


Tribune de Genève, Luca Sabbatini, 26 Juin 2008	
Le vote électronique, foyer de polémique	
E-VOTING Le projet genevois de vote par Internet pourrait être débattu ces jours au Grand Conseil. Innovation nécessaire pour renforcer la démocratie ou mauvaise idée?	Commentaires
	Un projet pilote qui semble devoir être appelé : "Plan Neuf d'Outre-Vote" ¹
Le projet genevois de vote par Internet figure en 23 ^e position de l'ordre du jour du Grand Conseil. Les députés auront-ils le temps d'en débattre lors des sessions de jeudi ou vendredi? La discussion, repoussée depuis plusieurs mois, aura-t-elle lieu à la rentrée? Impossible de le prévoir. Ce qui est sûr en revanche, c'est que le projet de loi constitutionnelle pour l'introduction du vote électronique dans le canton de Genève suscite une farouche opposition.	Il y a en fait deux projets de loi : L'un est constitutionnel et de portée générale, il autorise la voie du vote électronique, et définit surtout la création d'une commission électorale, formée de politiciens devant surveiller le processus des scrutins. L'autre projet est un complément à la loi sur les droits politiques et définit l'utilisation du canal électronique pour les scrutins; ce dernier projet a fait fausse route, car il n'est pas neutre technologiquement et même étroitement lié au système pilote actuel, notoirement insuffisant. De ce fait, le second projet de loi limite l'avenir du vote électronique dans le canton. Le débat sur les projets de loi au Grand Conseil devrait avoir lieu le 28 août 2008.
Alors que le chancelier Robert Hensler assure que le dispositif d'e-voting mis au point par ses services est parfaitement sûr et fiable,	La sécurité parfaite n'existe pas : "Informatique: la sécurité à 100% n'existe pas" Communiqué du Conseil Fédéral 15/03/2002. La fiabilité parfaite non plus, particulièrement en informatique : « Il faut accepter que les ordinateurs ne sont pas infallibles, et que toute affirmation du contraire tient davantage de la croyance que de la logique. » Chantal Enguehard, Laboratoire d'Informatique de l'Université de Nante.
de nombreux experts en sécurité informatique restent sceptiques, voire violemment contraires à cette innovation.	« Le paradoxe, dans cette affaire, c'est que les politiques qui défendent les machines à voter – sans, bien souvent, s'y connaître en informatique – accusent leurs opposants d'être rétifs au progrès technique. Alors que la majeure partie de ces opposants, eux-même informaticiens – et donc a priori peu suspects de luddisme ² borné –, se retrouvent à investir le champ citoyen pour donner des leçons de civisme aux politiques qui sont censés défendre et incarner notre démocratie. Jean-Marc Manach, journaliste
Leurs doutes se sont d'ailleurs insinués sur l'échiquier politique.	Il est à remarquer que le front de ces doutes, qui est en fait une franche opposition, ne suit pas une ligne de démarcation politique usuelle; il n'y a aucun clivage gauche-droite : Pour : PS (s'effrite?), PDC, Contre : UDC, Verts, MCG, SolidaritéS,

