Audition de Chantal Enguehard
Maître de conférences en informatique à l'Université de Nantes
Laboratoire des Sciences du Numérique de Nantes (UMR CNRS 6004)

Jeudi 25 janvier 2018 à 14 h 30
au Sénat
Palais du Luxembourg
15, rue de Vaugirard
75006 Paris

par Mme Jacky Deromedi et M. Yves Détraigne
Rapporteurs de la mission d'information de la commission des lois du Sénat
consacrée au vote électronique

Deux concepts clés

Une élection réussie

Nous croyons savoir ce qu'est une élection alors qu'il s'agit d'un dispositif très original et, nous le verrons plus tard, résistant à la numérisation. Nous connaissons le but d'une élection : désigner un candidat comme représentant des électeurs en fonction du nombre de suffrages qu'il a recueilli. En revanche, nous savons moins ce qu'est une élection réussie.

Une élection permet de prendre une décision controversée en un temps limité tout en évitant les ***désordres publics****. Imaginons que nous devions choisir le prochain président de la République sans élection : il y aurait beaucoup de discussions et il n'est pas garanti qu'un accord soit trouvé dans un temps raisonnable. Une élection peut être qualifiée de réussie si les partisans des candidats perdants* ***acceptent la défaite*** *sans provoquer de désordres publics (tels des manifestations ou, pire, des émeutes). Une élection peut donc aussi être considérée comme un dispositif de maintien de la paix publique.*

Un processus électoral sécurisé

La sécurité repose sur deux aspects : la sûreté et la fiabilité. La ***sûreté*** *englobe l'ensemble des moyens matériels, humains, organisationnels visant à* ***éviter ou contrer toute action malveillante****. Le niveau de sûreté est total si aucune attaque ne peut réussir. La* ***fiabilité*** *désigne la capacité d'un système à* ***fonctionner sans produire d'erreur et sans se bloquer****. Le niveau de fiabilité est total si aucun dysfonctionnement ne peut survenir.*

Propriétés d'une élection avec urnes transparentes

Intéressons-nous maintenant à quelques-unes des propriétés que vérifie une élection organisée avec des urnes transparentes.

Le secret du vote. *Chaque électeur doit pouvoir exprimer son choix librement, sans subir de pressions de son entourage (famille, collègues, amis, etc.). Il doit donc pouvoir voter de manière confidentielle et être certain que son choix va bien rester secret. Le passage obligatoire dans*

l'isoloir et l'usage d'une enveloppe pour dissimuler le bulletin choisi sont des dispositifs qui protègent le secret du vote.

L'électeur ne doit pas non plus pouvoir constituer une preuve de la nature de son vote qui l'exposerait à des pressions ou lui permettrait de vendre son vote. Dans un bureau de vote, si un électeur voulait se filmer en continu depuis la mise sous enveloppe du bulletin qu'il a choisi jusqu'au dépôt dans l'urne, constituant ainsi une preuve de son vote qu'il pourrait montrer à un tiers, un membre du bureau de vote l'en empêcherait.

Unicité. *L'unicité du vote s'exprime souvent par la formule : « un électeur, une voix ». Dans les bureaux de vote, son respect est assuré par la tenue d'un cahier d'émargements que les électeurs signent après avoir voté.*

Sincérité. *Ce terme juridique désigne le fait qu'une élection est juste au sens où les candidats sélectionnés sont bien les candidats majoritairement choisis par les électeurs. Une fraude comme un bourrage d'urnes est une atteinte à la sincérité de l'élection.*

Transparence. *Les électeurs ayant voté pour un candidat perdant doivent avoir confiance dans le système de vote pour admettre la défaite. Cette confiance est fondée sur l'observation du scrutin pendant que celui-ci se déroule. Les délégués des candidats et les électeurs peuvent, par exemple, constater que l'urne est vide au début de l'élection. Tout au long de la journée, ils peuvent vérifier que les bulletins ajoutés le sont de manière licite, constater que l'urne n'est pas dissimulée ou emmenée en dehors du bureau de vote, remarquer si des électeurs subissent des pressions ou encore si des personnes font campagne dans le bureau de vote, etc. Ces observations sont directes : elles procèdent directement des sens des observateurs sans passer par une personne tierce où un dispositif technique intermédiaire (caméra, logiciel, etc.). Le dépouillement est effectué en fin de journée par des électeurs, sous le contrôle des membres du bureau de vote.*

Lorsque certaines de ces règles ne sont pas respectées, les personnes présentes peuvent faire inscrire leurs observations sur le procès-verbal du bureau de vote. En cas de contentieux électoral, le juge pourra s'appuyer sur ces procès-verbaux pour éventuellement faire annuler l'élection.

