Le vote électronique presque aussi peu fiable que le papier

La sécurité du vote électronique est souvent pointée du doigt. Des militants réclament un choix éclairé pour le code informatique qui le constitue. Aucun mode de scrutin n'est parfait.

Les élections ont connu quelques ratés, ce dimanche, à Bruxelles. En cause, un problème informatique qui a touché les clés USB censées charger le logiciel des appareils de vote électronique. Dans les bureaux de vote d'Auderghem et d'Uccle, l'ouverture a été retardée jusqu'aux environs de midi.

Des bugs sans trop de gravité qui donnent toutefois du grain à moudre à ceux que le recours à de telles machines inquiète. Et il est vrai que les questions sont nombreuses.

1 Un code trop opaque ? Un des principaux reproches faits aux isoloirs numériques vient du manque de transparence de leurs logiciels. *« La création des programmes devrait être la responsabilité des gouvernements*, estime Yves Roggeman, professeur de sécurité informatique à la faculté des sciences de l'ULB. *Or on achète les appareils et les logiciels à une société privée* (Smartmatic, une entreprise vénézuélienne, NDLR). *Et c'en est une autre, PwC, qui est chargée de contrôler son fonctionnement. »* PwC avait déjà réalisé les contrôles de la génération précédente de bornes et était donc *« passée à côté »* du bug des élections de 2014. Mais en décembre dernier, suite à un appel d'offres où elle était la seule à répondre, c'est à nouveau elle qui a été chargée par les autorités de vérifier les appareils et leur logiciel.

« Pour être certain de la qualité du code et permettre à tous les citoyens de savoir si leur vote est effectivement pris en compte de la manière dont ils le souhaitent, il devrait être public et accessible à tous, en le publiant, par exemple, au Moniteur belge. *Si tous les groupes de pressions et les différentes communautés de spécialistes peuvent avoir accès à ce code, cela permettrait d'améliorer en permanence le mode de fonctionnement des appareils et cela renforcerait la sécurité tout en évitant les bugs. »*

Pour Olivier Pereira, professeur de cryptographie à l'UCLouvain, toutefois, le système mixte tel qu'il a été utilisé ce dimanche au nord du pays et dans la capitale est probablement le meilleur compromis. *« Le fait d'imprimer le choix de l'électeur sur papier en plus de l'enregistrer électroniquement permet un meilleur contrôle a posteriori. Si on a des suspicions, un audit peut être réalisé pour analyser les correspondances entre l'impression et le vote enregistré. S'il n'y a pas de différences sur un échantillon représentatif, on peut alors se dire que le résultat des votes est fiable. Car il serait très difficile de pirater les deux en même temps. »*

A Bruxelles, on assure que les contrôles sont très poussés : *« Une fois le matériel et le logiciel certifiés par PwC, les services de la Région contrôlent une nouvelle fois toutes les clés USB*, explique Hélène Herman, chargée de communication de Bruxelles Pouvoirs locaux. *Une fois les élections terminées, on analyse à nouveau les clés pour s'assurer que le logiciel qu'elles contiennent est bien le bon. Un collège d'experts mandatés par le Parlement se charge par ailleurs de s'assurer de la concordance entre un échantillon les votes "papier" et les votes enregistrés dans la machine. Ces vérifications sont toujours en cours actuellement. Pour résumer, rien n'est plus contrôlé que le vote électronique »*, résume la porte-parole.

2 La fiabilité des machines en question En août dernier, les participants du « Voting Village » de la DefCon, la conférence de hackers la plus célèbre au monde qui se tient chaque année à Las Vegas, ont mis en évidence la facilité avec laquelle ils pouvaient compromettre la sécurité de la plupart des bornes de vote utilisées aux Etats-Unis. En bidouillant, dans le public, une personne a ainsi pu transformer une des machines en juke-box, une autre a pu récupérer les autorisations d'administrateur d'une autre borne en moins de deux minutes. Depuis des années, ces hackers éthiques cherchent à sensibiliser sur le risque du recours à ces machines.

