



Groupe de travail sur le vote électronique déclaration de la délégation CGT

Lors de notre courrier à Mr De jekhowski du 29 novembre 2016 (resté sans réponse) nous rappelions la position de la fédération CGT des finances lors du premier groupe de travail dédié .

Nous sommes opposés à ce projet qui ne garantit en rien une meilleure démocratie et une meilleure efficacité de ce vote . Qui plus est , et malgré les arguments comparatifs présentés par le ministre, la très forte implication actuelle des agents du ministère dans le vote aux élections professionnelle ne peut souffrir la prise de risques pouvant entacher le bon déroulement d'un scrutin qui jusqu'à aujourd'hui était exemplaire.

Enfin lors de ce groupe de travail nous avions précisé qu'aucune discussion ne pourrait même être envisagée tant que les réponses aux questions techniques et de sécurité que nous avions posées ne seraient pas apportées. Le fait qu'un ministre affirme que les systèmes de vote électronique sont désormais à maturité n'en fait pas, loin s'en faut, une certitude technique au regard de tous les experts qui écrivent le contraire j'y reviendrai . Ce n'est parce que j'utilise un ordinateur que je suis un expert en informatique .

Aucun système n'est inviolable, le ministre ne peut pas garantir totalement la sécurité du vote. Des chercheurs ont réussi à montrer qu'il était possible de pirater à distance une urne électronique alors qu'elle n'était même pas reliée au réseau. Et nombre de sites Internet, même ceux dont la sécurité est extrêmement renforcée, se font pirater en permanence. Aucun logiciel n'est exempt de bug, donc par définition, le logiciel de vote pourra être « buggé » malgré tous les efforts qui pourront être mis en œuvre. Et c'est, en soi, un problème.

Le vote électronique a principalement été envisagé pour deux raisons. La première est de lutter contre l'abstention, notamment dans les élections politiques. La seconde est de réduire leur coût d'organisation (en particulier avec la fin de l'impression du matériel de vote mais aussi du temps nécessaire au dépouillement).

Dans nos ministères, l'abstention est très faible et l'a pour ainsi dire toujours été. Il n'est donc ici pas question d'augmenter les votes pour améliorer la légitimité des organisations syndicale, déjà très forte. Mais peut-être s'agit-il d'une volonté ministérielle d'affaiblir artificiellement les organisations syndicales. Pour ne prendre qu'un exemple, le taux de participation à l'Éducation nationale est passé de 61 % en 2008 (vote à l'urne) à 38 % en 2011 (vote électronique). Et malgré les efforts déployés, cette participation n'est remontée qu'à 41 % en 2014.

La faute en incombe à de nombreux dysfonctionnements dans le système de vote mais aussi à la complexité du vote électronique par rapport au vote à l'urne. Cette complexité impacte d'ailleurs plus fortement certaines catégories de personnel du fait des compétences informatiques nécessaires pour pouvoir voter. En cela, nous ne pouvons que considérer que **le vote électronique tel qu'il a été instauré dans la Fonction publique créé une rupture d'égalité devant le vote**.

Pour ce qui est de la réduction des coûts, si cet argument conserve une certaine pertinence, il faut toutefois faire **attention aux dérives budgétaires liées à l'informatique lorsqu'elle est mal maîtrisée**. Les exemples ont été nombreux par le passé, malgré les alertes de la CGT, qui, à tort, n'a pas été écoutée comme ce fut le cas pour Hélios, Chorus, Copernic, ONP, etc. Inutile de rappeler les dérives économiques importantes entraînées par ces mauvais choix quand il n'a pas été nécessaire de totalement abandonner les projets.

Sans parler aujourd'hui des difficultés techniques de Cybele ou du TES.

A l'heure actuelle, **le vote électronique a pour conséquence dans quasiment tous les endroits où il a été mis en place une baisse dans la légitimité des résultats électoraux**. Certes, le vote électronique peut faciliter les choses, mais seulement pour l'organisation du scrutin. Et surtout, à quel prix pour la démocratie ?

Car là est le vrai problème . Cette volonté de casser le système actuel ressemble plus à la volonté de fragiliser l'audience des OS qu'à faire prévaloir une véritable démocratie sociale dans le ministère . Et ce n'est pas le niveau catastrophique du dialogue social dans ce ministère et ses administrations qui peut nous rassurer .

Aucun système n'est pas fiable à 100% aujourd'hui.

La CNIL dans une délibération de 2010 indique « qu 'au cours des travaux qu'elle a menée , elle a pu constater que les systèmes de vote électronique existants (il s'agit ici d'élection politique mais cela ne change rien à l'affaire) ne fournissent pas encore toutes les garanties exigées par les textes légaux . Elle préconise en outre (j'y reviendrais puisque c'est une de nos propositions restées sans réponse) la nécessité pour tout vote électronique d'une expertise indépendante portant sur une série de mesures décrites dans la note de référence et que nous avons déjà demandé.

