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

Date de dépôt : 6 janvier 2026

Rapport du Conseil d'Etat

au Grand Conseil sur la 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

En date du 22 mars 2024, le Grand Conseil a renvoyé au Conseil d'Etat une motion qui a la teneur suivante :

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 ;*

ATAR ROTO PRESSE – 80 ex. – 01.26

– *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.

RÉPONSE DU CONSEIL D'ÉTAT

Le Conseil d'Etat a pris acte du rapport de la commission judiciaire et de la police chargée d'étudier la proposition de motion 2922 (M 2922-A).

Dans ce contexte, il convient de faire un état des lieux de cette problématique. La sécurité numérique est souvent considérée selon 3 dimensions : la cyberdéfense, de compétence fédérale, la lutte contre la cybercriminalité et, enfin, la cybersécurité, de l'Etat comme des entreprises ou encore de la population. En 2024, l'Office fédéral de la cybersécurité (OFCS) a ainsi comptabilisé quelque 63 000 signalements, les cybercriminels ayant recours à tous les canaux (notamment appels téléphoniques, courriels, textos, lettres, faux QR codes). Les menaces se renforcent avec les technologies liées aux systèmes d'intelligence artificielle générative, à l'image des *deepfakes.* De fait, les mesures visant à réduire les cybermenaces et leurs conséquences sont un prérequis à la réalisation des avantages promis par la transition numérique de notre canton.

La problématique de la sécurité numérique est un sujet qui transcende les niveaux des Etats et qui constitue un thème de discussion sur le plan multilatéral, pour lequel la Genève internationale est régulièrement évoquée. C'est d'ailleurs à Genève qu'a été installé en 2019 le CyberPeace Institute visant à promouvoir les comportements responsables dans le cyberespace.

D'une manière générale, il est important de pouvoir unir les divers acteurs politiques, techniques et opérationnels dans une stratégie de mutualisation des moyens avec une haute valeur ajoutée et de s'engager dans un partenariat avec le secteur privé, entre autres pour développer une véritable stratégie de prévention et de mitigation des risques. Pour cette raison, les partenariats, tant publics que privés, académiques ou encore institutionnels, sont indispensables. En ce sens, la Confédération et les cantons ont adopté la troisième cyberstratégie nationale (CSN)[1] en avril 2023. Celle-ci pose une vision et formalise des objectifs, des mesures et une méthode en 4 principes visant à organiser les travaux :

– la CSN s'appuie sur une approche exhaustive basée sur les risques, qui a pour objectif d'améliorer la résilience de la Suisse face aux cybermenaces;
– la protection de la Suisse contre les cybermenaces est une tâche commune de la société, des milieux économiques et de l'Etat;
– la cyberstratégie nationale repose sur une conception du rôle subsidiaire et partenarial de l'Etat;

[1] https://www.ncsc.admin.ch/ncsc/fr/home/strategie/cyberstrategie-ncs.html

– pour autant que cela ne compromette pas l'efficacité des mesures décidées, la mise en œuvre de la CSN obéit au principe de la transparence (et donc de la communication active).

La cyberstratégie de la Confédération et des cantons vise à contribuer à la réalisation des 5 objectifs stratégiques suivants :

1) responsabilisation;
2) fiabilité et disponibilité de l'infrastructure et des services numériques;
3) défense contre les cyberattaques – détection, prévention et gestion efficaces;
4) lutte et poursuites pénales efficaces contre la cybercriminalité;
5) rôle de premier plan dans la coopération internationale.

La CSN sert de cadre de référence aux actions de l'Etat de Genève en la matière. Ce rapport aborde les actions de l'Etat qui contribuent à ces objectifs stratégiques selon 4 axes : la lutte contre la cybercriminalité, la cybersécurité de l'Etat, la cybersécurité du tissu économique et la cybersécurité de la population.