1 En souvenir du film "Plan 9 from Outer Space" d'Ed Wood (1959).

2 "Luddisme" - opposition aux nouvelles technologies


	Très partagés : Libéraux, PRD.
Ainsi, le mouvement Solidarités a-t-il adressé lundi une lettre aux députés genevois les enjoignant à ne pas soutenir le projet.	Excellente lettre (23/06/2008, Pierre Vanek), qui met le doigt sur un point crucial : La nécessaire " <i>transparence et le contrôle citoyen possible sur l'ensemble du déroulement des opérations électorales</i> ". En opposition à l'option actuelle où " <i>le citoyen est invité à «faire confiance»</i> ", alors qu" <i>une saine méfiance et un esprit critique envers les autorités sont des qualités citoyennes et démocratiques qu'il faut pour le moins admettre, voire à [ses] yeux encourager.</i> "
Du côté de la chancellerie d'Etat, qui porte à bout de bras le projet depuis six ans et qui jouit du soutien financier de la Confédération,	<p>Imprécision ! Le pilote <u>a</u> été cofinancé par la Confédération durant la phase de développement, et ce n'est plus le cas depuis longtemps. Plus précisément :</p> <p>"Les projets pilotes avaient pour but d'étudier la faisabilité, les chances et les risques du vote électronique." Introduction du "Rapport sur les projets pilotes en matière de vote électronique" (06.056 du 31 mai 2006)</p> <p>"Les accords [entre le Conseil Fédéral et les cantons pilotes] prévoient expressément que les projets pilotes ne préjugent en rien d'une future solution fédérale" Introduction aux projets pilotes de vote électronique (http://www.bk.admin.ch/themen/pore/evoting/00774/index.html?lang=fr)</p> <p>Le but fondamental de la Chancellerie Fédérale dans le projet des pilotes e-Voting a été d'acquérir l'expérience de l'utilisation de ce troisième mode de vote par la population, et non de produire un ou plusieurs systèmes informatiques de vote électronique pour les diffuser ensuite auprès de l'ensemble des cantons.</p> <p><i>"Le paragraphe essentiel est [celui-ci ↑], il synthétise la situation et est parfaitement correct"</i> M. Hans-Urs Wili, chef de la section des Droits Politiques de la Chancellerie Fédérale.</p>
on se veut rassurant. «Je respecte l'opinion de ceux qui se méfient du vote électronique, déclare Robert Hensler.	Il est étonnant de parler de respect, et pourtant de réduire la contradiction à l'"émotif" ou au "subjectif". C'est un total déni de l'argumentation rationnelle et objective.
C'est un sujet émotif, affectif, subjectif.	"La démocratie n'est pas un gadget pour quelques hommes politiques en mal d'image, conseillés par des docteurs Folamour de l'administration" Vote électronique : les boîtes noires de la démocratie , Perline, Thierry Noisette
Mais nous avons effectué neuf tests grandeur nature lors de votations municipales, cantonales et fédérales. Notre système offre toutes les garanties en matière de sécurité.»	Les tests ne prouvent rien quant à la sécurité – ils ne peuvent que prouver qu'il y a une faille, si celle-ci est apparue; mais pas qu'il n'y en a pas. Les essais de piratage commandités lors de ces tests ne sont que des coups de sonde depuis l'extérieur.

	<p>"Cessez d'assumer que les systèmes sont sûrs, car on n'y a pas démontré d'insécurité; commencez d'admettre que les systèmes ne sont pas sûrs s'ils n'ont pas été conçus sécuritairement [dès l'origine]."³</p> <p>Bruce Schneier, célèbre expert en cryptographie et sécurité.</p> <p>Ensuite, seule une vaste étude publique de l'architecture, des algorithmes et de l'implantation, au sein d'un débat critique ouvert, peut fonder la confiance.</p>
Pour le chancelier, le vote électronique est avant tout un moyen supplémentaire donné aux citoyens pour exprimer leur opinion.	Certes, mais il doit être de même niveau de sécurité et de respect des principes que les précédents modes (confiance, sécurité, secret, etc.) !
«Le vote par correspondance a permis d'augmenter le taux de participation, rappelle-t-il. Plusieurs études le montrent, l'offre par Internet est un moyen d'attirer les jeunes électeurs.	
Sans oublier les Suisses de l'étranger, pour qui voter reste compliqué.»	Mais pour qui le vote par internet ⁴ serait aussi compliqué, si l'on poursuit l'actuelle limitation aux pays parties de l'arrangement de Wassenaar ⁵ (car seuls 40 pays en sont membres -les occidentaux); ensuite dont la valeur de l'identification sera entamée par l'absence du cadre légal national.
<p>L'e-voting marque-t-il réellement un progrès? Va-t-il renforcer les droits populaires ou au contraire les diminuer?</p>	
«En tant que citoyen, la question qui me gêne le plus, c'est celle de la vérification», lance Martin Vuagnoux, un chercheur au LASEC, le laboratoire de sécurité et cryptographie informatique de l'EPFL, qui a travaillé comme consultant sur le projet genevois.	<p><u>Des votations sans transparence démocratique</u> Exact, c'est l'ignorance grossière du principe de "<u>Transparence</u>" (avec celle des principes corrélés de "<u>Recomptabilité</u>" et de "<u>Prouvabilité</u>")</p> <p><u>Un vote sans protection du secret</u> Par ailleurs, on peut relever aussi l'irrespect négligeant du principe du "<u>Secret du vote</u>" (et celui de "<u>Temporalité</u>").</p>
<p>Sécurité et anonymat</p>	
S'il est tenu au secret quant aux détails du logiciel lui-même, l'informaticien reste libre de s'exprimer sur le concept global. «J'identifie plusieurs problèmes à régler dans un système d'e-voting.	
D'abord, il faut développer un algorithme de cryptographie pour garantir à la fois la sécurité et l'anonymat des transactions entre le PC du citoyen et le	La garantie constitutionnelle du droit de vote [par Internet] se traduit par des exigences relatives au secret et à la sécurité du vote ainsi qu'à l'identification de l'électeur. Selon Prof. A. Auer ⁶ , résumé ⁷ par le Prof. Sébastien Grammond

