17 février 2019, 19h14 **19.113**

**Interpellation Lionel Rieder**

**État de situation du vote électronique dans le canton de Neuchâtel ?**

*Le vote électronique subit en ce moment des assauts de la part d'un comité d'initiative, qui fait suite à une attaque des pirates zurichois du Chaos Computer Club sur le système d'e-voting du canton de Genève. Dans ce contexte, nous avons besoin d'avoir des informations concernant le système Scytl, implanté par La Poste à Neuchâtel.*

*Nous souhaiterions avoir des réponses aux questions suivantes :*

1. *Comment et quelles données sont traitées, par La Poste et par le canton ?*
2. *Quels sont les mécanismes en place qui permettent de « garantir » que les données des votants ne peuvent être manipulées ?*
3. *Quel est le bilan de l'exploitation du vote électronique depuis 2005 ?*
   a) *Combien de scrutins ?*
   b) *Avons-nous connaissance de l'évolution, notamment par tranche d'âge, du taux de participation ?*
   c) *Combien de failles de sécurité, de problèmes techniques ou de pannes se sont produits ?*
   d) *Considérant la phase de test, est-ce que la Confédération nous demande de prendre des mesures particulières ?*
4. *Quelle est la procédure à la fin du scrutin pour vérifier et valider les résultats ?*
   a) *Comment les voix sont-elles comptabilisées ?*
   b) *Les votes sont-ils identifiés et identifiables ?*
   c) *Des recomptages sont-ils possibles ?*
   d) *Dans quelle mesure est-il possible pour des citoyens sans compétences particulières de vérifier les étapes essentielles du scrutin ?*
5. *Quel est le coût financier pour le canton de Neuchâtel, d'un point de vue technique et des ressources humaines ?*
   a) *À des fins de comparaison, quel est le coût financier du point de vue des ressources humaines lors d'un vote papier ?*
6. *Quel serait l'impact d'un moratoire pour le canton de Neuchâtel ?*

*Signataire: L. Rieder.*

19 février 2019, 13h36 **19.118**

**Interpellation Fabien Fivaz**

**Vote électronique : la démocratie mérite mieux**

*Le Conseil d'État est prié de répondre aux questions suivantes :*

1. *Au moment du transfert de la solution neuchâteloise à La Poste, le canton a-t-il « vendu » son savoir-faire dans le domaine ? À quelles conditions ? À quel prix ?*
2. *Combien la solution de La Poste coûte-t-elle annuellement au canton ?*
3. *Le contrat qui lie Scytl et La Poste n'est pas public. Quelle crédibilité peut-on accorder à la solution dans ce contexte d'opacité ?*

*Et concernant la sécurité :*

1. *Le code source de la solution e-voting a été piraté, quelles sont les conséquences de ce vol sur la sécurité du programme de vote électronique ?*
2. *Les attaques informatiques les plus courantes n'ont pas pu être testées par les hackeurs. Quelle crédibilité peut-on attendre du test effectué par La Poste ?*

*Développement :*

*À partir de 2020, La Poste sera l'unique prestataire pour le vote électronique en Suisse, pour la majorité des cantons, sans alternative. Elle n'a pas développé sa propre solution, elle a repris le système neuchâtelois, développé par le géant espagnol du secteur : Scytl. Les conditions du transfert du savoir-faire neuchâtelois à La Poste ne sont pas connues. Pire, les conditions du contrat qui lie Scytl à La Poste ne sont pas publiques. Pour un système qui met en jeu notre démocratie, c'est léger.*

*Pour prouver sa bonne volonté, La Poste a largement communiqué sa volonté d'ouverture. Elle a offert 250'000 francs pour mettre à l'épreuve la sécurité de sa solution. Elle a pourtant fait preuve d'une rare frilosité, en interdisant aux hackeurs d'attaquer le système en utilisant les méthodes les plus courantes (par exemple le denial-of-service, la plus simple et la plus efficace). Le test de sécurité est en fait une vaste supercherie.*

*Surtout, pendant que La Poste vantait les mérites et la sécurité de sa solution, elle s'est fait pirater le code source… C'est une bonne nouvelle pour les détracteurs du vote électronique qui demandent depuis longtemps que les solutions d'e-voting soient obligatoirement open source. C'est moins une bonne nouvelle pour l'image sécuritaire et la crédibilité de La Poste.*

*Signataire : F. Fivaz.*

## Réponse écrite du Conseil d'Etat, transmise aux membres du Grand Conseil le 27 mars 2019

Nous tenons à remercier les auteurs des interpellations pour l'intérêt qu'ils portent à la prestation de vote électronique offerte aux électrices et électeurs au travers du Guichet unique. C'est aussi l'occasion pour le Conseil d'État d'apporter des réponses aux informations parfois erronées reprises sur les Réseaux sociaux et, surtout, de défendre une prestation qui a permis à son origine le développement du Guichet unique.

