GRAND CONSEIL **M 2922-A**
de la République et canton de Genève

Date de dépôt : 5 mars 2024

Rapport

de la commission judiciaire et de la police chargée d'étudier la proposition de motion de Grégoire Carasso, Léna Strasser, Alberto Velasco, Boris Calame, Sylvain Thévoz, Diego Esteban, Jocelyne Haller, Youniss Mussa, Amanda Gavilanes, Thomas Wenger, Caroline Marti, Françoise Nyffeler, Salika Wenger pour améliorer la sécurité numérique des personnes face à la cybercriminalité

Rapport de Murat-Julian Alder (page 3)

ATAR ROTO PRESSE – 80 ex. – 03.24

Proposition de motion
(2922-A)

pour améliorer la sécurité numérique des personnes face à la cybercriminalité

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

– les développements rapides des technologies de l'information, de la communication et de l'intelligence artificielle, et les risques croissants que celles-ci font peser sur la sécurité des personnes physiques et morales, mais aussi sur le fonctionnement des collectivités publiques ;
– l'augmentation massive des cas de cyberattaques au cours des dernières années dans la plupart des pays industrialisés, y compris en Suisse ;
– la complexité de la lutte contre ce type nouveau de menaces, notamment en lien avec leur caractère protéiforme et les très nombreuses cibles potentielles ;
– la relative faiblesse des outils disponibles en Suisse et à Genève en particulier pour prévenir et lutter contre ce nouveau type de criminalité ;
– le désarroi dans lequel peuvent se trouver, par voie de conséquence, les victimes de cyberattaque, qui n'osent parfois même pas dénoncer ces actes ;
– le vote du Grand Conseil en septembre 2022 en faveur de l'introduction d'un nouveau droit fondamental relatif à l'intégrité numérique dans la constitution genevoise,

invite le Conseil d'Etat

à présenter au Grand Conseil un rapport sur la stratégie cantonale en matière de sécurité numérique.

Rapport de Murat-Julian Alder

La Commission judiciaire et de la police (ci-après : « la Commission ») a consacré 5 séances au traitement de la motion M 2922 « pour améliorer la sécurité numérique des personnes face à la cybercriminalité » (ci-après : « la motion »), soit les jeudis 25 mai, 24 août, 28 septembre, 30 novembre 2023 et 11 janvier 2024, sous la présidence de M[me] la députée Xhevrie Osmani (S).

M[me] Carole-Anne Kast, conseillère d'Etat en charge du département des institutions et du numérique (ci-après : « le DIN »), M. Sébastien Grosdemange, secrétaire général adjoint (DIN) et M. Jean-Luc Constant, secrétaire scientifique de la Commission judiciaire et de la police (SGGC), ont participé aux séances.

Les procès-verbaux ont été rédigés par M. Clément Magnenat.

Qu'ils soient tous remerciés de leur précieuse contribution aux travaux.

1. Présentation de la motion par M. le député Grégoire Carasso, premier signataire (25.05.2023)

Par souci de concision et afin d'éviter d'inutiles redites, le rapporteur de la Commission se bornera à se référer à la motion M 2922, ainsi qu'à son exposé des motifs[1].

A l'issue de cette présentation, la Commission décide, sans opposition, d'auditionner le DIN.

2. Audition du DIN (24.08.2023)

La Commission reçoit M[me] Carole Anne-Kast, conseillère d'Etat en charge du DIN, accompagnée de M[me] Monica Bonfanti, commandante de la police, M. Sébastien Grosdemange, secrétaire général adjoint chargé de la sécurité (DIN) et M. Alexander Barclay, délégué cantonal au numérique.

A cette occasion, il a été rappelé aux membres de la Commission que le Conseil d'Etat a publié le 10 mai 2023 un rapport dressant un premier bilan et présentant les perspectives de sa politique numérique[2].

