourvus de technologie. Il doit seulement faire confiance à ses concitoyens scrutateurs pour ne pas ouvrir l'urne avant le

---

1 L'ACM, association d'informaticiens fondée en 1947, comptant 80 000 membres, demande des systèmes de vote conçus plus rigoureusement et avec impression d'un bulletin vérifié par l'électeur.

2 Roberto Di Cosmo : E-duquons l'e-citoyen !, également intéressant par son analyse de nos rapports avec l'informatique.

3 L'Irlande devait voter électroniquement dès 2004. 7300 machines sont toujours dans un entrepot, une commission indépendante n'ayant pû recommander leur utilisation.A la toute origine de ce mouvement de rejet, une étudiante en informatique faisant sa thèse sur le vote électronique.

4 Plus de 50% des électeurs voteront par électronique en Novembre 2005. Parmi les villes de plus de 50 000 habitants, seules Laval, Saguenay, Terrebonne et Repentigny n'utiliseront pas le vote électronique. Il n'est actuellement autorisé que pour les élections et référendums municipaux. Liste des villes, et explications sur les technologies.

5 Non au vote high-tech par J.F. Lisée. Détournement de démocratie, le vote électronique ? et articles suivants, par Michel Monette.

6 "Gare aux machines à voter électroniques", par Claude Côté, Le Soleil du 31 octobre 2005.
"Loi électorale et technologie font-elles bon ménage ?", par Claude Côté, Le Soleil du 1er Novembre 2005.
"La fiabilité des machines électroniques remise en question", La Presse du 1er Novembre 2005.
"Des questions soulevées quant à l'utilisation des appareils électroniques", Radio-Canada du 31 octobre 2005.

7 Version la plus récente de ce texte à l'adresse http://www.recul-democratique.org/article.php3?id_article=124

dépouillement, lequel est une opération publique et compréhensible par tous. Le grand nombre de personnes impliquées dans une élection, chacune faisant une petite part du contrôle, ne permet que des fraudes sporadiques et de portée limitée.

Qui peut répondre à son interrogation dans le cas du vote électronique ?

- lui-même ? Comprend-il le fonctionnement intime d'un ordinateur ? Même en étant informaticien, il ne pourrait en savoir plus, le code source du logiciel intégré à l'urne électronique étant un secret industriel.
- les scrutateurs ? Peuvent-ils garantir autre chose que d'avoir respecté des procédures techniques énumérées dans un mode d'emploi ? Par exemple, le matin, au lieu d'une urne dont ils auraient pu contrôler la vacuité de leurs propres yeux, un ordinateur a imprimé un ticket affirmant que sa mémoire était vide. Que peuvent-ils réellement en savoir ?
- sa municipalité ? Elle se fie à la sélection faite par le Directeur Général des Élections. Parfois, l'organisation technique de l'élection est confiée à une société extérieure.
- le Directeur Général des Élections ? Comment a-t-il sélectionné les machines autorisées ? A-t-il obtenu l'accès au code source de leur logiciel ? Quels tests de sécurité a-t-il conduit ?
- En fin de compte, une lourde responsabilité pèse sur le fabricant qui, accessoirement, est parfois étranger[8]. Quelques programmeurs ou quelques techniciens de la chaîne de fabrication peuvent, d'une action unique, compromettre des centaines de machines, et donc une élection entière. En règle générale, l'informatique permet de faire ce qui était auparavant manuel, à plus grande échelle, sans se déplacer et avec moins de personnel. C'était un simple exemple, choisi car le plus efficace. Au fait, que deviennent les machines entre deux élections ? Quel est le mécanisme garantissant que, le jour de l'élection, aucune machine n'ait été altérée depuis sa fabrication ?

Pourquoi demande-t-on à l'électeur une telle confiance aveugle ?

D'autre part, sur un plan technique, les systèmes de vote électronique ont une particularité les différenciant des autres systèmes informatiques : le secret du vote. On pourrait même parler d'anonymat : on ne peut relier un électeur et son suffrage. On contrôle habituellement un système informatique en examinant ce qui y entre, et ce qui en sort. On est ici dans un cas particulier : le secret du vote empêche de connaître les entrées.

