*Date de dépôt : 7 janvier 2016*

# Rapport

**de la Commission des droits politiques et du règlement du Grand Conseil chargée d'étudier le projet de loi du Conseil d'Etat modifiant la loi sur l'exercice des droits politiques (LEDP) (A 5 05)**
*(Accès au code source du vote électronique)*

**Rapport de M^me^ Anne Marie von Arx-Vernon**

Mesdames et
Messieurs les députés,

Sous la présidence de M. Pierre Vanek, la Commission a étudié le présent projet de loi lors des séances des 7 et 14 octobre 2015.

Il a été excellemment assisté par M. Fabien Mangilli, Directeur à la Direction des affaires juridiques de la Chancellerie et M^me^ Irène Renfer, Secrétaire scientifique du SGGC. Les procès-verbaux ont été pris par M. Grégoire Pfaeffli.

La rapporteure les remercie tout particulièrement.

**07.10.2015 : Présentation du PL 11701 par M^me^ Anja Wyden Guelpa, Chancelière, ainsi que M. Yves Favre, Directeur général de la DGSI, et M. Arni-Bloch, Directeur de la Direction du support et des opérations de vote.**

***Présentation par M^me^ Wyden Guelpa qui utilise un document pour sa présentation (en annexe).***

*Confiance*

Les droits politiques sans confiance ne sont pas possibles, qu'il s'agisse de vote à l'urne, postal ou électronique. Plus encore qu'il y a vingt ans, la confiance n'est aujourd'hui possible qu'avec une certaine transparence.

Le vote électronique est important pour les personnes avec un handicap de vue, puisqu'il est possible d'agrandir le bulletin de vote. Depuis le 8 mars, une

ATAR ROTO PRESSE – 200 ex. – 01.16

adaptation a été faite pour les tablettes et les smartphones. Lors d'élections avec de nombreux candidats, un bulletin électronique est aussi plus lisible qu'un bulletin postal. En outre, cela donne une image plus moderne de la démocratie et permet donc de toucher un public plus large.

*Canal de vote*

Ce PL répond à un besoin. Ainsi, il s'agit du premier canal de vote des Suisses de l'étranger, puisque plus de 50%, voire 60% d'entre eux l'utilisent. Cela a même amené lors des dernières élections un taux de participation des Suisses de l'étranger votant à Genève de 100% dans cinq pays. Pour ce qui est des résidents à Genève, le vote électronique est le deuxième canal de vote, encore loin devant le vote à l'urne.

*Continuité*

Ce PL s'inscrit dans la continuité du projet, qui reste depuis sa création un projet public propre et indépendant d'une entreprise privée. En 2009, le Grand Conseil a donné la possibilité aux citoyens utilisant le système d'accéder au code source sur demande. Cela a été fait à deux reprises, par le Parti Pirate et la Haute école de gestion bernoise disposant d'un centre de compétence sur le vote électronique.

*Transparence*

Aujourd'hui il est indispensable de faire un pas de plus vers la transparence. Le vote électronique doit répondre aux mêmes valeurs et exigences que le vote à l'urne ou par courrier. L'image de l'urne transparente représente la possibilité qu'ont les citoyens d'aller vérifier le dimanche du vote que celui-ci est bien pris en compte sans modification, contrôle qui s'ajoute au rôle de la commission électorale centrale (ci-après CEC). De la même manière, il doit être possible pour les citoyens de vérifier que le vote électronique est fait dans les règles et avec la sécurité qu'engendre la transparence.

*Risque*

Aujourd'hui aucun système électronique ou mécanique n'est exempt de risque. La seule chose que l'on peut faire est de le réduire au maximum.

Dans le cadre du vote électronique, le risque le plus grand est qu'un hacker tente de s'infiltrer dans le système. La transparence agit sur l'envie du hacker de se confronter au système de vote électronique. L'idée est aussi que ces milieux hackers/open source s'approprient cet outil.

L'un des buts du PL est la mise à disposition de M. Favre d'un demi ETP afin de modérer ces milieux pour qu'ils aident à faire avancer le projet, probablement en partie gratuitement.

*Système genevois*

Berne, Lucerne et Bâle utilisent le système de vote genevois. Un changement dans la cartographie du vote électronique est intervenu cet été. Auparavant, trois systèmes existaient, les deux autres étant privés, par opposition au système public genevois. L'un de ces deux systèmes privés, Unisys, n'a pas reçu l'autorisation fédérale et ne peut donc plus être sur le marché suisse, ce qui a amené le consortium des neuf cantons qui en avaient l'usage à chercher un nouvel outil. L'autre système privé, Scytl, est espagnol et utilisé par la Poste, qui est rentré sur ce marché. Scytl a forcé Neuchâtel à travailler avec la Poste afin de ne pas avoir deux interlocuteurs en Suisse. La situation est donc actuellement une sorte de lutte entre David et Goliath. Les deux systèmes ont une philosophie diamétralement différente. Pour Genève, le vote est une compétence régalienne. De la même manière qu'il n'est pas envisageable de déléguer le dépouillement papier à une entreprise privée, il ne serait pas imaginable non plus de le faire en ce qui concerne le dépouillement électronique.

***Précisions sur le code source apportées par M. Favre et M. Arni-Bloch***

*Code source*

Le code source est rédigé dans un langage informatique, avec des termes universels que tous les informaticiens connaissent et que la machine comprend. Ouvrir le code source, c'est mettre à disposition la programmation de la machine à n'importe quel informaticien de la planète qui peut y jeter un regard, analyser le contenu quant au fonctionnement et vérifier que celui-ci soit bien conforme à l'intention. De manière générale, le monde informatique a de plus en plus tendance à publier les codes source. Même les grands acteurs du marché publient leurs programmes pour bénéficier des yeux de la planète. Il y a cinq à dix ans en arrière, la position était inverse, car on estimait que publier le code source exposait au regard des hackers. Il est toujours vrai que c'est un risque qui existe, mais cela permet surtout aux universitaires de travailler sur ces questions et de proposer des modifications par l'intermédiaire de communautés d'informaticiens qui animent la création de leurs codes sources.

*Vote électronique à Genève*

Il représente environ 72'000 lignes de codes regroupées dans plus de 1000 fichiers.

Le code source du système de vote électronique genevois est riche et représente un grand travail, qui pourrait bénéficier de l'apport d'autres prestataires ou partenaires.

*Contrôle*

Aujourd'hui, le contrôle se fait sous différents angles, notamment par la CEC. Des audits sont faits pendant lesquels des auditionnés viennent et bénéficient d'un accès provisoire au code source avant de rendre un rapport. Un des bénéfices de l'ouverture du code source est l'augmentation de la fiabilité à travers le contrôle par un large public.

La Suisse, avec ses particularités de démocratie directe, est très en avance dans le domaine du vote électronique et un grand nombre de personnes s'y intéresse.

*Risques*

Ils existent, principalement d'image, par exemple à travers la divulgation de faiblesses par un hacker qui serait relayée par la presse. Dans la pesée d'intérêts, il faut donc remarquer que si les risques de sécurité diminuent, les risques d'image augmentent. Le risque existe que des hackers tentent de pénétrer le système « par jeu ».

