# Vote électronique

Véronique Cortier [1, 2]

De nombreux actes de la vie citoyenne sont désormais dématérialisés ou en passe de l'être : déclaration des impôts en ligne, gestion de ses comptes bancaires, demande d'allocations, etc. Le vote est également un candidat naturel avec la possibilité de voter par Internet : nul besoin de se déplacer ni de tenir un bureau de vote, facilité du dépouillement, les avantages pratiques sont nombreux. Le vote électronique est également mis en avant comme un remède possible à l'abstention même si il n'y a pas d'étude claire à ce sujet (voir par exemple le rapport Anziani-Lefèvre [3]). À l'inverse, le vote électronique suscite, à raison, de nombreuses craintes. Comment s'assurer de la confidentialité des votes ? Comment se convaincre que son bulletin a bien été pris en compte ? Comment assurer la sincérité du scrutin ? L'objectif de cet article est de dresser un panorama des enjeux du vote électronique.

*Une première distinction.* Le terme « vote électronique » recouvre deux grandes familles de vote. Le *vote par Internet* permet aux électeurs de voter de chez eux, à l'aide de leur ordinateur, tablette ou smartphone. À l'inverse, les *machines à voter* sont des ordinateurs placés dans des bureaux de vote. Nous nous focaliserons ici essentiellement sur le vote par Internet (que nous appellerons aussi vote électronique) même si les problématiques du vote par Internet sont souvent transposables aux machines à voter.

1. CNRS, Laboratoire Lorrain de Recherche en Informatique et ses Applications (LORIA), UMR 7503 CNRS, INRIA et Université de Lorraine.

2. Cet article reprend en partie des billets publiés sur le blog BINAIRE ainsi qu'un article publié dans Interstices [11].

## Qui est concerné par le vote électronique ?

Plusieurs pays ont adopté le vote électronique. C'est en particulier le cas de l'Estonie qui l'utilise pour ses municipales depuis 2006 et pour ses élections nationales depuis 2007. L'Australie vient de réaliser en 2015 l'une des plus grosses élections électroniques (avec plus de 280 000 votants électroniques) au sein de l'état de New South Wales. La Suisse effectue de nombreux essais avec une volonté de monter en puissance pour consulter la population encore plus régulièrement. Le Canada et les États-Unis sont également des utilisateurs réguliers du vote électronique.

À l'inverse, les Pays-Bas ont aboli le vote électronique (aussi bien par Internet que les machines à voter) après une longue utilisation des machines à voter [20]. L'Allemagne a jugé les machines à voter Nedap *contraires à la constitution*. La décision prend également position implicitement contre le vote par Internet puisqu'« il doit être possible pour un citoyen de vérifier les étapes essentielles d'un processus électoral, sans expertise particulière » [1]. La Norvège a stoppé les essais, après plusieurs élections au sein de municipalités en 2011 et 2013, pour la raison suivante : le fait que les électeurs craignent que l'anonymat du vote ne soit pas respecté (même sans fraude avérée) pourrait saper le processus démocratique.

En France, l'utilisation du vote par Internet dans des élections politiques est réservée pour le moment aux Français de l'étranger [3]. Les Français de l'étranger ont ainsi élu leurs députés en 2012 et leurs conseillers consulaires en 2014. Il serait cependant erroné de croire que le vote par Internet est marginal en France. Il est largement utilisé dans des élections professionnelles (banques, chambres de commerce) ou encore par les mutuelles. Citons par exemple l'élection au sein de l'Éducation nationale avec environ un million d'électeurs ou celle de la MGEN en 2016. Ces élections ont probablement moins d'enjeux que des élections nationales mais un cas d'élections particulièrement intéressant et problématique est celui des primaires de partis politiques. L'UMP a eu recours au vote électronique en 2014 pour l'élection de son président et le parti des Républicains a envisagé de l'utiliser pour les primaires de 2016 [14] (son usage sera finalement limité aux Français de l'étranger habitant loin des grandes villes [22]). Le parti socialiste a lui aussi utilisé le vote électronique pour consulter ses adhérents en 2015. Si le vote électronique venait à être utilisé lors de primaires de grands partis politiques, les enjeux (et donc les menaces) seraient tout à fait similaires à ceux d'une grande élection nationale comme les présidentielles.

3. Nous parlons bien ici du vote par Internet. Les machines à voter ont été utilisées en France et continuent de l'être dans un petit nombre de municipalités.

## Quelles sont les menaces ?

Les craintes que suscite le vote électronique ne sont pas infondées. Ainsi, Alex Halderman et son équipe (Université du Michigan) se sont rendus célèbres en attaquant divers systèmes de vote électronique. Par exemple, en 2010, la ville de Washington avait mis en place un système de vote par Internet pour permettre aux militaires en mission à l'étranger de voter à distance. Quelques jours avant l'ouverture du scrutin, la ville a autorisé le public à attaquer le système, pour le tester. En moins de 48 heures, Alex Halderman et son équipe ont réussi à prendre pied sur le serveur, à modifier le contenu de l'urne, à récupérer l'ensemble des mots de passe envoyés aux militaires et à prendre le contrôle des caméras de surveillance (ce qui leur permettait d'évaluer le niveau de nervosité des employés) [26]. Pour marquer leur attaque, ils ont ajouté l'hymne de leur université à la dernière étape du processus de vote et c'est seulement 36 heures plus tard et grâce à cet hymne que les autorités, alertées par une autre équipe testeuse, ont pris connaissance de l'attaque et mis un terme à l'expérience (ainsi qu'à l'élection prévue). Au-delà du système mis en place à Washington, Alex Halderman s'est attaqué aussi bien au vote par Internet (en Estonie [24] ou en Australie [18]) qu'aux machines à voter, installant PacMan sur les machines Sequoia AVC Edge (USA) [17] ou en manipulant la mémoire des machines fabriquées en Inde [25].