Des comparaisons infondées sont souvent faites avec les procédures bancaires. Vous pouvez contrôler l'exactitude d'une transaction bancaire a posteriori, par exemple en vérifiant vos relevés de compte. Et deux systèmes informatiques sont en jeu dans chaque transaction. Et surtout, ils peuvent garder toutes les informations nécessaires à l'intégrité des données : il n'y a pas de secret entre vous et votre banque.

Chronologie de l'alerte de sécurité sur les Diebold Accuvote

1) 4 juillet 2005 : l'organisation non partisane américaine BlackBoxVoting.org publie le rapport de l'expert informatique finlandais Harri Hursti. Il qualifie les Accuvotes de "maison avec une porte tambour inverrouillable".

Il révèle l'architecture très particulière de ces machines. Leur carte mémoire, qui ne devrait contenir que des données (noms des candidats, résultats...), comprend également la partie du logiciel servant, entre autres, à imprimer les résultats. En conséquence, **on peut modifier leur comportement par simple programmation de ces cartes mémoires, sans avoir à ouvrir la machine elle-même**. Voire sans même accéder physiquement aux cartes mémoires, **en agissant à l'avance sur l'ordinateur chargé de les programmer**.

L'extrême facilité de manipulation est définie par Harri Hursti comme une « **attaque solitaire exceptionnellement flexible nécessitant quelques centaines de dollars, des compétences techniques médiocres et une modeste capacité de persuasion** (ou, au lieu de persuasion, un peu d'accès privilégié) ».

Ce rapport[9] (en anglais) est assez spectaculaire : c'est une démonstration d'impression de tickets falsifiés, de bourrage d'urne, et de prise de contrôle de l'afficheur LCD. Nous avons écrit un article, en français, basé principalement sur ce rapport, mais allégé au maximum des aspects techniques.

2) Septembre : nous envoyons quelques courriels à des journalistes publiant au sujet du vote électronique. Radio-Canada réagit, et enquête auprès du Directeur Général des Élections et des officiels de la ville de Sherbrooke. Leur réponse est le déni. Comme un universitaire confirme que le vote électronique pose problème, un reportage TV est diffusé. L'actualité étant chargée en France, nous nous concentrons dessus, pensant avoir au moins éveillé la

8 La machine PG Elections Perfas MV provient du fabricant américain Microvote. La machine Accuvote provient du fabricant américain Diebold.

9 The Black Box Report - Critical Security Issues with Diebold Optical Scan Design, par Harri Hursti.

curiosité, et que ce rapport serait lu.

3) Octobre : le GAO (Government Accountability Office, agence d'audit du Congrès des États-Unis) publie un rapport[10] critique sur l'organisation du processus électoral américain, et ce rapport référence le rapport Hursti[11]. Sa crédibilité en étant renforcée, nous prenons le temps de voir comment la situation a évolué au Québec. Aucune des trois villes concernées que nous avons contactées n'a reçu de mise en garde, ni pris de mesure particulière cette année.

Nous avons obtenu un court entretien avec un cadre de l'entreprise qui gère la partie technique de l'élection de ces villes. Il nous a confirmé qu'aucune nouvelle précaution n'était prise cette année, et que Diebold ne les a pas informés du rapport Hursti.

Par ailleurs, le Directeur Général des Élections ne répond pas à nos questions, que ce soit sur l'Accuvote ou les conditions de sélection des appareils autorisés.

Quelle solution proposons-nous ?

Tout d'abord un éclaircissement. Notre propos n'est pas prédire une catastrophe. Nous pointons des problèmes **POTENTIELS**. Souhaitons que ces élections 2005 se déroulent bien. Mais n'oublions pas que l'enjeu est le pouvoir, objet de luttes depuis la nuit des temps. Les élections sont une forme civilisée et plutôt récente de ces luttes.

La réponse officielle est souvent : « Ces appareils ont été utilisés dans de nombreuses élections, et il n'y a jamais eu de problème »[12] ou "Les dangers sont hypothétiques. Jusqu'à maintenant aucun des incidents soulevés n'est survenu"[13]. C'est succomber à une illusion classique : au motif qu'une élection s'est déroulée sans incident, elle serait intègre. Une manipulation informatique passe malheureusement inaperçue, pour peu que les résultats restent vraisemblables. **Il ne faut pas confondre fiabilité** (les machines sont-elles exactes, leurs composants électroniques tombent-ils en panne) **et sécurité** (sont-elles vulnérables à des attaques informatiques, et avez-vous, dans chaque endroit de vote, le jour de l'élection, une machine strictement identique à celle conçue).