*Processus d'ouverture du code source*

L'ouverture se ferait sur trois ans, et serait définie par un cadre, car le vote électronique ne représente pas uniquement ce que les votants voient sur leurs bulletins, mais aussi tout ce qui concerne le backoffice. Le code source rédigé par les collaborateurs ne l'a pas été dans un but de publication, et certaines retouches doivent être faites. Après le cadrage, il s'agira d'ouvrir le code source et de décider à travers quels médias cela se ferait, dans un but de communication réciproque avec les communautés d'informaticiens pour déterminer dans quelle mesure les modifications seraient entreprises sur la base des retours. De plus, de nouveaux acteurs seraient prêts à travailler avec l'Etat de Genève, certains de manière gratuite.

*Actuellement*

Le code source ne peut être accédé que par des électeurs genevois ou des cantons hébergés. Des dispositions ne permettent pas d'ouvrir de manière plus large le code. Des modifications des articles de loi sont donc proposées tout en maintenant des dispositions transitoires afin de garantir que ce qui est possible à l'heure actuelle le reste pendant la période de trois ans d'ouverture progressive. À la fin de la période de trois ans, un rapport sera fait qui permettra d'établir définitivement les dispositions souhaitables pour la LEDP

*Quelques chiffres*

A Genève, la participation par voie électronique est en général comprise entre 18 et 20 %. Chez les Suisses de l'étranger, elle est comprise entre 51 et 60%. Pour l'instant, la Confédération limite l'offre du vote électronique à 30%

de la population pour les résidents, mais au fur et à mesure des progressions en matière de sécurité, il sera possible de l'offrir à 50% puis à 100% de la population résidente après deux autres étapes de sécurité.

Pour passer la prochaine étape de vérification, il faut qu'une entreprise vérifie qu'un système a bien été mis en place et empêche qu'un intermédiaire intercepte les communications entre les votants et le système, un procédé appelé *man in the middle attack*.

Actuellement, aucune entreprise suisse ne dispose de la compétence nécessaire pour certifier. Ceci devrait se faire donc au début de l'année 2016, et à la fin 2016, la votation électronique devrait pouvoir être offerte à 50% des votants résidant en Suisse. La dernière étape sera la vérifiabilité universelle, avec des serveurs qui permettront à tout moment de contrôler l'ensemble des processus.

*Perspectives*

Entre 2018 et 2019, le vote électronique pourra être offert à 100% des votants. Le processus serait le même qu'avec le vote postal : tant qu'il s'agissait d'un projet nécessitant une inscription, peu de personnes utilisaient le système, mais dès que cela s'est généralisé, le vote postal s'est répandu, et consiste aujourd'hui en 95% des votes.

*Les autres cantons*

L'open source améliore la sécurité et réduit les risques, cela ne dispense pas d'avoir à tout moment le plus haut niveau possible de sécurité, et cela coûte. La participation de plus de cantons permettrait une mutualisation des coûts plus intéressante. Il ne serait toutefois pas possible d'accueillir les beaucoup de cantons simultanément, l'optimal étant environ trois par année.

***Discussion de la Commission***

La majorité des commissaires estimerait contre-productif de retenir ce code source. Toutefois concernant l'importance de la transparence soulignée par la Chancelière, il est à relever que, même distribué au grand public, le code source resterait impénétrable de par son langage, incompréhensible pour l'immense majorité de la population. De plus, même pour un informaticien connaissant le langage de programmation du code source, le contrôle d'un code de 72'000 lignes représente un certain investissement en temps non négligeable.

Aux questions des commissaires, Mme Wyden Guelpa propose une analogie avec la Landsgemeinde que si elle garantit une transparence, elle ne permet pas le secret du vote. Elle remarque que c'est d'ailleurs pour cette

raison de secret du vote que le Conseil Fédéral a décidé d'interdire le programme jusqu'alors utilisé par le consortium de neuf cantons.

Elle confirme que c'est le souci de transparence qui pousse l'Etat à vouloir ouvrir le code source. Jusqu'à maintenant, la transparence est totale pour les citoyens, mais cela nécessite un certain temps : Les deux personnes ayant demandé à avoir accès sont le Parti Pirate et la Haute Ecole de Gestion de Berne.

Aux questions des commissaires, M. Favre indique que si la Confédération a commencé à édicter des normes, très sévères, depuis maintenant 18 mois, c'est justement pour adresser ce souci de transparence. La vérifiabilité universelle nécessaire à l'ouverture du vote électronique à l'entier des votants consiste à pouvoir garantir l'intégralité et la cohérence de l'ensemble du vote.

Il relève que ce projet est en avance sur son époque. Tout le monde aujourd'hui utilise des moyens informatiques, et tous ces moyens impliquent un processeur et un ordinateur programmé de la même manière qu'il l'a présenté auparavant. Il est convaincu que nos enfants et petits-enfants apprendront les langages informatiques comme nous apprenons le français, l'anglais ou l'allemand, ce qui les rendra plus aptes à juger de la sécurité de ce projet. Il conclut que parmi tous les projets qui sont sous sa responsabilité, celui-ci est réellement le plus innovant. À ce titre, il propose de déjà prendre un pas d'avance.

Concernant les moyens informatiques pour la signature des initiatives et des référendums, Mme Wyden Guelpa indique que cela figure dans les objectifs de la Confédération. Les réticences viennent parfois de Partis qui disent que si l'on facilite la récolte, il faut augmenter le nombre de signatures.

Elle précise que la problématique de la signature d'initiative et de référendum en ligne est plus simple, car elle n'implique justement pas une anonymisation des signataires, ce qui pose beaucoup de problèmes pour l'anonymat du vote en conjonction avec la nécessité de pouvoir établir qu'une personne a bien voté et que son vote n'est pas altéré.

A des questions des commissaires, Mme Wyden Guelpa confirme que ce PL ajoute de la transparence. La CEC continuera à fonctionner pour le vote électronique comme pour tous les autres moyens de vote. Il s'agit d'un contrôle citoyen supplémentaire.

A des questions des commissaires, Mme Wyden Guelpa répond que le risque que des hackers se servent de ce code source pour attaquer le système de vote électronique d'une manière ou d'une autre sera confronté à la réalité du chemin de transparence puisque les citoyens ont déjà accès au code. La décision est d'une part philosophique, en rapport avec la transparence aux

citoyens, mais d'autre part sécuritaire, car la publication du code source réduit drastiquement le risque de hacking. Si un coût de CHF 200'000.- est nécessaire la première année, cela permet d'être en contact avec les communautés d'informaticiens et de scientifiques, ce qui amènera certainement une baisse des coûts de l'étape suivante, à savoir la vérifiabilité universelle. Le but est aussi que ces milieux s'approprient cet outil, car eux ont la compétence de comprendre ce code.