3 http://www.schneier.com/blog/archives/2008/07/the_dns_vulnera.html (29/07/2008)


4 Le premier essai, 01/06/2008 basé sur le système neuchâtelois, était limité aux inscrits du "guichet unique" (garantissant la bonne identification) et résidant dans un pays de l'UE ou partie de l'arrangement de Wassenaar (à cause des restrictions à l'exportation des moyens cryptographiques mis en oeuvre).
<http://www.news-service.admin.ch/NSBSubscriber/message/fr/19093>

5 Entente sur le contrôle de l'exportation des produits militaires, ou à double usage, dont les moyens cryptographiques.

serveur de l'Etat.	(U.Ottawa/CAN).
Si la cryptographie fonctionne en général assez bien, son implémentation dans un système reste difficile.»	
Pourtant, l'e-banking, par exemple, a depuis longtemps fait ses preuves en matière de sécurité sur Internet. En quoi l'e-voting serait-il différent? « La comparaison ne tient pas», lance José Nunes, président du Groupement romand des utilisateurs de logiciels libres et adversaire déclaré du vote par Internet.	Exact ! Consulter aussi la contribution " Faire de l'eBanking n'ouvre pas la voie à l'eVoting, ne pas confondre ! " du sujet " Le vote électronique sur la sellette à Genève " du WikiForum de la Radio Suisse Romande.
«Dans l'e-banking, les deux parties veulent cacher la transaction de l'extérieur, mais elles n'ont pas de secret entre elles	C'est justement la collaboration entre les deux parties (client et banquier), qui ne se cachent ni leur identité (client), ni le contenu de leurs transactions (ordres) qui apporte la meilleure sécurité en permettant la vérification et l'éventuelle correction du contenu de la transaction. Ce n'est absolument pas le cas dans le vote !
Dans le vote par Internet, on veut aussi cacher la transaction, mais en plus l'Etat doit protéger l'anonymat du vote, ce qui est beaucoup plus compliqué.»	En effet, quiconque, y compris l'État, ne doit pouvoir relier un bulletin, et son contenu, à un citoyen l'ayant rempli ! Une douzaine de textes de loi fédérale , et de jurisprudence du Tribunal Fédéral, réaffirment constamment ce principe de votation démocratique.
Pour José Nunes, il serait plus judicieux d'utiliser le Web pour les signatures des initiatives et référendums, «puisque l'anonymat n'est pas requis».	Ce qui nécessite la possession par les éventuels signataires d'une identité numérique dont la qualité permette la signature (donc la mise en oeuvre d'un service de délivrance, de maintenance et reconnaissance, et de révocation de ces identités fortes).
Cryptage de bout en bout	La chancellerie genevoise place toujours le débat sur la sécurité (par ailleurs inconnue) du système de vote électronique, alors que le premier but à atteindre doit être l'adéquation aux principes du vote démocratiques.
«Pour rendre inviolable la transaction, plusieurs innovations ont été introduites» depuis le dernier test en avril 2005, rétorque	A-t-on doté d'une serrure "invulnerable" (sic) la salle du trésor où on peut simplement entrer par la fenêtre, à moins qu'on ait sécurisé la porte de la fragile cabane en bois des trois petits cochons ? Ce n'est pas la transaction qui compte, c'est toute la chaîne de vote qui doit être fiable, le moindre anneau faible affaiblit le tout : il faut que le système soit résistant aux tentatives extérieures et aussi intérieures (bien plus dangereuses), et ce du lancement de la session à la fin de la période de recours.
Michel Warynski, responsable des systèmes d'information au sein de la chancellerie d'Etat et à ce titre chef du	