Une autre réaction officielle est de mettre en avant les procédures de test effectuées en présence des candidats. Le rapport Hursti en démontre l'inutilité[14], en termes de sécurité. Ils sont même trompeurs puisqu'ils donnent l'illusion d'avoir exercé un contrôle. Leur seul intérêt est de détecter une erreur involontaire dans la préparation des machines, comme par exemple deux candidats inversés, ou de tester l'état de marche des composants électroniques et de l'imprimante.

Plus généralement, demander à un ordinateur de vérifier sa propre intégrité est absurde. Le logiciel intégré à l'urne électronique a toute latitude d'afficher ou d'imprimer ce qu'il souhaite. Une version modifiée de ce logiciel agira en apparence de la façon dont on attend qu'il se comporte. Dans le cas d'un logiciel en deux parties, tel l'Accuvote (une partie intégrée, une autre dans la carte mémoire), la première pourrait contrôler la seconde. Il serait logique que la machine n'accepte pas des cartes mémoires contenant n'importe quoi. Ce n'est hélas même pas le cas.

M. Hursti, dans ses conclusions, considère que les procédures opérationnelles requises pour **sécuriser le système seraient un fardeau insoutenable**[15]. La sécurité informatique n'est pas assurée en copiant les procédures issues des élections "papier". Surveiller physiquement les machines le jour de l'élection, ou même depuis leur préparation, est insuffisant.

Que faire alors ? Heureusement, ce ne sont pas des machines tout-électronique (que 67 villes vont néanmoins utiliser, mais c'est une autre question, abordée plus loin). La procédure habituelle est de faire un dépouillement manuel lorsque des anomalies sont détectées. Elle ne suffit pas, vu la discrétion d'une manipulation informatique. **Le dépouillement doit être systématique**. Nous sommes bien conscients que cela est difficile à entendre, puisque s'épargner la charge du dépouillement est une raison de passer au vote électronique.

Il reste ensuite à trancher si on recompte tous les bulletins, ou une partie choisie aléatoirement. Lourde tâche, puisqu'il n'existe à l'heure actuelle aucune mise en oeuvre satisfaisante du vote électronique. Les États-Unis se sont heurtés à des difficultés de recompte manuel, juridiques ou parce qu'il n'était pas vraiment aléatoire. Les autres pays n'ont rien qui puisse être recompté, car ils utilisent des machines tout-électronique. Comme nous

10 Federal Efforts to Improve Security and Reliability of Electronic Voting...
11 Pages 25 et 26.
12 Élection municipale à Sherbrooke: l'appareil électronique utilisé soulève des questions, Radio-Canada du 9 septembre 2005.
13 Le DGEQ dans "La fiabilité des machines électroniques remise en question", La Presse du 1er Novembre 2005.
14 Page 20 du rapport Hursti, "logic and accuracy tests".
15 « Operational procedures required to secure the system would put un-sustainable burden in perimeter defense, training of the personnel and supervision among the other layers of security. » page 21 du rapport.

n’avons pas d’illusions sur la volonté de dépouiller manuellement la totalité des bulletins, nous ne pouvons que suggérer, sans que cela nous satisfasse vraiment, de dépouiller 16% des machines[16]. Dans chaque endroit de vote serait lancé un dé (d’où le 16% = 1/6) afin de décider si le dépouillement aura lieu. Nous sommes désolés de ne pas être plus affirmatifs, mais nous ne nous sentons pas l’obligation de résoudre tous les problèmes que d’autres ont créés. Les signaler nous demande déjà beaucoup d’énergie. Nous ne nous prononcerons pas non plus sur l’intérêt du vote électronique, une fois correctement sécurisé par un recompte manuel...

Ce n’est pas tout. Encore quelque chose de difficile à entendre. Ce recompte manuel ne doit pas être compris comme une vérification ponctuelle de la fiabilité de ces machines. Ou comme une opération de communication destinée à rassurer le citoyen. Il faudra **le répéter à chaque élection à l’avenir**, afin d’en garantir l’intégrité. **Ne pas confondre fiabilité et sécurité**.

