GRAND CONSEIL **M 3052-A**
de la République et canton de Genève

Date de dépôt : 12 août 2025

Rapport

de la commission législative chargée d'étudier la proposition de motion de Guy Mettan, Christo Ivanov, Lionel Dugerdil, Daniel Noël, Florian Dugerdil, Julien Ramu, André Pfeffer, Stéphane Florey, Marc Falquet, Patrick Lussi, Thierry Oppikofer, Murat-Julian Alder, Jean-Pierre Pasquier pour préserver la souveraineté numérique du canton de Genève

Rapport de Diego Esteban (page 3)

ATAR ROTO PRESSE – 80 ex. – 08.25

Proposition de motion
(3052-A)

pour préserver la souveraineté numérique du canton de Genève

Le GRAND CONSEIL de la République et canton de Genève
considérant :

– le nouvel article constitutionnel relatif au droit à l'intégrité numérique (art. 21A) ;
– que l'intégrité numérique inclut notamment le droit d'être protégé contre le traitement abusif des données liées à sa vie numérique, le droit à la sécurité dans l'espace numérique, le droit à une vie hors ligne ainsi que le droit à l'oubli ;
– les risques liés au hacking, à la cybersécurité et à la protection des données personnelles des citoyens ;
– que, d'après la disposition constitutionnelle, le traitement des données personnelles dont la responsabilité incombe à l'Etat ne peut s'effectuer à l'étranger que dans la mesure où un niveau de protection adéquat est assuré ;
– qu'en pratique les GAFAM imposent aux collectivités publiques de déposer leurs données dans le cloud en privilégiant des entreprises ayant des activités sur deux continents (et donc aux Etats-Unis) et non seulement sur le continent européen ;
– les risques inhérents à transférer et à héberger des données personnelles ou sensibles dans des pays ne présentant pas un haut niveau de protection ou pouvant les utiliser à des fins non souhaitées ;
– les possibilités de s'appuyer sur le savoir-faire des entreprises genevoises et suisses pour préserver notre souveraineté numérique,

invite le Conseil d'Etat

– à établir une stratégie de protection et de souveraineté numérique cantonale, en concertation avec les communes ;
– à utiliser les ressources et les entreprises locales (par exemple Infomaniak, Protonmail, ID Quantique) ou nationales (par exemple Threema, Sharekey, The Cosmic Dolphins) et à stocker les données dans des datacenters basés exclusivement en Suisse et ne transférant pas les données à des tiers.

Rapport de Diego Esteban

La commission législative a étudié cette proposition de motion sous la présidence de M. Vincent Canonica lors des séances des 6 décembre 2024 et 10 janvier 2025. Les procès-verbaux ont été tenus par M[mes] Clara Veuthey et Selma Bentaleb. M[mes] Athina Hanna, directrice des affaires juridiques de la Chancellerie, Coralie Pasche, directrice adjointe (DAJ – CHA), et Tina Rodriguez, secrétaire scientifique du secrétariat général du Grand Conseil (SGGC), ont suivi les travaux sur cet objet parlementaire. Ces personnes sont remerciées pour leurs précieuses contributions aux travaux de la commission.

Synthèse

Les travaux de la commission sur cet objet ont été brefs, limités à l'audition du premier signataire et à celle du département et de l'office compétents.

Le but de la motion est de permettre à l'Etat de se doter d'une stratégie cohérente en matière de protection des données, de favoriser les entreprises locales lorsque l'Etat a recours à des prestataires externes, et de stocker ses données sur le territoire suisse.

Auditionnés à ce sujet, le Conseil d'Etat et les services de l'administration compétents ont fourni des informations détaillées sur le cadre légal, la stratégie de l'administration cantonale et les enjeux de collaboration avec la Confédération et les autres cantons.

Il ressort de cette audition que la réglementation relative aux marchés publics ne permet pas de favoriser des entreprises locales au détriment des autres. Cette motion ne permettrait pas de s'en affranchir. Il semble également évident que l'Etat de Genève dispose d'une stratégie complète en matière de souveraineté numérique, mais que cette souveraineté doit être fédérale, pas seulement cantonale. Genève s'engage ainsi à l'échelle fédérale sur ces questions.

Au vu de la qualité et de la quantité des informations fournies par le Conseil d'Etat et par l'administration, une majorité incontestée de la commission a estimé que la motion pouvait être rejetée. Non pas en raison de l'irrecevabilité de ses demandes, mais du fait qu'en cas d'adoption de la motion, le futur rapport du Conseil d'Etat n'apporterait rien de neuf au Grand Conseil par rapport au contenu de l'audition précitée.

