Mail de M. Jean-Paul Kroepfli à Laurent Ballif le 15 octobre 2009

Vote électronique - un sujet qui devrait intéresser un politicien utilisateur historique de l'informatique ! ou l'e-Vote et le cyber-politicien-journaliste-mémorialiste.

Je suis tombé -par hasard- sur votre site. il y a quelques quarts d'heure; car le temps passe vite, ayant lu avec beaucoup de gourmandise plusieurs de vos textes.

Pour ce premier contact, afin que vous compreniez mieux la suite, je me permets d'abord de me présenter:

De formation scientifique (mathématique et informatique), j'ai été conseiller indépendant pour l'industrie (concepteur de logiciels scientifiques) dans les années huitante, puis pour les banques et les assurances (consultant en stratégie internet et pour la sécurité) dans les années nonante, et enfin la Confédération (chef de projet identité numérique) et les cantons (audit de systèmes électoraux et surtout conseiller pour le vote électronique) au début de la présente décennie.

Comme vous observez la société en tant que journaliste, agissez dessus comme politicien, réfléchissez à ses trajectoires comme historien, et j'oublie certainement d'autres qualités (mais je n'ai rien trouvé comme maître ès natations, peut-être de nous mettre dans le bain tout en nous évitant de couler au fond du bassin, ce pourrait être très pertinent dans le cas de l'e-Voting) et qu'en plus vous connaissez l'informatique depuis la protohistoire du PC, il m'a semblé que vous devriez être intéressé au vote électronique ... qui arrive aujourd'hui, pour le bien ou le mal. Pour le moment c'est en mal, comme vous le verrez ci-dessous, mais ce pourrait être mieux, et on pourra en reparler.

(*) N'étant pas beaucoup plus jeune que vous, j'ai commencé à l'Uni avec les cartes perforées, et vu apparaître la plupart des machines que vous avez décrites.

Ci-dessous, justement, vous trouverez mes commentaires de la réponse de Philippe Leuba à la récente question d'Isabelle Chevalley sur le vote électronique. Un mode de vote, et ici un système particulier, qui est en cours de reprise pour les expatriés du canton (puis très naturellement pour les résidents). La semaine passée, j'avais reçu le texte de cette réponse par un correspondant avisé; en la lisant, j'ai été choqué par toutes les inexactitudes qu'elle contient. J'ai envoyé cette analyse critique des arguments du DINT directement au chef du département, trois jours après sa réponse orale faite le 6 octobre au Grand Conseil.

Vous verrez qu'il est important de faire changer d'avis le Conseil d'État. Il n'y a qu'un bon mouvement de protestation qui pourra convaincre le département de Leuba de soit reprendre beaucoup plus sérieusement ses études, soit -au moins- de patienter longuement plutôt que de se précipiter sur une véritable souricière à bulletins.

Et, si vous êtes intéressé à aller plus loin, j'aimerais vous faire parvenir un petit tableau des caractéristiques que le droit fédéral et les principes démocratiques imposent à un vrai vote électronique, avec une analyse non technique des manquements du système que Philippe Leuba annonce vouloir reprendre pour le canton. Mais, comme la copie de ce courriel est déjà un peu longue, et j'en suis désolé, je garde ces deux autres petits textes en réserve pour le cas où vous me feriez le plaisir de les demander. Ensuite, si le sujet continue de vous concerner, nous pourrons avancer vers l'esquisse des possibilités qui s'offrent aux citoyens et au canton.

Bonne lecture et à votre disposition pour tout dialogue (je suis un voisin de la Riviéra).

Avec mes meilleures salutations.

Jean-Paul Kroepfli

Réponse de L. Ballif le 19 octobre 2009

Cher Monsieur,

J'ai parcouru rapidement les lignes que vous m'avez transmises, et je vous assure d'emblée que je suis tout aussi réservé que vous face au vote électronique. Je vais même plus loin puisque je pense qu'il n'est pas possible, si l'on veut préserver l'anonymat du votant, de concevoir un système informatique de vote qui réponde aux exigences de contrôle statistique et individuel.