Le vote électronique prête le flanc à des attaques de toutes sortes. Tout d'abord, le serveur de vote peut être l'objet d'attaques extérieures comme celles d'Alex Halderman. Mais des attaques plus directes sont également envisageables : un accès physique au serveur de vote (par un employé ou après effraction) peut souvent permettre des modifications très dommageables dans son comportement. D'autre part, les développeurs du système peuvent avoir laissé quelques « bugs » malencontreux ou au contraire avoir introduit délibérément des failles. Dans tous ces cas, un serveur modifié peut enregistrer l'ensemble des échanges, et pour beaucoup de systèmes, supprimer ou ajouter des bulletins. À l'autre bout de la chaîne, l'ordinateur du votant est en général peu protégé contre des attaques informatiques. Ainsi, des logiciels malveillants comme des virus ou *keyloggers* peuvent enregistrer et divulguer les votes, brisant ainsi l'anonymat. D'autres logiciels peuvent non seulement divulguer les votes mais également changer leur valeur, sans être détectés. Lors des élections législatives en 2012 des Français de l'étranger, Laurent Grégoire, ingénieur français travaillant aux Pays-Bas, en a fait la démonstration [16] en mettant au point un logiciel capable de remplacer le choix de l'électeur pour un parti pirate, au moment où l'électeur votait. En 2007, en Estonie, un étudiant en informatique, Paavo Pihelgas, a également construit un logiciel pour produire des bulletins valides, pour le candidat de son choix. Dans les deux cas, il s'agissait de systèmes de vote dont le fonctionnement et le code source n'étaient pas connus des personnes ayant mené l'attaque. Ceci démontre que le secret du fonctionnement du système ne garantit pas

la sécurité. Au contraire, il est souhaitable que la description du système et le code source soient ouverts pour permettre à un maximum de personnes de procéder à une analyse de sécurité.

## Quelles sont les bonnes propriétés ?

L'irruption des scrutins par voie numérique soulève de nouveaux enjeux en termes de garanties de bon fonctionnement et de sécurité informatique. Nous faisons ici un tour d'horizon des propriétés souhaitables pour le vote électronique en nous appuyant sur l'exemple du vote traditionnel à l'urne tel qu'il est organisé en France lors des élections municipales par exemple.

### *Confidentialité*

Nul ne doit connaître le vote d'un électeur. Dans le cas d'un vote à l'urne, on parle alors d'un vote à bulletins secrets : l'électeur glisse son bulletin dans une enveloppe, à l'abri des regards dans l'isoloir. Pour des élections à enjeux importants, la confidentialité stricte ne suffit pas : un électeur ne doit pas pouvoir révéler comment il a voté, même s'il le souhaite. Pourquoi donc ? Tout simplement pour se protéger contre l'achat de vote ou la coercition. Si je peux prouver comment j'ai voté, alors il m'est possible de vendre mon vote : contre une certaine somme d'argent (ou sous la menace), je peux donner une preuve que j'ai bien voté comme un tiers l'aurait souhaité. C'est pour cette raison que, lors d'un vote à l'urne, ni l'enveloppe ni le bulletin ne doivent porter un quelconque signe permettant d'identifier l'électeur, sous peine d'être considérés comme nuls. Notons au passage que le vote traditionnel à l'urne permet donc *l'abstention forcée* : il est possible de forcer un électeur à voter « nul » en lui demandant d'apposer sur son bulletin un signe particulier, convenu à l'avance. La présence de signe peut être vérifiée lors du dépouillement public.

### *Sincérité et transparence du scrutin*

Le principe même d'une élection est que les électeurs dans leur ensemble acceptent de se conformer au résultat de l'élection. Encore faut-il avoir confiance en la sincérité du scrutin, c'est-à-dire pouvoir se convaincre que le résultat de l'élection correspond bien aux votes exprimés par les électeurs. On parle alors de *vérifiabilité*. Toujours dans le cas d'un vote traditionnel à l'urne, et quitte à surveiller l'urne toute la journée, il est possible de s'assurer que son bulletin est bien présent dans l'urne (*vérifiabilité individuelle*) et que les bulletins proviennent tous bien d'électeurs légitimes (*vérifiabilité de la légitimité*). Puis lors du dépouillement public, chacun peut se convaincre que le décompte des voix correspond bien aux bulletins déposés par les électeurs (*vérifiabilité universelle*).

### *Disponibilité et accessibilité*

Tous les électeurs doivent pouvoir voter. Voter ne doit pas demander de compétence technique particulière et doit rester accessible à des personnes en situation de handicap. D'autre part, il doit être possible de voter à tout moment pendant la durée du scrutin. Dans le cas du vote à l'urne, il est ainsi important que les bureaux de vote soient accessibles, en nombre suffisant et ouverts suffisamment longtemps pour éviter de longues files d'attente. Dans le cas du vote électronique, il faut que les serveurs de vote soient disponibles pendant toute la phase de vote et que l'interface de vote soit compréhensible et utilisable par tous les électeurs.