« Il existe de plus en plus de documentation sur la manière de pirater ce genre de machines, note Olivier Pereira. *Jusqu'ici, les chercheurs ont pu démontrer que le piratage de ces bornes était faisable. Mais on n'a pas encore démontré que cela avait été fait. Il y a par contre eu des soupçons d'ingérence russe lors des élections présidentielles américaines, mais cela n'a pas été démontré. Mais c'est certain, ces machines sont vulnérables. On peut par exemple imaginer qu'un pirate ait accès aux machines entre deux élections, ou aux clés USB qui chargent le programme au matin du vote. »*

3 Ne pas sanctifier le crayon *« Des bugs, il y en aura, peu importe la manière dont le vote s'effectue. Pour avoir été assesseur à plusieurs reprises, j'ai pu constater que des bugs, il y en aussi avec le vote papier. L'humain n'est pas irréprochable. Il peut être difficile, parfois, de savoir si un bulletin papier est nul ou s'il doit au contraire être pris en compte. Le problème, ici est que l'on tente de reproduire le fonctionnement du papier avec celui de l'informatique. Et du coup, on cumule les inconvénients des deux modes. Revenir au papier n'a pas de sens. Ce qu'il faut, en revanche, c'est revoir la loi pour permettre d'imaginer une manière de voter électroniquement »*, conclut le professeur Roggeman.

« Il faut éviter de sacraliser le vote papier, considère Olivier Pereira. *On a tendance à sous-évaluer les erreurs induites par le dépouillage du vote papier. Mais la littérature scientifique montre bien que les erreurs sont plus fréquentes que l'on pense. Il n'y a pas d'un côté les multinationales informatiques qui cherchent à modifier les résultats et de l'autre, les citoyens exempts de tout défaut qui ne font aucune erreur. L'informatique doit pouvoir permettre le recomptage de manière transparente et sans se tromper. »* ■

THOMAS CASAVECCHIA

EN SUISSE

Voter depuis son canapé

En Suisse, on vote souvent. Et de plus en plus derrière son écran. Depuis 2004, le pays introduit progressivement le recours au vote électronique. Mais dans la fédération helvétique, le terme recouvre la possibilité de voter où l'on veut depuis internet.

Pour l'heure, toujours en phase de test, l'« E-voting », concerne les cantons de Genève, de Berne, Lucerne, Bâle-Ville, Saint-Gall et d'Argov.

A l'avenir, la possibilité devrait être étendue à l'ensemble du pays. La semaine dernière, le Conseil fédéral a annoncé vouloir organiser une consultation populaire à la fin de l'automne pour savoir si oui ou non cette possibilité sera généralisée.

TH.CA.

POINT DE VUE

« La démocratie est trop importante pour la laisser dans les mains des informaticiens »

Thierry Bingen est ingénieur informaticien, spécialiste en cybersécurité, mais il est également un militant de PourEVA (Pour une éthique du vote automatisé), une association citoyenne qui conteste le recours au vote électronique. Pour lui, on s'expose tôt ou tard à des attaques informatiques.

Qu'est-ce que votre association reproche au vote électronique ?

Il y a un réel manque de transparence et de sécurité. Il est anormal que le contrôle du logiciel soit effectué par une entreprise privée. En ne rendant pas public le code du logiciel, le citoyen ne peut pas s'assurer de sa protection. Le citoyen est supposé avoir une confiance aveugle en la machine et les assesseurs également. Si ce code était rendu public, il pourrait y avoir un contrôle des pairs pour s'assurer qu'il reste sécurisé. Or là, on s'expose tôt ou tard à l'attaque de pirates malveillants. Par ailleurs, les avantages du vote électronique ne sont pas assez nombreux pour prendre autant de risques. On parle par exemple de la rapidité du processus. Ça, c'est quand il n'y a pas de bug. Et on peut se poser la question de l'intérêt d'aller si vite. Ce ne sont pas deux heures supplémentaires qui vont empêcher les négociations d'avoir lieu. Dans beaucoup de communes, elles sont encore en cours.

Tout de même, on assure que les contrôles existent et que ces bornes sont sécurisées…

Il existe effectivement des contrôles, les présidents de chaque bureau étaient obligés pour ces élections de recompter au moins une urne pour s'assurer de la concordance entre les impressions et les votes enregistrés dans l'ordinateur. Mais je me pose la question de la validité statistique de ce recomptage. Est-ce suffisant ? Et puis, quel est réellement le contrôle que peuvent effectuer les assesseurs et présidents puisque la plupart ne maîtrisent pas les machines avec lesquelles ils travaillent ? D'ailleurs, quand un bug survient, ce sont les informaticiens et l'aide technique que l'on appelle à la rescousse. Mais la démocratie est trop importante que pour être laissée entre les mains des informaticiens.

TH.CA.