Enfin, il faudra médiatiser cela, afin d’obtenir un effet dissuasif. Et définir la procédure en cas de discordance entre résultats papier et électronique. **Le papier doit naturellement primer**, mais le cadre légal peut en décider autrement.

La triste réalité est que la sécurité informatique, c’est compliqué et **coûteux**. Le recompte manuel reste le moyen le plus simple d’éviter une cascade de vulnérabilités informatiques. Pour peu que les modalités soient correctement définies, on retourne aux problèmes de sécurité du vote papier, très bien connus, et sans conséquences à grande échelle.

Il reste à aborder la délicate question de la totalisation des résultats provenant des différentes Accuvote d'une ville. En résumé, **le rapport bénéfices/risques est ici particulièrement désavantageux**.

Les bénéfices : on économise des additions nécessitant quelques personnes avec des calculatrices pendant, disons, une heure. Les risques : on emploie pour cela un ordinateur faiblement sécurisé. Mentionnons déjà qu’il fonctionne sous Windows, système grand public particulièrement difficile à sécuriser. Est-il ensuite nécessaire d’évoquer les péripéties du logiciel GEMS, plusieurs fois mis en cause aux États-Unis en janvier 2004[17], septembre 2004[18] et mai 2005[19] ? Faut-il même se demander si il est connecté à une ligne téléphonique ? En effet, la possibilité existe de centraliser les résultats des endroits de vote par informatique.

Certaines municipalités nous ont dit se fier à l'ordinateur, telle Montréal (mais qui n'utilise ni l'Accuvote, ni GEMS). Heureusement, d'autres font ou refont les additions avec une calculatrice. Les différents candidats exercent-ils un contrôle suffisant ?

A ce jour, concernant le rapport Hursti, il n’y a pas eu de véritable réponse de Diebold. Il y a d’abord eu une lettre plus ou moins menaçante à Ion Sancho, le directeur d’élections du Leon County (Floride) qui a autorisé la démonstration de vulnérabilité, puis de curieuses réponses à ses homologues[20]. La société Diebold est probablement trop occupée à promouvoir désespérément ses nouvelles machines à écran tactile, surtout depuis que l'État de Californie les a rejetées pour manque de fiabilité[21].

Le code source, définition

L’essentiel de l’intelligence d’un système informatique est dans son logiciel (en anglais : “software”). Celui-ci existe sous deux formes :

- le “code source” : écrit et lisible par des humains, plus précisément une peuplade appelée programmeurs ou développeurs. C’est la description méthodique, et dans les moindres détails, de tout ce que fait le logiciel. Cette description est tapée comme vous taperiez une lettre, mais au lieu du français, dans un langage informatique. Il en existe des centaines, les plus connus ont pour nom : C, C++, Pascal, Basic, Java... Ces langages ont comme particularité de ne permettre aucune ambiguïté, contrairement aux langages naturels où un mot peut avoir plusieurs sens.
- l’“exécutable” formé de 0 et de 1, donc uniquement exploitable par l’ordinateur. Il est produit automatiquement à partir du “code source” au moyen d’une moulinette appelée compilateur. Il va faire s’animer l’ordinateur, au départ simple assemblage électronique inerte (en anglais : “hardware”, traduit par “matériel”).

16 16% des machines, et au minimum une par ville.
17 RABA Trusted Agent Report for Maryland General Assembly (lui aussi référencé par le rapport du GAO), pages 20 à 22.
18 E-voting critics report new flaws, CNET News.
19 Rapport Hursti, page 4.
20 Diebold Lies Move Up the Ladder, BlackBoxVoting.org, 10 octobre 2005.
21 “A Firewall for Democracy” par Andrew Gumbel, Los Angeles Times du 4 août 2005.

A l'exception notable des Logiciels Libres, vous n'achetez qu'un droit d'utilisation de l'exécutable. Le code source reste secret et propriété de son concepteur. Sans lui, vous ne pourrez qu'observer le comportement apparent de l'exécutable. Des fonctionnalités cachées (oeuf de Pâques, cheat codes, backdoor...) ne se révéleront pas si on ne connaît pas l'astuce pour les déclencher.

Une machine emblématique ?