M. Favre indique que si faire des audits est bien et permet d'obtenir une vue en coupe de la situation actuelle, elle ne donne pas une vue d'ensemble. Une attaque de hacker est possible déjà aujourd'hui. Un hacker pourrait simplement décider de surcharger le système pendant un jour de vote, ce qui ne modifierait pas le vote, mais empêcherait le système de fonctionner. De la même manière, il est possible de détourner un fourgon contenant des bulletins de vote. Il faut donc se rassurer sur la sécurité du vote électronique.

En conclusion, M. Favre rappelle qu'avant que le code source ne soit ouvert au public, il faudra encore trois ans pendant lesquels les risques de sécurité seront examinés. Il faut aussi vérifier que ce qui est publié représente un intérêt, sinon il ne sert à rien de le publier, et ce sera donc certainement une grande partie du code source qui au final ne sera pas publiée.

M[me] Wyden Guelpa indique que depuis l'été 2015, de nombreuses interventions parlementaires, dont cinq au niveau fédéral et plusieurs autres dans des parlements cantonaux, plébiscitent le système genevois et demandent à leurs exécutifs pourquoi ils ont fait le choix d'un système étranger, et au niveau fédéral pourquoi il est nécessaire d'avoir deux systèmes. En répondant à la motion de Christophe Darbellay, le Conseil fédéral a indiqué qu'il réfléchissait à ce que l'open source soit une condition d'autorisation d'un système de vote électronique.

A une question de commissaire, M. Favre indique que la plupart des serveurs sur internet, y compris ceux des banques, sont basés sur un système d'exploitation appelé Linux, qui est entièrement en open source et s'y est principalement développé. Il y a au moins autant de gens qui désirent aider et protéger un tel système que de gens qui désirent en trouver les failles et les utiliser. Linux est donc l'un des systèmes d'exploitation les plus fiables de la planète. La NASA se sert de ce système pour faire décoller ses fusées.

A une question de commissaire, au sujet d'une éventuelle corrélation entre vote électronique et vote des jeunes, Mme Wyden Guelpa indique qu'Andreas Auer, professeur à l'Université de Zurich et directeur du Centre d'étude et de documentation sur la démocratie directe, a indiqué dans une récente étude sur

le vote électronique qu'il faudra attendre une génération après la généralisation du vote électronique pour qu'un effet vraiment important puisse être constaté.

La participation n'est donc pas un objectif principal aujourd'hui pour ce projet en particulier. Pour les Suisses de l'étranger, c'est le seul moyen de voter, puisqu'ils reçoivent le matériel de vote à quelques jours des votations.

A une question de commissaire sur l'ambiguïté du qualificatif de « transparence » tel que les patients genevois avec mondossiermédical.ch, M^me^ Wyden Guelpa indique que la question s'est posée, et qu'il n'est pas exclu qu'elle puisse un jour jouer un rôle en la matière. Là où cela diffère de mondossiermedical.ch, c'est que la Poste a recours pour le vote à une entreprise privée étrangère, ce qui n'est pas acceptable pour Genève. Si ces liens n'existent plus, il sera envisageable de travailler ensemble.

A une question de commissaire sur les 3 systèmes mentionnés, M^me^ Wyden Guelpa indique que le système américain Unisys s'est mis en difficulté tout seul. Les trois systèmes existaient jusqu'au 12 août, date où Unisys n'a plus pu continuer à être utilisé par le consortium, suite à une décision du Conseil Fédéral. Le consortium s'est dissout il y a trois semaines. Simultanément, Neuchâtel a rejoint la Poste, un peu sous pression de Scytl, afin que ce dernier n'ait plus qu'un seul interlocuteur en Suisse.

Il s'agit donc maintenant d'un marché réduit et qui est devenu concurrentiel.

A une question de commissaire sur la possibilité qu'en famille une personne vote pour tout le monde, Mme Wyden Guelpa remarque que le vote familial ne peut être exclu ni pour le vote électoral ni pour le vote par correspondance, puisqu'il n'existe pas de registre des signatures. Cela fait donc partie des risques connus.

A une question de commissaire concernant des précisions quant au timing en rapport avec le fait que « le périmètre d'application et les modalités de publication du code source doivent toutefois encore être précisés et normés, consécutivement à l'analyse des risques et des opportunités actuellement en cours, et qui pourra être confiée aux députés lors de l'examen du présent projet de loi » (exposé des motifs, p. 10) il semblerait que l'on voterait un PL pour plus de transparence, alors que simultanément des incertitudes apparaissent déjà dans l'exposé des motifs, M. Favre indique qu'avant de présenter ce PL, des contacts avaient été pris avec des spécialistes en sécurité. Les incertitudes qui régnaient au moment de la rédaction du PL ont aujourd'hui des réponses, qui seront formulées dans un rapport en cours de rédaction, raison pour laquelle il n'a pas été amené aujourd'hui. Il sera distribué aux députés.

Le concept est de passer à l'étape finale par de petits mouvements maîtrisés, car il est certain que le jour où quelqu'un indiquera une faille du système, cela alertera toute la République.

**Proposition d'audition**

L'audition de M. Alexis Roussel *ad personam* est acceptée à l'unanimité de la commission.

Le Président indique que M. José Nunes, alors président du GULL (Groupe romand des utilisateurs/trices de GNU/Linux et de Logiciels libres), s'était exprimé en 2008 sur le sujet et propose son audition ou celle de son successeur à la présidence du GULL, puisque Linux a été cité en exemple par M. Favre.

Un commissaire propose de regarder avec le CUI (Centre Universitaire d'Informatique) de Genève si l'on veut avoir une opinion indépendante. Le CUI est en effet en pointe dans le domaine. Une autre proposition est faite : l'audition de la CEC étudie des rapports sur l'évolution du vote électronique. Cela permettrait aussi d'avoir un regard sur l'accessibilité du code source aujourd'hui. Il propose donc d'écrire au président de la CEC pour savoir si elle s'est penchée sur la problématique de l'accessibilité au code source. Si ce n'est pas le cas, une audition n'est pas nécessaire, mais dans le cas contraire, la demande sera maintenue

***Cette proposition est adoptée à l'unanimité de la commission.***

**14.10.2015, Audition de M. Alexis Roussel (Fondateur du Parti Pirate)**

M. Roussel rappelle que Genève fut l'un des premiers endroits dans le monde à mettre en place le vote par internet. Il remarque que cette technologie est particulière, puisqu'elle s'inscrit dans un changement profond de la société. Celui-ci réside dans la manière de communiquer, de travailler et de prendre des décisions, qui a beaucoup évolué avec la technologie. En tant qu'outil au cœur du processus démocratique, le vote électronique pose forcément des questions.

*Evolution de la technologie*

Elle a amené certains changements de paradigme dont on commence à prendre la teneur. Le phénomène de la distribution et décentralisation des réseaux en est un excellent exemple. Auparavant, une personne ou une institution avait le savoir, et tout le monde devait passer par cette personne ou institution pour obtenir la connaissance. M. Roussel explique que la société actuelle, et notamment internet, est en train de passer à un système décentralisé – soit dont l'information est répartie en plusieurs lieu, plus proches des

individus – ou même à un système distribué – où chaque point du réseau peut communiquer avec un autre. Ceci se voit en premier lieu dans la communication avec internet, qui permet de communiquer à travers toute la planète. Par conséquent, les notions de sécurité et de tiers de confiance ont évolué.