Je vais vous expliquer rapidement cette première série d'arguments, qui vous sont familiers puisqu'ils concernent prioritairement l'aspect informatique de la question.

Il y a quelques années, lorsque j'ai participé à plusieurs séances du GLLA (Groupe pour les Logiciels Libres) à Lausanne, j'avais été frappé par l'hostilité déclarée de tous les fous d'informatiques qui le fréquentaient face au vote électronique. Comme il s'agissait de gens qui prônaient l'usage des logiciels libres, j'avais imaginé qu'ils seraient les mieux à même de définir le cahier des charges d'un tel système avec une option citoyenne.

Eh bien, tous m'ont affirmé qu'il n'y avait pas de possibilité de réaliser un logiciel qui réponde à tous les critères suivants:

- contrôle de la corrélation exacte entre les votants et les votes effectivement enregistrés
- possibilité de recomptage en cas d'incertitude
- possibilité de vérifier statistiquement la corrélation entre l'avis d'une population donnée et le résultat de ses votes (ce qu'on appelle souvent les "quartiers témoins")
- traçabilité d'un vote individuel si nécessaire
- anonymat du vote comme situation de base

Il y a certainement d'autres critères encore, qui confirmeraient l'impossibilité de réaliser un tel logiciel. On constate déjà ce problème avec les machines à voter américaines, qui n'avaient pas, dans leur première version, de comptabilisation des votes entrés.

Par ailleurs, si l'on prend ces machines à voter comme le "modèle" de ce que pourrait être le vote électronique, on se rend immédiatement compte que, même si nous utilisons un logiciel libre dont le code est parfaitement transparent et la procédure contrôlable, nous n'avons aucune possibilité de déceler dans le résultat l'effet d'une possible intervention pirate extérieure. Avec un bulletin papier, il est toujours possible de revenir vers l'objet et de contrôler l'écriture, l'encre, le papier, etc., avec un + ou un - électronique, c'est impossible.

Et l'argument massue de ces hackers, cela a été de dire: Si un groupe de pression est prêt à mettre 1 million, voire plus, pour une campagne d'affichage tendancieuse, pour faire du lobbying diffamatoire, pour mouiller des adversaires politiques, ne trouvera-t-il pas plus économique de donner 200'000 francs à un pirate pour qu'il trouve le moyen de craquer le système de vote ? Tous ont affirmé qu'il n'y avait pas de système inviolable, et que les pires systèmes étaient ceux où l'on ne pouvait pas remonter à la source du vote, ce qui est la définition de la machine à voter.

Dans ces conditions, et pour ces seules raisons, je me sens déjà fondé à ne pas souscrire au vote électronique.

Mais il y a également un autre volet, plus philosophique, qui compte tout autant pour moi. Il s'agit de l'importance que l'on donne à l'acte de voter. On a déjà vu que la généralisation du vote par correspondance a obligé les partis à avancer notablement le début des campagnes. Aujourd'hui, avec l'enveloppe de vote qui arrive dans les ménages 4 semaines avant la date

de la votation, les partis doivent prendre des positions 8 semaines avant le vote au moins et diffuser leurs positions au minimum 6 semaines avant cette date.

Même si vous n'êtes pas un politicien dans l'âme et avez l'impression que le rôle des partis est secondaire, il faut que vous compreniez que leur rôle défini par la Constitution, tant fédérale que cantonale, est de structurer la population et de servir de porte-voix pour les groupes de votants. Ils jouent également un rôle essentiel pour la création des lois et la constitution des parlements, donc ils doivent avoir une démarche didactique et expliquer les enjeux. Même si l'on considère que certains font du populisme ou mentent, il n'empêche que tous permettent aux électeurs de se positionner face à une question.