Comme personne n'a examiné le code source de l'Accuvote, on ne pouvait déceler ses vulnérabilités. En Australie[22], en Belgique[23] et aux Pays-Bas[24], le code source de systèmes de vote est publié sur Internet. En France[25], le code source de certaines des machines est analysé par l'organisme indépendant chargé de les évaluer. Une élection doit être transparente. Tous les outils employés devraient être ouverts à l'examen par les citoyens. **Pourquoi les intérêts commerciaux priment-ils sur la démocratie ?**

Analyser le code source ne suffit pas. Il faut s'assurer que, le jour de l'élection, chaque machine contienne bien le même logiciel. Garantir cela est particulièrement difficile dans le cas de l'Accuvote, une partie du logiciel se trouvant dans une carte mémoire amovible et programmable. Beaucoup d'autres machines placent prudemment tout leur logiciel dans une puce à l'intérieur. Mais ces puces sont reprogrammables, plus ou moins difficilement. Qui fait ce contrôle d'intégrité, que certains jugent impossible ?

Heureusement, il reste une trace de l'intention de l'électeur : le bulletin qu'il a rempli avant de le glisser dans l'urne électronique. Encore faut-il donner à cette trace le rôle de contrôle qu'elle devrait avoir. Du fait des conséquences informatiques (exposées au début) du secret du vote, et de la discrétion d'une fraude électronique, ces bulletins doivent être recomptés, qu'un incident ait eu lieu ou non. Ceci est vrai pour l'Accuvote comme pour les autres machines semblables, telle la Perfas-Tab.

Et les machines tout-électronique ?

Toujours à cause de ces mêmes conséquences informatiques du secret du vote, on ne peut avoir aucune garantie de l'enregistrement et du compte de son bulletin. Comme l'a fort justement déclaré James M. Ries Jr., « Parce qu'aucune identité n'est associée aux enregistrements, il n'y a réellement aucun moyen qui me permettrait de prouver à un électeur, après le dépouillement, que les votes aient été exactement comptés tels qu'ils ont été exprimés. »[26]

Mais qui est donc ce M. Ries ? C'est le président de Microvote, société qui a conçu les machines connues au Québec sous le nom de Perfas-MV.

Une solution imaginée en réponse à cette incertitude est l'impression d'un bulletin vérifié par l'électeur[27]. La machine, une fois le vote composé, imprime un bulletin reprenant les choix effectués. Ce bulletin est montré à l'électeur, derrière une vitre. Il le compare avec l'écran, et le valide. Le bulletin est ensuite conservé dans la machine.

L'électeur a donc vu une preuve matérielle de l'enregistrement de son vote. Il faut également garantir que tous les votes exprimés soient comptés. Cela se fait au moyen d'un dépouillement manuel des bulletins imprimés : en quelque sorte un recompte des voix, le premier compte étant informatique.

Les modalités légales de recompte doivent être soigneusement étudiées. Le diable est dans les détails. En cas de discordance avec le résultat de la machine, **le dépouillement manuel doit primer**.

Ne recompter qu'en cas de scrutin serré est insuffisant. C'est **copier sans réfléchir** les procédures existantes. Cela est justifié pour une élection "papier", car augmente alors la probabilité que des erreurs humaines jouent sur l'issue du scrutin. Il est envisageable que quelques bulletins aient été mal dépouillés, mais des milliers, c'est hautement improbable. En revanche, un ordinateur n'obéit pas aux mêmes règles : un bug peut affecter une seule voix ou des milliers, indifféremment de sa probabilité d'apparition. Et bien sûr, une manipulation s'arrangerait pour ne jamais produire un résultat serré.

Comme avec les machines scannant les bulletins, il faut un dépouillement manuel **SYSTÉMATIQUE** d'une partie

22 eVACS, bien que développé par une société privée, a son code source publié.
23 A la suite d'un procès engagé par un citoyen contre l'Etat.
24 Aux Pays-Bas, le code source du système de vote par Internet a été publié. Toutefois, celui du vote en bureau de vote (machines Nedap) reste secret.
25 Pourquoi quasiment personne en France n'a vu le code source..., recul-democratique.org
26 "Because of identity or lack of identity with records, there's really no way that I could prove to a voter, post tally, that their vote exactly counted the way that they voted it.", Excerpts from Interviews with MicroVote Executives, WishTV.
27 Le bulletin imprimé vérifié par l'électeur (VVPB/VVAT), recul-democratique.org

statistiquement significative des machines.