**Quel est le bilan de l'exploitation du vote électronique depuis 2005 ?**

En préambule, il est nécessaire de rappeler que le vote électronique a été introduit dans le canton de Neuchâtel lors de la votation du 25 septembre 2005 sous l'impulsion de la Chancellerie fédérale, ce qui a coïncidé avec l'ouverture du Guichet unique. Cette démarche avant-gardiste s'inscrivait dans le cadre des changements sociaux liés à la transition numérique et qui touchent, aujourd'hui, tous les jours, les citoyennes et citoyens dans leurs activités. Il n'est donc simplement pas imaginable que l'État soit absent de cette évolution de la société, dans un domaine qui touche toutes les citoyennes et tous les citoyens.

Depuis l'introduction du vote électronique, le canton de Neuchâtel a procédé à 56 tests de vote électronique, tous types de scrutins confondus, sans aucune faille de sécurité, de problème techniques ou de panne. Ainsi, lors de la dernière votation fédérale, plus de 30'000 électrices et électeurs avaient la possibilité d'utiliser le vote électronique. Seuls 4'759 d'entre-eux ont utilisé ce canal pour voter (15,65%), Toutefois, ce chiffre doit être nuancé par un taux de participation relativement faible lors de ce scrutin (32,07%). Quant à la répartition par classes d'âge, le vote électronique touche tous les âges de 18 à 94 ans, même si l'essentiel des utilisateurs-trices se situent dans les tranches de 45 à 74 ans (lien vers les statistiques).

Depuis décembre 2013, la vérifiabilité individuelle et universelle est au cœur des nouvelles dispositions fédérales (ordonnance sur le vote électronique). Elle doit garantir l'identification de tout dysfonctionnement systématique dans le processus de vote à la suite d'une erreur logicielle, humaine ou d'une tentative de manipulation. Ainsi, pour qu'il y ait vérifiabilité individuelle, il faut notamment que les votant-e-s puissent contrôler de manière fiable que leur suffrage a été pris en compte par le système sans avoir été modifié et qu'il n'a donc pas été manipulé (codes de vérification). Quant à la vérifiabilité universelle, elle consiste à vérifier l'intégrité des données à chaque étape du processus de dépouillement de l'urne électronique.

La première de ces nouvelles exigences (vérifiabilité individuelle) a été introduite avec succès lors de la votation du 8 mars 2015. Jusqu'à l'introduction de cette nouvelle solution, l'électeur-trice pouvait vérifier la prise en compte du vote mais en revanche, il ne pouvait pas contrôler l'exactitude du vote transmis dans l'urne électronique. Désormais, c'est possible. Après avoir validé son vote, l'électeur-trice voit s'afficher sur son écran des codes de vérification personnels qu'il doit comparer avec ceux figurant sur sa carte de vote. C'est grâce à des opérations cryptographiques que les codes de vérification sont générés et envoyés à l'électeur-trice. Après contrôle de ceux-ci, il en confirme l'exactitude, validant ainsi définitivement son vote.

Ces développements améliorent sensiblement la sécurité du vote électronique mais ne permettent pas encore d'augmenter au-delà de 30% la limite des électeurs-trices qui peuvent participer au vote électronique. Sachant qu'aujourd'hui le Guichet unique compte plus de 37'000 utilisateurs-trices (+3'000 par année), cette limite sera très vite atteinte. Pour la franchir et afin de permettre graduellement à 100% de l'électorat d'utiliser le vote électronique, les exigences de la Confédération sont multiples. Le passage à la limite de 50% nécessite, d'une part, que la vérifiabilité individuelle soit intégrée et, d'autre part, que des certifications (audits) soient obtenues. Pour atteindre le 100%, il faut non seulement pouvoir apporter la preuve que tous les suffrages n'ont pas été manipulés durant le processus de dépouillement de l'urne électronique (vérifiabilité universelle), mais il faut entre autres que le code source ait été publié et des tests d'intrusion faits, ceci afin de pouvoir s'assurer de la qualité du produit et de bénéficier de l'apports d'expert-e-s du monde entier.