La lutte contre la cybercriminalité

Sur le plan cantonal genevois, rappelons que la lutte contre la cybercriminalité est un axe prioritaire de la politique criminelle commune (PCC) depuis 2014. L'édition 2024-2026 a consolidé cet axe, en particulier contre les phénomènes d'extorsion, de pillage de données publiques ou privées, ainsi que de pédopornographie et d'autres infractions à caractère sexuel. Elle a également intégré les défis posés par le métavers, l'intelligence artificielle et le recours aux cryptomonnaies. Par ailleurs, un accent particulier est mis sur l'avènement des médias synthétiques (*deepfakes*). Les enjeux majeurs relatifs aux éléments de preuve (image, vidéo, audio, document, etc.) concernent beaucoup de secteurs, dont celui de la poursuite pénale.

A cet égard, il est essentiel d'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 visant, entre autres, à obtenir une vue d'ensemble de la cybercriminalité sur un territoire donné.

Outre l'accueil dans les postes de police, il y a lieu de renforcer la disponibilité et la visibilité des prestations offertes aux personnes physiques au travers d'outils en ligne, tels que les cyberkiosques qui ont été mis en place par l'Office fédéral de la cybersécurité (OFCS – nouvelle dénomination du Centre national pour la cybersécurité [NCSC] depuis le 1er janvier 2024), ainsi que par le canton de Genève. Ces outils vont, en l'état, dans le sens d'une prestation à la population dotée d'une économie de moyens.

A terme, l'objectif est de renoncer au cyberkiosque genevois dès lors que celui de l'OFCS sera en mesure de restituer à notre canton les signalements émanant de la population genevoise. Avec le développement du formulaire d'annonce de cet office fédéral et l'engagement de 5 équivalents temps plein (ETP) supplémentaires pour le rendre accessible aux PME et aux citoyennes et citoyens, la perspective de désactivation du cyberkiosque genevois se rapproche. Il s'avère ainsi cohérent de disposer d'un seul formulaire d'annonce national, selon un objectif de regroupement des forces, et de bénéficier de la vue d'ensemble précitée. L'intérêt d'une prévention ciblée à partir des cas signalés à Genève demeure essentiel.

La police genevoise possède déjà une organisation de lutte contre la cybercriminalité de haut niveau sous la forme d'un triptyque INVESTIGATION-ANALYSE-FORENSIQUE. Ce triptyque est utilisé dans le cadre du Centre régional de compétence cyber pour la Suisse occidentale (RC3) doté d'une liste de prestations au niveau intercantonal, principalement la Romandie. Certaines prestations s'étendent au-delà de ce périmètre; par exemple la collecte et le traitement des données liées à l'informatique embarquée dans les véhicules. A cet égard, la police genevoise contribue à développer une visibilité sur un plan supracantonal, national et international[2]. Des partenariats sont développés, visant à permettre notamment la mutualisation de développements informatiques ou encore la participation à des projets académiques dans une logique prospective. De plus, la police genevoise représente également la Romandie au sein du réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK).

---

[2] Cette visibilité comprend notamment des représentations à l'échelle du réseau international francophone de formation policière (FRANCOPOL), les groupes de travail spécialisés d'INTERPOL, comme le *Metaverse Expert Group* et le *Cybercrime Expert Group* ou certaines organisations telles que le RSA *International Cyber Security Forum*. Par ailleurs, des partenariats stratégiques ont été conclus, par exemple avec le Commandement cyber du ministère français de l'Intérieur (COMCyberMI), l'Université de Québec à Trois-Rivières, l'Institut de lutte contre la criminalité économique (ILCE) de la Haute Ecole Arc.

Les partenariats public-privé académiques sont indispensables dans le domaine de la sécurité informatique, comme dans la lutte contre la cybercriminalité. A titre d'exemple, on peut citer le concept de *Cyber Fusion Center*, tel que mis en place auprès d'INTERPOL à Singapour. Ceci est directement lié à l'attractivité du tissu économique visant à assurer la prospérité du canton, appuyée par des partenariats public privé (PPP)[3]. Il s'agit à l'avenir de continuer à encourager et à renforcer les partenariats, les collaborations et les échanges d'informations avec les acteurs de la lutte contre la cybercriminalité.

De plus, 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, renforce les points évoqués plus haut.