Aujourd'hui déjà, il y a des gens qui votent par retour du courrier et qui ne tiennent pas compte du débat politique ouvert à l'occasion des votations. Pour certains, c'est parce qu'ils connaissent bien le sujet et ont pu se faire un avis. Mais pour beaucoup d'autres, c'est une démarche hâtive qui ne prend pas en compte l'entier du problème, voire qui ne discerne pas réellement les enjeux pour différents groupes de population.

Avec cet éloignement progressif entre le votant et le formateur d'opinion (le parti), on se prépare à une dérive similaire à la "peoplisation" de la politique. Les gens ne sont déjà plus guère capables de faire la différence entre un sondage, une enquête, une pétition et une initiative ou un référendum. La machine médiatique a donné l'impression que tout le monde pouvait avoir raison sur tout, que le fait de dire "Oui je trouve qu'on paie trop d'impôt" équivalait à dire "Je vote pour les gens qui ont l'intention de baisser les impôts sans savoir par quelle baisse de prestations cela va se traduire".

On le voit avec le "sondage" quotidien de 24 Heures, qui est vraiment une guignolade sans nom. En tant que politicien, on reçoit régulièrement des infos du genre: Actuellement, sur ce sujet, c'est telle opinion qui prédomine, alors il faudrait que vous alliez faire quelques clics dans un autre sens pour corriger la donne". Et tout le monde fait pareil. Après quoi, le lendemain, les "journalistes" nous expliquent doctement que 57% des Vaudois estiment que ceci ou cela. Et les gens finissent par croire qu'ils ont voté cela, et que les gouvernants vont le mettre en oeuvre.

On perd de vue totalement les notions de droit de vote, d'unicité du vote, de territoire votant, de représentativité (d'un échantillon ou d'un thème), de formulation des questions. La population sciemment aliénée (c'est ma formation de politologue qui ressort, c'est un mot qu'on utilisait beaucoup en 1968 mais qui n'est malheureusement plus du tout compris aujourd'hui) mélange ainsi tout et n'importe quoi.

En résumé, je crains infiniment, et même de manière panique, que le vote électronique soit perçu par la population exactement de la même manière que le sondage de 24 Heures, et qu'il perde ainsi toute sa majesté constitutionnelle. Je ne fais pas de l'emphase pour le plaisir en disant cela, mais c'est réellement ma principale hostilité face au vote électronique.

J'espère ne pas vous avoir ennuyé avec ce plaidoyer contre le vote électronique, mais c'était également pour moi une bonne occasion de mettre par écrit des sentiments que je n'ai pas encore eu l'occasion d'exprimer en séance politique. Je sais d'ailleurs que, si je m'exprime ainsi, je passerai pour un vieux con ringard, mais j'ai l'habitude... !

Meilleures salutations.

L. Ballif

Réponses circonstanciées de Jean-Paul Kroepfli aux objections de L. Ballif

Je vais même plus loin puisque je pense qu'il n'est pas possible, si l'on veut préserver l'anonymat du votant, de concevoir un système informatique de vote qui réponde aux exigences de contrôle statistique et individuel.

Réponse: En fait OUI, c'est possible; mais tout différemment de ce qui c'est fait.

[...] Mais il y a également un autre volet, plus philosophique, qui compte tout autant pour moi. Il s'agit de l'importance que l'on donne à l'acte de voter.

Réponse: Pas de problème, il est possible d'avoir le même sens, et de manière toute individuelle, avec le débat toujours possible.

Bonjour Cher Monsieur,

Voilà, je reviens vers vous à propos de votre aimable réponse du 19 octobre.

Je vous donne ici une réponse succincte du premier point, je reviendrai pour le second dans un autre message.

