Contribution de Ardita Driza Maurer ardita.driza@sefanet.ch
Adressée à Mme Evelyn Mayer evelyn.mayer@bk.admin.ch

Consultation concernant la révision partielle de l'ODP et la révision totale de l'OVotE

Gimel, le 17 août 2021

Madame,

Dans le cadre de la consultation mentionnée et faisant suite à l'invitation à contribuer étendue aux milieux de la recherche, je vous prie de trouver ci-dessous ma contribution. Je vous remercie pour l'attention.

Salutations distinguées,
Ardita Driza Maurer
Juriste, Consultante en droits politiques et nouvelles technologies
1188 Gimel, Vaud

Introduction

D'un point de vue juridique, le canal de vote électronique par internet (VE) – en tant que canal complémentaire de vote – a comme objectif principal la mise en œuvre optimale des exigences découlant des principes constitutionnels régissant l'expression du vote : suffrage universel, égal, libre, secret et direct, inclus dans le concept plus large de liberté de vote (article 34 al. 2 Cst). D'autres principes constitutionnels, tels que l'organisation fédéraliste des droits politiques, l'état de droit et ses éléments, en particulier la légalité, relèvent également des principes applicables. Les exigences découlant des principes constitutionnels sont autant d'objectifs à atteindre et de limites à respecter par le VE.

Dans les lignes qui suivent nous interrogeons la conformité avec les principes supérieurs de certains aspects du VE, proposés dans le projet. Nous nous limitons à soulever des questions et à formuler des suggestions. La conformité constitutionnelle du projet mérite, à notre avis, une évaluation plus approfondie. L'examen juridique devrait, par ailleurs, précéder et guider le développement technique.

Caractère expérimental de la réglementation proposée ?

L'objectif du Conseil fédéral (CF) est de permettre aux cantons de reprendre des essais limités de VE sur de nouvelles bases, comprenant des exigences de sécurité plus précises, des règles de transparence plus rigoureuses, une collaboration plus étroite avec des experts indépendants et un contrôle efficace effectué sur mandat de la Confédération (rapport, chiffre 2.1). L'amélioration de la réglementation des essais, le renforcement de la sécurité et la collaboration avec la recherche sont à saluer.

Le rapport indique que, en plus de la reprise des essais sur des bases plus strictes, le but est de « mettre en place un processus d'amélioration continue » comprenant des mesures à court, moyen et long terme. Lors de l'ouverture de la présente procédure de consultation, la Chancellerie fédérale indiquait par ailleurs dans son communiqué de presse être déjà en train de préparer les modalités du contrôle des futurs systèmes et invitait les différents acteurs à se préparer à leur futur environnement réglementaire dans la perspective de la reprise prochaine des essais.

Une première question concerne le caractère de la réglementation proposée.

S'il s'agit d'une réglementation expérimentale, visant à prouver la faisabilité des mesures envisagées, l'on doit s'interroger sur : Quels sont les buts de l'expérimentation ? Que visent à prouver les essais ? Quelle est la durée de l'expérimentation ou de quoi dépend-elle ? Quelles évaluations sont prévues, à quel moment, selon quels critères ? Quelle suite est envisagée en fonction de quels résultats obtenus de l'évaluation ? L'abandon de l'expérimentation est-il envisagé ? Etc. Le rapport et les dispositions ne traitent pas du lien entre réalisation des objectifs et durée de la phase d'essai. Le suivi scientifique est prévu (art. 27o al. 2 ODP) toutefois seulement dans l'objectif de « donner des orientations en vue de l'amélioration de la phase d'essai », selon le rapport. La récolte et la mise en valeur des données n'est pas réglée en détail. En particulier le lien entre buts, évaluation et répercussions sur les essais n'est pas explicité.

Si, en revanche, il s'agit d'une réglementation durable du VE, alors la question principale est de savoir si une telle réglementation est compatible avec l'art. 8a LDP. Ne faudrait-il pas au préalable modifier l'art. 8a LDP afin de donner au CF la compétence d'autoriser le développement régulier, même qu'initialement limité, du VE ?