La cybersécurité de l'Etat

Relativement à la cybersécurité, l'administration cantonale genevoise, par le biais notamment de l'office cantonal des systèmes d'information et du numérique (OCSIN), met en œuvre un certain nombre de mesures de divers types afin de préserver la confidentialité, l'intégrité et la disponibilité des données qui lui sont confiées par les citoyens, les entreprises et les membres du personnel.

En premier lieu, des mesures techniques appliquent un très ancien principe militaire, la défense en profondeur. Il s'agit ici de préserver les données par un ensemble de systèmes et de logiciels de protection élaborés, modernes et conformes aux standards du marché, répartis en plusieurs « lignes de défense ». Ces mesures couvrent l'entièreté de l'infrastructure informatique de l'Etat, depuis les connexions à Internet jusqu'aux postes de travail des utilisatrices et utilisateurs, en passant par la messagerie ou les serveurs. Elles sont complémentées par des systèmes de détection avancés qui permettent de découvrir les anomalies surgissant dans les environnements informatiques.

En second lieu, de nombreuses mesures organisationnelles complètent les mesures techniques. Tout d'abord, des campagnes régulières de sensibilisation, couplées avec des modules de formation, des vidéos explicatives ou des conférences dédiées, permettent par exemple au personnel de l'administration cantonale d'avoir une capacité accrue pour détecter des messages suspects, déterminer les tentatives d'usurpation d'identité, savoir comment réagir, et plus généralement pour appliquer ces compétences dans

[3] Voir la référence à l'exemple de la *Trust Valley* plus bas dans le présent rapport.

leur vie professionnelle comme dans leur vie privée. L'OCSIN dispose aussi de capacités élaborées en gestion de crise et de continuité des services afin de pallier tout incident affectant les systèmes et données sous sa responsabilité. Enfin, la gestion des risques au sein de l'administration cantonale prend pleinement en compte les aspects en lien avec cette problématique.

Par ailleurs, pour compléter les dispositifs internes, des tests sont régulièrement effectués pour éprouver et adapter continuellement leur résilience face à des attaques.

Une cybersécurité efficace nécessite des collaborations intenses entre différentes parties. Sur le plan cantonal, les responsables de la sécurité de l'information des administrations cantonale et communales ainsi que des établissements publics autonomes sont regroupés en un comité (SécuSIGE); celui-ci favorise l'entraide sur tous les aspects communs, tels les alertes, mais également les mesures de protection ou l'acquisition de matériel, de logiciel ou de prestations. De même, à l'échelle intercantonale, les responsables informatiques des 7 cantons latins (Fribourg, Genève, Jura, Neuchâtel, Tessin, Vaud et Valais) se réunissent et échangent régulièrement dans les mêmes buts notamment. Sur le plan politique, les 7 cantons latins se sont regroupés au sein de la Conférence latine des directrices et des directeurs du numérique (CLDN), qui traite notamment de questions de cybersécurité ou encore de souveraineté numérique. De plus, au niveau national, l'OFCS et le Réseau national de sécurité (RNS) sont également des partenaires importants pour la diffusion d'alertes, la gestion centralisée de certaines mesures techniques, et plus généralement la défense globale vis-à-vis d'attaques provenant d'acteurs malveillants d'importance. Ces collaborations multiples s'avèrent être un avantage décisif pour la réactivité et la résilience des infrastructures informatiques.

De plus, il est important de prendre en compte le cadre légal et réglementaire. La cybersécurité fait partie intégrante d'actes comme la constitution de la République et canton de Genève, du 14 octobre 2012 (Cst-GE; rs/GE A 2 00), la loi sur l'information du public, l'accès aux documents et la protection des données personnelles, du 5 octobre 2001 (LIPAD; rs/GE A 2 08), ou la loi sur l'administration en ligne, du 23 septembre 2016 (LAeL; rs/GE B 4 23), au niveau cantonal, ainsi que la loi fédérale sur la protection des données, du 25 septembre 2020 (LPD; RS 235.1), ou la loi fédérale sur la sécurité de l'information, du 18 décembre 2020 (LSI; RS 128), au niveau fédéral. En outre, au sein de l'administration cantonale, 2 règlements (règlement sur l'organisation et la gouvernance des systèmes d'information et de communication, du 26 juin 2013 (ROGSIC; rs/GE B 4 23.03), et règlement sur la gestion des risques, du 18 septembre