6 Constitutionnaliste, "Research Centre on Direct Democracy" université de Zurich, anciennement à l'U. de Genève


7 Chronique bibliographique, U. Laval, p.211, <http://fd.ulaval.ca/cahiers/docprotege/45-1-p.pdf>

<p>projet de vote par Internet.</p> <p>«Nous avons installé un canal de sécurisation entre le PC du votant et le serveur de l'Etat. Le cryptage s'effectue ainsi d'un bout à l'autre de la chaîne.»</p>	<p>Ce "canal de sécurisation", emphatiquement cité ici, est celui du transport; il représente l'équivalent de l'enveloppe extérieure du vote par correspondance, qui -comme dit ici- s'arrête au serveur de l'État. Or, il faut de plus protéger le bulletin des personnes pouvant atteindre les serveurs⁸, en conséquence le bulletin ne doit jamais quitter le poste du votant sans avoir été préalablement chiffré (enveloppe intérieure du vote par correspondance), et le rester absolument jusqu'au dépouillement.</p>
<p>Sauf que le maillon faible, l'ordinateur du citoyen, «reste, lui, souvent mal protégé et vulnérable contre des attaques malveillantes», selon José Nunes. Un «hacker» peut facilement prendre le contrôle d'une machine à distance.</p>	<p>"Lors de son élaboration, un bulletin de vote peut être modifié par un virus dormant, être ensuite crypté, puis émis vers le site de vote officiel où il sera compté avec les autres votes sans que quiconque puisse diagnostiquer son altération. Les votes peuvent être compromis sans que le cryptage n'y puisse rien changer."⁹</p> <p>Chantal Enguehard, maître de conférence en informatique, Uni. de Nante</p> <p>En commentaire d'un co-rapport¹⁰, le premier assistant du Laboratoire de Sécurité et Cryptographie évaluait à 40% le nombre de bulletins potentiellement falsifiables par une attaque du poste du votant.</p> <p>En résumé, le "canal de sécurisation" mentionné plus haut, ne protège nullement contre ces attaques, même le chiffrement local du bulletin n'y fait rien.</p> <p>L'affichage alternatif de confirmation avec verrouillage cryptographique de l'intégrité du bulletin peut largement y subvenir, mais le mieux est d'isoler le processus de vote dans une machine virtuelle le protégeant des compromissions du système originel du poste.</p>
<p>Le rôle des scrutateurs</p>	
<p>Mais plus encore que le piratage informatique, Martin Vuagnoux redoute le risque de manipulation par l'Etat lui-même.</p>	<p></p>
<p>«Dans le vote traditionnel par bulletin, des scrutateurs contrôlent le bon déroulement du décompte des voix.</p>	<p>"Le vote traditionnel – y compris le vote par bulletin manuscrit et les fiches de saisie permettant le comptage électronique des voix – repose sur l'existence bien réelle d'un registre électoral, de certificats de capacité civique, de bulletins, de fiches de saisie, d'une urne, de signatures manuscrites, etc. Les endroits où peuvent s'opérer des manipulations sont donc visibles au sens propre, ce qui permet – en cas de panne ou d'abus – d'opérer des contrôles ou des recomptages au vu et au su de chacun."</p> <p>Rapport du Conseil Fédéral 02.009 sur le vote électronique, chances,</p>


8 «Il est extrêmement difficile d'arrêter un informaticien qui veut vraiment faire du mal.» Claude Chollet, cité dans l'article "[Informaticiens, un pouvoir démesuré et incontrôlé](#)" de Gabriel Sigrist (03 juin 2008) sur Largeur.com

9 in "Querelle sur le e-voting", au sujet du débat avec le chancelier Hensler, Tribune de Genève, 31 déc. 2007