De plus, le 18 juin 2023, le peuple genevois a approuvé la loi constitutionnelle modifiant la constitution de la République et canton de

1 Disponible sous le lien suivant : https://ge.ch/grandconseil/data/texte/M02922.pdf
2 Disponible sous le lien suivant : https://www.ge.ch/document/32004/telecharger

Genève (Cst-GE) (Pour une protection forte de l'individu dans l'espace numérique) (A 2 00 – 12945), du 22 septembre 2022.

M. Barclay a en particulier souligné le fait que les questions de sécurité numérique ne sont pas seulement techniques, mais aussi humaines. Ces dossiers évoluent très vite, notamment dans les domaines de l'intelligence artificielle (IA) et du *metavers*. Ces avancées constantes représentent d'importantes opportunités, mais aussi de grandes menaces.

L'actualité en matière de cybersécurité est très importante au niveau fédéral et dans plusieurs cantons. La motion comprend 11 invites que l'on peut regrouper dans 5 groupes :

1. la communication à la population (la formation, la prévention) ;
2. le public particulier des PME ;
3. les enjeux de gouvernance ;
4. la logique d'écosystème (partenariats) ;
5. la Genève internationale.

M. Barclay rappelle, concernant la Genève internationale (5.) et la piste de la création d'une agence européenne ou internationale basée à Genève, que notre canton compte déjà plusieurs organisations qui contribuent à ces objectifs-là, notamment la Geneva Internet Platform[3] qui assure un suivi des développements sur le plan multilatéral.

Concernant le public particulier des PME (2.), la motion propose une offre public-privée de prestations de cybersécurité. En effet, cela n'existe pas actuellement. M. Barclay relève cependant que des offres de sensibilisation et d'autoévaluation existent déjà au niveau du DEE pour les entreprises.

S'agissant de la formation (1.), la culture numérique est au cœur du projet d'éducation au numérique autour de trois grandes dimensions que sont la formation à l'utilisation des médias, les sciences informatiques et les usages qui comprennent notamment les questions liées au droit à l'image. Par ailleurs, le plan harcèlement mis en place au niveau du DIP comprend le cyberharcèlement.

Sur la gouvernance (3.), M. Barclay mentionne la création à Genève d'une collaboration depuis 2018 entre les communes et le canton concernant les échanges d'informations sur la menace cyber.

---

3 https://www.giplatform.org/

Sur les écosystèmes et partenariats (4.), il indique qu'il y a une opportunité pour Genève au niveau de l'économie de la confiance, raison pour laquelle le Conseil d'Etat soutient la Trust Valley[4].

M. Barclay conclut en indiquant qu'une réflexion autour des acteurs qui s'adressent à des projets concrets en la matière, notamment sur la conservation des données personnelles, serait intéressante à ajouter dans la motion.

3. Suite des travaux (28.09.2023)

Après une brève discussion à propos de la suite des travaux, sur proposition d'un député (PLR), la Commission décide à l'unanimité d'auditionner M^me^ la professeure Solange Ghernaouti, docteure en informatique, directrice du Swiss Cybersecurity Advisory & Research Group (UNIL) pionnière de l'interdisciplinarité de la sécurité numérique et experte internationale en cybersécurité et cyberdéfense.

4. Audition de M^me^ la Professeure Solange Ghernaouti (30.11.2023)

Par souci de concision et afin d'éviter d'inutiles redites, le rapporteur de la Commission prie respectueusement le lecteur de bien vouloir se référer à la prise de position écrite adressée par M^me^ la Professeure Solange Ghernaouti à la Commission le 16 décembre 2023 (cf. annexe).

5. Discussions et votes (11.01.2024)

Un député (**PLR**) reprend les différents commentaires de M^me^ la professeure Solange Ghernaouti et parvient à la conclusion qu'en réalité, cette motion constitue, à elle seule, un véritable programme de législature en matière de sécurité numérique.

Un député (**S**) considère que cette motion n'a pas nécessairement besoin d'être comprise de la sorte. La raison pour laquelle cette motion est aussi large, c'est précisément parce qu'elle cherche à la fois à demander au Conseil d'Etat de présenter les mesures déjà mises en place et de prévoir de nouvelles mesures pour répondre aux enjeux de la cybersécurité.