*Sécurité*

Autrefois, la sécurité résidait dans la confiance en une personne ou institution, alors que c'est maintenant le réseau en lui-même qui créé la confiance dans un réseau centralisé ou distribué. C'est comme cela que fonctionne internet.

M. Roussel indique que dans le monde physique, la sécurité est assurée par un milieu fermé hermétiquement. C'est sur ce modèle qu'ont été construits les systèmes sur internet jusqu'à peu. Mais un changement est apparu, parce que dans un modèle décentralisé ou distribué, la transparence amène la sécurité. La transparence dans le monde informatique consiste à avoir un protocole de communication ouvert et partagé, afin que personne ne puisse retirer une information ou la mettre en doute, car elle a déjà été partagée et distribuée. C'est en mettant à la vue de tous le processus que l'on peut sécuriser l'information.

Le premier grand changement est donc le tiers de confiance, qui devient réseau de confiance, et le second changement est la sécurité, qui n'est plus synonyme d'obscurité et de garde armée, mais de transparence et de distribution. Cette facette de la sécurité est possible par un autre élément qu'est la cryptographie, et qui permet à des moments précis de venir occulter une information particulière qui ne doit pas être partagée. Aujourd'hui, on voit tout le processus, mais certains des éléments, que l'on veut protéger particulièrement, le sont par un processus extrêmement puissant.

Dans le cadre de Genève, qui est l'un des premiers cantons à avoir obtenu cette technologie, un apprentissage est en cours. Les difficultés d'entrer dans un monde numérique ne résident pas dans un seul projet, mais dans tous, en particulier pour les processus et interactions.

Pour ce qui est du PL en soi, M. Roussel indique que la loi actuelle traduit une sécurité par l'occultation, plus physique qu'informatique, et qui, avec des gens compétents et selon des processus humains, permet de s'assurer que le système et le code ne puisse être atteint de l'extérieur.

*PL 11701 et nouvelle approche*

M. Roussel estime que cette approche présente deux failles. La première est celle de ne pas prendre en compte l'évolution qu'il a décrite précédemment.

La seconde est le fait de cacher quelque chose, ce qui signifie qu'il y a quelque chose à trouver. La réaction est naturelle : si on cache, on incite à fouiller.

Là où ce PL est très intéressant, c'est qu'il s'agit d'une des premières fois où, en partant d'un processus informatique extrêmement liant entre le citoyen et l'Etat, on cherche à l'ouvrir dans un objectif de création de confiance. À terme, cette confiance ne peut résider que dans un réseau. L'un des enjeux de ce PL est donc de paver la route à un univers où la confiance résidera dans le réseau et non dans des tiers de confiance.

*Expérience du Parti Pirate*

M. Roussel rappelle que le Parti Pirate avait fait un audit citoyen du vote électronique. Des conditions ont été fixées pour ce faire, qui ne sont pas idéales, puisque le Parti Pirate a eu accès au code sur un ordinateur dans une salle du bâtiment du Département, et les informaticiens ont dû lire le code sans outil informatique à disposition, ce qui est un procédé archaïque dans le domaine informatique. Si l'informaticien est capable de lire le code sans outil, le travail s'effectue aujourd'hui grâce à des programmes qui permettent de repérer les défauts du code, de l'éprouver et de vérifier sa sécurité.

Un peu par hasard, le Parti Pirate a découvert qu'un informaticien avait reconstruit une partie du code de son côté. Il l'a ensuite testé et attaqué dans ce milieu clos et a repéré un certain nombre de failles de sécurité, qu'il a présenté lors la « nuit du hack » 2013, un sommet de hackers à Paris. Cela a représenté un investissement en temps énorme de sa part, pour simuler une infrastructure de l'Etat et l'attaquer.

Une première étape est d'indiquer que par défaut le code source doit être public dans la loi. Évidemment, le Conseil d'Etat se garde encore la réserve de fixer des conditions pratiques. Pour ce qui est du contrôle de la CEC, qui peut se faire en tout temps, M. Roussel estime qu'il s'agit d'un autre point très important auquel il a participé pendant un an jusqu'à ce qu'il déménage sur le territoire d'un autre canton. La CEC est aussi en train d'évoluer et tente d'avoir en son sein les outils et les compétences pour assurer une surveillance effective du vote électronique. Le PL permet à la CEC d'avoir d'abord les moyens légaux et ensuite humains de contrôler la sécurité. Il est aussi nécessaire que le code source puisse être vérifié par le public, et pas seulement les citoyens genevois, car un grand nombre de personne partout dans le monde est intéressé au vote électronique, simplement de manière idéale. Par ailleurs, lorsqu'il est en cours d'utilisation, donc pendant une période de vote, le vote électronique est ouvert au monde entier. Bloquer l'accès à des frontières étatiques alors que sur internet il est disponible ne paraît donc pas adéquat, surtout lorsque des

millions d'informaticiens de par le monde pourraient l'étudier et le critiquer de manière à l'améliorer.

***Questions de la commission***

A la question d'un commissaire concernant la motivation du Parti Pirate à avoir accès au code, M. Roussel répond que cela a pris presqu'une année entre le moment ou le Parti Pirate a voulu avoir accès et le moment où il l'a eu, mais quelques mois seulement entre le moment de la demande et la dernière séance de consultation.

Sur les raisons, il explique que le Parti Pirate, en tant que jeune parti au niveau européen, et comme tout mouvement politique neuf, vivait un moment d'établissement de sa personnalité. À ce titre, il est arrivé dans une approche forte demandant à ce que le code source soit ouvert, faute de quoi il ne valait à rien. C'est en effet connu dans le monde informatique qu'un logiciel ouvert apporte des garanties supplémentaires en matière de sécurité. À travers les différents échanges, il a été suggéré au parti de participer à l'audit, pendant plusieurs séances. Le code source n'a pas pu être étudié dans son intégralité, et donc un rapport n'a pu être donné que sur une vue d'ensemble.

D'un point de vue plus personnel, M. Roussel explique que lors de ses études, il a fait partie de l'un des premiers 3ème s cycles qui alliaient numérique et institution, et donc ces questions étaient très suivies à la fois par les juristes et les informaticiens. Sa réflexion à l'époque était de se dire qu'il aurait fallu d'abord informatiser les autres processus de la société, afin d'avoir d'autres expériences et d'acquérir une certaine maîtrise de ces processus, et ensuite informatiser le vote. L'Etat de Genève a décidé un geste fort, en faisant des erreurs de jeunesse naturelles, qui ont résulté principalement de la volonté d'appliquer la meilleure approche connue à l'époque, et qui est encore utilisée par les entreprises, mais qui ne peut fonctionner au sein d'une démocratie, et qui est celle d'une centralisation de la sécurité. Encore une fois, la confiance que l'on a en une institution se fabrique différemment de celle que l'on a en une personne.

Dans la communauté informatique, beaucoup de personnes estiment que parce que les outils ne sont pas encore parfaits, il faut refuser le vote électronique. Le parti pirate a préféré accompagner le canton dans sa démarche.

