GRAND CONSEIL **PL 13277**
de la République et canton de Genève

Signataires : Grégoire Carasso, Léna Strasser, Alberto Velasco, Jean-Pierre Pasquier, Céline Zuber-Roy, Glenna Baillon-Lopez, Boris Calame, Sylvain Thévoz, Diego Esteban, Jocelyne Haller, Youniss Mussa, Amanda Gavilanes, Thomas Wenger, Caroline Marti, Françoise Nyffeler, Salika Wenger, Denis Chiaradonna

Date de dépôt : 6 mars 2023

Projet de loi

modifiant la loi sur la police (LPol) (F 1 05) *(Pour améliorer la sécurité numérique des personnes face à la cybercriminalité)*

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

Art. 1 **Modifications**

La loi sur la police, du 9 septembre 2014, est modifiée comme suit :

Art. 10, al. 1 (nouvelle teneur)

[1] La gendarmerie assure auprès de la population une présence effective et préventive, et assume les prérogatives répressives prévues par la loi, notamment dans les domaines de la circulation, du secours d'urgence, de la cybersécurité et de la proximité.

Art. 11, al. 1 (nouvelle teneur)

[1] La police judiciaire élucide notamment les crimes, cybercrimes, délits et cyberdélits qui, en raison de leur gravité, de leur récurrence ou de leur complexité, nécessitent un travail d'enquête approfondi.

Art. 2 **Entrée en vigueur**

La présente loi entre en vigueur le lendemain de sa promulgation dans la Feuille d'avis officielle.

ATAR ROTO PRESSE – 100 ex. – 03bis.23

EXPOSÉ DES MOTIFS

Les développements rapides des technologies de l'information, de la communication et de l'intelligence artificielle (internet, réseaux sociaux, télétravail, visioconférence, domotique, ChatGPT, métavers, etc.) ouvrent de formidables opportunités sociales et économiques. Ils représentent aussi de vertigineux risques pour la sécurité des personnes (physiques et morales) et des collectivités publiques. Cette transformation numérique de notre société doit être accompagnée par le déploiement de ressources en mesure de répondre à l'explosion des activités illégales menaçant l'intégrité, la confidentialité et la disponibilité des systèmes informatiques et des données.

La cybercriminalité est un phénomène complexe, international, aux facettes multiples, depuis les crimes dont la prévalence, l'impact et l'échelle sont accélérés par des outils informatiques (pédopornographie ou désinformation, par exemple) jusqu'aux crimes où l'informatique est la source et la cible des cyberattaques (rançongiciel ou cyberespionnage, par exemple). L'ingéniosité et l'impunité des cybercriminels s'appuient sur un écosystème criminel international extrêmement agile et coopératif.

En décembre dernier, le directeur de Zurich Insurance, l'une des plus grandes sociétés d'assurances en Europe, déclarait au Financial Times que les cyberattaques, plus que les catastrophes naturelles, pourraient devenir « inassurables »[1]. Selon Interpol, la cybercriminalité est devenue une menace majeure[2]. Le montant des pertes estimé en 2021 rien qu'aux Etats-Unis est de 6,9 milliards de dollars[3]. Or la Suisse est encore mal outillée pour prévenir et gérer ces nouvelles formes de menaces. Le Global Cybersecurity Index, publié par l'Union internationale des télécommunications, classe notre pays à la 42e place, derrière Chypre et devant le Ghana[4].

Au niveau de la Confédération, 30 351 infractions cybercriminelles ont été dénombrées selon l'Office fédéral de la statistique en 2021[5]. En termes de cyberagressions, on estime qu'une attaque a lieu toutes les 11 secondes en

---

1 « The chief executive of one of Europe's biggest insurance companies has warned that cyber attacks, rather than natural catastrophes, will become "uninsurable" as the disruption from hacks continues to grow » (FT, 26 décembre 2022 « Cyber attacks set to become "uninsurable", says Zurich chief »).

2 Le Temps, 25 octobre 2022, p. 15.

3 FBI, IC3, Internet Crime Report, 2021.

4 International Telecommunication Union, Global Cybersecurity Index 2020, p. 30.

5 OFS, Statistique policière de la criminalité (SPC) 2021.

Suisse (env. 2,9 millions/an)[6]. Des sources évoquent des taux de croissance à trois chiffres, faisant écho à la numérisation de pans toujours plus nombreux de la société et donc à l'augmentation de la surface d'attaque disponible[7]. Ainsi, les risques concernent le fonctionnement et les données non seulement des infrastructures publiques (dans les domaines de la santé, de l'impôt, de l'énergie, des transports, de la sécurité, etc.) mais aussi des structures privées (grandes ou petites) et des personnes physiques (toutes les catégories d'âges sont concernées).

En regard de ce très large éventail de cibles et de victimes potentielles, les cybermenaces sont elles aussi d'une grande diversité : rançongiciels, phishing-vishing-smishing, fraude à l'investissement, arnaque au président, fake sextortion, courriels de menace des autorités, escroquerie au chèque, cybersquatting, piratage sur les réseaux sociaux, pièges d'abonnement aux paquets, etc.[8].

A l'échelle suisse, le Centre national pour la cybersécurité (NCSC)[9] a réalisé une évaluation de la stratégie nationale de protection de la Suisse contre les cyberrisques[10]. Dans ses recommandations, il invite notamment à augmenter les ressources et à associer plus étroitement les PME, les cantons, les villes, les communes et la population à la gouvernance et mise en œuvre de cette stratégie[11]. Sur le terrain des enquêtes, ainsi que le rappelle Yves Nicolet, procureur fédéral chargé de la cybercriminalité, la « majeure partie des enquêtes liées à la cybercriminalité sont menées par les polices et les procureurs des cantons »[12]. Selon la même source, la référence en Suisse se trouve depuis 2013 dans le canton de Zurich avec la création d'un centre de compétence rassemblant toutes les expertises pour faire face à cette forme spécifique de criminalité.