Séance du 6 décembre 2024 : audition de M. Guy Mettan, premier signataire

M. Mettan indique à la commission que ses réflexions sont nées d'un séminaire organisé par la Banque cantonale de Genève et d'auditions du responsable de la cybersécurité de la police cantonale comme du préposé à la protection des données du canton du Valais. Il observe des lacunes en matière de protection des données dans les administrations publiques suisses ainsi qu'une tendance à l'externalisation de la gestion de ces données à des entreprises étrangères, alors que des solutions locales existent. Il estime que la posture de l'Etat de Genève quant à la gestion de ces enjeux n'est pas uniforme et que le recours à des entreprises locales doit devenir la norme.

Questions des commissaires

Des commissaires (MCG) questionnent l'adéquation des moyens destinés à la lutte contre les cyberattaques, précisant que ce questionnement ne se limite pas à Genève et serait partagé par la direction d'Infomaniak. M. Mettan n'est effectivement pas certain que les solutions locales puissent remplacer l'ensemble des outils dans l'immédiat, mais que cet objectif pourrait être atteint à un plus long terme. Il insiste sur le fait que recourir à plusieurs entreprises permet de renforcer la sécurité en évitant la concentration des données au sein d'un même groupe restreint de prestataires.

Des commissaires (S) demandent si la motion est une réaction aux attaques informatiques visant des communes et qui ont récemment été médiatisées. M. Mettan répond que les services de l'Etat sont également concernés et que le risque est accru à partir du moment où des données sont stockées à l'étranger. Il indique que c'est la raison pour laquelle les banques évitent de stocker leurs données dans un autre pays. Le secteur public devrait s'en inspirer.

Ces mêmes commissaires (S) demandent ce que cette motion apporterait de nouveau à la suite de l'adoption de l'article 21A de la constitution genevoise en 2023 qui couvre globalement les mêmes enjeux. M. Mettan répond que l'objectif de la motion est de mettre en œuvre cette disposition.

Des commissaires (PLR) demandent une précision concernant la première invite afin de savoir si la stratégie vise l'Etat ou concerne l'ensemble de la population située sur le canton. M. Mettan répond que cela vise les collectivités publiques.

Ces mêmes commissaires (PLR) évoquent un postulat récemment adopté à l'unanimité par le Grand Conseil[1], précisant que les travaux à son sujet avaient identifié des outils proposés à Google et pour lesquels les entreprises locales ne proposent aucune alternative, et demandent si cette motion permet de tenir compte de ce fait. M. Mettan confirme que la motion demande de recourir aux solutions locales lorsqu'elles existent. Il s'agit également de renégocier les contrats en vue de garantir le stockage des données en Suisse, car il existe un potentiel d'amélioration sur ce point.

Des commissaires (Ve) évoquent le même postulat et demandent ce que la motion apporte de plus. M. Mettan considère que la motion est plus large que le postulat, étant donné que l'enjeu pour l'administration ne se limite pas au DIP.

Des commissaires (PLR) demandent en quoi la situation actuelle n'est pas conforme à la constitution. M. Mettan explique que l'article constitutionnel est récent, la motion vise à donner une impulsion relative à sa mise en œuvre. Il évoque la « fausse gratuité » des produits développés par les GAFAM, ce qui permet de contourner les règles relatives aux marchés publics. Une fois qu'un contrat est en place, les renouvellements se font automatiquement, sans recherche d'alternatives.

Des commissaires (LC) demandent comment l'administration fédérale gère ces enjeux. M. Mettan indique qu'en 2018, un objet parlementaire déposé par M. Fathi Derder demandait que l'administration fédérale se dote d'une stratégie, mais cette initiative n'a pas abouti.

Des commissaires (UDC) demandent s'il existe des exemples dans le secteur bancaire d'un établissement qui traite exclusivement ses données en Suisse. M. Mettan ne peut citer d'exemple précis.

Ces mêmes commissaires (UDC) demandent si la deuxième invite, qui emploie le terme « exclusivement » alors que les normes européennes offrent parfois une protection supérieure au droit suisse, peut être amendée dans le sens de lui préférer l'expression « de préférence ». M. Mettan ne voit pas de raisons de s'y opposer. Il relève toutefois que les forces de l'ordre ont de la peine à accéder à certaines données en raison du RGPD, qui répond à certains problèmes, mais en crée d'autres.

