30 mai 2018

Vote électronique : publication du code source

Rapport explicatif sur la modification de l’ordonnance de la ChF sur le vote électronique (OVotE)

1 Contexte

Lors de sa séance du 5 avril 2017, le Conseil fédéral a arrêté les prochaines étapes en vue de l'introduction généralisée du vote électronique. Il s'agissait notamment de mesures visant à accroître la transparence et du passage de la phase d'essais actuelle à la mise en exploitation du vote électronique.

Pour accroître la transparence, le Conseil fédéral a décidé d'inscrire une condition supplémentaire dans le droit fédéral pour pouvoir recourir au vote électronique, à savoir la publication du code source. Le Conseil fédéral a chargé la Chancellerie fédérale de procéder aux modifications nécessaires de l'ordonnance de la ChF sur le vote électronique (OVotE ; RS 161.116).

2 Davantage de transparence demandé

La vérifiabilité individuelle et la vérifiabilité complète (art. 4 et 5 OVotE) sont deux exigences que la Confédération pose dans le domaine de la transparence. La vérifiabilité complète, qui repose sur les données générées pendant un scrutin, permet d'établir que les suffrages ont été enregistrés et traités correctement. Ce n'est qu'une fois que la vérifiabilité complète aura été mise en œuvre et que les systèmes auront été certifiés que les conditions juridiques nécessaires à l'introduction généralisée du vote électronique seront remplies. Le développement de la vérifiabilité complète est en cours et devrait être achevé d'ici à la fin de l'année 2018, d'après la planification établie par les fournisseurs des systèmes de vote électronique.

Dans le cadre de l'examen d'interventions parlementaires ou dans les réponses qu'il leur a données, le Conseil fédéral a assuré à plusieurs reprises à l'Assemblée fédérale qu'il avait « l'intention d'examiner de manière approfondie avec les cantons la question de l'accès au code source, en vue de conditionner l'autorisation des systèmes à cet accès lors de la prochaine révision des bases légales »[1]. Par ailleurs, lors du débat concernant la motion Schwaab 13.3808, intitulée « Pas de précipitation en matière d'extension du vote électronique », l'assurance a été donné que la Confédération et les cantons examineraient la question de l'organisation de tests publics d'intrusion. Cet examen a eu lieu en 2016 dans le cadre des travaux du sous-groupe de travail « Transparence et public ». Dans le souci d'accroître la transparence, les fournisseurs des systèmes de vote électronique ont déjà pris des mesures et publié des informations sur le fonctionnement des systèmes.

[1] Motion Romano (Darbellay) 15.3492 « Pour un système de vote électronique public et transparent », motion Reimann 15.4237 « Vote électronique. Transparence indispensable » et question Schwaab 16.1076 « Un test grandeur nature de la sécurité du vote électronique ? »

3 Commentaire des dispositions

Le code source est le texte d'un programme informatique. Écrit par l'homme et pouvant être lu par l'homme, il décrit le fonctionnement du programme informatique. Il convient d'opérer une distinction claire entre la publication du code source et la mise en œuvre de la vérifiabilité complète. Alors que le code source établit *comment* les suffrages *doivent* être enregistrés et traités par le système, les informations recueillies aux fins de la vérifiabilité complète établissent *que* les suffrages *ont été* enregistrés et traités correctement.

La publication d'informations peut renforcer la confiance du grand public et la pérenniser. D'une part, elle permet aux milieux spécialisés d'acquérir à tout moment la conviction que les systèmes sont sûrs et de qualité. À l'inverse, les autorités ont la possibilité d'opérer préalablement les améliorations nécessaires au cas où des experts externes découvriraient des lacunes. D'autre part, la publication d'informations contribue à rendre le débat objectif et agit contre la dépendance vis-à-vis de certaines organisations ou personnes.

Art. 7, al. 2, let. f, et 3, OVotE

L'art. 7 OVotE est complété par une distinction relative au contrôle. Cette distinction a un rapport direct avec les nouvelles dispositions sur la publication du code source, lesquelles figurent aux art. 7*a* et 7*b* OVotE. La publication du code source doit intervenir *après* la fin du développement de la vérifiabilité complète et *après* la certification. La modification de l'art. 7 OVotE pose le principe selon lequel l'utilisation d'un système proposant la vérifiabilité complète requiert des certifications, indépendamment du plafond sur lequel porte la demande. Cependant, dans les cas où il s'agit de permettre à 30 % au maximum de l'électorat cantonal de participer à un essai, la certification peut se limiter, du côté des fournisseurs de système, au système et à son exploitation. La certification des procédures cantonales, de l'imprimerie et du logiciel du portail de cyberadministration n'est toutefois pas requise dans ce cas de figure (voir notamment les restrictions visées à l'art. 7, al. 3, let. b et c, OVotE).

Art. 7a, al. 1, OVotE

Le code source du logiciel du système doit être publié dans une forme bien lisible. Le terme « logiciel » désigne la mise en œuvre, au niveau de l'application, du protocole cryptographique pour la vérifiabilité complète. Sont ainsi concernés en particulier la génération des éléments cryptographiques secrets, le contrôle de la validité, l'enregistrement des suffrages entrants, le mélange cryptographique des suffrages enregistrés, le décryptage des suffrages et l'établissement des preuves qui résultent de la vérifiabilité complète au sens de l'art. 5 OVotE moyennant l'utilisation des composants de contrôle.