Pour ce premier point, il faut faire du vote électronique un vrai vote démocratique, c'est-à-dire représentant sans ambiguïté le choix de l'électorat et protégeant la liberté du votant; il faut à la fois magnifier le bulletin et sa traçabilité, mais aussi absolument découpler celui-ci de l'identité du votant, en donnant à ce dernier le plein pouvoir sur son vote. Enfin, le contrôle politique doit être total, y compris durant le scrutin.

On y arrive, en utilisant les architectures sécuritaires et les techniques cryptographiques. En fait, il s'agit aussi de pensée latérale et de bon sens (ou, autrement dit, de créativité et d'ouverture d'esprit).

En simplifiant beaucoup, ici il s'agit premièrement de rendre le bulletin totalement représentatif du contenu, des motivations et de son origine, et de le rendre infalsifiable et d'origine contrôlée, secondement de lier le bulletin, par lui-même, avec la qualité d'électeur du citoyen, mais pas avec l'identité de celui-ci. La première condition s'obtient (essentiellement) avec un sceau cryptographique sur un bulletin textuellement complet, la seconde en plaçant l'élaboration de ce sceau du côté du citoyen, qui dissocie la qualité de l'identité.

Les bulletins étant vérifiables comme authentiques et intègres, ils peuvent être valablement recomptés; ils ne peuvent par contre pas être reliés aux électeurs individuels.

Pour assurer la vérité de l'opération, ainsi que sa transparence dynamique, il n'y a pas que l'administration (les serveurs la représentant) en face de l'électeur, mais aussi le contrôle politique (les serveurs ~). Donc un protocole en triangle, où chaque partie peut vérifier que les deux autres opèrent loyalement. Pour maintenir le secret, il y a partition stricte de l'information: l'administration qui habilite l'électeur le connaît nominalement, mais ne reçoit pas directement son bulletin; le représentant politique qui scrute le processus reçoit le bulletin (comme intermédiaire) mais n'a qu'une relation anonyme (mais qualifiée) avec l'électeur. Le poste du citoyen est en clef de voûte et constate la bonne fin de l'opération individuelle.

Ceci sans entrer plus dans les détails, car il y a beaucoup de couches et d'opérations imbriquées pour parer aux fraudes potentielles des uns et des autres, ainsi qu'aux attaques externes, et apporter les éléments probants en cas de contestations tout en garantissant inconditionnellement le secret.

Nota Bene: sous le capot du processeur opère la cuisine technologique, qui brasse et rôtit les bits, mais pour le citoyen c'est une métaphore exacte et compréhensible qui est présentée.

A un niveau plus élevé, je vous ai mis ci-dessous un tableau des dix critères que doivent respecter tous systèmes de vote acceptables démocratiquement (donc aussi, mais pas uniquement, les votes électroniques). Ces critères sont basés sur le droit fédéral et les principes reconnus. Les références à la loi et jurisprudence helvétiques sont chaque fois données en lien.

Les informaticiens de l'Etat sont classiquement de gestion administrative, ils n'ont pas les spécialités requises pour un (vrai) système de vote électronique, nettement orienté hautes technologies scientifiques. Par ailleurs, l'informatique de gestion administrative est essentiellement basée sur le paradigme d'un client pauvre qui passe des ordres de transactions simples à un serveur muni d'une logique métier et accédant à une ou plusieurs bases de données volumineuses. Ici, ce n'est pas du tout ce schéma binaire "consommateur passif et fournisseur de service", mais coopèrent plusieurs nœuds de traitement; et le (poste du) citoyen est l'un d'eux, en tant qu'électeur républicain détenteur de droits responsables.

Sans entrer dans l'aspect technique, je vous aussi joint, toujours ci-dessous, un petit texte relevant les principales inadéquations (graves) des trois systèmes de vote électroniques actuellement proposés aux cantons.

Déjà pour votre premier point, je suis à votre disposition pour poursuivre cet intéressant et précieux dialogue, ou répondre à vos questions. En parallèle, je poursuivrai dans un autre message à propos de votre seconde et juste remarque.