[1] https://ge.ch/grandconseil/data/loisvotee/POV00007.pdf

Discussion interne

La proposition (S) d'auditionner le Conseil d'Etat pour connaître sa stratégie dans le domaine et renseigner sur la mise en œuvre de la nouvelle disposition constitutionnelle ne suscite guère d'oppositions.

Il est proposé (MCG) d'auditionner la direction d'Infomaniak. La commission semble partagée quant à l'opportunité d'auditionner des opérateurs économiques spécifiques. Des commissaires (UDC) proposent par conséquent d'auditionner la Chambre de commerce, d'industrie et des services de Genève.

Des commissaires (LJS) rappellent que la problématique est globale et concerne la Confédération dans son ensemble. Des commissaires (PLR) proposent donc d'auditionner d'abord l'administration, puis de décider d'éventuelles auditions supplémentaires. Cette proposition ne suscite aucune opposition.

Séance du 10 janvier 2025 : audition de M^me^ Carole-Anne Kast, conseillère d'Etat (DIN), de M. Alain Bachmann, directeur général (OCSIN), de M. Olivier Baujard, chef de la gouvernance (OCSIN), et de M. Alexander Barclay, délégué au numérique (DIN) ; discussion et vote

M^me^ Kast revient sur le vote de 2023 relatif au nouveau droit fondamental à l'intégrité numérique. Elle indique que ce vote donnait pour mandat à l'Etat de favoriser l'inclusion numérique et de sensibiliser la population aux enjeux numériques, mais aussi de soutenir et de contribuer à la matérialisation de la souveraineté numérique de la Suisse. Elle mentionne que Neuchâtel vient d'adopter une disposition similaire. M. Barclay précise que si la formulation est quasiment identique, la part du « oui » y était plus faible qu'à Genève.

M^me^ Kast relève que ces dispositions constitutionnelles s'inspirent des travaux de la Conférence latine des directeurs du numérique (CLDN) et d'autres travaux fédéraux. Ces travaux ne sont pas limités à Genève. Elle constate en outre que la tendance est à une réglementation plus légère, sous l'influence de la politique états-unienne. Dans le domaine de la sécurité, les moyens du numérique servent à commettre des infractions, par exemple avec les « deepfakes » (création de toutes pièces d'une vidéo prêtant des propos ou des actes à une personne, qui se voit ainsi atteinte dans son image), et qu'une récente affaire impliquant deux adversaires politiques a débouché sur un jugement reconnaissant l'atteinte à l'image. Si le volet pénal n'a pas encore été jugé, il s'agit d'un débat nouveau et complexe.

Concernant la motion, M^me^ Kast déclare que la stratégie cantonale doit être concertée avec la Confédération, vu le caractère particulièrement international

de ces enjeux. Les communes sont preneuses des propositions que le canton peut leur relayer dans ce contexte, ce qui a été fait récemment concernant l'usage de l'intelligence artificielle avec la création d'un guide. M. Barclay précise à ce titre qu'une première convention-cadre sur l'intelligence artificielle et les droits de l'homme, la démocratie et l'Etat de droit a été adoptée au niveau européen. M^me^ Kast ajoute qu'il s'agit de la première réglementation dans le monde sur l'intelligence artificielle.

S'agissant de la deuxième invite, M^me^ Kast soulève des enjeux opérationnels. Elle relève en particulier que les règles sur les marchés publics n'offrent pas à l'Etat la possibilité de choisir ses prestataires pour ne favoriser que les entreprises locales et que des appels d'offres sont obligatoires.

M. Baujard évoque l'évolution du cadre législatif. La conformité de la LIPAD, de la LAEL et des autres lois avec la disposition constitutionnelle a été vérifiée, la LIPAD ayant été révisée l'an dernier. Des actions concrètes de gouvernance ont été mises en place : la CLDN a élaboré une nouvelle définition opérationnelle de la souveraineté numérique, les contrats des fournisseurs sont désormais systématiquement évalués, le contrôle des transferts de données à l'étranger a été renforcé et des partenariats stratégiques (notamment avec la Ville de Genève) ont été développés.