## Que préconisent les autorités ?

Si chaque électeur peut juger de la disponibilité et de la clarté d'un système de vote, force est de constater qu'il est difficile de juger de la confidentialité et de la transparence en matière de vote électronique puisque le fonctionnement de ces systèmes est inconnu dans la grande majorité des cas. Par exemple, le fonctionnement du système mis en œuvre lors des élections au sein de l'UMP en 2014 n'est pas public. On peut alors se tourner vers les exigences ou recommandations émises par les autorités au sujet du vote électronique.

En France, l'autorité la plus reconnue en termes de vote électronique est la CNIL (Commission Nationale de l'Informatique et des Libertés). Ses dernières recommandations datent de 2010 [23]. Ces recommandations commencent par affirmer que « *la commission est réservée quant à l'utilisation de dispositifs de vote électronique pour des élections politiques* ». La suite de ses exigences portent essentiellement sur le respect du secret du vote : « *Le bulletin de vote doit être chiffré par un algorithme public réputé « fort » dès son émission sur le poste de l'électeur et être stocké dans l'urne, en vue du dépouillement, sans avoir été déchiffré à aucun moment, même de manière transitoire.* » Lors du dépouillement, il doit être impossible de faire le lien entre un bulletin et l'électeur correspondant. Ces recommandations visent à empêcher des personnes malveillantes d'avoir accès aux votes des électeurs lors du déroulé du scrutin ou du dépouillement, même s'il reste difficile de se prémunir contre des attaques menées directement sur l'ordinateur de l'électeur (un ordinateur infecté par un virus pourrait modifier le choix de l'électeur ou tout simplement l'envoyer à une personne tierce).

### *La transparence, parent pauvre du vote électronique !*

Malheureusement, ces recommandations ne parlent en rien de la transparence du scrutin et n'exigent absolument pas qu'un électeur puisse vérifier que son vote a bien été compté et encore moins qu'il ait accès au système comptabilisant les votes.

Au lieu d'exiger la transparence, les recommandations de la CNIL font reposer la sécurité du système sur l'expertise indépendante, « *tout système de vote électronique*

*doit faire l'objet d'une expertise indépendante* », et sur le contrôle (par l'expert et les autorités de vote) pendant le processus du vote : « *Avant le début du scrutin, les systèmes de vote électronique utilisés, la liste des candidats et la liste des électeurs doivent faire l'objet d'un scellement, c'est-à-dire d'un procédé permettant de déceler toute modification du système. Avant cette procédure de scellement, il est vérifié que les modules ayant fait l'objet d'une expertise n'ont pas été modifiés.* » Pourtant, toute personne ayant une expérience en informatique sait qu'il est impossible de s'assurer que les programmes informatiques qui tournent sur un ordinateur (dans le cas du vote, un ou plusieurs serveurs connectés à Internet) correspondent bien au code source que l'on a expertisé. Concrètement, la vérification consiste en général à assister à l'installation du programme informatique, en exécutant une suite de commandes prédéfinies à l'avance. Il est impossible de savoir quels sont les programmes réellement exécutés lors de l'installation. D'autre part, il est également très difficile à un expert de déceler des failles pendant les quelques jours passés à examiner le code source, *a fortiori* si ces failles ne sont pas des erreurs (ou « bugs ») mais des manipulations délibérées.

Ce manque d'exigence en matière de transparence se retrouve dans les systèmes commercialisés en France à l'heure actuelle : point d'urne visible, point de dépouillement vérifiable par le public ! Et bien sûr, pas d'information sur les méthodes utilisées. Même si des précautions sont prises et que des « experts en informatique » ont pu avoir accès au système, l'électeur, lui, n'a *a priori* aucun moyen de s'assurer que son bulletin a bien été déposé dans l'urne, ni que le résultat annoncé correspond aux bulletins reçus. Les électeurs n'ont actuellement pas d'autre choix que de faire confiance aux autorités de l'élection et aux experts indépendants qui ont analysé le système.

La vérifiabilité a tout de même fait timidement son entrée lors du dernier appel d'offre (2015) du ministère des Affaires étrangères, lors du renouvellement du marché pour les prochaines élections des Français de l'étranger. Ainsi, l'exigence 383 (sur un total de 419 exigences) indique que : « *un électeur doit pouvoir vérifier que son vote a été correctement pris en compte, et ce jusqu'à la phase de dépouillement. Le mécanisme ne doit pas permettre à un tiers (organisateur, administrateur, etc.) de relier un bulletin à son électeur.* » Il n'est cependant pas prévu que l'électeur puisse vérifier le dépouillement ni qu'il ait accès au fonctionnement du système mis en place.

### *Ce que dit la Suisse*

La situation française contraste avec celle de la Suisse. En décembre 2013, la chancellerie suisse a émis une ordonnance sur le vote électronique [2]. Cette ordonnance ne porte pas sur les procédures de mise en place et de contrôle de l'élection mais fixe des objectifs clairs de sécurité. On retrouve à nouveau la confidentialité

au cœur des préoccupations : « *Il faut garantir que ni des collaborateurs ni des personnes externes n'auront connaissance de données qui permettent d'établir un lien entre l'identité des votants et le suffrage qu'ils auront exprimé.* »

La vérifiabilité apparaît dès que le pourcentage d'électeurs par voie électronique atteint un certain seuil :

— *Pour qu'un système permettant à plus de 30 % de l'électorat cantonal de voter par voie électronique soit agréé, les votants doivent avoir la possibilité de déterminer si le suffrage qu'ils ont exprimé a été manipulé ou intercepté sur la plate-forme utilisateur ou pendant la transmission* (vérifiabilité individuelle).