2013 (RGR; rs/GE D 1 05.10)), des directives transversales et l'application d'un ensemble de standards et de normes (ISO et NIST) régissent les aspects pratiques et la mise en œuvre des mesures de cybersécurité, ainsi que les risques associés. Tous ces aspects sont pris en compte pour la définition des mesures de cybersécurité, leur implémentation et leur suivi.

La cybersécurité du tissu économique

L'attractivité du tissu économique dépend fortement de la sécurité globale, et notamment numérique. Les personnes morales, particulièrement les petites et moyennes entreprises (PME), sont des acteurs majeurs de la prospérité du canton et nécessitent une attention particulière.

L'Etat de Genève entreprend un ensemble d'actions visant en priorité à garantir la disponibilité des outils de travail des entreprises, à mitiger ou prévenir les risques économiques, industriels, juridiques et d'image, contribuant ainsi à la stabilité économique du canton et renforçant la confiance dans nos entreprises.

En particulier, l'office cantonal de l'économie et de l'innovation (OCEI) propose une gamme de mesures et d'outils en lien avec la cybersécurité permettant aux entreprises, et en particulier aux PME, d'adopter les meilleures pratiques. Voici les principales initiatives :

– une offre d'information et de sensibilisation aux cyber-risques dispensée dans le cadre des formations en présentiel du programme « Entreprises & Numérique ». Ces sessions, qui couvrent notamment les thématiques de la Responsabilité Numérique des Entreprises (RNE), permettent aux entreprises, en particulier aux PME, de mieux comprendre les menaces numériques courantes, d'identifier leurs vulnérabilités et d'adopter les bonnes pratiques pour renforcer leur sécurité opérationnelle;
– des guides thématiques de la collection « Entreprises & Numérique » : publication de guides pratiques pour sensibiliser les entreprises et les aider à prendre les actions pour mieux se protéger, mitiger les risques numériques, réagir en cas d'incident et gérer les impacts (gestion de crise), soit un guide sur les cyber-risques et un guide responsabilité numérique des entreprises;
– une offre de formations en ligne sur les cyber-risques, sur la responsabilité numérique des entreprises et sur la protection des données;
– une collaboration avec la *Trust Valley*, initiative conjointe portée avec le canton de Vaud, engageant des hautes écoles et des acteurs privés, qui vise à renforcer la confiance numérique en réunissant les compétences publiques et privées dans le domaine de la cybersécurité au sein d'un

cluster économique (avec des programmes tels *Tech4Trust*, *Tech4SMEs*, *Trust Village* à Genève);

– une collaboration avec la Fédération des entreprises romandes à Genève (FER) qui propose une offre complète d'accompagnement en cybersécurité pour les entreprises.

L'étude de la création d'une offre publique-privée de prestations de cybersécurité mise à la disposition spécifique des PME vise tout particulièrement à protéger et promouvoir le tissu économique local. Le fait d'organiser les ressources publiques et privées autour d'un axe de développement commun constituerait un renforcement de la place genevoise pour ces entreprises.