Il évoque ensuite la question complexe du « cloud souverain » qui fait appel à plusieurs défis. En particulier : la dépendance croissante aux infrastructures numériques, la continuité des services publics, l'autonomie technologique et décisionnelle, la protection des données et le maintien de la confiance publique. La CLDN a lancé plusieurs études pluridisciplinaires. L'une d'elles a été confiée à la société AWK pour analyser les opportunités de « cloud souverain » et les moyens disponibles pour le concrétiser. D'autres études ont été confiées à l'Université de Genève pour analyser des aspects plus juridiques et socio-économiques, par exemple la définition du concept de souveraineté numérique et ses effets. Enfin, une autre étude a été menée par Ethix dans le but d'analyser les enjeux éthiques et de formuler des recommandations en vue d'adopter une approche responsable.

Ces études ont permis d'adopter une définition de la souveraineté numérique : « *Capacité des autorités à maintenir leur autonomie stratégique dans l'utilisation et le contrôle des biens numériques impactant l'économie, la société et la démocratie*. » Elles ont également permis d'identifier des axes prioritaires et de formuler des recommandations pour la concrétisation du « cloud souverain ».

M. Baujard précise que d'autres acteurs travaillent sur ce sujet, comme la Confédération qui développe le « Swiss Government Cloud » (SGC) à travers

un programme national qui couvre 2025 à 2032 avec un budget d'environ 320 millions de francs. Les principaux aspects sont les suivants : le stockage des données est obligatoirement situé en Suisse, dans des infrastructures de la Confédération sous-traitées à des partenaires externes (qui peuvent être étrangers), aux côtés d'un « cloud privé » strictement maîtrisé par les équipes de la Confédération. Cette approche comporte des avantages, notamment l'équilibre entre protection des données et innovation, la mutualisation des ressources de la Confédération et des cantons, la consultation des cantons, et l'exclusion du secteur privé.

Concernant l'approche cantonale, M. Baujard déclare que la stratégie de l'OCSIN est le développement d'un « cloud hybride », similaire au projet de la Confédération. Les services critiques du canton disposent déjà d'un « cloud privé » entièrement contrôlé par l'Etat. Le « cloud public » est utilisé de manière ciblée. L'Etat se prépare à une possible intégration au sein du SGC, en coopération avec les établissements publics autonomes. L'idée est à la fois de développer les services de cloud publics pour des raisons d'innovation et de maintenir les infrastructures privées pour les données les plus sensibles. Des alternatives *open source* sont également à l'étude, sachant que les services achetés sont eux-mêmes quasiment toujours basés sur des systèmes *open source*. Ces solutions sont évaluées selon différents critères : origine des contributions, qualité et sécurité des solutions, compatibilité avec les exigences de souveraineté. Le projet « Second Source » de l'administration numérique suisse (ANS) vise à étudier les alternatives, avec par exemple le scénario dans lequel les services de Microsoft deviendraient inaccessibles, alors que le canton les utilise. Il précise enfin que le canton publie le code développé en interne. M^me^ Kast précise que l'ANS est une organisation financée par la Confédération et les cantons, ce qui permet à ceux-ci d'orienter le développement de ses projets.

M. Barclay indique que des informations sont disponibles à ce sujet sur le site *www.administration-numerique-suisse.ch*. L'ANS date de 2022 et est encadrée par une convention-cadre qui lie la Confédération aux cantons. Le projet e-ID est une des réalisations issues de cette structure. Le 20 décembre dernier, le Parlement fédéral a voté la « loi correspondance ». Deux partis politiques ont déjà annoncé lancer un référendum. Si ce système entre en vigueur en 2026, il s'agirait d'une étape fondamentale pour la souveraineté numérique de la Suisse.

M. Baujard évoque le cadre juridique de la protection des données qui contient en particulier la LPD fédérale et, sur le plan genevois, la LIPAD et le RIPAD. L'accord Swiss-US Data Privacy de 2024 a remis les USA dans la liste des pays dont le droit est éligible au traitement des données personnelles.

La compatibilité avec d'autres lois états-uniennes comme la FISA n'est pas encore réglée par exemple, et un cabinet juridique spécialisé a été mandaté sous la supervision du préposé cantonal à la protection des données et à la transparence (PPDT). Les avis de droit sont à bout touchant.

Il rappelle l'application des règles relatives aux marchés publics qui sont fixées à tous les niveaux (accords internationaux, droit fédéral, AIMP). Les principes fondamentaux sont la non-discrimination, la concurrence efficace, la transparence et l'utilisation optimale des ressources. Les critères d'évaluation sont le prix (20-40%), l'adéquation technique (50-60%), les références (10%) et l'expérience (5-10%).

