N°1528
Entrée le 20.12.2024
Chambre des Députés

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère de la Justice

Réponse de Madame la ministre de la Justice, Elisabeth Margue, et de Monsieur le ministre des Finances, Gilles Roth, à la question parlementaire n° 1528 du 18 novembre 2024 de l'honorable député Laurent Mosar relative aux outils informatiques utilisés à des fins criminelles.

Il devient de plus en plus facile de trouver des outils facilitant la mise en œuvre des scénarios de fraude décrits dans l'article de presse auquel l'honorable député fait référence.

La sophistication et l'émergence de technologies basées sur l'intelligence artificielle ont favorisé l'émergence du CaaS (Crime-as-a-Service) permettant aux criminels, même sans expertise technique, d'accéder à des outils sophistiqués prêts à l'emploi.

Alors que des statistiques détaillées ne sont pas disponibles, les autorités ont identifié les risques suivants, auxquels la place financière est principalement exposée :

- l'utilisation de faux documents impossibles à distinguer des vrais (factures, pièces d'identité), obtenus par des moyens illicites, pour mettre en œuvre différentes fraudes (comme la fraude au président) ou pour blanchir des revenus ou créer de fausses entreprises ;

- l'utilisation des moyens technologiques pour contourner les dispositifs d'entrée en relation d'affaires à distance (« remote customer onboarding ») ou LBC/FT des institutions financières ;

- l'utilisation des « mules financières » pour dissimuler l'origine des revenus illicites.

Au niveau européen et international, des efforts significatifs ont été entrepris sur le plan législatif pour développer des outils adaptés à la lutte contre la cybercriminalité. Il convient de citer à cet égard la Convention de Budapest élaborée par le Conseil de l'Europe et le « paquet e-evidence » adopté par l'Union Européenne.

En ce qui concerne la législation nationale, il faut noter que les relations d'affaires à distance sont encadrées par la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et le financement du terrorisme. Cette loi impose aux professionnels des mesures de mitigation des risques liés aux entrées en relation d'affaires à distance.

Alors que les autorités de contrôle ne supervisent pas les fournisseurs de solutions d'entrée en relation d'affaires à distance, il faut noter que l'utilisation de ce type de solutions par des entités supervisées constitue une externalisation qui doit être notifiée aux autorités. Les autorités examinent ces notifications d'externalisation pour vérifier que les principes mentionnés dans les lignes directrices de l'Autorité bancaire européenne sur l'utilisation de solutions d'accueil des clients à distance ont été respectées par le professionnel.

De même, les autorités poursuivent une veille technologique et réglementaire constante sur ces risques. Au vu des évolutions récentes, elles prévoient de rencontrer les principaux acteurs fournissant des solutions d'entrée en relation d'affaires à distance aux professionnels sous leur surveillance afin d'évaluer les contrôles qu'ils ont mis en place et afin de mitiger les risques potentiels qui en découleraient. Il convient aussi de souligner que le Luxembourg participe activement à des projets pilotes européens concernant la création d'un portefeuille européen d'identité numérique.

Puis, il convient de noter que le Gouvernement continue les efforts à mettre à disposition des entités de poursuite nationales les ressources personnelles et matérielles requises pour lutter contre la cybercriminalité.

Pour renforcer la prévention, le Gouvernement a également lancé plusieurs initiatives de sensibilisation, dont notamment celles de BEE SECURE pour faire face aux menaces liées à la cybercriminalité. Ces initiatives visent en particulier à sensibiliser le public à une utilisation plus sûre et responsable des technologies numériques.

Luxembourg, le 20 décembre 2024.

La Ministre de la Justice

(s.) Elisabeth Margue