# Interprétation incorrecte de la "vérifiabilité" du vote électronique CH

Le principal argument invoqué en faveur de la sécurité est la vérifiabilité : l'individu, où chacun peut vérifier son propre vote, ainsi que l'universel, où un bureau central peut vérifier l'exactitude du résultat.

**Résumé :**

**La vérifiabilité universelle est formellement exigée par la Chancellerie fédérale en tant que "vérifiabilité complète". Mais elle ne peut jamais être atteinte, car elle exige qu'il soit possible de déterminer au niveau central si tous les votes de ceux qui ont le droit de vote sont arrivés correctement et ont été traités correctement. Cependant, si cela ne peut pas être garanti déjà dans l'appareil de l'utilisateur (à cause de l'insécurité du processus d'orientation de l'utilisateur), c'est impossible jusqu'au bout. Ces faits sont également reconnus et communiqués par la BFH. Néanmoins, la Chancellerie fédérale n'en tient pas compte, ce qui conduit à la reconnaissance des solutions existantes.**

- **Pourquoi avons-nous besoin d'une vérifiabilité individuelle (VI) ?**

Avec VI, l'électeur obtient son droit de vote en toute sécurité. Avec VI, l'électeur peut vérifier si son vote est arrivé comme il le souhaitait. Si le processus sur le périphérique d'entrée fonctionne parfaitement et n'est pas falsifié par une cyberattaque, il est guidé par l'utilisateur et sait toujours ce qui vient ensuite et comment interpréter les affichages. Les entrées de code et les contrôles de code alternent avec la carte de vote reçue par la poste.

Cette carte de vote avec ses codes doit être envoyée par la poste, car tout code généré électroniquement pourrait être falsifié par la même cyberattaque et avoir au mieux l'effet inverse de ce que l'utilisateur souhaite. L'utilisation d'un 2ème chemin de communication pour la transmission du code fait partie de la sécurité que vous voulez créer.

Seule cette procédure manuelle encombrante garantit VI sur l'appareil d'entrée non sécurisé. Si le processus sur l'appareil de saisie (téléphone portable, ordinateur) ne fonctionne plus correctement à 100% ou si quelque chose d'incorrect s'affiche, l'utilisateur doit le reconnaître et n'a alors la possibilité de voter que sur le chemin postal ou à pied jusqu'à l'urne.

Malheureusement, il est facile d'utiliser des informations linguistiques manipulées à l'écran et des invites qui ne devraient pas être prises en compte afin de ne pas mettre en danger l'intraveineuse. L'absence d'un seul code de vérification ou de finalisation ou l'entrée prématurée du code de confirmation peut entraîner une manipulation ou un vote manqué, ce que l'utilisateur ne remarquera que s'il mémorise le processus complexe.

Toute simplification par des moyens électroniques tels que les "nouvelles applications" qui pourraient être utilisées pour la saisie comporterait à nouveau le risque inhérent de manipulation et ne pourrait plus être surmontée avec VI. Par conséquent, toute approche visant à simplifier cette procédure compliquée porterait un coup fatal à la vérifiabilité de E-Voting CH, car la vérifiabilité universelle offerte par E-Voting CH n'est pas indépendante et ne fonctionne qu'avec l'application complète de VI.. Les fournisseurs de ces aides devraient être reconnus immédiatement et à l'unisson

comme des manipulateurs potentiels et donc interdits. S'il était connu, le BK émettrait certainement des recommandations pour ne pas les utiliser.

Cependant, comme on ne peut ni supposer que tous les utilisateurs se comportent correctement ni qu'il n'y a jamais d'incitation à simplifier cette procédure compliquée, VI ne peut être reconnue que comme une garantie théorique de la découverte d'une manipulation possible. Cependant, en tant que droit de l'individu, la procédure répond aux exigences.

- **Pourquoi avons-nous besoin d'une vérifiabilité universelle ?**

Comme ce fait est connu des gens qui travaillent dans le domaine scientifique, ils ont exigé la vérifiabilité universelle en plus de la vérifiabilité individuelle. Il s'agit là d'une question de vérification par tout organe central de l'exactitude du résultat global, ce qui est une obligation de l'État d'assurer la détermination correcte de la volonté du peuple.

Désormais, chaque électeur devrait donc pouvoir communiquer en toute sécurité à l'État si son vote est arrivé à bon port. Comme nous l'avons vu à VI, il l'a fait, mais seulement dans les cas où il n'utilise pas un dispositif manipulé ou reconnaît la manipulation de celui-ci et utilise ensuite un canal d'accord alternatif.

Tous les autres cas (non-détection, remise, vol de code, etc.) ne peuvent être détectés que si tout le monde doit divulguer publiquement s'il a été capable d'utiliser VI correctement. Mais cela n'est pas possible non plus, car ces informations sont également soumises au secret du vote. Nul ne peut être contraint de révéler s'il a voté ou non. D'ailleurs, presque personne n'annoncerait publiquement qu'il ne maîtrise pas la procédure, parce qu'on n'est jamais sûr d'avoir tout fait comme il faut.

Étant donné que l'individu a également droit à la détermination correcte de l'ensemble de la volonté du peuple, et pas seulement du droit de faire compter correctement son propre vote, la vérifiabilité universelle doit se faire de telle sorte qu'elle ne dépende pas de tous les autres électeurs, qui n'ont peut-être pas compris toutes les procédures complexes ou qui ont été trompés par une attaque informatique.