Il faut éviter de se focaliser sur une technologie : on peut voir comme semblables tous ces appareils, leur seule différence étant dans l'acquisition des données. Un appui sur un écran tactile, ou un bouton, un scanner de bulletin ou un lecteur de cartes perforées, tout cela amenant à un noyau à peu près conçu selon les mêmes principes.

Et posant tous la même question: peut-on vérifier leur intégrité, qui est encore plus cruciale que leur fiabilité, en recomptant manuellement quelque chose.

Plus généralement, il s'agit d'envisager cela comme un contrôle permanent, utilisé à toutes les élections, du bon fonctionnement des machines, et non pas comme une opération de communication essayant de prouver ponctuellement que le vote électronique est fiable.

Enfin, il faut comprendre que cette solution, dont le principe semble simple, pourrait se révéler difficile à mettre en pratique. On entre en terre inconnue. Un pays s'y essaie résolument : les États-Unis. Les expériences belges et brésiliennes n'ont pas été convaincantes. Au moins un autre pays d'Amérique du Sud l'a utilisé, le Vénézuela, mais nous manquons d'informations.

Les limites du concept de bulletin imprimé

La mise en oeuvre demande de répondre à la question suivante : que faire en cas de discordance entre l'affichage à l'écran et l'impression ?

On annule votre vote, et on recommence ? Et si ça fait à nouveau une discordance ? Une partie des bugs se reproduisent indéfiniment, l'ordinateur est infatigable pour cela...

Que faire dans ce cas là ?

Il faut alors annuler l'élection dans tout le pays, examiner le logiciel, le corriger et le replacer dans toutes les machines, puis convoquer à nouveau les électeurs. Comment ça, les citoyens n'ont plus confiance ?

Comment ça, il vaut mieux ne rien imprimer afin que personne ne s'aperçoive d'une erreur ?

Comment ça, chaque fois que j'achète quelque chose par carte de crédit, on me donne un reçu, et là, on me refuse un malheureux ticket une fois tous les quatre ans ?

POURQUOI CETTE LETTRE ?

La majorité des électeurs voteront par électronique le 6 novembre 2005. Ce mode de scrutin n'est pourtant autorisé qu'à titre d'essai[28]. Le jeu en vaut-il la chandelle ? La question se pose quand on sait que le vote électronique peut sérieusement faire augmenter le coût des élections[29] [30].

Quoiqu'il en soit, nous appelons à la vigilance lors du déroulement des élections et à un débat public sur l'opportunité du vote électronique à l'occasion des travaux de la commission spéciale sur la Loi électorale du Québec[31] qui ont démarré le 1er novembre. Par ailleurs, ce sujet, et notamment le vote par Internet, sera certainement abordé lors de la consultation de Communautique[32], un organisme à but non lucratif visant l'appropriation sociale et démocratique des technologies de l'information et de la communication oeuvrant pour les organismes communautaires et les populations à risque d'exclusion des technologies.

Les problèmes qui se posent vont en effet au-delà des dimensions sécuritaires et financières.

Pierre Muller, fondateur de recul-democratique.org

Courriel : contact@recul-democratique.org

---

28 Selon la LERM (Loi sur les élections et les référendums dans les municipalités), il s'agit de "faire l'essai, lors d'un scrutin, de nouveaux mécanismes de votation." (art. 659.2). Le terme "essai" est également celui employé dans un document récent du DGEQ.

29 En réponse à notre questionnaire sur leur utilisation du vote électronique, deux municipalités (sur la dizaine qui ont répondu vite) nous ont avancé le surcoût par rapport au vote traditionnel comme obstacle.

30 Infomètre (CÉFRIO). E-Poll, l'appareil de votation de demain? Bulletin du 7 octobre 2005. « ...le vote électronique reviendra toujours plus cher que le vote papier. », avec toutes les limites des comparaisons entre pays.

31 Assemblée nationale du Québec. Commission spéciale sur la Loi électorale. 37e législature, 1ere session.

32 Communautique réalise une consultation du 24 octobre au 16 décembre 2005: gouvernement en ligne, cyberdémocratie, administration électronique... Rencontres régionales et consultation en ligne.

Pétition

Vous pouvez signer sur Internet une pétition[33] sur les points suivants, cela **même au-delà** de l'élection du 6 Novembre 2005.