Questions des commissaires

Des commissaires (PLR) demandent quel serait l'apport de la motion. M[me] Kast répond que celle-ci ne changerait rien dans la mesure où les invites qu'elle formule ne répondent pas aux critères prévus par la LRGC et demandent à l'Etat d'effectuer le travail qu'il fait déjà dans le cadre de la loi.

Ces mêmes commissaires (PLR) comprennent que la stratégie consiste à écarter l'intervention du privé et demandent si les réflexions prennent en compte le risque d'avoir un temps de retard sur les évolutions technologiques ou s'il existe au sein du personnel de l'Etat des personnes qui travaillent également pour le privé. M[me] Kast répond que la souveraineté numérique porte en particulier sur la maîtrise par l'Etat de l'infrastructure et que, par définition, il n'est pas possible de la déléguer au privé. Si l'Etat gère l'infrastructure, cela n'exclut pas de s'inspirer des développements réalisés par le secteur privé. M. Bachmann ajoute que l'administration lutte constamment contre l'obsolescence et met régulièrement à jour ses logiciels et ses connaissances grâce à des équipes performantes en interne. L'objectif est de récupérer les développements utiles venant de l'extérieur et de les tester avant de les mettre en service au sein de l'Etat.

Ces mêmes commissaires (PLR) demandent ce qu'il en est du secteur privé suisse. M[me] Kast répond que la réponse est la même. Elle rappelle l'enjeu opérationnel lié aux marchés publics : si l'Etat lance un appel d'offres, il ne peut pas décider aujourd'hui de ne prendre en considération que celles issues d'entreprises suisses. Donc garantir une infrastructure souveraine nationale est incompatible avec la privatisation.

Ces mêmes commissaires (PLR) évoquent l'accord avec les USA et demandent si celui-ci a impliqué que la Suisse ait dû réduire ses attentes. M. Baujard précise qu'il s'agit d'un accord européen que la Suisse a repris et qu'il a permis à la Suisse d'élever ses propres standards. Cumulé à des

modifications législatives aux États-Unis, cela a permis de rendre les USA compatibles avec le droit européen et suisse. M. Barclay indique qu'il n'est pas exclu que cet accord soit remis en cause devant les tribunaux. Mme Kast évoque aussi la possibilité que le gouvernement états-unien change d'avis. S'agissant du référendum sur l'e-ID, elle constate que l'enjeu est l'ouverture ou non de la prestation aux entreprises privées. M. Barclay rappelle également que selon la loi sur l'e-ID, cet outil est facultatif.

Des commissaires (S) comprennent la motion comme demandant une stratégie, et demandent si celle-ci est publiée ou si le rapport en réponse à cette motion permettrait de la rendre publique dans un même document. Mme Kast réfute cette interprétation, considérant que la motion demande à l'Etat d'effectuer son travail, ce qui reviendrait à rendre un rapport sur le travail quotidien de l'administration. Le texte de la motion devrait être modifié si l'objectif est d'obtenir un rapport. Les commissaires évoquent la variante du postulat. Mme Kast déclare son accord avec cette voie. Les commissaires ont l'impression que la présentation qui accompagne l'audition pourrait réaliser les invites de la motion.

Des commissaires (LC) demandent quels sont les services critiques et les données sensibles. Mme Kast indique qu'il s'agit des infrastructures désignées comme critiques par la Confédération dans tous les cantons, car nécessaires au bon fonctionnement de la société. Ce sont celles qui doivent être particulièrement protégées en cas de catastrophe ou de pénurie énergétique par exemple. A Genève, il s'agit de l'aéroport et des HUG ainsi que des entreprises privées. M. Barclay précise que la liste des infrastructures critiques n'est pas rendue publique. Mme Kast évoque les entreprises privées cruciales pour approvisionner les infrastructures publiques nécessaires, notamment en matière de stockage et de transport. Quant aux données sensibles, il s'agit d'une définition contenue dans la LIPAD, même si elle ne règle pas toutes les questions. On trouve dans les données sensibles les données biométriques ou certaines données médicales, par exemple. M. Baujard ajoute que les cantons et la Confédération définissent quatre niveaux de catégories de données : publiques, non publiques, confidentielles, secrètes. Cette classification permet de déterminer le niveau de sécurisation de l'infrastructure.