10 Description d'une famille d'attaques possibles contre l'eVoting : http://www.kroepfli.ch/ext/20040831_0925.pdf

	risques et faisabilité (p. 16)
Avec le vote électronique, le citoyen vote depuis son PC, mais la suite du processus s'apparente pour lui à une boîte noire.»	"La régularité de la procédure de vote, et le contrôle [démocratique*] de cette régularité, sont ainsi des éléments décisifs et irremplaçables de la légitimité démocratique" (*) "les experts ne contrôlent que ce qu'ils veulent, ou ce qu'ils peuvent" Prof. Andreas Auer (ex.Uni.Genève), cité ⁹ par Ch.Enguehard
Une vision des choses que Robert Hensler conteste. «Les scrutateurs agréés par les partis et par le Conseil d'Etat ne disparaissent pas avec l'e-voting.	Des scrutateurs qui ont des yeux pour voir, mais qui ne voient plus rien ... à peine la boîte de métal d'un serveur abscons. Les scrutateurs ne disparaissent peut-être pas, mais la scrutation a bel et bien disparu. Voir -infra- l'avis de Martin Vuagnoux : "c'est comme si on ne vérifiait pas l'urne. On n'a pas d'autre choix que de faire confiance à l'Etat."
Ils seront même plus que jamais les garants du résultat, car ils sont les seuls à posséder les clés électroniques qui permettent d'ouvrir l'urne virtuelle.	Ils peuvent seuls ¹¹ déclencher le déchiffrement des bulletins contenus dans l'urne électronique. Mais ceci ne garantit pas que ces bulletins : - soient les bons (pas plus), - soient dans l'état d'origines (pas modifiés/échangés), - soient la totalité de tous les bulletins remplis (pas moins). C'est dans la surveillance efficiente de l'ensemble du processus de vote que la scrutation a un sens.
Et le recomptage reste tout à fait possible.»	Faux ! Seules les réponses aux questions du bulletin sont enregistrées, aussi il ne fait aucun sens de recompter -c.-à-d. compter une seconde fois de la même manière- des suites de "oui" ou de "non", sans indications d'authenticité (est-ce un vrai vote d'un vrai citoyen), ni possibilité de vérification d'intégrité (a-t-il subi des falsifications), ni vérifier l'exhaustivité (n'en manque-t-il pas). Par ailleurs, "Recompter" en se basant sur les journaux ^o (ou "log") du serveur enfreint le secret du vote, ceci à cause du fonctionnement du système pilote (l'identification du votant s'y trouve). De plus cela ne prouve rien (pas plus d'authenticité, ni d'intégrité des bulletins transitant). (o) Ainsi que cela a été précisé par le chef de projet, lors des séances de la Commission des Droits Politiques.
Certes, mais «les scrutateurs n'ont pas accès à l'entier du déroulement du vote», regrette Martin Vuagnoux.	
«Il faudrait pour cela qu'ils possèdent des connaissances techniques	Ils ne verraient surtout que des enregistrements électroniques non probants, ayant pu être modifiés, et

11 Éventuellement, mis à part une copie de sauvegarde de la clef de déchiffrement en cas de défaut des scrutateurs.