Avant que les cantons déposent leur demande d'octroi d'une autorisation générale, il faut laisser suffisamment de temps pour que des personnes intéressées aient la possibilité d'analyser les documents et de présenter leurs résultats aux autorités et aux fournisseurs des systèmes de vote électronique.

Vote électronique : publication du code source, modification de l'OVotE

Art. 7a, al. 2, OVotE
Le code source des systèmes doit être publié *après* la fin du développement de la vérifiabilité complète et *après* la certification. La date de la publication est fixée par le renvoi à la réglementation figurant à l'art. 7, al. 2 et 3, OVotE. La publication du code source peut potentiellement déclencher des réactions de la part du public (par ex. des fausses nouvelles (*fake news*). En effectuant un contrôle préalable crédible, il est possible de faire en sorte que les opportunités liées à la publication l'emportent sur les risques inhérents à cette publication.

Art. 7a, al. 3, OVotE

- Let. a : Le recours à des composants propriétaires standard (systèmes d'exploitation, bases de données, serveurs web, serveurs d'application, systèmes de gestion des droits, pare-feu, routeurs) doit aussi être possible sans que leur code source soit publié. À cet égard, une réserve s'applique, à savoir que le composant standard soit utilisé à grande échelle et, par conséquent, mis à jour en permanence. Par ailleurs, la configuration du composant standard doit être décrite dans la documentation relative au système et à l'exploitation si elle revêt une importance pour instaurer la confiance.

- Let. b : Le code source d'un portail de cyberadministration par lequel transitent les suffrages cryptés avant d'aboutir dans le système de vote électronique ne doit pas obligatoirement être publié si les opérations essentielles pour la conformité avec l'art. 5 OVotE sont effectuées dans le système de vote électronique.

Art. 7b, al. 1, OVotE

Cette disposition règle la manière dont le code source doit être publié. Pour ce faire, on renvoie aux bonnes pratiques usuelles qui concernent notamment la lisibilité et la structure du code source, ou encore les possibilités de réagir :

- Le code source doit répondre aux critères de lisibilité usuels pour qu'il puisse être lu et compris par les personnes intéressées. Ces critères concernent notamment le formatage, le commentaire et la complexité de certaines parties du code.

- La structure générale du code devrait apparaître clairement. La publication de documents et d'illustrations supplémentaires peut y contribuer.

- La publication du code source a notamment pour but de donner la possibilité au public de détecter des failles. Pour cela, il faudrait expliquer, lors de la publication, la manière dont les personnes intéressées peuvent faire part de leurs réactions. En publiant sans délai des explications sur la manière dont les réactions seront exploitées, on peut continuer à renforcer la confiance dans le code source.

Vote électronique : publication du code source, modification de l'OVotE

Art. 7b, al. 2, OVotE

Les personnes intéressées doivent, dans toute la mesure du possible, pouvoir accéder au code source sans difficultés. Quiconque décide de télécharger le code source à partir d'Internet doit pouvoir le faire aussi directement que possible. Il est exclu de percevoir un émolument (art. 86 LDP).

Art. 7b, al. 3, OVotE

Toutes les tâches pertinentes pour la sécurité d'un système ne peuvent pas être effectuées au niveau du logiciel. Le code source, à lui seul, ne donne aucune indication sur l'infrastructure dans laquelle le système est exploité et entretenu, ni sur les mesures de sécurité organisationnelles qui sont mises en œuvre. Pour instaurer la transparence permettant aux milieux spécialisés d'évaluer la fiabilité du système, il faut que le code source soit replacé dans son contexte.

Art. 7b, al. 4, OVotE

Les cantons ne sont pas tenus d'utiliser des logiciels publiés sous une licence open source étant donné que les critères en la matière renferment des objectifs qui vont au-delà de l'instauration de la confiance. Dans le souci d'instaurer la confiance, il faut cependant faire en sorte, en cas d'utilisation d'un logiciel propriétaire, que l'on puisse se procurer facilement par Internet le code source des programmes et l'analyser dans la sphère privée, mais aussi que le code source – comme c'est le cas quand on travaille avec des logiciels open source – puisse être modifié, compilé et exécuté en toute légalité et servir de base à des travaux scientifiques. Les dispositions régissant le droit d'auteur doivent être aménagées en conséquence. Le propriétaire du code source peut autoriser l'utilisation de ce dernier à d'autres fins, par exemple pour l'exécution d'un scrutin, ou la subordonner à des conditions.

Annexe, ch. 2.7.2

Cette disposition interdit la conservation des suffrages. En même temps, la conservation des suffrages est nécessaire jusqu'à l'échéance du délai de validation. À titre d'exemple, l'examen des preuves cryptographiques résultant de l'application de l'art. 5 OVotE présuppose la disponibilité des différents bulletins de vote. Le traitement confidentiel des bulletins de vote préalablement anonymisés est déjà garanti par le ch. 2.8.6 de l'annexe de l'OVotE.