Le chapitre 2.3 du rapport « Orientations de la restructuration » laisse ouvertes les deux interprétations. Certaines mesures telles que la limitation de l'électorat suggèrent qu'il s'agit d'une réglementation expérimentale (cf. commentaire art. 27*f* al. 1 ODP). En revanche, la mise en place d'un processus d'amélioration continue et d'un train de mesures à moyen et long terme, ainsi que la perspective d'adapter les plafonds vraisemblablement vers le haut (cf. commentaire art. 27*f* al. 2 ODP) suggèrent une réglementation durable d'un VE qui progresse graduellement. Le rapport note par exemple que « …l'on travaillera en permanence à la mise en œuvre des objectifs à moyen et à long termes » (ch. 2.3).

Une réglementation expérimentale vise à prouver la faisabilité d'une approche choisie. En cas de résultats insatisfaisants, l'abandon de l'approche, à terme de l'expérimentation, est envisageable. Un processus d'amélioration continue semble, en revanche, partir de l'idée que l'approche choisie est faisable et qu'il faut l'améliorer et la faire progresser. Son abandon n'est pas envisagé. Cela s'apparente à une réglementation durable, à notre sens. Toute réglementation durable est par ailleurs sujette à amélioration continue.

L'amélioration continue prévue dans le projet dépasse à notre sens le cadre strict de l'expérimentation du VE (art. 8a LDP). Elle consacre l'usage régulier, quoi qu'initialement limité, du VE. Il est par ailleurs prévu que les plafonds initiaux de 30%, resp. 10% de l'électorat puissent être revus régulièrement et modifiés sur proposition de la Chancellerie fédérale au Conseil fédéral (cf. ch. 3 du rapport, premier tiret « Poursuite de la phase d'essai », ainsi que le commentaire de l'art. 27f al. 2 ODP). La légalité d'une telle approche, notamment sa compatibilité avec l'art. 8a LDP mérite discussion.

Solutions techniques *vs* Choix juridiques et politiques

Certains approches et solutions techniques prévues dans le projet reflètent et impliquent des choix juridiques. En principe, les choix juridiques importants doivent être sanctionnés par le législateur. La marge de manœuvre juridique du CF et de la Chancellerie fédérale (par rapport à l'ODP et OVotE) est définie à l'article 8*a* LDP, dont l'alinéa 2 stipule que « le contrôle de la qualité d'électeur, le secret du vote et le dépouillement de la totalité des suffrages doivent être garantis. Tout risque d'abus doit être écarté ». L'ODP et OVotE ne peuvent dès lors pas s'écarter de l'interprétation donnée à ces principes par le TF.

Ci-dessous nous discutons quelques choix retenus dans le projet et dont la conformité avec l'art. 8a al. 2 LDP mérite discussion, d'autant plus si le projet est une réglementation durable.

Vérifiabilité et sécurité du VE

La vérifiabilité est la mesure majeure destinée à garantir la sécurité du VE car elle permet d'identifier toute manipulation des suffrages exprimés par voie électronique, selon le rapport (cf. commentaire art. 27*i* al. 2 ODP). Ceci appelle des précisions.

La vérifiabilité permet au votant d'identifier des manipulations du suffrage individuel et aux vérificateurs, équipés de dispositifs techniques, de s'assurer du dépouillement correct de la totalité des suffrages valablement émis et de l'absence de « bourrage » de l'urne. La sécurité, en revanche, se réfère aux garanties de réalisation de l'ensemble des principes applicables ce qui comprend, en plus de l'intégrité, aussi le contrôle de la qualité d'électeur et le secret du vote (art. 8*a* al. 2 LDP). Alors que la vérifiabilité complète joue un rôle important pour assurer l'intégrité du vote et du résultat, elle n'a pas pour vocation d'assurer les autres principes. Les mécanismes permettant d'assurer le contrôle de la qualité d'électeur et le secret du vote, notamment vis-à-vis des tiers, sont, d'un point de vue juridique, tout aussi importants et indispensables que la vérifiabilité complète. Ceci mérite d'être mentionné dans la perspective d'une réglementation durable.