Un député (**UDC**) estime que l'on ne peut rien faire de cette motion malgré les propositions d'amélioration formulées par M^me^ la professeure Solange Ghernaouti. La cybersécurité est un domaine important, mais ce n'est pas au niveau d'un parlement cantonal que l'on peut régler ce problème. Sous réserve

[4] https://trustvalley.swiss/

d'une invite qui consiste à demander un rapport au Conseil d'Etat, cette motion doit être purement et simplement rejetée.

M^me^ Kast rappelle que la motion est définie par l'article 143 LRGC comme suit :

« La motion est une proposition faite au Grand Conseil par un de ses membres. Elle a pour but :

a) soit d'inviter le Conseil d'Etat à étudier une question déterminée en vue de :

1° présenter un projet de loi,

2° adopter ou modifier un règlement, ou prendre un arrêté ;

b) soit de charger une commission d'élaborer, sur un objet déterminé :

1° un projet de loi,

2° une motion,

3° une résolution,

4° un rapport. »

M^me^ Kast constate que de plus en plus de motions programmatiques de ce type, déposées par l'ensemble des groupes parlementaires, sont déposées. Son département est naturellement disposé à répondre à la motion, que ce soit sous la forme d'un projet de loi ou d'un rapport. Toutefois, la commission doit être plus précise dans ses attentes. En effet, que ce soit avec ou sans les propositions de M^me^ la Professeure Solange Ghernaouti, le Conseil d'Etat n'aura guère d'autre choix que de répondre à la motion en expliquant qu'en l'absence de ressources supplémentaires, il se limitera à garantir la sécurité des installations existantes et à mettre en place les projets qui ont fait l'objet d'une couverture financière.

Un député (**PLR**) partage parfaitement cet avis et propose de remplacer toutes les invites de la motion par une invite unique demandant au Conseil d'Etat un rapport sur la mise en œuvre de sa stratégie en matière de cybersécurité. Sur la base de ce rapport, la commission pourra ensuite déterminer si des modifications législatives sont nécessaires.

Une députée (**Ve**) partage le constat de M^me^ Kast mais considère que le fait de modifier les invites dans le sens proposé par son collègue (PLR) ne change rien à propos de ce qui sera reçu de la part du Conseil d'Etat.

Un député (**S**) ajoute que pour lui, il est tout à fait possible d'adresser la motion telle quelle au Conseil d'Etat, qui répondra sur chacune des invites.

Un député (**S**) demande à M^me^ Kast si cela veut dire que le Conseil d'Etat n'entend plus répondre dans le délai légal de 6 mois aux motions qui ne respectent pas la forme prévue par l'article 143 LRGC.

M^me^ Kast lui répond que ce délai n'est qu'un délai d'ordre. Elle répète que si la motion est adressée en l'état au Conseil d'Etat, ce dernier n'aura malheureusement guère d'autre choix que de répondre que le département n'a pas les moyens nécessaires pour mettre en œuvre ces objectifs sans ressources supplémentaires. Il se contentera de faire l'inventaire de ce qui existe déjà, en y associant le DEE concernant la sécurité numérique dans les entreprises et le DIP s'agissant des établissements scolaires.

Un député (**S**) précise que sa question était générale, car les sept motions qui sont à l'ordre du jour de la commission ne correspondent pas exactement à ce qui est prévu par l'article 143 LRGC. C'est la raison pour laquelle il a posé sa question sur un éventuel changement de pratique du Conseil d'Etat pour des motions de ce style-là.

M^me^ Kast indique qu'elle aimerait que le Grand Conseil se rende compte que, de plus en plus, les motions sont utilisées comme des questions écrites. Il serait plus efficient d'adresser une question écrite non urgente au Conseil d'Etat. Le parlement recevrait les mêmes éléments de réponse, mais il n'y aurait pas de rapport et cela aurait également l'avantage de ne pas alourdir l'ordre du jour de la plénière.

Un député (**PLR**) remercie M^me^ Kast pour son honnêteté intellectuelle et institutionnelle. Il ressort de cette discussion que la réponse du DIN à la motion est déjà toute écrite et qu'il serait effectivement préférable de commencer par demander un rapport au Conseil d'Etat sur sa stratégie en matière de cybersécurité.

