

Note technique sur le vote par internet

Chantal Enguehard (LINA - UMR CNRS 6241)

Le 11 juillet 2014

Le vote par internet devient de plus en plus usité en France dans le cadre d'élections professionnelles voire même politiques (pour les français habitant hors de France). Après une brève présentation de ce nouveau mode de vote, nous passons en revue quelques enjeux (avec leurs difficultés). Nous concluons que le vote par internet, sous sa forme actuelle, ne devrait pas être utilisé dans le cadre d'élections dans lesquelles le secret du vote doit être respecté.

1. Le vote par internet

Le vote par internet est aussi désigné par les termes "vote en ligne" et "vote à distance par voie électronique".

Les électeurs procèdent depuis n'importe quel ordinateur connecté à internet, que cet ordinateur soit chez eux, au travail, dans un lieu public ou un cybercafé. Le vote par internet est un mode de vote à distance, il peut donc être comparé au vote par correspondance postale.

La connexion avec internet est parfois réalisée via un réseau intranet intermédiaire (par exemple, le réseau intranet de l'école, de l'université ou de l'entreprise d'où l'électeur procède à son vote) lui-même connecté à la toile internet. Le centre serveur de vote est composé de plusieurs serveurs ou systèmes virtuels hébergés sur une seule machine se chargeant de différentes tâches : authentification des électeurs, réception des bulletins, gestion des émargements, stockage des bulletins, dépouillement, etc. Ces serveurs et systèmes sont souvent dupliqués afin de faire face à d'éventuelles pannes.

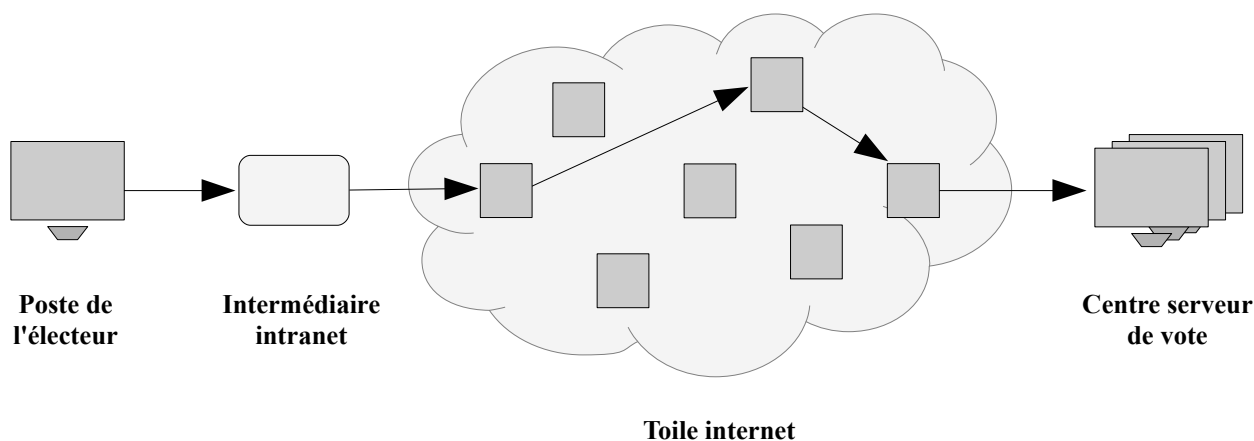


Figure 1 : Vote par internet (avec présence d'un intranet)

2. Enjeux et difficultés

Unicité

Pour assurer le respect du principe d'unicité (un électeur - une voix), le système de vote par internet doit tenir à jour une liste des émargements afin d'empêcher tout vote multiple. Il est donc indispensable que, pour chaque bulletin reçu, le centre serveur ait connaissance des codes ayant autorisé le vote.

Lorsqu'un vote est émis, deux types de données sont donc utilisées : un code d'autorisation (séparée du vote) et le vote lui-même. Une difficulté est que, afin de préserver l'anonymat il est nécessaire de mettre en place des mécanismes sophistiqués visant à ne pas révéler ces informations aux dispositifs relayant l'information sur la toile depuis le poste de la personne ayant voté jusqu'au centre serveur de vote. Le centre serveur de vote lui-même ainsi que les personnes ayant accès aux machines de vote ne doivent pas être mesure de reconstituer le lien entre un vote et le code d'autorisation qui l'accompagnait.

Sincérité

Lorsque qu'un électeur vote via internet, il exprime son choix par un clic de souris. Cette force mécanique de quelques joules est convertie en une impulsion électrique, elle-même transformée en une information codée en binaire susceptible de connaître ensuite d'autres traitements (comme le chiffrement, etc.). Tous les votes, sans exception, sont donc soumis à plusieurs transformations. Du fait de la protection du secret du vote, l'ensemble de ces transformations ne peut être suivi

pas à pas. Par conséquent, des transformations modifiant le sens du vote de certains bulletins pourraient passer inaperçues, y compris si une grande quantité de bulletins étaient affectés.

Sur ce point, le vote par internet diffère considérablement du vote par correspondance pour lequel les bulletins dénombrés sont censés être ceux que les électeurs ont envoyés, sans aucune transformation intermédiaire. De plus, l'identité de l'électeur peut être établie d'après des éléments accompagnant l'enveloppe fermée contenant le bulletin de vote. La transformation, l'ajout ou le retrait de bulletins en grande quantité peuvent difficilement être dissimulés du fait de la manipulation de bulletins matériels, des nécessaires complicités, des éventuels témoignages, etc.¹

Dans le cas du vote par internet, il apparaît finalement que personne (ni les électeurs, ni les candidats, ni les experts, ni les partis, ni le ministère, etc.) ne peut être certain que les choix des électeurs n'ont pas été modifiés avant leur comptage ou même que les votes apparemment recensés aient été émis par les électeurs eux-mêmes.