Des commissaires (MCG) s'intéressent à la valorisation des acteurs locaux et demandent des précisions quant à la collaboration avec le Centre universitaire d'informatique (CUI) et la Ville de Genève. M. Barclay explique que le CUI est un centre interfacultaire regroupant un ensemble de professeurs travaillant sur cette thématique. L'Université de Genève a une autonomie organisationnelle à cet égard. L'une des études évoquées lors de l'audition a été confiée à l'Université de Genève, mais aucun des trois chercheurs mandatés

n'est rattaché au CUI. M. Barclay affirme que le CUI est précieux. S'agissant des communes, il évoque des tensions quant aux niveaux de responsabilité, car la constitution ne demande pas une souveraineté numérique cantonale, mais seulement que Genève contribue à la souveraineté numérique de la Suisse et à sa mise en œuvre. Il estime que Genève et d'autres cantons ont activement cherché à avancer la vision latine sur ces questions qui touchent l'ensemble du pays. Le premier sujet de discussion dans ce contexte était la problématique technique du « cloud », mais les enjeux de sensibilisation du public ont également été évoqués. La Confédération travaillait déjà sur ces questions, mais les cantons latins ont demandé au Conseil fédéral que les débats soient ouverts à l'ensemble des cantons. Les communes sont au plus proche de la population et sont les mieux placées pour réaliser l'inclusion numérique, et le canton soutient leurs projets. La Ville de Genève a justement élaboré un projet pilote de permanences publiques que le canton soutient.

Discussion interne et vote

Des commissaires (S) voient dans cette motion l'envie de préciser et de rendre transparentes les intentions du canton dans le domaine de la souveraineté numérique. Le but était de communiquer ces intentions à la population. L'audition qui vient de s'achever contient les informations demandées par la motion. Le rapport de la commission devrait ainsi suffire à en remplir les objectifs.

Des commissaires (Ve) abondent dans ce sens.

La présidence soumet au vote la **M 3052 :**

Oui :	–
Non :	5 (1 S, 1 Ve, 2 PLR, 1 LJS)
Abstentions :	3 (1 LC, 1 MCG, 1 UDC)

La motion M 3052 est refusée.

Des commissaires (PLR) demandent un traitement en catégorie IV. Faute d'unanimité, cette motion sera traitée en catégorie de débat III.

Conclusion

Si tel était l'objet du vote, il y a fort à parier qu'une large majorité de la commission aurait exprimé son adhésion aux principes qui sous-tendent cette motion. Cependant, compte tenu du cadre légal actuel et des informations transmises par le Conseil d'Etat et l'administration cantonale, il semble évident

que l'adoption de la présente motion ne permettrait pas d'obtenir de meilleurs résultats que ceux produits pas son seul examen devant la commission.

La publication du présent rapport, dans la mesure où il contient des informations intéressantes et complètes sur la stratégie adoptée tant par l'Etat de Genève que par la Confédération, répond déjà à une partie des demandes de la motion. En revanche, s'agissant de la volonté de favoriser des entreprises locales pour l'infrastructure numérique du canton, une motion ne permettrait pas de s'affranchir des règles applicables aux marchés publics. Un projet de loi serait nécessaire, sachant toutefois que ces règles sont également contenues dans le droit supérieur intercantonal, fédéral et international.

Pour toutes ces raisons, une majorité incontestée de la commission vous recommande de rejeter cette motion, tout en remerciant ses auteurs d'avoir permis, par le dépôt de ce texte, de mettre en lumière l'excellent travail réalisé par l'Etat dans le domaine de la souveraineté numérique.

ANNEXE

Agenda

- Mise en œuvre des droits fondamentaux numériques
- Le Cloud souverain : contexte et enjeux
- Stratégie nationale et mise en œuvre
- Approche cantonale et alternatives
- Cadre juridique
- Perspectives et prochaines étapes

Mise en œuvre des droits fondamentaux numériques

Évolutions du cadre législatif

- Introduction de l'intégrité numérique dans la Constitution comme droit fondamental
- Révision majeure de la LIPAD :
  - Adaptation aux avancées technologiques
  - Nouvelles obligations pour les collectivités publiques
  - Dispositions spécifiques sur la conservation et l'effacement des données
- LAEL : Garantie d'accès physique aux prestations parallèlement aux services numériques