— *Pour qu'un système permettant à plus de 50 % de l'électorat cantonal de voter par voie électronique soit agréé, les votants ou les vérificateurs doivent avoir la possibilité, dans le respect du secret du vote, d'identifier toute manipulation aboutissant à une falsification des résultats* (vérifiabilité complète).

La CNIL doit mettre au point de nouvelles recommandations en 2016. Cependant, au vu de la proposition soumise lors de la consultation réalisée début 2016, il ne semble pas prévu d'inclure des recommandations sur la transparence et vérifiabilité du système.

## Un exemple de système de vote : Belenios

*Je ne dois pas montrer pour qui j'ai voté et pourtant je dois pouvoir vérifier que mon vote a été compté...*

Mettre au point un système de vote électronique sûr est un exercice délicat. En particulier, la vérifiabilité et le secret du vote sont des propriétés antagonistes [4] : il faut à la fois pouvoir se convaincre que son vote a été inclus dans le résultat et ne pas pouvoir montrer à un tiers comment on a voté. Au niveau académique, plusieurs protocoles ont pu être construits de manière à satisfaire ces deux propriétés, avec un recours important à la cryptographie. Ainsi, le système Civitas [21, 8] implémente un protocole qui vise à la fois la vérifiabilité et la résistance à la coercition. Le système Helios [12, 4, 19] assure la vérifiabilité et l'anonymat. Contrairement à Civitas, il ne garantit plus la résistance à la coercition, mais il est plus facile à mettre en œuvre. Depuis 2012, nous développons au sein du Loria une évolution d'Helios, appelée Belenios [6, 15] (qui protège contre le bourrage d'urne même pour un attaquant qui contrôle le serveur de vote). C'est ce système que nous avons choisi de présenter ici.

Belenios [5] est développé sous licence libre par Stéphane Glondu (ingénieur de recherche Inria), en collaboration avec Pierrick Gaudry (directeur de recherche CNRS)

4. Pour certaines définitions, il a même été formellement démontré que vérifiabilité et résistance à la coercition sont incompatibles [7].

5. `http://belenios.gforge.inria.fr/`

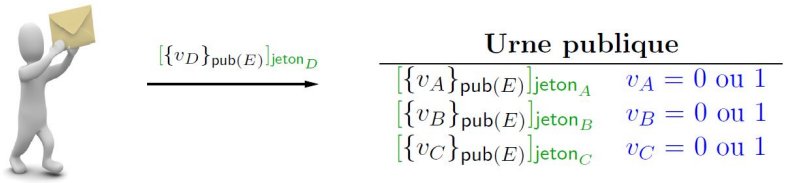


Illustration © skvoor - Fotolia.com.

FIGURE 1. Belenios : phase de vote. L'électeur, à l'aide de son ordinateur, sélectionne son choix, ici $v_D$ et forme son bulletin $[\{v_D\}_{\mathsf{pub}(E)}]_{\mathsf{jeton}_D}$. Une fois le bulletin envoyé, l'électeur pourra vérifier que son bulletin apparaît bien sur l'urne publique, accessible depuis une page web.

et Véronique Cortier (directrice de recherche CNRS). La plateforme de vote associée [6] permet de mettre facilement en place une élection, sans installation de logiciel. Belenios a déjà été utilisé dans une vingtaine d'élections. Ainsi, il est utilisé depuis l'automne 2015 par les sections nationales du CNRS en remplacement d'un système de vote par téléphone. Il est également utilisé depuis 2016 par Inria pour l'élection des représentants aux comités de centres.

Il s'agit d'un protocole en trois phases, comme le système de vote papier classique : la phase de mise en place de l'élection, la phase de vote à proprement parler et la phase de dépouillement. Pour simplifier les explications, le cas présenté ci-dessous est l'exemple d'un référendum où chaque électeur peut voter 0 (pour non) ou 1 (pour oui).

### *Phase de préparation*

Avant le début de l'élection, chaque électeur reçoit le matériel nécessaire pour voter, à savoir un login et mot de passe pour s'authentifier, ainsi qu'un autre identifiant privé, appelé *jeton de vote*, qui permettra à l'électeur de prouver qu'il a bien le droit de voter. Ce jeton de vote est en fait une clé de signature.

### *Phase de vote*

La phase de vote est représentée à la Figure 1. À chaque élection est associée une clef publique (notée $\mathsf{pub}(E)$ dans la figure). Le chiffrement à clef publique est un système de chiffrement dit asymétrique : la clef de chiffrement est publique — tout le monde peut chiffrer — alors que la clef de déchiffrement est privée — seules les personnes ayant la clef de déchiffrement peuvent déchiffrer. Pour voter, David,

6. https://belenios.loria.fr/

au travers de son navigateur, chiffre son choix $v_D$ (0 ou 1) avec la clef publique de l'élection. Ce chiffrement est noté $\{v_D\}_{\mathsf{pub}(E)}$. Il fournit également la preuve qu'il a bien chiffré l'une des deux valeurs 0 ou 1 et non une autre valeur. Cela est possible grâce aux preuves à divulgation nulle qui prouvent que le contenu d'un chiffré vérifie une certaine propriété, sans fournir aucune autre indication sur le contenu du chiffré.