A la question d'un commissaire qui demande ce que signifient exactement les termes « pirates » et « hacker », M. Roussel explique que hacker est très mal utilisé. Le terme signifie en anglais « ouvrir le capot », ou encore « bidouiller ». Il y a une culture du hacker, dont le Parti Pirate est issu.

Aujourd'hui on appelle cela Maker, cela représente le fait que le hacker, ou informaticien, plonge ses mains dans le cambouis d'un moteur que serait le programme pour travailler dessus. C'est l'idée du « do it yourself », avec les outils à disposition. Sur internet, il existe différents types de hackers, que l'on appelle « white hat » ou « black hat ». Les seconds sont ceux qui ont donné cette mauvaise consonance au terme hacker, même s'ils n'en représentent pas la majorité

A la question d'un commissaire qui remarque que M. Roussel a mentionné la cryptologie pour certains éléments de sécurité qui ne sont pas transparents, M. Roussel indique qu'une sécurité centralisée est à l'image d'une banque. Si on l'attaque, il suffit de percer un coffre pour accéder aux lingots de tout le monde. Dans le cas d'un réseau distribué, chaque point du réseau ne peut être attaqué que sur l'information qu'il va produire pour l'ensemble du réseau. Si le réseau dans son ensemble était attaqué, il serait peut-être paralysé, mais aucune information ne pourrait être lue. De même, il faudrait pirater l'ordinateur d'un citoyen pour connaître son vote. La situation actuelle est celle d'un réseau centralisé, et si une attaque réussissait sur le serveur de l'Etat, cela permettrait de modifier l'ensemble du vote. Il s'agit par exemple du cas de l'affaire Ashley Madison, qui centralisait ses données. Certains réseaux distribués sont connus du grand public, comme TOR ou BitTorrent. Leur maîtrise n'est pas possible, car chaque utilisateur dispose d'une partie du code, dupliquée des milliers de fois. Cela amène donc un autre changement de société, qui est l'éducation informatique, car la sécurité réside dans chaque ordinateur. Il faut donc accompagner la population dans cet apprentissage.

A la question d'un commissaire qui demande si le partage du code source se fait déjà au niveau d'institutions ou d'entités qui demanderaient de grandes sécurités, M. Roussel indique qu'en Norvège, une expérience de vote électronique a été faite en 2011 et 2013. Au début, la communauté a été violente, et le Gouvernement a donc pris la mesure de publier le code source pendant une période donnée. Il y a eu deux à trois cents téléchargements, et aucun retour. Le fait que le code source ait été ouvert, a donc calmé la communauté informatique, car il a été téléchargé par quelques personnes qui n'ont pas trouvé de choses flagrantes, et la communauté est passée à autre chose. L'état de Washington désirait créer un système de vote informatique, et a décidé de tester sa sécurité en 2010 au cours d'une fausse élection en invitant n'importe qui à tenter de le pirater. Ce fut fait en deux jours par une équipe d'étudiants, qui a changé les votes, les noms des candidats, et toutes les autres données disponibles, ce qui serait passé inaperçu si certains changements n'étaient pas trop visibles. Ceci a donc très bénéfique, parce que l'Etat allait mettre en production un système facilement piratable, qui a été retiré.

Dans le domaine des banques, qu'il connaît bien parce qu'il travaille en fintech (technologie financière), un changement de paradigme très fort est en cours. Les gros systèmes propriétaires et les consultants très chers existent toujours, mais la fintech est aujourd'hui entièrement en open source. C'est plus sûr, et cela permet de ne pas réinventer un système chaque fois qu'il est nécessaire, mais de prendre ce qui existe déjà.

*Pour ou contre le vote électronique ?*

Le Président demande si la réflexion que M. Roussel avait eue il y a quelques années sur la nécessité de d'abord habituer la population à l'utilisation de l'informatique dans d'autres domaines avant de l'appliquer au vote est toujours d'actualité. Il remarque que le Groupe romand des utilisateurs/trices de GNU/Linux et de Logiciels libres (GULL) s'oppose au vote électronique pour des raisons de logiciel propriétaire.

Le Président demande à M. Roussel de prendre position pour ou contre le vote électronique.

M. Roussel indique qu'il a aujourd'hui clairement changé d'avis. Ce qui a évolué, c'est que le changement doit accompagner le monde existant, et les nouveaux mécanismes de l'humain doivent venir naturellement. La construction actuelle de la sécurité s'est faite par l'expérience de l'humain et des technologies de l'époque. Demain on aura toujours de l'humain et des technologies renouvelées, et il faut garder ce mécanisme d'apprentissage et de renouvellement. Il estime que la Suisse a des institutions à taille humaine et réactives, où la réflexion se fait. Les débats restent terre à terre sur l'application réelle de ces outils au quotidien. Tout en se rendant compte que le vote électronique et le passage de processus à l'informatique de manière générale amène la réflexion sur des choses fondamentales que l'on croyait établies depuis des centaines d'années. Dans le domaine de la finance, on se demande ce qu'est l'argent, et dans l'information, ce qu'est l'information et un texte écrit. Dans le vote informatique, on se pose la question de la relation de l'Etat et du citoyen.

Derrière cela se posent aussi des questions d'identité et de la manière dont elle est reconnue par l'Etat. Jusqu'à présent, on avait des humains qui se retrouvaient ensemble, et qui décidaient ensemble de créer une société à travers des institutions. Ce mécanisme doit se recréer à travers l'informatique, et c'est une faiblesse partagée par toutes les institutions, simplement parce que la technologie est en cours de développement dans ce domaine. En attendant, on dispose d'un système d'identification où c'est l'Etat, des entreprises ou des institutions qui donnent l'identité à un système. Par exemple, dans la procédure du vote électronique, le chiffrage de la base de données se fait par des membres

de la CEC. Pour ce faire, un ordinateur de l'Etat est mis à disposition, et les membres de la CEC entrent des mots de passe pour protéger les clés de sécurité générées sur l'ordinateur de l'Etat. Donc la clé est créée par l'Etat et protégée par un mot de passe détenu par la commission. Si on compare cela avec la signature, cela revient au fait que l'Etat impose la manière dont on doit signer. Dans le monde physique, on invente sa signature et cela certifie que cela vient bien de soi.

M. Roussel estime qu'il faut arriver à un système ou lui en tant que citoyen dispose d'une signature informatique qu'il doit pouvoir utiliser pour signer des actes numériques et chiffrer l'urne électronique. On peut même imaginer que cette clé soit validée par un mandat. Cela permettrait à un auditeur externe de voir que la signature de M. Roussel a bien été utilisée à cette date-là, et qu'elle avait été autorisée pour un certain nombre d'opérations électorales. Il n'existe pas de technologie qui permette réellement cela. Le SwissID ne répond pas à ces normes, car la signature est attribuée par la Confédération. La situation actuelle est la même que celle des gens qui ne savaient pas encore lire et écrire et qui signaient avec une croix. M. ROUSSEL a bon espoir que cela change, car il s'agit aussi d'une facette des droits fondamentaux.