Les citoyens québécois signataires de cette pétition :

1. souscrivent à l'analyse des problèmes du vote électronique exposée dans le paragraphe "Quels problèmes voyons-nous ?",
2. demandent un débat public sur l'opportunité même du vote électronique, en évitant de se cantonner d'emblée à en chercher les meilleures mises en oeuvre,
3. demandent que toute la lumière soit faite sur les vulnérabilités de la machine Diebold Accuvote,
4. demandent le dépouillement manuel SYSTÉMATIQUE d'une partie statistiquement significative de tous les scrutins électroniques, et que toutes les machines permettent ce dépouillement manuel,
5. demandent que la totalisation des résultats provenant des différentes machines se fasse manuellement,
6. demandent la publication du code source de tous les logiciels de vote électronique,
7. demandent une évaluation claire et publique des économies réalisées ou des surcoûts engendrés,
8. demandent que l'activité politique des cadres et actionnaires des entreprises du secteur du vote électronique, ainsi que leur possibilité de financer des partis politiques, soit réglementée spécifiquement.

Liste des villes concernées, avec type de machine utilisée

- **Accuvote** : Amos, Beauharnois, Beloeil, Brownsburg-Chatham, Candiac, Chambly, Châteauguay, Chertsey, Dolbeau-Mistassini, Donnacona, Drummondville, Gatineau, Granby (Canton), Hudson, L'Assomption, L'Île-Perrot, La Prairie, Lachute, Les Cèdres, Lévis, Longueuil, Lorraine, Marieville, Mascouche, Mercier, Mont-Laurier, Mont-Saint-Hilaire, Morin Heights, Notre-Dame-de-l'Île-Perrot , Pays-d'en-Haut (MRC), Pincourt, Rimouski, Roberval, Saint-Adolphe-d'Howard, Saint-Eustache, Saint-Félicien, Saint-Jean-sur-Richelieu, Saint-Lambert-de-Lauzon, Saint-Nicéphore, Sainte-Anne-des-Plaines, Sainte-Catherine, Sainte-Julienne, Sainte-Marie, Salaberry-de-Valleyfield, Sherbrooke, Sorel-Tracy, Val-d'Or, Vaudreuil-Dorion, Warwick.
- Toutes les villes et autres machines : page suivante.

Cette liste a été faite à partir des "Ententes concernant de nouveaux mécanismes de votation", accords entre la municipalité, le MAMR (ministre des Affaires municipales et des Régions) et le DGE (Directeur général des élections). Ces ententes sont publiées dans la Gazette officielle du Québec. Cette procédure a été définie par l'article 659.2 de la Loi sur les élections et les référendums dans les municipalités (LERM). Il a pu y avoir des utilisations du vote électronique avant cette loi, et une municipalité peut demander cette entente sans s'en servir en pratique, ou ne l'avoir fait qu'une année, et ne pas recommencer cette année.

Cette liste est donc indicative. Contactez votre municipalité pour avoir une certitude. Cette liste comprend 125 lignes. Le chiffre officiel du DGE est de 156 villes, dont 67 en tout-électronique. La différence peut s'expliquer par le fait que certaines lignes sont des cantons.

Le vote électronique ne peut actuellement être utilisé qu'uniquement dans le cadre d'élections et de référendums municipaux.

BVI = "bureau de vote informatisé".