considérables, notamment en matière de cryptographie.	sans laisser la moindre trace.
Au final, c'est comme si on ne vérifiait pas l'urne. On n'a pas d'autre choix que de faire confiance à l'Etat.»	
Et José Nunes de surenchérir: «En écartant les citoyens de la possibilité de contrôle, on court le danger de créer une nomenklatura.»	
Comment ça marche?	
- Lors d'une votation, l'électeur se rend sur le site www.geneve.ch/ge-vote . Il s'identifie au moyen d'un code PIN personnel figurant sur sa carte de vote. Ce code change à chaque scrutin.	
- Pour être certain qu'il se trouve bien sur le site de vote de l'Etat de Genève, l'électeur doit vérifier la signature du certificat électronique, codé et infalsifiable.	On ne peut dire "infalsifiable" : car le certificat du site de vote peut-être vulnérable à une attaque par collision. Il est possible de générer deux certificats de sujet identique, dont un seul est signé, mais la signature de l'Autorité de Certification est valable pour les deux (certificats des clefs d'authentification de site). L'empreinte numérique à vérifier étant la même pour les deux certificats, le votant ne peut donc pas voir la différence entre le vrai et le faux site. Voir point 6 en page 4 du document " Notes sur les pilotes fédéraux ".
En outre, chaque électeur reçoit une image qui lui est propre et qui est mêlée à la confirmation de son vote. Seul le serveur de l'Etat peut associer la bonne image avec le numéro d'électeur correspondant.	Ce qui fait que le serveur de l'État a reçu le contenu du bulletin en clair, ce qui enfreint le principe du secret du vote –on sait ⁰ qui a voté quoi– et de la temporalité –on sait ¹ ce qui est voté avant la clôture du scrutin et le dépouillement de l'urne. (0) L'État connaît le lien entre l'identification numérique et le nom du votant, car il a généré et doit garder cette liste. (1) L'État connaît le contenu des bulletins déposés, et peut donc éventuellement réagir selon l'orientation que prend progressivement le résultat provisoire du scrutin au cours des trois semaines de votations. Par ailleurs, diverses attaques permettent de contourner la pseudo-protection de l'image filigrane utilisée : Les codes filigranes des image(tte)s identifiantes peuvent être décodés et donc recomposés. Voir point 1 al. 3 en page 4 du document " Notes sur les pilotes fédéraux ".
- Les votes envoyés par Internet sont stockés dans une urne électronique cryptée.	C'est la moindre des choses, et c'est très insuffisant.
Après la clôture du vote, l'urne électronique est décryptée par les contrôleurs qui en possèdent seuls les clés et ses résultats ajoutés à ceux des votes	Puisque le bulletin a été envoyé ^a "en clair" (non chiffré) au serveur pour obtenir l'image(tte) de confirmation, l'urne aurait tout aussi bien pu être remplie de bulletins non chiffrés; en conséquence, que les contrôleurs "soient seuls

«physiques».	à pouvoir la décrypter" n'est pas très pertinent. (a) le "canal de sécurisation entre le PC du votant et le serveur de l'Etat", pompeusement mentionné supra, ne chiffre que durant le transport entre le poste et le serveur; il est donc ouvert en arrivant dans l'ordinateur de l'État.
«Un système évolutif»	
Développé à l'origine par Hewlett-Packard,	D'après une personne bien informée, il semblerait que ce fut développé par une petite entreprise sous-traitante de H-P, créée de manière ad hoc et dissoute après.
le système d'e-voting genevois a «beaucoup évolué» depuis ses premiers essais en 2003.	D'après les descriptions dans le rapport de projet de loi (PL 9931), celles du site de l'état ou des discours récents, ou encore les interventions des responsables repris dans les derniers articles, l'architecture fondamentale du système n'a pas changé et les griefs restent les mêmes ! Donc, si la chancellerie insiste depuis fin mai pour dire que son système "a beaucoup évolué", ces éventuels changements sont manifestement négligeables face à l'irrespect des principes du vote démocratique.
Les critiques les plus virulents lui reprochaient de s'appuyer sur des partenaires privés et des solutions «propriétaires». «Dans sa version actuelle, la quasi-totalité des composants provient de l'open source», souligne le chef de projet Michel Warynski.	Ridicule ! Il y a, dans cette affirmation propagandiste, une douteuse confusion avec un ensemble de logiciels standards utilisés par la moitié des sites Web du monde, et sur lequel s'appuie le logiciel de vote. Le logiciel de vote proprement dit est en fait bel et bien entièrement secret. Voir les contributions (surtout celle du 18 juillet "eVoting - de la fumée dans l'espace public genevois") de l'article du Prof. J-D. Delley " Genève: quand la souris s'invite à l'exercice de la démocratie " de la revue <i>Domaine Public</i> .
Désormais «entièrement sous contrôle de l'Etat de Genève, aussi bien pour son développement que pour la maintenance et l'exploitation», ce système «évolutif» pourra incorporer à l'avenir l'authentification par signature électronique, «dès que ce moyen d'identification numérique sera suffisamment répandu», promet Michel Warynski.	À la suite de toutes ces déclarations promotionnelles, le souvenir irrépissable d'une ancienne chanson remonte à la surface de la mémoire : <i>Encore des mots toujours des mots les mêmes mots Rien que des mots Des mots faciles des mots fragiles (...) Des mots magiques des mots tactiques qui sonnent faux Oui, tellement faux (...) Merci, pas pour moi (...) Parole, parole, parole Parole, parole, parole Parole, parole, parole (...)</i> Dalida, 1973