En vous remerciant encore de votre intérêt sur ce sujet.

Bonne lecture et avec mes cordiales salutations.

Jean-Paul Kroepfli

Les dix critères minimaux à remplir pour un mode de votation démocratique actuel

N°	Principe	Critère		Bases dans le droit suisse
1.	Une et une seule voix pour tout citoyen ayant le droit de vote (universalité et unicité).	**justesse**		Universalité: CF art.136 al.2 part. LDP art.8a al.2 part., ODP art. 27d al.1a & 1b Unicité : ODP art.27f al.4, ODP art. 27j
2.	L'anonymat du votant et la confidentialité de son bulletin sont garantis inconditionnellement.	**secret**		Anonymat: ODP art 27f al.1 & 2, ODP art.27g al.1 & 4, ODP art.27h al.2 Confidentialité: LDP art.5 al.7, (anticipé:LDP art.7 al.4, correspondance:LDP art.8 al.1), LDP art.8a al.2, ODP art.27d al.1d, ODP art.27f al.3, ODP art.27g al.1

3.	Le bulletin doit contenir la motivation du votant.	**conformité**		CF art.34 al.2, ODP art. 27e al.7, ATF 121 I 187
4.	Le votant de ne doit pas pouvoir voter par procuration, ni obtenir une preuve lui permettant de vendre son vote.	**incessibilité**		Non procuration : ODP art.27a al.4 Non vente : ODP art.27h al.4 sec.part. (assimilé)
5.	Le contenu du bulletin ne peut être connu avant la clôture du scrutin.	**temporalité**		ODP art.27f al.5, ODP art.27m al.2 (inverse)
6.	L'urne ne doit contenir que et doit contenir tous les bulletins recueillis (fidélité et exhaustivité).	**exactitude**		Fidélité: CF art.34 al.2note Exhaustivité: LDP art.8a al.2 part., ODP art. 27d al.1e, Préservation: ODP art.27k)
7.	Les bulletins doivent pouvoir être recomptés sensément (vérifiabilité de leur authenticité et de leur intégrité).	**recomptabilité**		ATF 114 Ia 42note, ATF 131 I 442, ODP art. 27n
8.	Les réclamations (avant clôture) et contestations (après) doivent être résolvables sans ambiguïté.	**prouvabilité**		ODP art. 27nbis
9.	L'ensemble de la session, ainsi que chaque vote, doit pouvoir être surveillée.	**transparence**		... note1, note2
10.	Toute tentative de fraude est empêchée, ou détectée sans délai.	**sécurité**		ODP art. 27d al.1c & al.1f

Note : CF = Constitution Fédérale, LDP = Loi fédérale sur les Droits Politiques, ODP = Ordonnance sur les Droits Politiques (Etat 1 janvier 2008); ATF = Arrêt du Tribunal Fédéral.

Ces critères sont commentés dans ce document.

Quelques exemples succincts et non exhaustifs de dérive concrète des pilotes de vote électronique par rapport aux exigences démocratiques.

Dans les pilotes genevois et zurichois, le bulletin contenant les choix de l'électeur est envoyé -lors d'une étape intermédiaire- non-chiffré, donc avec ses choix lisibles, au serveur pour générer la page de confirmation contenant les imagettes pour le premier ou le filigrane pour le second (pour mémoire, le code des imagettes, le motif du filigrane, dépend de l'électeur, et confirme la qualité du serveur). En conséquence, l'administration est en possession du résultat des votes électronique avant la clôture du scrutin, **ce qui rompt le principe de temporalité !**