*Langage informatique*

Le Président demande si, puisque la majorité des gens ne savent pas lire et écrire en langage informatique et donc que la transparence est réservée à une petite élite d'informaticiens, il ne vaudrait pas mieux attendre que l'alphabétisation atteigne un degré plus avancé.

M. Roussel rappelle que l'évolution de l'éducation va de pair avec celle des nécessités. Entre l'invention de l'imprimerie et la généralisation de l'éducation et donc de la lecture et de l'écriture, plusieurs centaines d'années se sont écoulées. Les processus démocratiques ont commencés bien avant, mais lors de l'évolution humaniste et du développement de la démocratie directe au début du XIX$^{e}$ siècle, seul 20% de la population en Suisse était capable de lire et écrire. Ce sont des processus qui vont ensemble, il n'y aura pas de volonté des domaines d'éducation d'apprendre une chose inutile.

A une question de commissaire s'inquiétant des risques encourus si les serveurs et les données se trouvaient ailleurs qu'en Suisse, M. Roussel estime que l'on peut se poser des questions sur certains appareils et technologies, mais que dans le cas du vote électronique, au moins le contrôle reste, selon le principe du coffre-fort unique, entre les mains de l'Etat et de ses employés. Il n'y a donc pas de risque avec le système actuel. Dans un réseau distribué, les données ne sont pas en Suisse ou aux Etats-Unis, mais partout en même temps. Des questions se posent donc sur la communication et la circulation des

informations, d'où l'importance d'avoir des sécurités. De ce côté-là, l'Etat de Genève et sa Chancellerie sont bien au clair, même si M. Roussel remarque que la Confédération ne s'implique pas assez dans ces problématiques car il lui manque encore une prise de conscience de l'importance de l'informatique dans ses infrastructures. Par exemple, cette dernière désirait mettre un Cloud chez HP, soit un serveur informatique aux Etats-Unis.

A une question de commissaire concernant des expériences de vote par internet dans d'autres cantons en Suisse, ainsi que de l'open source, M. Roussel indique qu'il existe deux projets de vote électronique en Suisse en plus de celui de Genève. Le premier est celui d'un conglomérat de cantons et utilise un programme américain. Le second est celui de Neuchâtel et utilise un logiciel espagnol appelé Scytl. Par ailleurs, le logiciel genevois est utilisé par certains autres cantons. Dans son souvenir, Neuchâtel le vote électronique à Neuchâtel est réservé aux Suisses de l'étranger. Il lui semble que Scytl utilise une technologie open source, et en tout cas, en tant qu'habitant du canton de Neuchâtel, il n'a vu aucun débat en ligne ou parmi la population neuchâteloise à ce sujet. Pour ce qui est du conglomérat, le code du programme n'est pas en open source.

*Chancellerie fédérale*

M. Roussel indique que la Chancelière fédérale fait un travail d'accompagnement du vote électronique dans les cantons par certaines étapes qui correspondent à certaines conditions, par exemple la vérifiabilité, qui, il lui semble, vient d'être mise en œuvre à Genève. On se rend compte que le projet open source neuchâtelois utilisé par d'autres institutions dans le monde a pu intégrer très facilement cette vérifiabilité, alors que Genève a un peu peiné et que le conglomérat n'a pu le faire, ce qui a disqualifié le système de vote utilisé pour les prochaines votations et élections. La Chancellerie fédérale est très consciente des évolutions et des nécessités du vote électronique, mais son approche se fait au rythme des cantons.

*Communauté informatique*

Pour ce qui est de la manière d'intéresser les informaticiens, M. Roussel explique que les raisons divergent grandement. Il indique que 95% des logiciels utilisés actuellement pour l'informatique ont été créés par des gens qui n'ont pas été rémunérés pour cela. Les raisons principales sont la possibilité de dupliquer le code pour un usage similaire, la mise à disposition d'un outil développé pour un usage privé, ou encore la reconnaissance. M. Roussel estime qu'il suffit de parler le langage des informaticiens, et à ce titre est très content de constater que la mise en place d'un poste pour le partage du code et la communication a été prévue par le PL.

À propos de la communication avec la population, il estime qu'à long terme, cela se fait par l'éducation. De manière plus immédiate, M. ROUSSEL estime que si un citoyen a des doutes quant à la publicité de son vote, la première chose qu'il fera est de se renseigner auprès de ses proches, et si possible auprès de celui qui est le plus doué en informatique. Si celui-ci ignore la réponse, il connaîtra peut-être quelqu'un qui la possède et le retour sera donc positif.

M. Roussel indique que certaines sociétés développent des logiciels et veulent les faire tester. Cette question s'est donc déjà posée et les réponses principales sont le bug bounty et la reconnaissance.

Le bug bounty est une rémunération pour la découverte de bugs inconnus du développeur. Facebook utilise ce procédé et rémunère 1000 dollars chaque personne qui découvre un bug inconnu jusqu'alors. Ce sont des coûts de développement externes.

Pour ce qui est de la reconnaissance, un grand nombre de logiciels propose de publier sur leur site par exemple le nom des informaticiens qui ont découverts des problèmes ou participé indirectement au développement de leur logiciel.

Le citoyen genevois ayant fait la présentation de son hack du système de vote genevois lors de la « nuit du hack » à Paris a fait son analyse de son côté, parce que lui utilisait ce programme et s'y intéressait. Si un tel travail avait été demandé à un consultant professionnel, le coût se chiffrerait en dizaines de milliers de francs, alors que ce citoyen l'a fait gratuitement par simple intérêt.

A une question de commissaire concernant le risque de fausser volontairement un vote, M. Roussel salue tout d'abord l'approche itérative de l'équipe qui développe actuellement le logiciel et garde donc une grande maitrise du système. Cette approche étape par étape est aussi présente du point de vue fédéral avec l'ouverture progressive accompagnée de critères, et qui limite aujourd'hui la participation à 30% des votants. Ceci permet de comparer les résultats du vote électronique avec ceux du vote papier ou à l'urne, et de vérifier que la moyenne est similaire.

M. Roussel estime que si le processus est intéressant pour la communauté informatique internationale, ce n'est pas le cas des résultats du vote du canton de Genève. Le problème serait certainement beaucoup plus important pour un pays comme les Etats-Unis. Au vu des investissements en temps et en argent qu'implique l'éventuelle attaque non détectée d'un tel logiciel, il est très peu probable que cela soit rentable.

**Conclusion**

Concernant ce PL 11701, M. Roussel indique qu'il s'agit du changement fondamental dans l'approche de la sécurité dans tous les domaines de l'informatique et où une information cachée attire la convoitise. Aujourd'hui, la manière de sécuriser une information est de rendre le processus, son emplacement et les protocoles publics. Cela permet un partage, qui assure que l'information, si elle est modifiée quelque part, ne puisse l'être partout.

Dans un monde entièrement transparent, on sécurise uniquement la partie importante, soit en l'occurrence le vote avec un chiffrement fort.