Le vote chiffré, accompagné de la preuve de validité, est signé par le jeton de vote envoyé préalablement à l'électeur. L'ensemble forme le bulletin, noté $[\{v_D\}_{\mathsf{pub}(E)}]_{\mathsf{jeton}_D}$ dans la Figure 1. Il est envoyé à l'urne de l'élection (un serveur) après une phase d'authentification par login et mot de passe. Une des caractéristiques clés de Belenios est que l'urne affiche sur une page web publique tous les bulletins reçus. Ainsi, David pourra bien vérifier que son bulletin est présent dans l'urne.

Bien entendu, le chiffrement utilise de l'aléa pour éviter que deux chiffrés soient identiques. Il est impossible, étant donnés $\{0\}_{\mathsf{pub}(E)}$, $\{1\}_{\mathsf{pub}(E)}$ et un nouveau chiffré $c$, de savoir si $c$ est le chiffré de 0 ou de 1.

### *Phase de dépouillement*

L'explication de la phase de dépouillement nécessite de détailler un peu plus le fonctionnement de l'algorithme de chiffrement. Le chiffrement employé dans Belenios est le système de chiffrement *El Gamal*. Il a une propriété essentielle ici : il s'agit d'un chiffrement dit « homomorphique ». En particulier, multiplier les chiffrés des votes permet d'obtenir le chiffrement de la somme des votes :

$$\{v_1\}_{\mathsf{pub}(E)} \times \cdots \times \{v_k\}_{\mathsf{pub}(E)} = \{v_1 + \cdots + v_k\}_{\mathsf{pub}(E)}.$$

Grâce à cette propriété, il est facile pour tous de calculer le résultat de l'élection, mais sous une forme chiffrée. En multipliant tous les bulletins présents dans l'urne virtuelle, on obtient une valeur $\{n\}_{\mathsf{pub}(E)}$ qui correspond au chiffrement de $n$ par la clef publique de l'élection, où $n$ est le nombre d'électeurs ayant voté 1 (oui). La preuve (à divulgation nulle) de bonne formation du bulletin empêche un votant malhonnête de chiffrer autre chose que 0 ou 1, il est donc impossible d'ajouter des votes « oui » par exemple.

Il reste ensuite à déchiffrer la valeur obtenue pour connaître le résultat en clair. Il serait dangereux de confier la clef de déchiffrement à une autorité unique. La clef privée est en fait un assemblage de plusieurs petites clefs (en général de 2 à 4 clefs), chacune des petites clefs étant détenue par une autorité de déchiffrement indépendante (parti, bureau de vote, association...). Chacune des autorités de déchiffrement contribue au déchiffrement du résultat chiffré, ce qui permet à la fin du processus d'obtenir le résultat exact du vote, qui peut être proclamé. Il est à noter que les autorités de déchiffrement produisent également une preuve qu'elles ont correctement déchiffré le résultat chiffré, ce qui permet à tout un chacun de vérifier les calculs, sans posséder la clef de déchiffrement.

### *Et si ce n'est pas un référendum ?*

Comment additionner des candidats s'il y en a plusieurs ? En fait, il est relativement facile de généraliser au cas où les électeurs choisissent $k$ candidats parmi un total de $n$ candidats. Supposons qu'il s'agisse de choisir trois candidats au plus parmi cinq. On fixe l'ordre des candidats et on représente le choix sous la forme d'une liste (ou plutôt d'un vecteur). Ainsi le vote $v_1 = (1, 1, 1, 0, 0)$ correspond à la sélection des 3 premiers candidats, $v_2 = (1, 0, 0, 0, 1)$ correspond à la sélection du premier et du dernier, $v_3 = (0, 0, 0, 0, 0)$ correspond à un vote blanc, etc.

Pour chiffrer un vote, on chiffre en fait chacune de ses composantes. Ainsi le chiffré $c_1$ de $v_1$ est en fait $\{1\}_{\mathsf{pub}(E)}, \{1\}_{\mathsf{pub}(E)}, \{1\}_{\mathsf{pub}(E)}, \{0\}_{\mathsf{pub}(E)}, \{0\}_{\mathsf{pub}(E)}$. Ce chiffré est accompagné d'une preuve à connaissance nulle que chaque « petit » chiffré contient un 0 ou un 1 et qu'il y a au plus trois 1 en tout dans les petits chiffrés. Le produit des chiffrés se fait alors colonne par colonne comme illustré ci-dessous sur l'exemple.

| | |
|---|---|
| $c_1 = \{v_1\}_{\mathsf{pub}(E)}$ | $\{1\}_{\mathsf{pub}(E)}\,\{1\}_{\mathsf{pub}(E)}\,\{1\}_{\mathsf{pub}(E)}\,\{0\}_{\mathsf{pub}(E)}\,\{0\}_{\mathsf{pub}(E)}$ |
| $c_2 = \{v_2\}_{\mathsf{pub}(E)}$ | $\{1\}_{\mathsf{pub}(E)}\,\{0\}_{\mathsf{pub}(E)}\,\{0\}_{\mathsf{pub}(E)}\,\{0\}_{\mathsf{pub}(E)}\,\{1\}_{\mathsf{pub}(E)}$ |
| $c_3 = \{v_3\}_{\mathsf{pub}(E)}$ | $\{0\}_{\mathsf{pub}(E)}\,\{0\}_{\mathsf{pub}(E)}\,\{0\}_{\mathsf{pub}(E)}\,\{0\}_{\mathsf{pub}(E)}\,\{0\}_{\mathsf{pub}(E)}$ |
| $c = c_1c_2c_3$ | $\{2\}_{\mathsf{pub}(E)}\,\{1\}_{\mathsf{pub}(E)}\,\{1\}_{\mathsf{pub}(E)}\,\{0\}_{\mathsf{pub}(E)}\,\{1\}_{\mathsf{pub}(E)}$ |