En 2013 le Sénat a publié un rapport d'information après avoir consulté un grand nombre de personnalités compétentes et indique en synthèse :

S'agissant de la sincérité du scrutin, aucune garantie n'existe que la personne qui a voté depuis l'ordinateur est le bon électeur. Les éléments d'authentification (identifiant et mot de passe) peuvent avoir été mal dirigés, détournés ou monnayés. En outre, lorsque l'électeur émet son vote, il n'a aucune certitude que le sens de son vote est celui finalement enregistré : il doit faire confiance au système électronique sans moyen concret de contrôle. Les membres du bureau de vote électronique et les délégués des candidats n'ont pas de moyens supplémentaires pour vérifier la fiabilité du système sans intermédiation technique. De même, aucun recomptage manuel n'est possible en cas de doute sur la fiabilité des résultats obtenus. S'agissant du secret du vote, contrairement à l'isoloir du bureau de vote, l'électeur peut voter depuis son ordinateur sous le regard d'un proche ou sous la menace. Enfin, cet exercice solitaire du devoir électoral rompt avec la solennité du vote, découlant du rituel républicain qui a cours dans un bureau de vote. ».

Enfin cerise sur le gâteau , lors d'une audition par la commission des lois constitutionnelles de l'assemblée nationale en Janvier de cette année, le Directeur général de l'anssi , c'est à dire l'Agence Nationale de Sécurité des Systèmes d'Information , agence qui dépend du 1er ministre , en charge des questions de cyber-sécurité et de prévention , indique « **ne pas être favorable au vote électronique , car lorsqu'on met en regard aujourd'hui les capacités de sécurisation dont nous disposons , même avec beaucoup d'efforts et l'intervention de gens très sérieux , et le niveau des attaquants potentiels , qui font probablement partie des meilleurs , il est difficile d'être totalement rassuré »**

Mais heureusement le Ministre lui , peut nous assurer que c'est sans risque ..

Enfin nous noterons que pour une fois , l'idée ne vient pas de l'étranger .. d'habitude on copie ce qui se fait ailleurs puisque c'est toujours mieux . La non ... vous savez pourquoi ?

Au Royaume Uni , le vote électronique a été envisagé puis abandonné . Idem en Irlande . Rien en Espagne , en Italie et au Portugal ...En Allemagne une décision de la cour suprême a conduit à la cessation complète de ce type de vote . Au pays Bas , abandonné depuis 2008 , pas assez sûr.

Heureusement il vous reste la Suisse et L'Estonie !

On nous dit il faut avoir confiance ...

Avoir confiance. C'est là le maître mot du vote électronique. Il faut avoir confiance. Confiance en la technologie. Confiance à la société qui a conçu et fourni la machine, le logiciel. Confiance à la société qui a agréé la machine. Confiance au Ministère de l'Intérieur qui a agréé la société d'agrément. Confiance dans le ministère qui l'a mise en service. Confiance aux liaisons numériques qui acheminent les résultats. Bref, il faut avoir un peu trop confiance à un peu trop de monde qui aurait intérêt à modifier les résultats, pour qu'un électeur puisse être confiant en la sincérité du vote. Or, cette confiance en la sincérité du vote est l'un des fondamentaux essentiels d'une démocratie. ».

Cette confiance nous ne l'avons pas . Le sénat a raison . Le vote c'est le rapport entre le votant et son bulletin , son bulletin et l'urne . Ce rituel républicain que le plus grand nombre pratique et apprécie.

Nous vous demandons solennellement de retirer ce projet . Nous ferons tout ce qui est en notre pouvoir et en celui de la CGT au plus haut niveau pour bloquer y compris sur le plan juridique cette réforme , même si nous devons aller contester les résultats en justice lorsque la réalité démontrera que nous avions , une fois de plus , raison .

1/ Transparence de la machine et du logiciel

Tout d'abord, le code source de l'ensemble des briques logicielles et système des machines sur lesquelles reposent le système de vote électronique doit être ouvert et ses licences libres. Il en va de même pour le logiciel de vote lui-même. Il ne peut être accepté de laisser une entreprise, dirigée par des capitaux ayant leurs propres intérêts, créer un système de vote dans lequel la confiance ne pourra être assurée. Il s'agit là d'une garantie de transparence indispensable à toute forme de démocratie.

Si dans cette entreprise les développeurs en charge du projet sont fortement opposés à la CGT, quelle qu'en soit la raison, alors il leur est possible de rendre le code volontairement complexe et d'introduire un petit mécanisme minimisant les votes réellement effectués pour notre organisation. Nous en revenons à mon avis à l'exigence principale qui doit être la nôtre si ce vote se confirmait c'est l'**obtention du code source du système de vote pour son analyse**. Dans ce cas, et suivant le langage utilisé, il faudra peut-être prévoir un recours à une entreprises d'audit pour vérifier que l'outil fait bien ce qu'il doit faire.

Lors d'un vote électronique, il est totalement impossible de suivre toute la mécanique du vote. C'est le plus gros point noir en matière de démocratie. A l'inverse, le vote à l'urne permet cette transparence.