Par ailleurs, les conséquences de l'absence de vérifiabilité individuelle lors d'une élection qui prévoit des champs de texte libre appellent une évaluation juridique.

Contrôle public

L'art. 27*m* al. 4 P-ODP stipule que des représentants des électeurs doivent pouvoir suivre le déroulement de toutes les opérations principales et accéder aux documents en la matière, sous réserve d'exceptions (cf. rapport). Le rapport souligne que, finalement, cet article ne doit pas mettre en péril le déroulement du scrutin en temps voulu. Ceci appelle des précisions.

L'art. 27*m* al. 4 P-ODP correspond à l'art. 27m al. 2 de l'ODP, version 2014 et trouve son origine dans l'art. 27*m* al. 2 de l'ODP, version 2009. Dans sa version 2009, l'article 27*m* se réfère à la *constatation du résultat*, et le passage en question « Des représentants des électeurs doivent pouvoir assister au dépouillement » visait à assurer le contrôle public sur l'étape jugée la plus importante : l'établissement du résultat. Premièrement, d'un point de vue systématique, cette disposition, élargie maintenant à toutes les opérations principales du scrutin, doit être insérée dans un article sur le contrôle public. En d'autres mots, l'art. 27*m* al. 4 P-ODP ne relève pas (simplement) de l'information du public, mais du contrôle public sur les étapes importantes du VE.

Deuxièmement, la question de savoir comment résoudre d'éventuels conflits entre les exigences du contrôle public et celles du respect des délais de déroulement du scrutin, est une question qui met en jeux des principes et doit être tranchée par le législateur. Elle ne peut pas être décidée au niveau des ordonnances, sans base légale expresse.

Définition du secret

La garantie du secret du vote (art. 7 OVotE) et son interprétation tout au long du rapport se basent sur une interprétation spécifique de la garantie du secret du vote : sont garantis le secret du résultat intermédiaire et le secret vis-à-vis des autorités et autres administrateurs de vote. En revanche, le secret vis-à-vis de tiers qui, sans connaissance du votant, pourraient corrompre son ordinateur et briser le secret de son vote, n'est pas protégé par le protocole cryptographique et, au final, est toléré.

La décision de tolérer une telle violation repose sur une interprétation particulière du secret. Dans le vote papier, les tiers qui, sans droit, briseraient le secret de vote d'une ou plusieurs personnes seraient pénalement punissables (art. 283 CP). Le vote électronique en revanche

semble s'accommoder de cette violation du secret. Il nous semble que la décision de tolérer ou pas une telle violation du secret de vote ne peut pas être prise au niveau de l'OVotE. Des motifs de convivialité sont évoqués (cf. commentaire ch. 2.7.3 Annexe OVotE). Cependant, une éventuelle pesée d'intérêts et décision sur « qui de la convivialité ou du secret prime ? » relève, à notre sens, des compétences du législateur/souverain.

Confiance dans les vérificateurs

Selon le commentaire à l'art. 2 let. h OVotE, les électeurs doivent partir du principe que les vérificateurs attireront en cas de doute leur attention sur une irrégularité. Par ailleurs, les vérificateurs sont considérés comme des représentants des électeurs au sens de l'art. 27*m* al. 4 P-ODP. Ceci appelle des précisions.

Les vérificateurs ne peuvent pas contrôler des questions autres que celles liées à l'intégrité du résultat global et absence de bourrage de l'urne (cf. discussion ci-dessus sur la vérifiabilité et sécurité). En ce qui concerne le respect des autres principes de l'art. 8*a* LDP, la vérification complète ne joue pas de rôle et le contrôle public doit être assuré par d'autres moyens.