### *Avantages et inconvénients de Belenios*

Belenios est un système de vote relativement simple comparativement aux autres systèmes existants. Il est facile à mettre en œuvre et il s'agit d'un logiciel libre, dont les sources sont disponibles. Belenios assure bien sûr la confidentialité des votes. Mais son principal avantage est d'être entièrement vérifiable et par tous : tout électeur peut suivre son bulletin dans l'urne, calculer le résultat de l'élection sous une forme chiffrée et vérifier les calculs effectués par les autorités de déchiffrement. Il s'agit d'une différence fondamentale par rapport à la plupart des solutions commerciales actuellement déployées : même si les entreprises développant ces solutions font un effort pour que leurs systèmes soient auditables par des experts habilités, elles ne permettent pas à tout un chacun de vérifier que le résultat proclamé est conforme.

Des systèmes ouverts et vérifiables comme Belenios représentent une avancée pour les élections qui ont lieu à distance. Cependant, nous tenons à souligner que Belenios, comme tout système de vote en ligne, ne nous semble pas adapté à des élections à forts enjeux, comme des élections politiques (présidentielles, législatives, primaires...). Tout d'abord, comme tout système de vote par Internet, il s'agit d'un vote par correspondance : il est impossible de s'assurer que l'électeur est seul lorsqu'il vote. D'autre part, l'électeur vote en utilisant des identifiants (mot de passe, jeton de vote) reçus par mail. Toute personne ayant accès à ces identifiants peut voter à la place de l'électeur. De plus, un ordinateur compromis pourrait transmettre la valeur du vote d'un électeur à une tierce personne, à l'insu de l'électeur. Il pourrait

également voter pour une autre personne comme l'a démontré Laurent Grégoire — pour un autre système — dans le contexte des législatives de 2012 [16]. Certains systèmes se protègent mieux contre la compromission éventuelle des ordinateurs de votants. C'est le cas par exemple des systèmes déployés en Estonie ou dans l'état australien New South Wales. Ces systèmes incorporent un mécanisme permettant aux votants de vérifier que leur vote est bien dans l'urne, au prix cependant de garanties moins fortes en termes de confidentialité. Ainsi, dans l'état du New South Wales, les électeurs pouvaient téléphoner pour écouter le vote associé à leur numéro — anonyme — de votant.

## Le vote papier est-il vraiment plus sûr ?

Si les craintes en matière de garanties de sécurité et transparence sont tout à fait légitimes vis-à-vis du vote électronique, les mêmes questions se posent pour les scrutins qui ont recours au « papier ». Pour analyser la sécurité du vote « papier », il faut distinguer deux scénarios bien différents : le vote à l'urne et le vote par correspondance.

### *Le cas du vote traditionnel à l'urne*

Le premier système de vote qui vient à l'esprit est le vote traditionnel à l'urne, où chaque électeur dépose son bulletin dans une urne. L'isoloir et l'enveloppe visent à assurer la confidentialité des votes. L'urne transparente et le dépouillement public permettent à tout un chacun de vérifier le décompte des voix. Même si des fraudes peuvent avoir lieu, le vote à l'urne offre un très bon niveau de sécurité, sous réserve que l'urne soit surveillée sans relâche, de l'ouverture du scrutin au dépouillement, par un groupe de personnes représentant si possible chaque partie en lice. La surveillance de l'urne semble une évidence mais n'est pas toujours facile à réaliser pour des élections à enjeux modérés où il est souvent difficile de trouver des volontaires pour tenir l'urne et assister au dépouillement.

### *Le vote par correspondance, un faux sentiment de sécurité*

Si le vote traditionnel à l'urne est bien compris et offre de bonnes garanties en matière de confidentialité et de transparence, il en est autrement du vote par correspondance. Comment voter par correspondance ? Le principe le plus simple consiste à mettre son bulletin dans une première enveloppe, glissée dans une deuxième enveloppe signée par l'électeur (pour permettre l'émargement), le tout envoyé dans une troisième enveloppe expédiée au centre gérant l'élection. Comment s'assurer que les trois enveloppes ne seront pas ouvertes en même temps, brisant ainsi la confidentialité du vote ? Comment être certain que des bulletins n'ont pas été ajoutés (ou supprimés) avant le dépouillement ? L'électeur doit faire une entière confiance aux organisateurs de l'élection ainsi qu'à toute la chaîne de traitement. Des fraudes provenant de personnes malveillantes extérieures à l'organisation de l'élection sont

également possibles. Il est techniquement facile d'imiter la signature de quelques abstentionnistes pour ajouter des votes de son choix. La participation étant souvent faible, le nombre de bulletins nécessaires pour modifier le résultat de l'élection est en général peu important.

***Des attaques existent aussi sur des systèmes plus complexes***

Des systèmes de vote par correspondance plus complexes ont été mis au point pour permettre un dépouillement mécanisé. Certains systèmes utilisent ainsi des codes à barres, notamment pour identifier (de façon anonyme) l'électeur. Le fait d'utiliser du papier rend le système rassurant mais pas sûr pour autant. Il a été démontré que, pour certains systèmes [10], il est possible de reconstituer l'ensemble des matériels de vote envoyés aux électeurs, ouvrant ainsi la porte à un « bourrage d'urne ».