La cybersécurité de la population

Les actions de sensibilisation s'inscrivent notamment dans le droit à l'intégrité numérique (art. 21A Cst-GE). Les aspects de prévention sont essentiels afin de perturber les activités des cybercriminels. Les messages y relatifs doivent être différenciés, notamment au bénéfice des enfants, des adolescentes et adolescents, des adultes, des seniors et des PME. Des actions spécifiques sont ciblées auprès des élèves par l'école, auprès du public âgé, ou encore du grand public de façon générale. L'augmentation des ressources publiques dédiées à la prévention et la lutte en matière de cybercriminalité afin d'améliorer la sécurité numérique des personnes physiques et morales à Genève est un enjeu majeur en regard de la perturbation des activités cybercriminelles. A l'aide d'une stratégie coordonnée, à moyen et long terme, l'augmentation du niveau de maturité général de la population va progressivement entraver les activités cybercriminelles et, partant, le flux financier y relatif. Ainsi, une stratégie de prévention avec des messages différenciés en fonction des publics-cibles, à l'aide de supports novateurs et ambitieux, favorisera les buts visés par une telle stratégie en s'appuyant sur le réseau actif d'acteurs de la prévention de proximité. Une coordination active des actions de prospective liées à l'évolution technologique, à l'image des médias synthétiques (*deepfakes*) visant à aligner les actions des acteurs concernés et évoqués dans le présent rapport, est indispensable.

Dans le cadre du programme numérique du département de l'instruction publique, de la formation et de la jeunesse (DIP), un fort accent est mis sur la prévention des risques afférents aux nouvelles technologies, dont la cybercriminalité fait bien entendu partie. Déjà présente dans le plan d'études romand en éducation numérique, la prévention fait en outre l'objet d'un éventail d'actions complémentaires en cours d'élaboration avec différents partenaires, parmi lesquels la police cantonale. Les moyens d'enseignement genevois d'éducation numérique sont un outil principal, en particulier : éducation numérique 1P-2P, 3P-4P, 5P-6P; informatique (9e année).

A cela s'ajoutent notamment : les interventions de la fondation Action Innocence « Prévention numérique » 3P (printemps 2025) auprès de l'ensemble des enseignantes et enseignants de 3P; les interventions « Prévention numérique » de l'Ordre des avocats de Genève et de la brigade de criminalité informatique (BCI) adressées à tous les élèves de 9e année en lien avec les questions de cyberharcèlement, de droit à l'image et de pédopornographie; la pièce de théâtre de la compagnie Caméléon « Un pour tous, tous pourris ! » - visant à la prévention du (cyber)harcèlement – proposée aux classes de 8P; les interventions du service écoles-médias (SEM) dans les établissements du cycle d'orientation pour sensibiliser les élèves de 11e année aux cyberdangers; les chartes numériques école primaire et cycle d'orientation, ainsi que les recommandations présentes dans les carnets de l'élève; la veille « Prévention des risques et bonnes pratiques numériques » sur le site pédagogique officiel *Enseignement*. Des actions sont également réalisées pour former le personnel à la prévention des risques numériques dont en particulier le (cyber)harcèlement entre pairs. Depuis 2024, une formation en ligne obligatoire intitulée « Harcèlement scolaire : prévenir, repérer et agir » a été déployée pour l'ensemble du personnel encadrant les élèves du DIP (plus de 7 300 personnes ont suivi cette formation). Afin de sensibiliser les familles, un flyer réalisé par la fondation Action Innocence a été distribué à tous les parents d'élèves de l'enseignement primaire et spécialisé à la rentrée 2025.

Enfin, en complément des actions entreprises par la police cantonale évoquée précédemment, l'Etat mène des actions de lutte contre l'illectronisme comprenant des mesures liées à la cybersécurité. Le rapport du Conseil d'Etat en réponse à la motion 2818 (M 2818-C) détaille ces mesures. L'Etat soutient également des acteurs de la société civile dans des projets pilotes de sensibilisation aux bonnes pratiques en matière de sécurité numérique, notamment, en 2024-2025, un projet du Cyberpeace Institute ainsi qu'un projet de médiation numérique de la Ville de Genève et de l'Oeuvre suisse d'entraide ouvrière (OSEO).

Au vu des enjeux énoncés et de la vitesse exponentielle du développement des nouvelles technologies, le Conseil d'Etat répond ainsi à la présente motion sur l'état des travaux en matière de stratégie de sécurité numérique.

Au bénéfice de ces explications, le Conseil d'Etat vous invite à prendre acte du présent rapport.

AU NOM DU CONSEIL D'ÉTAT

La chancelière :	Le président :
Michèle RIGHETTI-EL ZAYADI	Thierry APOTHÉLOZ