Persistance des bulletins. *Tous les bulletins utilisés pour porter les choix des électeurs sont inertes au sens où ils ne sont jamais modifiés entre le moment où ils sont choisis, mis sous enveloppe, placés dans l'urne et, enfin, décomptés. Évidemment, il faut que l'urne ait été correctement surveillée pour que son contenu ne soit pas modifié (bourrage d'urne ou substitution d'urnes).*

Le vote électronique

Les machines à voter ainsi que le vote par Internet sont fondés sur un modèle de boîte noire : les électeurs votent durant la période électorale et le dispositif énonce des résultats à la fin de cette période. Examinons, par comparaison, quelques propriétés de ces dispositifs de vote.

Opacité. *Les machines à voter et le vote par Internet ont un point commun :* ***tous les votes des électeurs, sans aucune exception, sont modifiés à plusieurs reprises****. En effet, chaque électeur fait son choix en appuyant sur un bouton, en désignant une zone sur un écran ou encore en cliquant à l'aide d'une souris. Ce geste est converti en une impulsion électrique, cette impulsion est ensuite convertie en une information de quelques bits. Cette information passe elle-même par d'autres transformations avant d'être agrégée. Et, en fin de période électorale, le dispositif énonce un*

résultat. Ces transformations sont effectuées au niveau électronique et ne sont pas directement observables.

Les systèmes de vote électroniques sont donc des systèmes opaques. Ils peuvent donc transformer un vote pour un candidat en un vote pour un autre candidat sans que ces modifications puissent être vues. Une autre conséquence importante est que, ***si la sincérité de l'élection a pu être compromise, il est impossible de présenter à un juge des témoignages ou des observations qui lui permettraient d'annuler l'élection.***

Résultats non vérifiables. *En 2017, la plupart des personnes sont familiarisées avec des dispositifs électroniques (ordinateur, tablette ou téléphones) et constatent que leur bon fonctionnement n'est pas toujours garanti : des dysfonctionnements apparaissent parfois, puis disparaissent sans que les utilisateurs sachent vraiment pourquoi. Il y a d'ailleurs de fréquentes mises à jour des applications qu'ils utilisent.*

Avec le vote électronique, chaque vote étant transformé à plusieurs reprises, il est légitime de se demander si les choix exprimés par les électeurs sont bien conservés. Autrement dit, est-il possible de savoir si les résultats énoncés par le dispositif de vote sont sincères ? Plusieurs propositions ont été émises pour évaluer a posteriori la sincérité d'un vote.

L'impossible preuve de la sincérité du vote électronique

Comment s'assurer que le vote électronique respecte le choix fait par les électeurs ?

Comparer les résultats à des sondages pré-électoraux ou sortis des urnes

Lorsqu'une élection se déroule avec des urnes transparentes, son résultat constitue la référence. La qualité de prédiction d'un sondage est d'ailleurs évaluée par rapport à cette référence. Vérifier le résultat d'une élection par rapport à un sondage renverse la situation : le sondage devient la référence. Dans ce cas, le processus électoral devient inutile : il suffirait de faire des sondages. Or, les sondages ne vérifient pas les propriétés des élections : ils ne portent que sur une partie de l'électorat, sont réalisés sans confidentialité, ne respectent pas l'unicité, sont sujets à des biais dans les réponses apportées, etc. Cette proposition ne peut donc pas être retenue.

Procéder à des tests du logiciel

Les tests sont toujours limités. Il n'existe pas de test ni d'expertise qui soient exhaustifs et permettent de trouver tous les bugs éventuels (si ces techniques existaient, elles seraient aussi mises en œuvre sur les applications utilisées au quotidien). De plus, qui dit élections, dit fraude possible, et cette éventualité ne peut être *a priori* écartée. Une fraude logicielle peut être volontairement dissimulée et donc bien plus difficile à trouver qu'un simple bug.