Le choix de déléguer le contrôle public de l'intégrité du résultat aux vérificateurs – s'il est effectué non pas dans un but expérimental mais de manière durable – exige à notre sens une discussion détaillée de la manière dont les vérificateurs sont désignés, de leur mode de fonctionnement et de la manière dont les autorités s'assurent que les vérificateurs, ou certains d'entre eux, remplissent leurs fonctions. Finalement, si elle est effectuée de manière durable, la délégation d'une telle compétence importante (contrôle de l'intégrité du résultat) à un cercle restreint d'experts *cum* dispositifs techniques relève du législateur/souverain.

En regardant de près certains détails, une exigence nous semble particulièrement problématique : les composants de contrôle ou les vérificateurs doivent recevoir, lors de la préparation du scrutin, les données d'authentification destinées à servir de moyen de comparaison lors de contrôles qu'ils vont effectuer en fin de scrutin (cf. commentaire ch. 2.6 Annexe OVotE). Or, les données d'authentification sont très sensibles et il ne faut absolument pas qu'elles tombent dans des mains hostiles. Comment concilier le fait qu'une majorité des vérificateurs peuvent être considérés non fiables avec le fait qu'on leur soumet lors de la préparation du scrutin les données d'authentification ?

Éléments fiables du système

Ces derniers jouent un rôle important du fait que le « protocole est défini de telle sorte que, tant que les participants fiables du système s'en tiennent au protocole, l'attaquant ne parviendra pas à ses fins, même s'il met sous son contrôle les autres participants, non fiables, du système » (cf. commentaire ch. 2 Annexe OVotE). Vu l'importance de tels éléments, il nous semble que leur choix doit faire l'objet d'une discussion et consensus qui dépasse le cercle étroit des chercheurs en informatique/cryptologie.

Caractère concluant des preuves

L'annexe et son commentaire discutent des exigences applicables au caractère concluant des preuves (cf. ch. 2.11 et aussi ch. 2.12 Annexe OVotE). Les valeurs discutées et les concepts impliqués sont techniques. Étant donné le rôle des preuves en cas de complications qui seront finalement tranchées par le juge, il nous parait que le caractère concluant des preuves relève

d'abord d'une discussion et décision juridiques. La solution technique doit, à notre sens, suivre et refléter les conclusions juridiques en matière de preuves requises. Par ailleurs, des explications comme « il n'est pas permis de faire effectuer aux votants une vérification pour des raisons purement psychologiques » (cf. commentaire ch. 2.12.5 Annexe OVotE) sont incompréhensibles en l'absence de contexte.

Rôle du votant

La sécurité du système relève en partie de l'implication du votant, lequel est très sollicité : il est, entre autres, *invité à faire le contrôle de vérifiabilité* individuelle ; *doit connaitre* la procédure correcte pour émettre le suffrage afin d'être protégé contre les attaques par ingénierie sociale (commentaire ch. 8.10 Annexe OVotE) ; est *tenu d'informer* l'autorité cantonale en cas d'affichage incorrect d'une preuve ou d'incertitude à cet égard (commentaire ch. 4.11 Annexe OVotE). En cas de doute le votant *peut* voter par correspondance ou à l'urne si aucun vote électronique n'a été enregistré à son nom (commentaire cf. ch. 4.11 Annexe OVotE).

Dans une perspective de réglementation durable du VE, il nous semble que le transfert de responsabilités (partielles) pour la sécurité du système (intégrité du résultat) sur les épaules du votant, dans un contexte techniquement aussi complexe, mérite une discussion approfondie et, finalement, l'aval du législateur/souverain.