La Poste a donc publié le code source en ce début d'année et organisé des tests d'intrusion. La première mesure a permis à des chercheurs de révéler une faille qui a été corrigée avec l'apport de ceux-ci. Ainsi, même si cette découverte n'est en soi pas une bonne nouvelle, nous ne pouvons que nous réjouir du processus mis en place avant la validation et l'utilisation de cette future solution par les cantons. Celui-ci aura permis de s'assurer de la conformité du code source et de s'assurer de la sécurité de ce canal de vote par des tests d'intrusions.

Finalement, la Confédération souhaite inscrire le canal électronique dans la loi comme une des procédures d'exercice du droit de vote. Le projet de modification de la loi fédérale sur les droits politiques est en cours de consultation auprès des cantons. Les modifications visent à régler au niveau fédéral l'utilisation du vote électronique et à sortir de la phase de tests. Les principes émis dans le projet de modification de la loi reprennent les exigences de l'ordonnance de la chancellerie fédérale sur le vote électronique, à savoir en particulier que le système doit être totalement vérifiable (vérifiabilité individuelle et universelle) et transparent (publication du code source).

**Comment et quelles données sont traitées, par la Poste et par le canton ?**

Les rôles et responsabilités sont clairement réglementés. La préparation des scrutins de vote et les dépouillements sont effectués par le canton. Ni le registre électoral, ni aucune autre donnée non chiffrée ou personnelle ne sort à un quelconque moment. Le registre électoral, l'ouverture et le contrôle des urnes ainsi que le décompte restent donc uniquement sous la responsabilité de notre canton. La Poste livre le contenu de l'urne de manière chiffrée à la commission électorale, qui procède ensuite à son déchiffrement et à son dépouillement. Pour le déchiffrement, les clés sont détenues exclusivement par les député-e-s de cette commission. Ainsi, seule la commission électorale réunie peut déchiffrer les votes et calculer les résultats. En résumé et pour être complet, les seules données qui reposent dans l'urne située à La Poste sont le numéro de la carte de vote et les votes chiffrés.

**Quels sont les mécanismes en place qui permettent de "garantir" que les données des votants ne peuvent être manipulées ?**

Le vote électronique doit être le plus sûr possible. C'est pour cette raison que les exigences de la Confédération et des cantons mentionnées en introduction sont très importantes et doivent permettre d'identifier toute manipulation du résultat. En effet, c'est à cette fin que les mécanismes de sécurité centraux du système de vote électronique ont été conçus : la vérifiabilité individuelle et universelle. Le contrôle des voix peut donc s'effectuer à trois niveaux : l'électeur-trice peut vérifier que son vote a été pris en compte correctement (en place) ; l'électeur-trice reçoit la confirmation que son vote a été enregistré tel qu'il l'a exprimé (en place) ; la commission électorale pourra s'assurer non seulement comptablement (en place) mais techniquement, dès 2020, que les voix comptabilisées correspondent aux suffrages tels qu'ils ont été enregistrés sans prendre connaissance des voix/sans ouvrir l'urne ou sans pouvoir remonter aux électeurs-trices.

Finalement, il est utile de rappeler que le canton de Neuchâtel est le seul à bénéficier d'une identification forte, au travers du Guichet unique. Ainsi, la prestation de vote n'est pas directement accessible sur Internet. Une attaque supplémentaire du Guichet unique et des mécanismes d'authentification serait nécessaire pour exploiter des failles éventuelles de la solution de vote électronique.

**Quelle est la procédure à la fin du scrutin pour vérifier et valider les résultats ?**

Comme indiqué en introduction, la vérification se fait d'abord comptablement par la comparaison du nombre de votes transmis par le Guichet unique, déposé dans l'urne et dépouillé. Il faut encore relever que tout au long du processus, les votes ne sont en aucun cas identifiés et identifiables. Le lien entre le vote et le votant est cassé, au même titre que l'enveloppe de vote est sortie de l'enveloppe de transmission pour être glissée dans l'urne du bureau électoral. Par ailleurs, grâce à la vérifiabilité universelle, d'éventuelles anomalies pourront être contrôlées par la commission électorale et les votes recomptés par les cantons ou par des expert-e-s indépendants.