Prouver que le programme informatique est valide

Il est possible de prouver mathématiquement qu'un programme fait exactement ce que son auteur veut qu'il fasse. Cette branche de l'informatique se nomme la « preuve de programme ». Mais cette approche a des limites. La preuve est effectuée sur une version du programme qui est ensuite traitée par un ou plusieurs programmes de post-traitement (un « compilateur » ou un « interpréteur ») pour devenir exécutable sur un ordinateur. Pour être certain du fonctionnement d'un programme, il faudrait également prouver ce programme de post-traitement. De plus, il n'existe pas de moyen de savoir si le programme qui est utilisé dans un ordinateur est bien exactement le même que celui qui a été prouvé. Enfin, il faut que le programme, une fois prouvé, reste absolument inchangé, la moindre modification (mise à jour, branchement d'une imprimante, ajout d'un dispositif audio pour les aveugles…) nécessitant de ré-effectuer la preuve. De plus, dans le cas du vote par internet, les ordinateurs utilisés par les électeurs sont hors de portée de tout examen. Or, ils sont susceptibles d'héberger des virus modifiant le vote saisi par un électeur. Et même pour un programme prouvé, une erreur d'exécution peut se produire. C'est ce qui est arrivé en 2003 à Schaerbeek (Belgique). Il a été décompté 4 096 voix supplémentaires par rapport au nombre d'inscrits. Le rapport d'experts a attribué cette erreur à *« l'inversion spontanée d'une position binaire dans la mémoire de l'ordinateur »*.

Analyser les traces informatiques d'exécution

Il est possible de suivre pas à pas les transformations que subissent les votes et de les noter dans un fichier appelé « trace d'exécution ». La consultation de ce fichier permettrait de constater si le sens de chaque vote est conservé, depuis sa réception jusqu'à l'agrégation finale.

Prenons le cas d'une élection à deux candidats : *Ubu* et *Shadock*. Si la trace d'exécution conserve l'ordre des votes, il est possible de savoir quel est le sens du vote de chaque électeur (le premier électeur a voté pour *Shadock*, le second pour *Ubu*, etc.), violant ainsi le secret du vote. Si la trace d'exécution ne conserve pas l'ordre des votes, **des modifications intervenant entre l'expression du vote et la réception de ce vote par le dispositif ne peuvent être détectées**. En effet, dans la trace d'exécution, il y aura plusieurs exemplaires de traces montrant que les votes pour *Shadock* ont conservé leur sens, ainsi que les votes pour *Ubu*, mais impossible de savoir, si chaque vote a bien été réceptionné conformément à l'expression de l'électeur. Ajouter une information permettant de relier chaque vote à son électeur (l'heure de réception, par exemple) ne constitue pas une solution car, à nouveau, le secret du vote serait violé.

Le bon fonctionnement d'un système de vote électronique ne peut donc pas être établi. Or, il n'est pas nécessaire de modifier un grand nombre de voix pour violer la sincérité d'une l'élection. L'observation des duels de candidats lors des quatre dernières élections législatives a permis de mesurer que détourner 5 % des voix au profit d'un candidat suffit pour changer l'issue du scrutin pour un quart des élections [Enguehard 2013]. Il est peu probable qu'un si faible détournement attire l'attention.

Donc, même si un système était absolument sécurisé, c'est-à-dire sans bug et totalement protégé (rappelons que cette hypothèse est peu réaliste), il serait impossible d'en apporter la preuve aux électeurs et donc de les convaincre de cette sécurité. Ce détail a son importance : puisqu'il n'existe aucun argument pour convaincre les électeurs, ceux-ci sont sommés d'accorder une confiance aveugle au dispositif de vote et d'accepter les résultats comme sincères, quels qu'ils soient. Le vote électronique s'appuie donc sur ***la foi****, et non sur* ***la raison****.*

Liberté de vote amoindrie dans le cas du vote par internet. *Pour voter en toute liberté, un électeur doit être protégé de toutes les formes de pressions.*

Deux conditions doivent être réunies pour assurer cette protection :

1 – l'électeur a la conviction que son vote reste secret.

Lors d'un vote par internet l'électeur fournit à la fois son identité et son choix à l'application informatique de recueil des votes. L'électeur peut alors légitimement douter du respect du secret de son choix.