Dans les trois pilotes, les systèmes informatiques sur le chemin des bulletins peuvent collecter (et en fait collectent pour leur bonne administration et pour l'analyse des tentatives

d'attaques) les données en transit. Il s'agit des routeurs, des garde-barrières (ou pare-feu), des serveurs frontaux (web) ou de transaction, des bases de données (urnes), qui journalisent très canoniquement leurs opérations. Or, l'identification de l'électeur et le dépôt du bulletin (chiffré) se font dans la même session, c'est-à-dire que le bulletin déposé est lié à l'identité de l'électeur. Après l'ouverture de l'urne, le déchiffrement donne les choix en clair. Ces choix déchiffrés sont donc, via la version chiffrée, reliables très simplement au citoyen, **ce qui rompt le principe du secret du vote (anonymat et confidentialité) !**

NB1: Ce lien entre le bulletin déposé et l'électeur existe même dans le cas des cantons identifiant les électeurs avec un numéro, porté avec le nom et l'adresse sur la carte de vote (p.ex. GE); car la liste reliant le numéro d'identification avec l'identité nominale doit être conservée jusqu'à la fin du délai de recours, puisqu'elle est nécessaire pour résoudre les réclamations et les contestations. P.ex. pour fournir une nouvelle liasse à un citoyen arguant avoir perdu son matériel de vote, il faut s'assurer que celui-ci n'a pas déjà voté électroniquement (nom->numéro->à voté); il en est de même en cas de fraude, p.ex. double vote, pour annuler le(s) bulletin(s) surnuméraire(s) et contacter le fraudeur, etc.

NB 2: L'urne électronique ne peut être "brassée", un ordinateur étant une machine déterministe (dite de Turing), il ne peut générer de hasard. Le brassage n'est qu'une permutation calculatoire de l'ordre, qui est toujours inversable (annulable). Par ailleurs, l'état antérieur de l'urne peut avoir été sauvegardé, et -avec la base de données de l'urne-, l'opération de permutation ou de lecture permutée est journalisée.

En outre, les journaux systèmes et serveurs -voir ci-dessus- gardent déjà le lien entre bulletin et votant.

Dans les deux pilotes "maisons" (GE & ZH), les bulletins enregistrés ne sont que la collecte des choix (oui/non/blanc), et ne portent aucun sceau d'intégrité ni d'authenticité (pas de métadonnée). Les bulletins peuvent donc avoir été modifiés ou remplacés sans laisser de trace. De plus, ils ne sont donc pas recomptables sensément (vérification non probante). **Ceci rompt les principes de conformité et d'exactitude !**

Les systèmes pilotes ayant été construits selon le paradigme de l'informatique administrative (clients passant des transactions à un serveur effectuant des mutations sur une base de données), le processus est une boîte noire, dont les opérations ne peuvent être valablement observées par une commission électorale. **Ceci rompt le principe de transparence, soit de scrutation populaire !**

Note: Par ailleurs, aucun des trois systèmes ne permet la consultation publique et libre de son texte source, ou de ses documents techniques.

Les systèmes confirment la réception du bulletin, mais il ne s'agit pas d'un accusé de réception à valeur probante; il n'est pas non plus possible de s'assurer qu'une personne a bien voté au sens que son propre bulletin est bien dans l'urne et qu'il sera/a été bien pris en compte dans le dépouillement. **Ce qui rompt le principe de prouvabilité !**

NB 1: Le récépissé (lié indirectement, mais fortement, au contenu) ne doit pas être probant face à un tiers, car il ne doit pas fournir preuve (des choix) en cas de vente du vote.

NB 2: Dans le vote papier (sp. au local), la garantie de bonne fin est induite par la scrutation constante du processus.

Je ne rentrerai pas dans le détail (documentés), mais les pilotes -surtout GE et ZH- sont très vulnérables à une attaque du poste de l'électeur; il est possible de falsifier (en quelques jours d'extension) aux alentours de la moitié des votes. Il n'y a donc pas une **sécurité** suffisante.

NB: En particulier, le système genevois -proposé pour le canton de Vaud- est potentiellement vulnérable à une gamme impressionnante d'attaques très graves envers les systèmes serveurs, tant internes (au sein de l'administration publique), qu'externes -depuis l'Internet.