## Les défis

Le vote électronique soulève encore de nombreux défis et représente de ce fait un domaine de recherche extrêmement actif. Nous en mentionnons ici quelques-uns, de façon non exhaustive.

***Authentification de l'électeur***

À l'heure actuelle, les électeurs s'authentifient en général à l'aide d'identifiants reçus par courrier, par mail ou SMS. Il est très difficile de s'assurer que la personne qui vote est bien l'électeur correspondant aux identifiants. En particulier, il est en général possible de transmettre (ou vendre !) ses identifiants à une personne tierce. À plus long terme, on pourrait imaginer que les électeurs s'identifient au moyen d'une carte d'identité numérique comme c'est le cas en Estonie par exemple. Cela pose alors de nouveaux défis en termes d'infalsifiabilité de l'identité numérique ainsi que de respect de la vie privée (il ne faut pas pouvoir « tracer » les citoyens par l'intermédiaire de leur carte).

***Un système de vote parfait ?***

Aucun système de vote proposé jusqu'ici n'assure toutes les propriétés souhaitées à la fois, de la résistance à la coercition à la vérifiabilité, sans avoir à faire confiance ni à l'ordinateur du votant ni aux autorités de l'élection. Ainsi, la sécurité de Helios, Belenios et Civitas repose sur la confiance en l'ordinateur de l'électeur, celle des systèmes déployés en Estonie, Norvège ou New South Wales (Australie) sur la confiance en les autorités et le prestataire. Au niveau académique, de nouveaux systèmes sont proposés chaque année. Chaque système dessine un nouveau compromis entre les différentes propriétés et les hypothèses de confiance et il est très probable que l'on doive encore pendant plusieurs années choisir quels défauts accepter lorsqu'on sélectionne une solution de vote.

### *Simplicité du système*

Un système comme Belenios est vérifiable car un électeur peut vérifier que son bulletin est dans l'urne. Cela semble une opération relativement simple à effectuer. Mais qui le fait vraiment ? Est-ce qu'un attaquant ne peut pas se contenter d'attaquer des électeurs peu susceptibles de vérifier (par exemple en ciblant des électeurs ayant des systèmes d'exploitation un peu trop anciens) ? Est-ce possible de rendre la vérification automatique ? Déléguable ? Comment expliquer ce que cette « vérification » apporte à l'électeur ? Tous les systèmes de vote ont clairement une grande marge de progression en termes de simplicité d'utilisation et de compréhension pour le grand public.

### *Définitions et modèles*

Curieusement, définir rigoureusement une propriété aussi fondamentale que la confidentialité du vote est encore un sujet très actif en recherche. Les définitions les plus simples [9, 13] ne couvrent pas tous les scénarios d'attaques et de nombreux problèmes ont été détectés sur les définitions plus complexes [5]. De la même façon, la plupart des systèmes de vote proposés dans le monde académique sont conçus pour assurer à la fois vérifiabilité et confidentialité mais la partie vérifiabilité est en général considérée comme évidente et n'est jamais prouvée ni même définie. Plus généralement, qu'est-ce qu'un « bon » système de vote ? Contre qui se défend-on ? (Les autorités de vote et le prestataire, une puissance étrangère, un candidat malhonnête ?) Il reste encore beaucoup de travail pour traduire en définitions rigoureuses les propriétés souhaitées et les différents types d'attaquants.

## Quand choisir le vote par Internet ?

À l'heure actuelle, le vote traditionnel à l'urne (sous réserve d'une surveillance effective de l'urne) offre de bien meilleures garanties de confidentialité et de transparence que toutes les solutions de vote électronique. Non seulement le vote électronique soulève de nouveaux défis techniques en matière de sécurité mais les solutions proposées sont complexes et accessibles uniquement à des spécialistes du sujet. Il semble impossible d'atteindre la simplicité du vote à l'urne. Même pour les systèmes les plus sûrs et les plus vérifiables, les mécanismes de vérification font appel à des théories mathématiques complexes dont la compréhension détaillée est réservée à des experts. Les autres utilisateurs doivent faire confiance à ces experts, contrairement au vote papier où les procédures sont comprises par une vaste majorité des citoyens.

Pour toutes ces raisons, il semble prématuré d'utiliser le vote par Internet pour des élections à forts enjeux comme des élections politiques importantes. Par contre, il serait réducteur de penser que le vote par Internet est plus dangereux que les autres

systèmes de vote en général. Ainsi, le vote par Internet est souvent utilisé pour remplacer le vote par correspondance, qui lui-même présente de nombreuses faiblesses. Contrairement au vote dans un bureau de vote, le processus du vote par correspondance ne peut être observé que par quelques personnes et les électeurs doivent faire pleinement confiance aux organisateurs de l'élection. De plus, le vote par correspondance peut être sujet au bourrage d'urne, comme l'ont montré certaines attaques [10]. En conclusion, le choix d'utiliser un système de vote électronique dépend fortement du système déjà en place et du type d'élection.

Quel que soit le mode de scrutin envisagé, il est important d'exercer le même esprit critique sur les systèmes de vote électronique que sur leurs homologues « papier », en exigeant à la fois confidentialité et transparence. Sur ce point, il est dommage que les recommandations de la CNIL comportent une forte asymétrie en mettant l'accent sur la confidentialité au détriment de la vérifiabilité ou transparence du scrutin. Ces recommandations poussent les prestataires de vote (en France) à se concentrer uniquement sur la confidentialité du vote alors que, sauf cas particuliers, les deux propriétés semblent également fondamentales.