En cas de doute, il peut décider de modifier le choix qu'il aurait exprimé s'il avait été convaincu que son vote resterait secret, et choisir finalement un candidat plus consensuel, plus conforme à la volonté des tiers dont il subit la pression, ou encore faire choix du vote "Blanc".

2 – l'électeur ne peut pas constituer de preuve de vote.

Une preuve de vote est un enregistrement permettant à un électeur de prouver à une tierce personne le sens de son vote.

Pour constituer une preuve de vote dans un bureau de vote avec une urne transparente, il faudrait par exemple qu'un électeur se filme en continu depuis le moment où il choisit le bulletin de vote et le glisse dans l'enveloppe (alors qu'il est dans l'isoloir) jusqu'au moment où il dépose publiquement cette enveloppe dans l'urne. Se filmer dans l'isoloir est aisé mais, lorsque l'électeur continuera de se filmer en sortant de l'isoloir jusqu'à déposer son enveloppe dans l'urne, le bureau

de vote chargé de veiller au respect de la confidentialité obligera l'électeur à arrêter de filmer et à recommencer les opérations électorales.

Dans un bureau de vote muni d'une machine à voter un électeur peut de manière similaire constituer une preuve de vote en se filmant en continu depuis le choix d'un candidat jusqu'à la confirmation de son vote. Comme ces opérations se déroulent à l'abri des regards (devant la machine à voter qui fait aussi office d'isoloir), le bureau de vote ne peut intervenir. Une preuve d'un vote en faveur de Ségolène Royal avait été publiée en 2007.

De même , lors d'un vote par internet, l'électeur peut se filmer en continu depuis son choix jusqu'à l'envoi de son vote au serveur de vote. De plus, si le vote ne se déroule pas dans un bureau de vote, il peut voter en présence (et éventuellement sous la pression) de tiers.

Promesse de sécurité et opacité

La promesse de sécurité est-elle en mesure de compenser l'absence de transparence ? Il faut distinguer quatre cas selon que le système de vote est sécurisé d'une part, et transparent d'autre part :

1. Sécurisé et transparent : les élections sont réussies.

2. Sécurisé et opaque : lors d'un scrutin serré et à fort enjeu, il est possible que des électeurs insatisfaits du résultat et doutant de la sincérité des élections manifestent leur mécontentement par des désordres publics.

3. Non sécurisé et transparent : les atteintes à la sincérité peuvent d'autant plus être observées qu'elles portent sur un nombre important de voix. Les observations et témoignages peuvent être portés devant le juge qui peut éventuellement annuler l'élection. Cette configuration correspond aux scrutins se déroulant dans des bureaux de vote équipés d'urnes transparentes.

4. Non sécurisé et opaque : la sincérité de l'élection peut être violée sans que cette atteinte ne soit constatée et sans que l'élection ne soit annulée. Cette configuration correspond aux systèmes de vote électronique déployés en France.

Ainsi, la sécurité et la transparence sont deux propriétés indépendantes, la transparence étant indispensable à tout mode de scrutin. Avec le vote électronique, la disparition de la transparence est avérée, ce qui amoindrit la confiance des électeurs dans le système électoral. Il est évidemment toujours souhaitable d'améliorer la sécurité mais, en aucun cas, l'amélioration de la sécurité ne peut compenser la disparition de la transparence.

Or, le ministère de l'intérieur poursuit l'expérimentation des machines à voter en l'absence de tout protocole d'évaluation et malgré les multiples analyses scientifiques. Ainsi, il a pu être observé qu'en moyenne, l'unicité est bien moins respectée dans les bureaux de vote avec machines à voter [Enguehard 2014], ou encore que des électeurs ne parviennent pas à voter comme ils le souhaitent sur des dispositifs proches de ceux utilisés en France [Conrad 2009]. De même, le Ministère des affaires étrangères maintient le vote par Internet alors qu'une ***preuve de possibilité de fraude*** *a été rendue publique [Grégoire 2012]... Interrogé lors d'une audition à l'Assemblée Nationale en janvier 2017, le directeur général de la très sérieuse Agence nationale de la sécurité des systèmes d'information (ANSSI) a indiqué ne pas être en faveur du vote électronique [Berne 2017].*

Systèmes de vote électronique dits vérifiables

La transparence étant définitivement perdue avec le vote électronique, les travaux de recherche se sont orientés vers la conception de systèmes de vote dont il serait possible de déterminer s'ils ont bien fonctionné. Il s'agit du modèle E2E (« end to end verifiable and auditable »). La vérification s'appuie sur deux points de contrôle que nous présentons ci-dessous (cas d'une machine à voter).