Quant aux citoyennes et citoyens, ils reçoivent des codes de vérification sur leur carte de vote. La comparaison des chiffres imprimés avec ceux affichés à l'écran leur permettent de vérifier que le vote déposé dans l'urne électronique est bien celui choisi. Finalement, le jour de la votation et dès la fermeture des bureaux de vote, les électrices et les électeurs peuvent vérifier à l'aide de leur accusé de réception que leur vote a bien été pris en compte lors du dépouillement.

Si les codes ne concordent pas, cela signifie qu'une irrégularité s'est produite. Les électeurs peuvent alors voter par correspondance ou déposer leur vote directement dans l'urne du bureau de vote.

**Quel est le coût financier pour le canton de Neuchâtel d'un point de vue technique et des ressources humaines ?**

Le coût d'organisation d'un scrutin cantonal est d'environ 200'000 francs. Quant au vote électronique, le prix d'un scrutin dépend du nombre d'électrices et électeurs inscrits au Guichet unique. Il s'élève actuellement à moins de 25'000 francs. Ces chiffres ne tiennent pas compte des ressources humaines engagées dans l'organisation du scrutin par l'État ou les communes, plus particulièrement, dans le processus de dépouillement, ainsi que des infrastructures techniques.

Outre le fait que la solution est conviviale pour les utilisateurs-trices, les travaux de dépouillement sont relativement brefs et simplifient grandement les tâches des communes. C'est naturellement le cas lors des votations, mais c'est encore plus évident lors d'élections.

Finalement, la chancellerie fédérale a mis en place un groupe d'expert-e-s pour examiner la possibilité de ne plus envoyer de matériel de vote. Les conclusions de ses travaux ne sont pas favorables, aujourd'hui, à la suppression totale du papier, ceci afin de respecter le principe de la vérifiabilité individuelle et, par conséquent, d'éviter que des hackers s'emparent des codes de vérification.

**Quel serait l'impact d'un moratoire pour le canton de Neuchâtel ?**

Sur un plan technique, un moratoire de cinq ans ne permettrait pas d'offrir après l'échéance plus de sécurité qu'aujourd'hui, puisque notre canton intègre déjà la vérifiabilité individuelle et a prévu de disposer de la vérifiabilité universelle dès 2020 afin de permettre à 100% des électrices et électeurs de voter. Il répond donc déjà aux attentes des détracteurs du vote électronique.

Par ailleurs, la Confédération a publié sa deuxième étude nationale sur la cyberadministration, dans laquelle un résultat précis est mis en exergue : « La population souhaite pouvoir voter en ligne ». Selon l'étude, deux tiers des personnes interrogées estiment que le vote électronique devrait être mis à la disposition de toutes les personnes ayant le droit de vote. Et près de la moitié des personnes sondées affirment qu'elles voteraient plus souvent s elles pouvaient le faire par voie électronique.

Un moratoire ne répondrait donc surtout pas aux besoins des électrices et électeurs, puisque ceux domiciliés dans le canton ne pourraient plus utiliser le vote électronique pendant cinq ans et devraient donc utiliser le vote par correspondance ou au bureau de vote, à moins qu'ils renoncent à voter. Quant aux Suisses et Suissesses de l'étranger, une partie de ceux-ci ne pourront plus voter du tout en raison des délais d'expédition et de retour par voie postale.

**Au moment du transfert de la solution neuchâteloise à la poste, le canton a-t-il « vendu » son savoir-faire dans le domaine ? À quelles conditions ? À quel prix ?**

La République et Canton de Neuchâtel n'a jamais été propriétaire de la solution de vote électronique. Celle-ci a été développée par la société espagnole Scytl, en partie pour la Suisse, afin de répondre aux exigences de la chancellerie fédérale.

Le savoir-faire neuchâtelois consistait en la maîtrise du processus d'organisation d'une votation en lien avec le vote électronique et celui-ci a naturellement été négocié lorsque La Poste a acquis les droits sur la solution informatique de Scytl. Ainsi, notre canton a pu exploiter la solution de La Poste sans frais de base en 2017 et à moitié prix en 2018.

**Le contrat qui lie Scytl et la Poste n'est pas publié. Quelle crédibilité peut-on accorder à la solution dans ce contexte d'opacité ?**

Le contrat entre Scytl et La Poste a été audité dans le cadre de la certification de la solution de vote électronique, afin de s'assurer que les exigences légales et règlementaires soient satisfaites. Par ailleurs, le contrat peut être consulté par la chancellerie fédérale et les cantons qui travaillent avec ce fournisseur.