Avec la conception actuelle de l'E-Voting CH, cela n'est pas garanti. Par conséquent, on ne peut pas parler de vérifiabilité universelle. L'expression "vérifiabilité totale", telle qu'elle est utilisée par la Chancellerie fédérale, ne représente rien de plus qu'une tentative d'obscurcir le problème par des termes apparemment scientifiques.

La première est (uniquement) liée au droit de l'individu et (uniquement) au devoir de l'Etat. Mais les deux devraient s'appliquer aux deux.

Par conséquent, nous arrivons à la conclusion que la vérifiabilité universelle du vote électronique CH n'est pas possible dans les conditions légales données et ne respecte pas le secret du vote.

La Chancellerie fédérale compte sur le fait que ceux qui remarquent une manipulation le signaleront quand même. C'est peut-être vrai, mais comment ces gens sont-ils traités et entendus par la suite ? Et quelle est la conclusion ultime à tirer quand on sait que seule une petite fraction de la personne lésée nous contacte ? Qui sera alors responsable de ce qui doit être fait ? Voulons-nous répéter le vote ou non ? Ces messages n'étaient-ils peut-être qu'un prétexte pour se répéter ? Qui va vérifier tout ça et comment ? Vous pouvez peut-être trouver des traces, mais combien ? Vous n'en trouvez

peut-être pas. Parce que ces enquêtes sont arbitrairement complexes, longues et exigent des connaissances médico-légales spéciales de la plus haute qualité. Le délai pour s'opposer à un résultat du vote est de 6 jours. Pendant ce temps, l'administration ne parviendra à rien du tout.

Alors qu'est-ce que ça veut dire ? Toutes ces questions relatives à la gestion des risques n'ont pas été clarifiées lors de l'introduction de l'E-Voting CH. Le seul résultat certain d'un tel processus est un chaos énorme et la perte de confiance dans les processus démocratiques.

- **Comment fonctionne la "vérifiabilité totale" du POST (vérification de l'authenticité du comptage) ?**

Lors du contrôle de comptage, le POST suppose qu'un problème éventuel (cyberattaque) se situe sur une partie du système et si cette partie est gérée de manière redondante et que la séquence est gérée via les deux redondances, que l'erreur est découverte par formation de différence. Cette hypothèse est correcte en principe, mais elle comporte un nombre énorme d'écueils.

Bien que les composants du système puissent être gérés de manière redondante, le fabricant (et pas seulement le fournisseur) doit également être géré de manière redondante. La question est de savoir si vous savez vraiment qui est le fabricant de ma pièce système ? Que se passe-t-il si "Fabricant 1" achète également ses pièces (puces, intergiciels, logiciels, compilateurs, etc.) auprès du même sous-traitant que "Fabricant 2" ? Quiconque travaille en informatique sait qu'il ne dispose jamais de ces informations et que de nombreux composants système proviennent des mêmes grandes entreprises (Intel, AMD, Microsoft, Apple, etc.). Il en résulte que les points faibles sont automatiquement localisés sur des systèmes redondants.

En outre, les opérateurs de ces systèmes devraient également être séparés, faute de quoi il ne serait pas garanti que l'un ou l'autre des opérateurs manipulerait les deux systèmes s'il y avait une incitation correspondante à le faire. Il faudrait aussi mener le contrôle des opérateurs de manière redondante, car sinon un supérieur hiérarchique pourrait initier une manipulation correspondante, par exemple sous le prétexte d'une mise à jour nécessaire.

En raison de la complexité de ces contrôles des écarts de toutes les parties du système, vous avez également besoin de procédures d'aide correspondantes qui affichent les écarts et, par conséquent, l'authenticité des résultats du comptage. Si ceux-ci n'indiquent pas de différence, on suppose qu'ils sont corrects. Mais maintenant, vous devez vous assurer que ces procédures ne sont pas manipulées. Vous ne pouvez vous en assurer que c'est le cas que si vous disposez d'autres outils pour le vérifier. Ce cycle pourrait se poursuivre jusqu'à ce qu'un chef opérateur intelligent dise : "J'ai tout sous contrôle". Mais je suppose qu'il est le seul à pouvoir juger ça. Ou parle-t-il par manque d'expérience ou par surestimation excessive de lui-même parce qu'il ne connaît pas ses adversaires ? Et : pouvons-nous ou devons-nous lui faire confiance ?

Même si tout était fait à la perfection et si les employés étaient dignes de confiance : Il est arbitrairement complexe et ne peut être négligé par des étrangers, surtout pas par la commission électorale qui en est responsable.

Le 11.9.2018, le Parlement a coulé un pas en avant qui exigeait la transparence des processus, tout comme cela est également exigé dans le cadre des droits de l'homme pour la crédibilité d'une démocratie. Avec cette édition, on ne voit plus aucune possibilité d'y utiliser le vote électronique et fait référence à des processus que tout le monde ne peut pas comprendre sans connaissances

spécifiques, même dans le cas du vote classique. La différence frappante entre les exigences pour comprendre le "double Pukelsheim" et l'informatique moderne est élégamment ignorée. Une deuxième avance, qui n'exigeait qu'un moratoire, n'avait aucune chance non plus.

Une conséquence demeure: la démocratie devient une expertocratie. La question est de savoir si nous le voulons.