---

6 Tribune de Genève, 8 juillet 2022, p. 5.

7 Le Temps, 15 décembre 2022, p. 11.

8 Cette liste exemplative a été établie sur la base de l'inventaire des cybermenaces du Centre national pour la cybersécurité (NCSC, 21 février 2023, https://www.ncsc.admin.ch/ncsc/fr/home/aktuell/aktuelle-zahlen.html).

9 Le NCSC deviendra un office fédéral en mars 2023 et disposera d'environ 70 postes de travail (Le Temps, 5 décembre 2022, p. 9). Relevons que du côté de l'armée, le Parlement a décidé de doter le commandement cyber de 6000 et 7000 militaires à l'horizon 2030 (Tribune de Genève, 14-15 avril 2022, p. 17).

10 NCSC, econcept AG, « Evaluation de l'efficacité de la stratégie nationale de protection de la Suisse contre les cyberrisques pour les années 2018 à 2022 », Rapport final, 28 mars 2022.

11 Voir pp. 42, 44-45 et 47.

12 Le Temps, 26 novembre 2022, p. 3.

A Genève, dans le cadre d'un sondage mené par l'institut Edgelands en 2022, 75% des personnes interrogées déclaraient se sentir en situation d'insécurité numérique et attendre des autorités une meilleure protection face aux dangers en ligne[13].

Du côté des collectivités publiques, et à la différence d'autres régions, 44 communes disposent de ressources mutualisées (via le service intercommunal d'informatique – SIACG) tandis que la Ville et l'Etat de Genève gèrent leur système d'information de manière autonome. Pour 2021, l'office cantonal des systèmes d'information et du numérique (OCSIN) indique avoir repéré 42 865 alertes, dont 104 ont nécessité des interventions spécifiques[14].

Au sein de la police genevoise, la Brigade de cyberenquête, créée en 2021, compte 18 agents spécialisés et a traité en 2021 2600 affaires[15]. Son capitaine, Patrick Ghion, considère que les PME sont parmi les cibles les plus vulnérables, « car elles rapportent davantage que des individus isolés et sont généralement moins bien protégées que les grosses entreprises »[16]. L'enquête conjoncturelle 2022 de la Chambre de commerce, d'industrie et des services de Genève montre d'ailleurs que la cybersécurité est en tête des préoccupations des entreprises[17].

Enfin, sur le plan légal, le Grand Conseil a adopté en septembre 2022 la loi constitutionnelle intitulée « Pour une protection forte de l'individu dans l'espace numérique » (L 12945). Prochainement soumise à l'approbation du peuple, cette loi introduit dans notre constitution un nouveau droit fondamental relatif à l'intégrité numérique, qui inclut notamment « le droit d'être protégé contre le traitement abusif des données liées à sa vie numérique » et « le droit à la sécurité dans l'espace numérique » (article 21A, alinéa 2).

---

13 Le Temps, 17 décembre 2022, p. 15.

14 Tribune de Genève, 27 juin 2022, p. 7. Le budget de l'OCSIN dédié à la sécurité est de 9 millions de francs par an et compte une quinzaine de spécialistes.

15 Tribune de Genève, 8 juillet 2022, p. 5. Cette brigade collabore avec deux autres services de police : la Brigade de criminalité informatique (19 personnes) et celle des renseignements criminels (3 personnes). Notons encore que la police genevoise héberge le Centre régional de compétence cyber pour la Suisse occidentale (RC3) au sein duquel ces trois groupes œuvrent en fonction de leur mission, respectivement investigation, forensique et analyse (Le Temps, 29 juillet 2022, p. 9).

16 *Ibidem*.

17 CCIG info, n° 6, juin 2022, p. 5.

Dans le sillage de cette modification légale, le présent projet de loi propose de modifier de manière ciblée la loi sur la police (LPol) (F 1 05) pour y inscrire formellement la cybersécurité dans les domaines d'action de la gendarmerie (article 10, alinéa 1) et les cybercrimes et cyberdélits dans le champ d'action de la police judiciaire (article 11, alinéa 1). Cette approche politique et symbolique forte est doublée d'une motion, la M 2922, demandant plusieurs mesures concrètes, à commencer par l'augmentation de ressources allouées à la prévention et à la lutte contre la cybercriminalité. Ces deux démarches sont complémentaires et visent le même but : renforcer la sécurité numérique des personnes (physiques et morales) à Genève.

Commentaire article par article du présent projet de loi

Art. 10, al. 1 (nouvelle teneur)

Cette proposition de modification de la teneur de l'article 10, alinéa 1, consiste à ajouter, dans la liste non exhaustive des domaines d'action de la gendarmerie, celui de la cybersécurité.

Art. 11, al. 1 (nouvelle teneur)

Par symétrie, cette proposition de modification de la teneur de l'article 11, alinéa 1, consiste à mentionner explicitement les cybercrimes et cyberdélits dans le champ d'action de la police judiciaire.

Conséquences financières

Au vu de l'importance et de la complexité de l'enjeu, des moyens conséquents devront assurément être déployés par l'Etat pour mieux protéger la sécurité numérique des personnes physiques et morales dans notre canton. Chiffrer le coût de cette politique n'est toutefois pas à la portée des auteurs, qui souhaitent avant tout, par ce projet de loi, ancrer légalement (et par là renforcer la légitimité de) l'action publique dans le domaine de la lutte contre la cybercriminalité.

Pour toutes ces raisons, nous vous remercions Mesdames les députées, Messieurs les députés, de réserver un bon accueil au présent projet de loi.