Un député (**UDC**) rappelle que la discussion sur le rôle de la motion est ancienne. La motion devrait avoir un rôle subsidiaire par rapport au projet de loi et à la question écrite. Le choix entre une motion ou une question est également la conséquence de la suppression de la forme de l'interpellation.

Un député (**S**) constate néanmoins que la première invite lui paraît très concrète.

M^me^ Kast note que cette première invite concerne les ressources, qui sont du ressort du Grand Conseil. Si le but est de demander des ressources supplémentaires, alors la motion doit demander au Conseil d'Etat de présenter un crédit supplémentaire pour la mise en place de la stratégie sur la cybersécurité.

La présidente met aux voix la proposition d'amendement général d'un député (PLR) visant à remplacer toutes les invites de la motion par une invite unique libellée comme suit :

« invite le Conseil d'Etat à présenter au Grand Conseil un rapport sur la stratégie cantonale en matière de sécurité numérique. »

Cet amendement général est approuvé à l'unanimité par :

Oui :	14 (3 S, 1 Ve, 1 LJS, 1 LC, 2 MCG, 4 PLR, 2 UDC)
Non :	0
Abstention :	0

Mise aux voix ainsi amendée, la motion M 2922 est adoptée par :

Oui :	12 (3 S, 1 Ve, 1 LJS, 1 LC, 4 PLR, 2 UDC)
Non :	2 (2 MCG)
Abstention :	0

Un député **(MCG)** précise que son groupe considère que cette motion est inutile, mais qu'il renonce à déposer un rapport de minorité.

Le préavis de la commission pour la catégorie de débat est **IV, extraits, procédure sans prise de parole sans débat**.

Annexe

Prise de position écrite de M^me^ la Professeure Solange Ghernaouti du 16.12.2023.

ANNEXE

Commentaires de la professeure Solange Ghernaouti (Université de Lausanne) relatifs à la proposition de motion - M 2922.

« Pour améliorer la sécurité numérique des personnes face à la cybercriminalité »

Lausanne, le 16 décembre 2023.

Remarques générales

I - La motion aborde différents thèmes « pour améliorer la sécurité numérique des personnes face à la cybercriminalité » sans pour autant traiter de manière globale et suffisamment exhaustive la problématique liée aux usages abusifs, détournés, criminels et conflictuels des technologies du numérique pour les personnes physiques, morales et les collectivités publiques. Les sources de l'insécurité numérique ne provenant pas de la cybercriminalité ne sont pas traités.

II - Le fait que les différents thèmes d'ordre politique, économique, juridique, social, organisationnel, associés sans distinction, avec des recommandations à la fois très génériques et parfois très pratiques, rend l'intérêt du document difficile à apprécier.

III - Des détails d'ordre opérationnel sont avancés sans pour autant faire référence à une stratégie, une politique ou encore à un plan d'actions dans lesquels ils doivent s'inscrire. Cela concerne à la fois, le marché de la cybersécurité et la lutte contre la cybercriminalité.

IV - Le fait de mélanger les niveaux local, national et international de ces deux dimensions très spécifiques, qui ne concernent pas les mêmes acteurs, ni n'ont les mêmes finalités, ne permet pas de dégager une vision claire et cohérente de ce qui est proposé dans la motion.

V - Il y a une grande confusion entre les champs d'action, les acteurs privés et publics et les moyens de la cybersécurité et ceux spécifiques de la cybercriminalité par les autorités judiciaires. Il est à regretter que des mesures concernant à proprement parlé les moyens de la lutte contre la cybercriminalité par les instances de justice et police ne soient pas spécifiquement présentées dans le cadre de cette motion traitée par la Commission judiciaire et de la police.

VI - Les propositions font partie du corpus de recommandations générales connues depuis longtemps. Il est étrange qu'elles ne soient pas plus spécialement contextualisées à la réalité du terrain genevois et mieux focalisées et précisées. Peuvent-elles être implémentées tel que proposé pour que la situation soit sous contrôle ?