Aujourd'hui, on a donc un coffre-fort devant lequel on met un garde et qui contient tous les votes, alors que demain, le but est d'avoir un champ ouvert que tout le monde peut voir, mais chaque vote sera protégé par un coffre-fort individuel dont chaque clé est différente de celle d'un autre.

À titre personnel, M. Roussel indique qu'il soutient, et son Parti aussi, la démarche de la Chancellerie. C'est à la fois quelque chose de nouveau, ce qui est très rare dans les institutions. Ce PL est aussi l'une des étapes du chamboulement actuel de la société, et ne sera pas la dernière.

**Votes**

Le président met aux voix l'entrée en matière du PL 11701.

| | |
|---|---|
| Pour : | **14** (1 EAG, 3 S, 1 Ve, 1 PDC, 3 PLR, 2 UDC, 3 MCG) |
| Contre : | **0** |
| Abstention : | **0** |

**L'entrée en matière du PL 11701 est acceptée.**

Le Président propose de procéder au vote de deuxième débat :

**Titre : pas d'opposition adopté ;**

**Art 1 souligné : pas d'opposition adopté ;**

**Art. 60 al. 8 : pas d'opposition adopté ;**

**Art. 60 al. 9 : pas d'opposition adopté ;**

**Abrogation de l'art. 60 al. 10 : pas d'opposition adopté ;**

**Art. 193 al. 3 (nouveau) : pas d'opposition adopté ;**

**Art. 193 al. 4 (nouveau) : pas d'opposition adopté ;**

**Art. 193 al. 5 (nouveau) : pas d'opposition adopté ;**

Suite à une remarque du président, M. Mangilli explique que les champs « (*à compléter)* » de l'art. 193 sont présents parce que lors de son dépôt, le Conseil d'Etat ignore quel numéro sera attribué au PL et à quelle date il sera voté. Si l'on peut déjà attribuer le numéro du PL dans le rapport, il sera encore nécessaire d'y intégrer la date où il sera adopté par la séance plénière cas échéant. On pourrait donc remplacer les champs « *(à compléter)* » par « 11701 du *(à compléter)* », même si cela peut être fait encore par la séance plénière, qui devra de toute manière compléter la date.

Le Président continue le vote en deuxième débat :

**Art. 2 souligné : pas d'opposition, adopté.**

Le Président propose de passer au troisième débat et demande s'il y a des déclarations de groupe avant le vote.

**Position des groupes**

Le MCG acceptera le PL. Si le groupe n'était pas au départ convaincu, la présentation du PL par la Chancellerie et l'audition de M. Roussel y ont remédié.

Le PLR indique avoir eu des réserves mais l'audition de M. Roussel a été rassurante et convaincante. Le PLR votera donc également en faveur du PL en soulignant l'importance de parler de « traçabilité » encore plus que de « transparence ».

Le groupe Socialiste se rallie au PL. Le groupe était déjà convaincu après la présentation par la Chancellerie, et l'exposé on ne peut plus clair de M. Roussel a confirmé sa position.

L'UDC votera le PL, mais relève l'importance de la communication destinée au public.

Le groupe des Verts votera ce PL pour faire suite aux deux interventions extrêmement complètes. Les Verts souhaitent féliciter le canton d'avoir pris l'initiative de financer son propre code source plutôt que de l'externaliser, ce qui lui permet de garder une totale maîtrise des processus.

Le PDC votera ce PL avec l'enthousiasme d'être pionnier en la matière.

Le Président indique, pour le groupe Ensemble à gauche, qu'il soutiendra ce PL.

**En troisième débat**

En conclusion, le président estime que c'est surtout sur le processus qu'il faut insister, car que l'on parle de transparence ou de traçabilité, c'est de lui et

non du vote en lui-même que l'on parle. Il fait confiance au rapporteur pour préciser ces éléments avec talent.

M. Mangilli indique qu'il est évident pour le Conseil d'Etat que la transparence doit être faite sur l'architecture et la mécanique du système de vote et non les votes eux-mêmes, dont le secret est garanti par un certains nombres ne normes législatives, tant cantonales et fédérales qu'internationales.

**Le Président met aux voix l'acceptation en troisième débat du PL 11701.**

| | |
|---|---|
| Pour : | **14** (1 EAG, 3 S, 1 Ve, 1 PDC, 3 PLR, 2 UDC, 3 MCG) |
| Contre : | **0** |
| Abstention : | **0** |

***L'acceptation en troisième débat du PL 11701 est approuvée à l'unanimité.***

*Il est proposé de traiter le présent PL aux extraits.*

# Projet de loi
**(11701)**

**modifiant la loi sur l'exercice des droits politiques (LEDP) (A 5 05)** *(Accès au code source du vote électronique)*

Le GRAND CONSEIL de la République et canton de Genève
décrète ce qui suit :

## Art. 1 Modifications

La loi sur l'exercice des droits politiques, du 15 octobre 1982, est modifiée comme suit :

**Art. 60, al. 8 et 9 (nouvelle teneur), al. 10 (abrogé)**

[8] Le Conseil d'Etat prend les mesures nécessaires afin de rendre public le code source des applications permettant de faire fonctionner le vote électronique. Il fixe les conditions, l'étendue et les modalités pratiques de cette publicité.

[9] Les membres de la commission électorale centrale ont accès en tout temps au code source mentionné à l'alinéa 8.

**Art. 193, al. 3 à 5 (nouveaux)**

***Modifications du … (à compléter)***

[3] Durant un délai de 3 ans à compter de l'entrée en vigueur de la loi 11701 du … *(à compléter)*, sous réserve de l'article 60, alinéa 8, et de l'alinéa 4 de la présente disposition, le code source des applications permettant de faire fonctionner le vote électronique, de même que les documents liés à la sécurisation du système, ne peuvent être communiqués à des tiers sur la base de la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001.

[4] Durant un délai de 3 ans à compter de l'entrée en vigueur de la loi 11701 du … *(à compléter)*, le code source mentionné à l'article 60, alinéa 8, peut être éprouvé, sans toutefois être reproduit, par tout électeur qui justifie d'un intérêt scientifique et purement idéal et qui s'engage à en respecter la confidentialité. Le Conseil d'Etat fixe les conditions et modalités de ce test.

[5] A l'échéance d'un délai de 3 ans à compter de l'entrée en vigueur de la loi 11701 du … *(à compléter)*, le Conseil d'Etat présente un rapport au Grand Conseil sur la mise en œuvre de l'article 60, alinéa 8 (publicité du code source).

**Art. 2 Entrée en vigueur**

Le Conseil d'Etat fixe la date d'entrée en vigueur de la présente loi.