Efficience, durabilité

Le projet de VE implique la mise en place d'un système complexe et de collaborations nouvelles entre le public et le système (cf. vérifiabilité), ou entre le système, les experts et les différentes autorités concernées, (cf. contrôles, bug bounties, etc.). Il s'agit pour l'essentiel de construire et de maintenir un système à la pointe des développements cryptographiques et informatiques, qui résiste aux changements fréquents dans ce domaine et, en parallèle, d'établir, maintenir et perfectionner tout un ensemble de connaissances, de pratiques, de processus impliquant le public, les autorités, les spécialistes. Ceci est très ambitieux. Les développements annoncés sont par ailleurs couteux et les couts en partie imprévisibles car dépendant de l'évolution incertaine des aspects de sécurité. Conformément à la répartition des tâches, la plupart des couts restera à la charge des cantons (ch. 4 du rapport). Les cantons faisant du vote électronique ont régulièrement été confrontés à la problématique des couts : le système genevois fut stoppé pour des raisons financières. Étant donné que les ressources sont limitées, des questions de proportionnalité et d'efficience de l'approche envisagée dans le projet ne tarderont pas à se poser. Un des principes directeurs est celui de l'utilisation raisonnable des ressources publiques de la part de l'administration. Le lien raisonnable entre les développements et efforts consentis et l'objectif visé devra être explicité. Cette discussion est en partie juridique et mérite d'être plus clairement menée dans le projet/rapport.

Renoncer à la certification formelle

Un changement majeur est proposé au niveau des contrôles : renoncer à la certification formelle, soit à l'évaluation par des entités externes accréditées. En lieu et place, la Confédération commandera les audits et assumera davantage de responsabilités et un rôle plus direct dans le contrôle des systèmes. Selon les explications fournies cette décision se base sur des constats faits dans le cadre de la restructuration de la phase d'essai (art. 27*l* al. 3 et 4

ODP et commentaire). Le projet prévoit un rôle accru des experts indépendants externes mandatés par la Chancellerie fédérale. Il semble par ailleurs qu'une telle décision soit motivée par l'échec de la certification menée en 2018 à découvrir des failles importantes dans le système de vérifiabilité de la Poste. Les faillent furent ensuite révélées lors de l'exercice de transparence (publication du code source) en février-mars 2019, par des chercheurs.

Le projet n'explique pas les raisons qui poussent à renoncer à la certification formelle. Si cette dernière se réfère à des standards–tels que Common Criteria et autre normes ISO, le projet ne dit pas quelles sont les normes/standards qui serviront de référence aux contrôles prévus dans le futur. La responsabilité des auditeurs et celle du mandant (Confédération) ne sont pas non plus expliquées. De même pour ce qui concerne la répartition des responsabilités et des coûts, en matière de contrôles et leur suivi, entre Confédération et cantons.

La nouvelle réglementation déclare tenir compte des résultats de l'exercice de transparence (2019) et des résultats du dialogue avec des experts en informatique et en sciences politiques (2020). Il manque cependant, à notre sens, une évaluation détaillée (publique) de l'exercice de transparence de 2019, des leçons qu'on en tire, notamment en matière de contrôles, et de la manière dont elles se reflètent dans le projet actuel. Une telle évaluation doit offrir de précieux renseignements, pour tout type contrôle (audit, etc.). Par exemple, un des points problématiques soulignés par les chercheurs lors de cet exercice était que certaines vulnérabilités, découvertes à cette occasion, avaient auparavant échappé non seulement à la certification mais aussi à d'autres types de contrôles et de preuves cryptographiques.[1] Quelles sont les conséquences de ce constat et comment cela se reflète dans le projet actuel ?

Les contrôles jouent un rôle majeur dans la sécurité du VE. Lorsque l'on décide de changer de type de contrôle (ici, suppression de la certification formelle), cela exige des explications détaillées. Le rapport aurait pu offrir plus d'explications sur ce point, à notre avis.

Risque restant

Plusieurs articles traitent de la gestion des menaces et du risque. Il manque en revanche le constat qu'il reste toujours un risque incompressible. La politique de gestion des risques en général et plus particulièrement la définition et l'examen du risque restant appellent une discussion juridique et politique préalable, en particulier si le projet introduit une réglementation durable du VE.

[1] A. Driza Maurer, *The Swiss Post/Scytl Transparency Exercise and Its Possible Impact on Internet Voting Regulation*, in R. Krimmer et al. (Eds.): E-Vote-ID 2019, LNCS 11759, pp. 83–99, 2019. Voir page 96 et références.