VII - Pour chaque proposition il manque un énoncé clair du besoin auquel la proposition répond ainsi qu'une appréciation de sa faisabilité opérationnelle et des gains attendus (résultats escomptés).
Pour schématiser, les propositions seraient des pièces disparates d'un puzzle dont il manquerait le cadre et si l'ensemble des propositions constituerait une raquette, alors cette dernière aurait des trous.

Remarques spécifiques à chaque proposition « Invite le Conseil d'État » (page 2)

1 - « *à augmenter les ressources publiques dédiées à la prévention et la lutte en matière de cybercriminalité afin d'améliorer à Genève la sécurité numérique des personnes physiques et morales* ».

Certes, mais pourquoi, pour qui, comment ?

De quelles ressources publiques parle-ton ? Pour répondre concrètement à quel plan d'actions et finalités ? A qui cette mesure s'adresse (autorités judiciaires, autres, ...). De quel pourcentage d'augmentation s'agit-il ? ...

2 - « *à encourager les victimes à dénoncer tout cyberincident, quel qu'en soit le degré de gravité, et ce notamment au moyen de larges campagnes d'information* ».

Pourquoi pas, mais les campagnes d'information ne permettront pas d'encourager les victimes à dénoncer tout cyberincident (quel qu'en soit le degré de gravité) si toute la chaine de justice et police ne peut pas leurs offrir un soutien effectif. Quelle structure opérationnelle derrière cette mesure ? quelles compétences, formations, etc. ? N' y a t- il pas d'autres moyens pour favoriser la dénonciation des cyberincidents ?

3 - « *à renforcer la disponibilité et la visibilité des prestations offertes aux personnes physiques (guichet du Centre national pour la cybersécurité, ligne téléphonique et accueil dans les postes de police)* ».

Mélange du niveau national (NCSC) et local, et des outils mis à disposition. Cela ne concerne que les personnes physiques ?

Une personne victime d'un cyber incident doit s'annoncer au NCSC et au poste de police ? Il n'est peut-être pas nécessaire de figer la proposition en citant des moyens qui peuvent évoluer dans le temps.

Il s'agit d'un problème organisationnel et procédural qui doit être traité au bon niveau avec une communication claire par les autorités. Est-ce que cette proposition ne devrait pas être sous entendue dans la proposition précédente comme étant un des objets des campagnes d'information ?

Proposition de formulation : renforcer les capacités des autorités en charge du traitement du recueil de plainte, mieux informer le public des prestations offertes.

4 - « *à étudier la création d'une offre publique-privée de prestations de cybersécurité mise à la disposition spécifique des PMEs* ».

Est-ce vraiment de la responsabilité de l'État ? Si oui pourquoi cela ne concernerait pas aussi des prestations de cybersécurité mise à la disposition spécifique des PMEs, des individus et des collectivités territoriales ?

Éclaircir le lien de cette proposition avec la proposition n° 10 qui aborde aussi la question du partenariat public – privé.

5 - « *à soutenir la formation dans le domaine de la sécurité numérique et la protection de la personnalité dans le champ numérique, de la prévention à l'école primaire jusqu'aux filières techniques et académiques les plus pointues* »

Soit la proposition est trop détaillée, soit elle n'est pas assez exhaustive et inclusive.

Proposition de formulation : à soutenir la formation et le développement des compétences dans le domaine de la maitrise des risques et de la sécurité numérique, de la protection des droits fondamentaux des personnes, pour toutes et tous. C'est- à dire à tous les niveaux de l'enseignement obligatoire, post obligatoire, en formation continue, dans toute les filières et disciplines, sans oublier les personnes qui ne sont pas en formation (séniors, demandeurs d'emploi, personnes précarisées, personnes en situation de handicap, ...).

6 - « *à rassembler, sur le modèle de Zurich, les compétences les plus pointues sur le front de la lutte contre la cybercriminalité (procureurs, gendarmes, inspecteurs, informaticiens, praticiens, académiques, etc.) afin, en particulier, de favoriser les échanges d'informations et approches interdisciplinaires* ».