33 A l'adresse http://www.recul-democratique.org/article.php3?id_article=123

Amos : AccuVote + BVI
Amqui : Votex
Assomption (L') : AccuVote + BVI
Baie-Comeau : Perfas-Tab
Basques (MRC des) : Votex
Beauharnois : AccuVote + BVI
Beaupré : Perfas-MV
Bécancour : Perfas-Tab + BVI
Beloeil : AccuVote
Blainville : Perfas-Tab
Bois-des-Filion : Perfas-MV
Boisbriand : Perfas-Tab
Brownsburg-Chatham : AccuVote
Candiac : AccuVote
Cèdres (Les) : AccuVote
Chambly : AccuVote
Chandler : Votex
Charlemagne : Perfas-MV
Châteauguay : AccuVote + BVI
Chertsey : AccuVote
Chibougamau : Votex
Compton : Votex
Cowansville : Perfas-MV
Deux-Montagnes : Perfas-Tab + BVI
Dolbeau-Mistassini : AccuVote
Donnacona : AccuVote
Drummondville : AccuVote
Farnham : Votex
Gatineau : AccuVote
Granby (Canton) : AccuVote
Granby : Perfas-MV
Grande-Rivière : Votex
Grenville-sur-la-Rouge : Perfas-MV
Harrington (canton) : Perfas-MV
Haute-Gaspésie (MRC de la) : Votex
Hudson : AccuVote
Île-Perrot (L') : AccuVote
Lac-Mégantic : Perfas-MV
Lachute : AccuVote
Lévis : AccuVote
Longueuil : AccuVote + BVI
Lorraine : AccuVote
Louiseville : Perfas-Tab + BVI
Magog : Perfas-MV
Mandeville : Perfas-MV
Marieville : AccuVote + BVI
Mascouche : AccuVote (+ BVI ?)
Mercier : AccuVote
Mont-Laurier : AccuVote
Mont-Saint-Hilaire : AccuVote
Montmagny : Perfas-MV
Montréal : Perfas-Tab + BVI
Morin Heights : AccuVote
Nicolet : Perfas-MV
Notre-Dame-de-l'Île-Perrot : AccuVote
Otterburn Park : Perfas-MV
Paspébiac : Votex
Pays-d'en-Haut (MRC) : Perfas-Tab ou AccuVote
Piedmont : Perfas-MV
Pincourt : AccuVote
Pocatière (La) : Perfas-MV
Pointe-Calumet : Perfas-MV
Pont-Rouge : Perfas-MV
Prairie (La) : AccuVote (+ BVI ?)
Princeville : Votex
Québec : Perfas-MV
Rawdon : Perfas-Tab + BVI
Rigaud : Perfas-Tab
Rimouski : AccuVote
Rivière-du-Loup : Perfas-MV
Roberval : AccuVote
Rosemère : Perfas-Tab
Saint-Adolphe-d'Howard : AccuVote
Saint-André-Avellin : Perfas-Tab
Saint-André-d'Argenteuil : Perfas-MV
Saint-Charles-Borromée : Perfas-MV
Saint-Colomban et Villes : Perfas-MV
Saint-Constant : Perfas-MV
Saint-Donat : Perfas-MV
Saint-Eustache : AccuVote
Saint-Félicien : AccuVote
Saint-Georges : Perfas-Tab + BVI
Saint-Hyacinthe : Perfas-MV
Saint-Jacques : Perfas-MV
Saint-Jean-sur-Richelieu : AccuVote + BVI
Saint-Jérôme : Perfas-Tab + BVI
Saint-Lambert-de-Lauzon : AccuVote
Saint-Lazare : Perfas-MV
Saint-Liboire : Perfas-MV
Saint-Mathias-sur-Richelieu : Perfas-MV
Saint-Michel-des-Saints : Perfas-MV
Saint-Nicéphore : AccuVote
Saint-Ours : Perfas-MV
Saint-Pascal : Perfas-Tab
Saint-Paul : Votex
Saint-Pie : Perfas-MV
Saint-Sauveur : Perfas-MV
Saint-Zotique : Perfas-MV
Sainte-Adèle : Perfas-Tab
Sainte-Agathe-des-Monts : Perfas-MV
Sainte-Anne-des-Monts : Votex
Sainte-Anne-des-Plaines : AccuVote
Sainte-Catherine : AccuVote + BVI
Sainte-Émélie-de-l'Énergie : Perfas-MV
Sainte-Julie : Perfas-Tab + BVI
Sainte-Julienne : AccuVote
Sainte-Marie : AccuVote + BVI
Sainte-Marthe-sur-le-Lac : Perfas-MV
Sainte-Thérèse : Perfas-Tab
Sainte-Victoire-de-Sorel : Perfas-MV
Salaberry-de-Valleyfield : AccuVote + BVI
Shawinigan : Perfas-MV
Sherbrooke : AccuVote
Sorel-Tracy : AccuVote
Stoneham-et-Tewkesbury (Cantons-Unis) : Perfas-MV
Thurso : Perfas-Tab + BVI
Trois-Pistoles : Votex
Trois-Rivières : Perfas-MV
Val-d'Or : AccuVote
Val-David : Perfas-MV
Val-Morin : Perfas-MV
Vaudreuil-Dorion : AccuVote
Victoriaville : Perfas-MV
Ville Causapscal : Perfas-MV
Warwick : AccuVote