1. Vérification individuelle : l'électeur vérifie que son vote est bien enregistré. Lorsque l'électeur choisit un candidat, la machine imprime un papier sur lequel ce choix est indiqué. L'électeur peut voir ce papier. Il valide son vote si son choix est bien noté et le bulletin est alors acheminé vers une urne. Dans le cas contraire, il peut annuler son vote et revoter.

2. Vérification universelle : Eventuellement, les bulletins de l'urne sont comptés pour vérifier si les résultats préalablement énoncés par la machine sont justes. Ce modèle peut être décliné pour le vote par Internet. La vérification, plus complexe, est alors fondée sur la cryptographie

Plusieurs points de ce modèle ne fonctionnent pas car le modèle ne prend pas en compte le caractère juridique d'une élection : un juge peut annuler une élection, pas un informaticien. Par manque de place, nous en détaillons un seul. [Enguehard 2013] est un article entièrement consacré à ce sujet.

Un électeur constatant que son vote a été modifié lors de la vérification individuelle (« j'ai voté Ubu mais il est écrit Shadok sur le papier ») ne peut apporter la preuve de cette modification sauf à se filmer en train de voter. Dans ce cas, il constitue une preuve de vote, ce qui n'est pas souhaitable. Donc, un électeur constatant que le dispositif de vote ne fonctionne pas bien ne peut faire mettre ce dispositif hors-service. Or, un dispositif changeant une proportion raisonnable de voix (par exemple, une voix sur 10) pourrait passer inaperçu car l'étape de la vérification individuelle est optionnelle (les expérimentations en la matière ont montré que peu d'électeurs l'effectuent [Sofie 2012]).

Le dispositif peut aussi favoriser l'apparition de rumeurs ; des électeurs pourraient prétendre avoir vu que leur vote a été modifié alors même que ce n'est pas vrai.

Conclusion

La confiance dans le système électoral est une condition indispensable à la tenue et à la réussite d'élections démocratique.

Toutes les formes de vote électronique que nous avons étudiées sont opaques et fournissent des résultats électoraux dont il est impossible de déterminer s'ils sont sincères. C'est pourquoi le vote électronique contribue à diminuer la confiance des électeurs dans le système électoral.

Références

[Berne 2017] Berne, Xavier., Le numéro un de l'ANSSI défavorable au vote électronique : NextINPACT, 18 janvier 2017.

[Conrad 2009] Frederick G. Conrad, Frederick G. Benjamin B. Bederson, Benjamin B..Brian Lewis, Brian.,Emilia Peytcheva, Emilia. Michael W. Traugott, Michael W.. Michael J. Hanmer, Michael J. Paul S. Herrnson, Paul S. Richard G. Niemi, Richard G. "Electronic voting eliminates

hanging chads but introduces new usability challenges" Pages 111-124, International Journal of Human-Computer Studies, Volume 67, Issue 1, Pages 1-124. January 2009.

[Enguehard 2013] Enguehard , Chantal. Les dispositifs de vote électronique dits vérifiables. In : Retour(s) sur le vote électronique, Institut d'Etudes Politiques de Grenoble, 30 octobre 2013.

[Enguehard 2014] Enguehard, Chantal. Graton, Jean.-Didier. Machines à voter et élections politiques en France : étude quantitative de la précision des bureaux de vote. Cahiers Droit Sciences et Technologie, n°4, p.159-198, Presses Universitaires d'Aix-Marseille, 2014.

[Grégoire 2012] Grégoire L., « Comment mon ordinateur a voté à ma place (et à mon insu) », 27 mai 2012, fr.scribd.com/document/94990325/Comment-mon-ordinateur-a-vote-a-ma-place-et-a-mon-insu

[Sofie 2012] Sofie I., Stenerud G., Bull C., "When Reality Comes Knocking Norwegian Experiences with Verifiable Electronic Voting", EVOTE 2012.