Portée de l'expertise d'un système de vote électronique.

L'expertise d'un système de vote électronique ne peut porter sur l'entièreté du système de vote puisqu'une partie importante de celui-ci (les ordinateurs à partir desquels les votes sont émis) ne peut être inspectée. Or ces ordinateurs sont susceptibles d'être le siège d'attaques externes visant à la fois la sincérité des élections et le secret du vote. Comme le note Jean-Didier Graton² « *dans l'état actuel du marché et des pratiques de l'industrie informatique, il est impossible de mettre en place une chaîne de responsabilité contractuelle pour tous les fournisseurs de matériels, réseaux et logiciels, intervenant dans les opérations électorales, qui permette de sanctionner les dysfonctionnements de PC et autres Apple dont la sécurité logicielle intrinsèque est aujourd'hui faible.* »

Du côté du centre serveur de vote, plusieurs mois seraient nécessaires pour une expertise complète, sans garantie de trouver tous les bugs ou éventuelles fraudes.

La portée de l'expertise d'un système de vote électronique apparaît donc réduite : des dysfonctionnements ou des fraudes peuvent se produire sans être détectés, même s'ils concernaient un nombre important de suffrages.

Efficacité du chiffrement du bulletin de vote

Bien que cette mesure soit efficace une fois qu'elle a été effectuée (sous réserve que les clés de chiffrement n'aient pas été divulguées ou obtenues frauduleusement), il reste toujours possible qu'un programme malveillant hébergé sur le poste de l'électeur copie ou modifie le bulletin de vote avant chiffrement. Cette mesure ne peut donc garantir que le vote de l'électeur n'a pas été modifié avant le dépouillement et qu'il est resté secret.

3. Conclusion

Le vote par internet apparaît donc plus fragile que le vote par correspondance postale car les bulletins sont modifiés en dehors de toute surveillance : le vote porté par un grand nombre de bulletins pourrait être changé par un bug malencontreux, ou du fait d'une manœuvre frauduleuse d'un individu isolé, sans que cette atteinte majeure à la sincérité de l'élection ne soit remarquée.

Cette conclusion rejoint les constats réalisés par une commission sénatoriale en 2014 et par l'association d'informaticiens ASTI en 2007.

Sénat

En 2014, une commission parlementaire du Sénat a travaillé sur le vote électronique. Une partie du rapport qui a été produit par cette commission est consacrée au vote par internet. Plusieurs remarques des parlementaires rejoignent l'analyse développée ici :

« Il y a donc un risque persistant, non seulement pour la sincérité du suffrage, mais aussi pour son secret. »

« En outre, il est impossible à l'électeur de savoir si l'information enregistrant son vote a correctement retranscrit le choix qu'il a effectué et si cette information, à la supposer correcte, n'a pas été modifiée en cours d'acheminement jusqu'au serveur collectant les "bulletins électroniques". »

« En d'autres termes, l'électeur valide son choix sur son ordinateur mais n'a aucune garantie que son vote ait été bien pris en compte, ni que le sens de son vote n'a pas été altéré. »

« Autre point d'achoppement : on ne peut savoir avec certitude quel a été le vote émis. Il n'est pas sûr, pour des raisons techniques, que ce soit le même que le vote enregistré. »

1 C'est d'ailleurs à la suite de fraudes massives (qui n'avaient pas pu rester dissimulées) que le vote par correspondance avait été banni des élections politiques en 1975.

2 Graton, Jean-Didier. Le contentieux électoral en matière politique. EHESS, Le genre humain "La démocratie dématérialisée – enjeux du vote électronique", septembre 2011. (ISBN 978-2-02-105480-4 – ISSN 0293-0277)

« En matière de vote à distance, la sécurité est d'autant plus délicate à garantir que la puissance publique n'a aucune prise ou moyen de contrôle sur le terminal qui sert à l'électeur à voter. L'électeur choisit librement le terminal de vote, le plus souvent un ordinateur personnel. Or, comme le rappelaient les représentants de l'agence nationale de sécurité des systèmes d'information (ANSSI), les moyens pour parer tous les risques informatiques sont hors de prix pour un simple particulier. Ce risque est d'autant plus fort que selon les électeurs, les terminaux varient, de même que les logiciels et les navigateurs. »

« En fait, le vote électronique relève aujourd'hui d'une modernité obsolète. »

Fédération des Associations Françaises des Sciences et des Technologies de l'Information (ASTI)

L'ASTI, aujourd'hui disparue, a fédéré des associations professionnelles et scientifiques d'informaticiens³ (rassemblant plusieurs milliers de membres dont de nombreux chercheurs). En 2007, l'ASTI a pris position sur le sujet du vote électronique (et donc du vote par internet) :

« La Fédération des Associations Françaises des Sciences et des Technologies de l'Information appelle à ne pas recourir au vote électronique anonyme au nom du principe de précaution.

L'ASTI est convaincue que les sciences et technologies de l'information peuvent contribuer positivement au développement de la démocratie. Elle tient cependant à alerter les pouvoirs publics sur l'impossibilité, en l'état actuel de la technologie, de réaliser un vote anonyme contrôlable directement par les électeurs et en conformité avec les dispositions de la Constitution et du Code électoral. Des recherches se développent mais n'ont pas encore abouti à des systèmes permettant l'exercice d'un contrôle démocratique indiscutable.

Dans l'attente de ces avancées scientifiques et technologiques, l'ASTI recommande que de telles recherches soient poursuivies et que pouvoirs publics, partis politiques et société civile ne recourent en aucune manière au vote électronique anonyme, y compris au moyen de machines à voter. »

³ <http://www.asti.asso.fr/>