Les systèmes décentralisés sans tiers de confiance un renouveau pour les protocoles électoraux ?

Stéphane Grumbach
INRIA

2 août 2014

Les systèmes de vote jouissent dans de nombreux pays d'un usage si ancien qu'ils paraissent aussi immuables que les institutions politiques et culturelles. Mais à l'évidence, alors que le nombre des gestes que l'on peut réaliser directement sur un terminal mobile, y compris de manière sécurisée comme les paiements par exemple, augmente, le vote papier semble relever d'un archaïsme grandissant, tant il est lourd et coûteux à mettre en oeuvre, et contraignant pour les électeurs. Ce sont bien sûr ses propriétés de fiabilité et de confidentialité, mais peut-être plus encore l'attachement à la solennité du rituel du vote, qui expliquent le maintien de ce moyen dont l'usage est encore tout à fait dominant.

Dans le secteur privé, le vote en ligne progresse rapidement et de nombreuses entreprises y ont recours tant pour leurs personnels que pour leurs usagers ou clients. Les entreprises offrant des services de vote en ligne fleurissent pour répondre à la croissance de la demande, sans que les garanties offertes ne soient vraiment normalisées. Mais le numérique fait également son entrée dans la sphère politique, tout au moins dans certains pays. C'est le cas en particulier en France pour le vote des Français de l'étranger. Un récent rapport [1] du Sénat suggère toutefois de maintenir le moratoire de 2007 sur l'utilisation des machines électroniques dans la sphère politique, et de limiter le vote en ligne aux circonscriptions à l'étranger.

Le vote électronique pose un problème fondamental. En effet, il est essentiellement impossible avec un protocole dématérialisé de préserver le même niveau de garantie que pour le protocole mécanique existant, en particulier le secret du vote et l'authenticité du suffrage comme le montre bien François Pellegrini [2]. La complexité des systèmes numériques, avec les différentes couches logicielles, matérielles et réseaux, rend illusoire aujourd'hui la vérification de l'ensemble du système et sa certification. De plus alors que le protocole mécanique est compréhensible et vérifiable par tout électeur, sans connaissance préalable, le recours à un système dématérialisé requiert une confiance dans la technologie.

0. https ://who.rocq.inria.fr/Stephane.Grumbach/
IXXI – ENS Lyon – Site Jacques Monod — 15 parvis René Descartes – BP 7000 — 69342 Lyon Cedex 07

1. http ://www.senat.fr/notice-rapport/2013/r13-445-notice.html

2. François Pellegrini. Chaînes de confiance et périmètres de certification : le cas des systèmes de vote électronique. Rapport de recherche INRIA n 8553. juin 2014.

Ces difficultés conduisent les responsables politiques à conserver les protocoles de vote mécanique existant afin de préserver ces propriétés essentielles pour la bonne tenue des élections. Le vote, fondement de notre système politique, est donc un point singulier dans notre environnement. Alors que le numérique pénètre tous les secteurs en bouleversant profondément le fonctionnement de la société, alors que le monde politique s'engage avec les données ouvertes à rendre transparente toute son action, alors que les citoyens ont une capacité d'expression décuplée par les media sociaux, notre système de vote semble devoir rester immuable.

Une telle singularité mérite qu'on s'y arrête. Serait-ce que le système de vote actuel donne pleinement satisfaction et que par conséquent rien ne justifierait l'évolution vers un système simplement moins bon ? Est-ce vraiment le cas ? On peut en douter. La participation aux scrutins politiques a tendance à baisser dans les démocraties européennes. Comme l'observe très bien Pierre Rosanvallon, la démocratie se complexifie, avec ce qu'il appelle la "contre-démocratie", qui "n'est pas le contraire de la démocratie ; c'est plutôt la forme de démocratie qui contrarie l'autre, la démocratie des pouvoirs indirects disséminés dans le corps social, la démocratie de la défiance organisée face à la démocratie de la légitimité électorale" [3].

Au-delà de la question technique du mode de recueil des suffrages, la manière de les exprimer et de les compter est également discutable. Fortement étudiés à l'époque de Condorcet, les modes de choix font l'objet d'un regain d'intérêt aujourd'hui, tant aux niveaux théorique qu'expérimental. Certaines études montrent clairement comment la limitation de la capacité de choisir des protocoles politiques actuels, basés sur le choix d'un unique candidat par l'électeur, peut conduire à des résultats contraires aux préférences de la population [4]. Les résultats de ces études ne sauraient être ignorés, tant le vote risque de devenir par trop réducteur face aux capacités décuplées d'exprimer et de recueillir des opinions offertes par le numérique.

Le risque que représenterait l'adoption de protocoles de vote en ligne est-il simplement limité à la perte des bonnes propriétés des protocoles mécaniques utilisés actuellement ? Nous ne le croyons pas. Il convient de rappeler deux points essentiels au sujet du risque.

Premièrement, les systèmes numériques contrôlent aujourd'hui des aspects fondamentaux de nos organisations, y compris dans les domaines les plus critiques. La sécurité nucléaire, le contrôle aérien, pour ne citer que des exemples médiatiquement sensibles, reposent sur des systèmes numériques dont on ne peut garantir la fiabilité de manière absolue. Les risques encourus par la société ne sont pas minces. Mais les choix ont été fait au niveau politique d'encourir de tels risques, jugés acceptables au vu des bénéfices.