*Remerciements.* Je tiens à remercier Pierrick Gaudry, Stéphane Glondu et Denis Pallez pour leur relecture attentive de cet article et pour leurs suggestions.

## Références

[1] Judgment of the Second Senate of 3 March 2009 on the basis of the oral hearing of 28 October 2008 – 2 BvC 3/07, 2 BvC 4/07 –.

[2] Catalogue des exigences à remplir pour recourir au vote électronique lors de votations populaires fédérales. https://www.bk.admin.ch/themen/pore/evoting/07979/index.html?lang=fr, 2014.

[3] Alain Anziani and Antoine Lefèvre. Vote électronique : préserver la confiance des électeurs. Technical Report 445, Sénat, 2014. Rapport d'information de MM. Alain ANZIANI et Antoine LEFÈVRE, fait au nom de la commission des lois.

[4] Josh Benaloh. Simple verifiable elections. In *EVT '06, Proceedings of the 1st Usenix/ACCURATE Electronic Voting Technology Workshop*, 2006. Available online at http://www.usenix.org/events/evt06/tech/.

[5] David Bernhard, Veronique Cortier, David Galindo, Olivier Pereira, and Bogdan Warinschi. A comprehensive analysis of game-based ballot privacy definitions. In *Proceedings of the 36th IEEE Symposium on Security and Privacy (S&P'15)*, pages 499–516, San Jose, CA, USA, May 2015. IEEE Computer Society Press.

[6] David Bernhard, Véronique Cortier, Olivier Pereira, Ben Smyth, and Bogdan Warinschi. Adapting Helios for provable ballot secrecy. In Springer, editor, *Proceedings of the 16th European Symposium on Research in Computer Security (ESORICS'11)*, volume 6879 of *Lecture Notes in Computer Science*, 2011.

[7] Benoit Chevallier-Mames, Pierre-Alain Fouque, David Pointcheval, Julien Stern, and Jacques Traoré. On some incompatible properties of voting schemes. In *Towards Trustworthy Elections 2010*, pages 191–199, 2010.

[8] The Civitas voting system. http://www.cs.cornell.edu/projects/civitas/.

[9] J. Cohen (Benaloh) and M. Fischer. A robust and verifiable cryptographically secure election scheme. In *26th Symposium on Foundations of Computer Science.*, pages 372–382, Portland, OR, 1985. IEEE.

[10] Véronique Cortier, Jérémie Detrey, Pierrick Gaudry, Frédéric Sur, Emmanuel Thomé, Mathieu Turuani, and Paul Zimmermann. Ballot stuffing in a postal voting system. In *Revote 2011 - International Workshop on Requirements Engineering for Electronic Voting Systems*, Trento, Italie, 2011. IEEE.

[11] Véronique Cortier and Steve Kremer. Vote par internet. In *Interstices*. Janvier 2013.

[12] R. Cramer, R. Gennaro, and B. Schoenmakers. A secure and optimally efficient multi-authority election scheme. In *Advances in Cryptology (EUROCRYPT'97)*, pages 103–118, 1997.

[13] Stéphanie Delaune, Steve Kremer, and Mark Ryan. Verifying privacy-type properties of electronic voting protocols. *Journal of Computer Security*, 17(4) :435–487, 2009.

[14] Olivier Duhamel. *Les primaires pour les Nuls*. Nuls en poche. First, 2016.

[15] Stéphane Glondu, Véronique Cortier, and Pierrick Gaudry. Belenios – Verifiable online voting system. http://belenios.gforge.inria.fr, September 2015.

[16] Laurent Grégoire. Comment mon ordinateur a voté à ma place, 2012.

[17] J. Alex Halderman and Ariel J. Feldman. https://jhalderm.com/pacman/, 2010. Rump session talk at EVT/WOTE 2010.

[18] J. Alex Halderman and Vanessa Teague. The New South Wales iVote System : Security Failures and Verification Flaws in a Live Online Election. In *5th International Conference on E-voting and Identity (VoteID '15)*, Bern, Switzerland, 2015.

[19] The Helios voting system. http://heliosvoting.org/.

[20] Bart Jacobs and Wolter Pieters. *Electronic Voting in the Netherlands : From Early Adoption to Early Abolishment*, pages 121–144. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[21] Ari Juels, Dario Catalano, and Markus Jakobsson. Coercion-resistant electronic elections. In *Towards Trustworthy Elections*, pages 37–63, 2010.

[22] Alexandre Lemarié. Primaire à droite : un compromis trouvé pour régler le litige sur le vote des français de l'étranger. *Le Monde*. 17 mai 2016.

[23] Commission nationale de l'informatique et des libertés (CNIL). Délibération 2010-371 du 21 octobre 2010 portant adoption d'une recommandation relative à la sécurité des systèmes de vote électronique. https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000023124205.

[24] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman. Security analysis of the Estonian internet voting system. In *21st ACM Conference on Computer and Communications Security (CCS'14)*, Scottsdale, AZ, USA, 2014.

[25] Scott Wolchok, Eric Wustrow, Alex Halderman, Hari Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp. Security analysis of India's electronic voting machine. In *17th ACM Conference on Computer and Communications Security CCS'10*, Chicago, USA, 2010.

[26] Scott Wolchok, Eric Wustrow, Dawn Isabel, and Alex Halderman. Attacking the Washington, D.C. Internet Voting System. In *Financial Cryptography 2012*, pages 114–128, 2012.