2/ Un expertise du code

L'administration doit garantir aux organisations syndicale qui le souhaitent, à ses frais, la possibilité de faire expertiser l'ensemble des briques logicielles et système sur lesquelles reposent le système de vote électronique. Idem pour le logiciel de vote lui-même. Chaque organisation syndicale doit pouvoir choisir le cabinet d'audit qui lui convient. De même, la sécurité du réseau informatique hébergeant le système de vote doit pouvoir être audité afin de s'assurer qu'il n'y a aucun filtrage en amont qui pourrait entraîner l'impossibilité de voter pour certains agents, certains services,...

3/ Un système d'authentification renforcé

Le système d'authentification permettant aux électeurs de voter devra être tout à la fois être simple et hautement sécurisé. Un système de jeton, à usage unique, pour chaque votant pourrait être mis en place. Avec un bulletin signé par ce jeton, il devra être possible de vérifier l'ensemble des bulletins présents dans l'urne et s'assurer qu'ils sont tous valables. L'ensemble du dispositif doit être crypté de bout en bout avec une sécurité forte et certifiée.

4/ Sécurité des machines

L'accès aux machines doit tout à la fois être hautement sécurisé et rendu possible à l'ensemble des organisations syndicales qui en feraient la demande. A tout moment, il doit être possible de vérifier que les machines n'ont pas fait l'objet d'un bourrage électronique, d'un piratage informatique, d'un changement dans le code source du logiciel, etc. Cette sécurité doit pouvoir être garantie par le fait qu'aucune des briques logicielles et système n'aient été modifiées après installation et expertise par les organisations syndicales ou le cabinet d'audit qu'elles auront choisi. Des systèmes de somme de contrôle peuvent être mis en place. Il en va de même du système de base de données, élément crucial puisque contenant l'ensemble des votes.

5/ Aucun système n'est inviolable

L'administration ne peut pas garantir totalement la sécurité du vote. Des chercheurs ont réussi à montrer qu'il était possible de pirater à distance une urne électronique alors qu'elles n'étaient même pas reliées au réseau. Et nombre de sites Internet, même ceux dont la sécurité est extrêmement renforcée, se font pirater en permanence. Est-il utile de rappeler le piratage de la Direction générale du Trésor par des hackers il y a

quelques années de cela ? Aucun logiciel ne contient aucun bug, donc par définition, le logiciel de vote sera buggé malgré tous les efforts qui pourraient être mis en oeuvre. Et c'est, en soi, un problème.

Par ailleurs, jusqu'ici, les logiciels de vote utilisés reposent principalement sur la technologie Java. Celle-ci est l'une de celles qui recensent chaque année le plus de failles de sécurité. Il s'agit donc d'un vrai appel pour les hackers en tout genre. Qui plus est, il est indispensable d'installer Java sur son ordinateur pour pouvoir voter. Et cette couche logicielle impose quasiment l'installation de logiciels espions sur l'ordinateur. Il n'est donc pas acceptable d'exiger ce type d'installation sur les ordinateurs des agents qui souhaiteront voter électroniquement à partir de leur domicile.

6/ Accessibilité du système de vote

Le système de vote doit être simple et permettre à chaque agent, quels que soient ses compétences, sa situation, son âge, ses handicaps, etc d'accéder facilement au vote. Le système de vote électronique ne doit pas créer de rupture entre les agents devant l'accès au vote. Il s'agit là d'un principe de base de la démocratie. Nous attirons particulièrement l'attention sur les ouvriers, agents de gardiennage, agents de nettoyage, etc qui n'utilisent pas l'outil informatique au quotidien. Mais aussi les agents non sédentaires (douaniers , vérificateurs ..)

L'autre catégorie de population pour laquelle il faut particulièrement veiller à l'accessibilité du système de vote sont les personnes en situation de handicap. Il faut impérativement que l'outil utilisé pour le vote leur permette de voter simplement.

Dans les questions d'accessibilité se pose aussi le bon fonctionnement de l'outil à partir de l'intranet mais aussi d'Internet. Chaque agent doit pouvoir voter d'où il le souhaite. Le système de vote doit également tenir la charge du vote et ne pas être indisponible pour les électeurs. Ce fut le cas en 2011 à l'Éducation nationale (entre autres dysfonctionnements) et cela a entraîné de nombreux découragements, en témoignent le niveau de participation.

7/ Quid du recomptage en cas de litige ?

En cas de doute ou de litige, il n'y a pas de recomptage possible. La machine ne fera que ce qu'on lui a dit de faire. Le vote électronique est donc lié au code (voir point 1), dans le cas qui nous préoccupe, d'une entreprise privée. En cas de vote à l'urne, le recomptage est possible.

Alors en attendant un vote électronique fiable, sécurisé et transparent, vive le vote à l'urne... transparente ! Nous devons considérer le vote électronique comme étant destiné à faire baisser artificiellement la représentativité de certaines organisations compte-tenu de la composition des votes observés lors des précédentes élections professionnelles. Nous utiliserons donc tous les recours possibles pour ne pas laisser ces manœuvres politiciennes et anti-démocratiques se mettre en place aux Finances.