Actions concrètes et gouvernance

- Définition opérationnelle de la souveraineté numérique par la Conférence Latine des Directeurs Numérique (CLDN)
- Mise en place d'un processus d'évaluation systématique des contrats fournisseurs
- Contrôle renforcé des transferts de données à l'étranger
- Développement de partenariats stratégiques :
  - Collaboration active avec la Ville de Genève
  - Soutien financier aux projets innovants

Le Cloud souverain : contexte et enjeux

Défis de la transformation numérique

- Augmentation de la dépendance aux infrastructures numériques
- Nécessité de garantir la continuité des services publics
- Enjeux de l'autonomie technologique et décisionnelle
- Protection des données citoyennes
- Maintien de la confiance publique

Études pluridisciplinaires

- Étude technique (AWK) :
  - Évaluation des opportunités d'un Cloud souverain
  - Analyse des architectures possibles
- Étude juridique et socio-économique (Université de Genève) :
  - Définition du concept de souveraineté numérique
  - Implications socio-économiques
- Étude éthique (Ethix) :
  - Analyse des enjeux éthiques
  - Recommandations pour une approche responsable

Résultats clés

- Définition de la souveraineté numérique : "Capacité des autorités à maintenir leur autonomie stratégique dans l'utilisation et le contrôle des biens numériques impactant l'économie, la société et la démocratie"
- Identification des axes prioritaires
- Recommandations pour la mise en œuvre

Stratégie nationale et mise en œuvre

Swiss Government Cloud (SGC)

- Programme national 2025-2032
- Budget : 319,4 millions CHF
- Architecture hybride multi-cloud à trois piliers :
  - Cloud public :
    - Évolutivité maximale
    - Services innovants
    - Stockage des données en Suisse obligatoire
  - Cloud public on-premise :
    - Solutions de fournisseurs dans les centres de calcul fédéraux
    - Contrôle accru sur l'infrastructure
  - Cloud privé on-premise :
    - Exploitation exclusive dans le réseau fédéral
    - Traitement des données sensibles
    - Niveau maximal de sécurité

Avantages de l'approche fédérale

- Équilibre entre protection des données et innovation
- Mutualisation des ressources
- Économies d'échelle
- Accessibilité pour les collectivités publiques
- Exclusion du secteur privé pour maintenir le contrôle

Approche cantonale et alternatives

Stratégie OCSIN

- Développement progressif d'une infrastructure Cloud hybride :
  - Cloud privé pour les services critiques
  - Utilisation ciblée du Cloud public
  - Préparation à l'intégration SGC

Convergence avec les Entités Publiques Autonomes

- Consultation approfondie des EPA
- Stratégie hybride commune :
  - Exploitation des Clouds publics pour l'innovation
  - Maintien d'infrastructures privées pour les données sensibles
  - Approche pragmatique et équilibrée

Alternatives open source

- Analyse systématique des solutions alternatives
- Critères d'évaluation :
  - Origine des contributions (30-50% privées)
  - Qualité et sécurité des solutions
  - Compatibilité avec les exigences de souveraineté
- Participation au projet "Second Source" de l'ANS
- Publication du code développé en interne

Cadre juridique
Protection des données

Conformité avec multiples cadres réglementaires
- LPD (niveau fédéral)
- LIPAD et RIPAD (niveau cantonal)
- Swiss-US Data Privacy Framework (2024)

Enjeux spécifiques
- Compatibilité avec FISA (Foreign Intelligence Surveillance Act)
- Impact des Executive Orders 14086 et 12333
- Validation juridique par cabinet spécialisé
- Supervision par le PPDT

Cadre juridique
Marchés publics

Cadre juridique multiniveau
- Accords internationaux
- Législation fédérale
- AIMP

Principes fondamentaux
- Non-discrimination
- Concurrence efficace
- Transparence
- Utilisation optimale des ressources

Critères d'évaluation
- Prix (20-40%)
- Adéquation technique (50-60%)
- Références (10%)
- Expérience (5-10%)

Perspectives et prochaines étapes

Opportunités

- Convergence des initiatives cantonales et fédérales
- Mutualisation des ressources
- Préservation de l'autonomie locale
- Optimisation des investissements publics

Actions futures

- Extension des consultations intercantonales
- Développement des synergies
- Renforcement de la cohérence des approches
- Intégration progressive au SGC

Facteurs clés de succès

- Équilibre entre innovation et souveraineté
- Respect du cadre juridique
- Approche collaborative
- Flexibilité et adaptabilité
- Maîtrise des coûts

Merci de votre attention

Olivier Baujard