La proposition n'apporte pas spécialement de plus-value car elle est trop générique, on ne sait pas en particulier à qui elle s'adresse et à quel niveau. De plus, des mesures relatives à ce type de proposition existent déjà. Y a-t-il eu une évaluation concrète de la situation et des besoins ?

La proposition pourrait se résumer en « favoriser les collaborations entre tous les acteurs en charge de la lutte contre la cybercriminalité ».

7 - « *à créer une délégation à la sécurité numérique rassemblant les autorités exécutives genevoises* ».

La création d'une nouvelle structure qui ne s'inscrit pas dans une stratégie a peu de chance d'être efficace mais aura un coût certain. La mesure pourrait avoir du sens à condition de définir à minima ses missions (rôles, fonctions, finalités), ses responsabilités, ses champs et moyens d'action.

8 - « *à veiller à ce que les communes, les villes, les structures privées et la population soient adéquatement intégrées à la stratégie nationale de protection contre les cyberrisques* ».

Là aussi l'énumération n'est pas complète ou est trop détaillée et la formulation imprécise.

Proposition de formulation : à veiller à ce que les besoins de tous les acteurs (population, communes, villes, structures privées et associatives, etc.) soient adéquatement pris en compte dans la stratégie nationale de protection contre les cyberrisques.

9 - « *à favoriser l'émergence d'un écosystème interdisciplinaire de recherche et d'innovation permettant de mettre en commun et développer les solutions et talents à même de contrer les modèles criminels* ».

Formulation confuse, insuffisante et pas tout à fait juste.

Proposition de formulation : à favoriser le développement d'un écosystème interdisciplinaire pour la formation, la recherche et l'innovation afin de contribuer à proposer des solutions nécessaires à la maitrise des cyberrisques.

10 - « *à développer et encourager les initiatives visant à renforcer les partenariats, collaborations et échanges d'informations (du local au global, entre acteurs aussi bien publics que privés), telles que le CyberPeace Institute, la Trust Valley, la Swiss Cyber-Security, Association ou CH++* ».

La question de la souveraineté de l'État, celle de la réalisation de ses missions régaliennes de l'État, ne sont ni identifiées, ni adressées. Elles sont pourtant cruciales en matière de sécurité.

Il est impératif d'être vigilant au risque de délégation de certaines missions régaliennes de l'État à des entreprises privées ou associations de celles-ci qui souvent représentent les intérêts d'entreprises hégémoniques étrangères.

Est-ce le rôle de l'État de mettre la lumière sur certaines structures, dont les modèles d'affaire, mode de fonctionnement, actionnaires, acteurs ne sont pas transparents ?

La liste des partenaires possibles est incomplète et porte uniquement sur des associations professionnelles, au détriment de toutes les autres structures qui existent et qui ne sont pas citées.

Ainsi, par exemple, la FER pourrait jouer un rôle prépondérant pour les PMEs.

Proposition de formulation : à développer et encourager les initiatives visant à renforcer les partenariats publics – privés, à renforcer les collaborations et les échanges d'informations nécessaires à tous les niveaux et dans tous les domaines de la cybersécurité, de la lutte contre la cybercriminalité et de la lutte informationnelle afin de mieux prévenir et de réagir aux cyberincidents.

11 - « *à travailler à la création d'une agence européenne et/ou internationale basée à Genève et visant à promouvoir la paix et la sécurité numériques* ».

Est-ce à la Commission judiciaire et de la police de se positionner sur cette question ?

Ce n'est pas la prolifération d'agences qui va résoudre le problème, ni aider les PMEs locales.

A quels besoins cette proposition répond, celui de faire du marketing de la Genève internationale, de certains acteurs, d'instrumentaliser le discours de la paix, celui de la guerre ?

Beaucoup d'agences, instances onusiennes, initiatives internationales traitent déjà de ces sujets, en rajouter augmenterait la confusion sans pour apporter une solution efficace et efficiente.

Est-ce que Genève serait la mieux placée en Europe pour héberger une agence européenne?