*ANNEXE 1*

# La transparence
# Gage de sécurité et de confiance

Anja Wyden Guelpa – Chancelière d'Etat
Eric Favre – Directeur Général de la DGSI
Nicolas Arni-Bloch – Directeur de la DSOV



## La confiance est indispensable pour les droits politiques et nécessite de la transparence

## Le vote électronique : une chance pour la démocratie?

**Une opportunité pour faciliter l'exercice des droits politiques**

Exemples: Suisses de l'étranger (1er canal de vote), personnes en situation de handicap

**Une plateforme technologique**

Promouvoir une nouvelle image de l'administration, administration en ligne

**Adapté aux nouveaux besoins**

Exemple : tablettes des électeurs



## La transparence, pourquoi une nouvelle étape?

- Suite logique, après 2003 (supervision par la CEC) et 2009 (consultation du code source sur demande)
- Le **vote électronique** : mêmes exigences, mêmes valeurs que le **vote papier**

## La transparence, pourquoi une nouvelle étape?


Ouvrir le code source permet à la communauté scientifique et hacker :

- de **s'approprier** l'outil démocratique et
- de **l'améliorer**

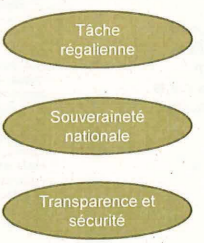


## Et les autres cantons?

Depuis septembre 2015, il ne reste plus que deux systèmes:

**Canton de Genève**
(VE depuis 2003)

**La Poste**
(Annonce d'un projet de VE en septembre 2015)



## CHVote Avantages du système genevois

### 100% PUBLIC

- Système développé en interne par l'Etat de Genève
- Pas de sous-traitance: Infrastructure et support par l'Etat de Genève, développement et exploitation intégralement assurés par les collaborateurs de la Direction générale des systèmes d'information
- Propriété intellectuelle appartenant à l'Etat de Genève

### FIABLE

- Près de 120'000 électeurs (Suisses de l'étranger et résidents) bénéficient du système genevois
- 39 opérations à Genève, près de 12 ans d'exploitation
- Votations, élections : CHVote est l'un des 2 systèmes de vote électronique autorisés par le Conseil Fédéral pour les élections des chambres fédérales (août 2015)
- 3 cantons hébergés nous font confiance depuis plusieurs années (BS, BE, LU)



## Qu'est-ce que le code source ?

Le code source est un ensemble de **textes** qui contiennent des **instructions** pour piloter des ordinateurs (ou robots, smartphones, TV, voitures, avions, etc.), **rédigées par des informaticiens,** dans un langage compréhensible à la fois par la machine et par d'autres informaticiens.

**CODE SOURCE**

```
public class HelloWorld {
    public static void main(String[] args) {
        System.out.println("Hello, World");
    }
}
```

*«Hello, World» est par coutume le premier programme écrit par chaque informaticien. Ce texte est ensuite interprété par la machine, qui affiche* Hello, World.
*Le langage informatique utilisé ici se nomme «Java». Très largement enseigné et employé, il est le langage informatique le plus populaire aujourd'hui.*
*Le système de vote électronique genevois est programmé en Java par la DGSI. L'ensemble du code source comporte environ 80'000 lignes.*

## Pourquoi ouvrir le code source ?

**Transparence** ⇒ **Confiance**

**Situation actuelle**

- Contrôle de la totalité du processus par une commission indépendante
- Gouvernance publique: Audits externes réguliers du système (2012, 2015,…)
- Code source analysé en 2012 (Parti Pirate, Haute école spécialisée bernoise –BFH-)

**Bénéfices de l'ouverture du code source**

- Plus de fiabilité : le cœur du système est accessible à tous pour l'analyse et la critique
- Plus d'innovation : susciter davantage d'intérêt et de suggestions de la part du public
- Plus de contrôle : le public peut vérifier la qualité du code

**Risque**

Consécutif par exemple à la découverte d'une faille ou à des critiques sur la qualité du code source



## Ouverture progressive du code source

**Cadrer**

- Définir les périmètres successifs à publier
- Réaliser les audits de code
- Définir le modèle de licence approprié, instaurer les "règles du jeu
- Produire la documentation associée et fournir un environnement de test si nécessaire

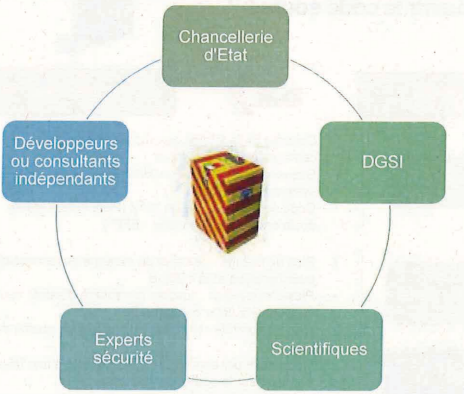
**Ouvrir**

- Définir les médias de communication : blog, forum, réseaux sociaux?
- Modérer les échanges

**Répondre**

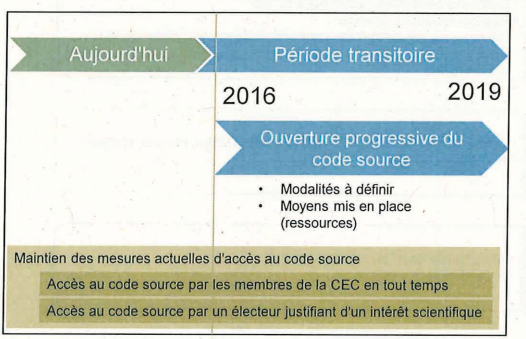
- Analyser les propositions de modification
- Faire évoluer le système

## Publication du code source : des acteurs diversifiés






## Projet de Loi et échéances



*ANNEXE 2*

REPUBLIQUE ET CANTON DE GENEVE
Chancellerie d'Etat
**Commission électorale centrale**

GRAND CONSEIL
reçu le 14 OCT. 2015

CHA - CEC
Case postale 3964
1211 Genève 3

Monsieur Pierre VANEK
Président de la Commission des droits politiques
Grand Conseil
Rue de l'Hôtel-de-Ville, 2
Case postale 3970
1211 Genève 3

*N/réf. : ST/VVB*

Genève, le 13 octobre 2015

**Concerne : PL 11701 Projet de loi du Conseil d'Etat modifiant la loi sur l'exercice des droits politiques (LEDP) (A 5 05) (Accès au code source du vote électronique)**

Monsieur le Président,

Je me réfère à votre correspondance du 8 octobre dernier au sujet du PL 11701 portant sur l'accès au code source du vote électronique.

La commission électorale centrale (CEC), selon le mandat que la loi sur l'exercice des droits politiques (LEDP) lui a confié, surveille l'utilisation et la fiabilité du système de vote électronique développé par le canton de Genève. Elle a créé en son sein, à cet effet, une sous-commission technique.

Le projet de loi en question va pleinement dans le sens défendu par la CEC vers plus de transparence. En effet, il apparaît aujourd'hui évident que le vote électronique, devenu le second canal de vote, est un outil précieux pour l'expression des droits politiques. Dans le contexte actuel, la publication du code source est le meilleur moyen de renforcer la fiabilité et la confiance dans le vote électronique.

Aussi, la CEC soutient pleinement ce projet de loi et se réjouit de l'accueil favorable que votre commission ne manquera certainement pas de lui accorder. Elle se réjouit également d'accompagner et de surveiller, une fois cette modification légale opérée, le processus de publication du code qui s'en suivra.

Je vous adresse, Monsieur le Président, mes salutations les meilleures.

Samuel Terrier
Président