**Le code source de la solution e-voting a été piraté, quelles sont les conséquences de ce vol sur la sécurité du programme de vote électronique ?**

Le code source du système de vote électronique de La Poste n'a pas été piraté. Le code source a été rendu public conformément aux exigences de la Confédération et des cantons. La Poste a donc publié le 7 février dernier le code source de son système de vote électronique (www.poste.ch/evoting-sourcecode). Le fait que des copies du code source ont été publiées n'a aucune influence sur la sécurité du système.

**Les attaques informatiques les plus courantes n'ont pas pu être testées par les hackeurs. Quelle crédibilité peut-on attendre du test effectué par la poste ?**

Notre fournisseur effectue le test d'intrusion de manière transparente et crédible, en allant souvent au-delà des pratiques en cours pour de tels tests, notamment pour les raisons suivantes :

- les conditions-cadres répondent aux exigences de la Confédération et des cantons ;
- les «best practices» pour les tests d'intrusion professionnels sont respectées ;
- tous les scénarios d'attaque visant à consulter ou à manipuler les suffrages sont autorisés ;
- tous les résultats sont publiés de manière transparente ;
- chaque participant a le droit de publier ses résultats après 45 jours au maximum ;
- il n'existe aucune restriction relative à la participation ;
- les testeurs peuvent demander plusieurs cartes de vote afin de lancer des attaques multiples contre le système.

L'exclusion concerne les attaques connues et pour lesquelles il existe déjà des mesures de sécurité. De tels scénarios ne fourniraient aucun retour d'expérience utile. Les suivants sont notamment exclus du test :

- attaques contre le PC, l'ordinateur portable ou la tablette dans la mesure où la vérifiabilité individuelle répond à ce problème ;
- social engineering car la vérifiabilité individuelle intègre déjà ce problème ;
- attaques par déni de service distribué DDoS (attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs-trices légitimes d'un service de l'utiliser) ne font cependant pas partie du test, car elles ne sont pas spécifiques au vote électronique et n'apporteraient aucun enseignement complémentaire. Cette limitation est normale dans le cadre d'un test d'intrusion. Outre le vote électronique, notre fournisseur exploite divers systèmes hautement critiques, comme l'e-banking. Il effectue régulièrement des tests DDoS pour se protéger de telles attaques. Ces tests ne sont pas réalisés à des moments définis, mais ont lieu à intervalles réguliers. La Poste connaît ainsi relativement bien les limites de la disponibilité du réseau et des différents systèmes, ainsi que les capacités de réaction.

  Si les tests d'intrusion concernent plus particulièrement l'infrastructure de La Poste, il faut encore préciser que le Guichet Unique, ainsi que notre fournisseur d'accès Internet, disposent de solutions techniques et organisationnelles pour se protéger et réagir en cas d'attaques criminelles de ce type. Par ailleurs, le déni de service sur le processus de votation n'est pas utile dans la mesure où les électrices et électeurs ne sont pas empêchés de voter (vote par correspondance ou au bureau électoral).

**Conclusion**

La transition numérique touche toutes les activités de la population. L'enquête de la Confédération le prouve. Les citoyennes et citoyens souhaitent aussi utiliser leurs outils informatiques pour voter. Notre canton s'est déjà inscrit en 2005 dans cette voie. Ainsi, même si le parcours est aujourd'hui difficile en raison des craintes et résistances, des dangers et, par conséquent de toutes les mesures qu'il faut prendre pour augmenter la sécurité, il entend continuer de développer toutes les prestations du Guichet unique dont le vote électronique.

Par ailleurs, les exigences de la Confédération et des cantons envers le fournisseur portent leurs fruits. L'intérêt et la participation de chercheurs du monde entier à l'examen du code source et aux tests d'intrusion auront permis de vérifier la sécurité et d'améliorer certains contrôles.

Les détracteurs du vote électronique reprochent à la Confédération et aux cantons un certain attentisme ou de laisser totalement la maîtrise de l'outil à leur fournisseur. Les conditions-cadres (certification, transparence et tests d'intrusion) pour s'assurer de la sécurité de la solution de vote électronique mises en place démontrent aujourd'hui toute leur pertinence.

Informations complémentaires :

Site Internet de l'État sur le vote électronique
Site internet de la Confédération sur le vote électronique
Site internet de notre fournisseur