Deuxièmement, le vote, comme beaucoup d'autres choses, n'est pas une opération dont on peut garantir la fiabilité de manière absolue. L'un des intérêts du vote avec des bulletins pré-imprimés introduits dans une urne transparente est d'être comprehensible par tous. Le protocole présente toutefois des failles, dont la presse se fait régulièrement l'écho. Les erreurs ou les fraudes dans le décompte des bulletins sont toujours possibles. De surcroît, les moyens de surveillance miniaturisés dont nous disposons aujourd'hui augmentent les risques. Il n'est désormais plus si facile de garantir le secret de l'isoloir, et d'éviter les problèmes de coercition

3. Pierre Rosanvallon. La contre-démocratie : La politique à l'âge de la défiance. Seuil, 2006.
4. Michel Balinski, Rida Laraki. Majority Judgment Measuring, Ranking, and Electing. MIT Press 2011

par exemple.

Les raisons des résistances à l'adoption de protocoles de vote en ligne sont, à notre sens, avant tout politiques. Le vote en ligne constitue une rupture fondamentale, qui est loin d'être seulement technologique. Le vote sur machine électronique, aujourd'hui largement utilisé aux Etats-Unis en particulier, s'il pose la question de la confiance — la machine électronique ayant des propriétés différentes de l'urne avec des bulletins papier purement mécanique — ne change pas radicalement l'organisation du vote, dans un espace spatio-temporel, le bureau de vote, bien délimité.

Le vote en ligne s'inscrit par contre dans l'espace déterritorialisé ouvert par la révolution numérique. Il met la capacité de voter au bout des doigts, où qu'on soit, à tout moment, abolissant le bureau de vote physique. La suppression de la complexité du vote, tant au niveau de l'organisation de l'élection que de la participation des électeurs, est une révolution majeure qui permet l'organisation d'un nombre potentiellement illimité d'élections, y compris hors cadre institutionnel, dont l'initiative peut revenir à n'importe quel citoyen.

Certains mouvements politiques appellent de leurs voeux le développement de telles capacités démocratiques. Certains pays comme l'Islande en ont fait l'expérience. Quelques soient les risques qu'il feront encourir aux systèmes politiques en place, il nous parait plus que probable que ces systèmes se développent et soit largement adoptés, parmi les autres media sociaux. Cette disruption politique parait répondre à l'aspiration qui se fait jour dans de nombreux pays d'une démocratie plus continue, permettant une expression des citoyens au fil de l'eau. L'organisation politique devra s'adapter. Il est donc nécessaire d'y réfléchir.

Les protocoles de vote en ligne utilisés aujourd'hui reposent massivement sur la cryptographie pour l'authentification des électeurs, et pour la transmission et le stockage de leurs votes. Nous pensons que la cryptographie ne saurait suffire pour assurer aux protocoles de vote en ligne des propriétés satisfaisantes. D'abord comme l'a bien montré François Pellegrini, "la cryptographie robuste protège contre les tiers absolus, mais aucunement contre les tiers de confiance chargés de la mettre en oeuvre". En d'autre termes, l'institution qui organise l'élection dans le cas du vote dématérialisé est toujours sujette à caution.

La concentration de la donnée est un enjeu de pouvoir essentiel dans le monde numérique. Les entreprises qui concentrent la donnée rivalisent désormais avec les pétroliers au rang des plus grandes capitalisations mondiales. Cette concentration soulève de nombreuses interrogations au niveau politique. Il a été montré par exemple qu'un biais dans les réponses d'un moteur de recherche pourrait influencer le choix des électeurs [5]. De telles interrogations invitent à repenser sérieusement les modes de choix utilisés pour designer les responsables politiques.

Reconsidérons le protocole de l'élection à proprement parler. La concentration des bulletins dématérialisés, aussi cryptés soient-ils, nous parait devoir être évitée. Même si l'organisateur est un tiers de confiance au-dessus de tout soupçon, même si le secret du vote a été préservé lors de l'élection, personne n'est en mesure de garantir que les données ne seront pas obtenues par des tiers malveillants. Les données peuvent alors faire l'objet de tentatives

5. http://www.washingtonpost.com/opinions/could-google-tilt-a-close-election/2013/03/29/c8d7f4e6-9587-11e2-b6f0-a5150a247b6a_story.html

de décryptage. En tout état de cause, l'évolution des technologies conduit aujourd'hui à une fragilité des techniques d'encryption à une échéance de dix à vingt ans, c'est-à-dire que les votes des électeurs ont une probabilité tout à fait non négligeable d'être découvert à terme.

Pour éviter l'écueil de la concentration, il suffit de distribuer les données du vote chez les électeurs eux-même et de décentraliser le contrôle du processus électoral. Nous avons proposé un tel système [6], dont l'objectif est d'offrir les propriétés suivantes :

— Tout citoyen peut initier une élection ;
— Personne ne peut interrompre une élection en cours ;
— Nul ne stocke plus qu'une petite quantité des données de l'élection ;
— Tout le monde participe au recueil des bulletins et au calcul du résultat.

Le système que nous avons développé repose sur les standards du Web, se charge comme une application sur le navigateur, permet à l'utilisateur de voter, et assure au nom de l'utilisateur d'échanger avec les autres électeurs pour concourir au calcul du résultat. De surcroit, les électeurs échangent des bulletins de vote anonymisés, évitant ainsi l'écueil de la plupart des systèmes de vote en ligne qui invitent les électeurs à transmettre leur vote, ce qui constitue une fragilité majeure.

Le système est conçu comme une plateforme, et permet de supporter n'importe quel protocole de vote quelque soit le système de choix social adopté. Ses propriétés, radicalement nouvelles, répondent aux nouveaux possibles du monde numérique, en essayant de faire face à l'évolution des défis politiques.

6. S. Frénot, S. Grumbach, D. Reimert. *A P2P Protocol for Privacy Preserving Cooperative Decision Making*. Manuscrit.