# ASSEMBLÉE NATIONALE

17ème législature

## Recrudescence des escroqueries en ligne

Question écrite n° 2584

### Texte de la question

Mme Florence Goulet attire l'attention de M. le ministre de l'intérieur sur la recrudescence des escroqueries en ligne usurpant l'identité de dispositifs ou de représentants d'organismes publics ou de collectivités. Ces pratiques malveillantes, en constante augmentation, exploitent la confiance des citoyens en se présentant comme des démarches administratives officielles, se faisant passer pour leurs représentants, par mail ou par téléphone. Des milliers d'euros sont ainsi extorqués à des victimes abusées par leurs interlocuteurs avec une facilité déconcertante sous prétexte de bénéficier d'un supposé « crédit Grenelle de l'environnement » ou autres aides diverses. Ces escrocs obtiennent ainsi toutes sortes de documents officiels et administratifs : RIB, carte d'identité, déclaration d'impôts, etc. Malgré les dépôts de plainte et les preuves, les victimes voient leurs requêtes classées sans suite, faute d'identification des auteurs. Souvent domiciliées à l'étranger, ces escroqueries profitent de montages complexes empêchant toute poursuite judiciaire. La nouvelle loi contre les fraudes aux aides n'aura qu'un effet à la marge sur ce type de réseaux. Aussi, elle lui demande quelles actions concrètes sont envisagées pour prévenir ce fléau d'escroquerie organisée de plus en plus répandu et répondre à la détresse des victimes.

### Texte de la réponse

L'explosion des crimes cybernétiques résulte de plusieurs facteurs combinés. Tout d'abord, l'omniprésence de la donnée dans les opérations quotidiennes des citoyens, y compris pour des activités sensibles telles que les impôts, la santé ou les finances, a considérablement accru les opportunités pour les cybercriminels. Ensuite, le contexte économique récent a joué un rôle facilitateur, en particulier avec l'accélération de la numérisation des services publics et des aides de l'État durant la pandémie de Covid-19. Enfin, le sentiment d'impunité ressenti par les malfaiteurs s'explique par le pseudonymat du cyberespace, la distance géographique des groupes criminels opérant souvent à l'étranger, la difficulté des coopérations judiciaires internationales avec certains pays, ainsi que la volatilité des données. Les modes opératoires employés par les cybercriminels sont bien connus, même s'ils évoluent en permanence pour déjouer les mesures de protection mises en place en réaction. Parmi les techniques les plus répandues figurent l'envoi de courriels reprenant les codes visuels et les logos d'entreprises légitimes pour tromper les victimes. Cet hameçonnage (phishing) est fréquent et parfois très ciblé, utilisant des informations obtenues par des recherches en sources ouvertes pour maximiser l'efficacité des stratagèmes. Les criminels recourent également à la création de faux sites web, ainsi qu'à des attaques sophistiquées combinant ingénierie sociale et intelligence artificielle pour atteindre leurs objectifs. L'analyse des procédures judiciaires des forces de sécurité intérieure permet d'identifier plusieurs groupes criminels étrangers spécialisés dans les fraudes cybernétiques usurpant l'identité de dispositifs ou de représentants d'organismes publics ou de collectivités. D'une part, les groupes de cybercriminels d'origine franco-israélienne, qui ont acquis depuis la fraude à la taxe carbone une expertise en escroqueries de haut niveau, se spécialisent dans des pratiques telles que les faux investissements ou les faux ordres de virements internationaux, ainsi que dans la fraude aux financements publics. Ces malfaiteurs chevronnés utilisent quasi systématiquement des identités usurpées pour commettre leurs méfaits initiaux, recyclant ensuite ces données pour d'autres escroqueries ou pour structurer des réseaux de blanchiment. D'autre part, les cybercriminels d'Afrique de l'Ouest se concentrent sur des escroqueries dites « à l'amour », au sentiment ou à la « sexcam ». Opérant souvent depuis des

cybercafés, ils exploitent des modes opératoires variés tels que les fausses demandes d'aide, les fausses locations, les fausses offres d'emploi en ligne, les « pornscams », les fraudes aux sentiments ou encore les arnaques au RGPD. L'usurpation d'identité constitue le cœur de leurs pratiques. Doit également être notée la cybercriminalité émanant des pays asiatiques, qui se caractérise par une fraude basée sur des investissements fictifs dans laquelle la victime est progressivement amenée à engager des sommes croissantes, généralement sous forme de cryptomonnaies, qui lui sont finalement dérobées. Le terme de « romance baiting » (l'appât de la romance) est utilisé pour évoquer ce phénomène criminel. En effet, ces escroqueries sont courantes sur les applications de réseaux sociaux et de rencontres entre adultes. Face à ces menaces, plusieurs dispositifs permettent déjà de signaler et de déclarer les faits délictueux commis dans le cyberespace. Les plateformes PHAROS et THESEE de la police nationale (rattachées à l'office anti-cybercriminalité - OFAC - de la direction nationale de la police judiciaire - DNPJ) et la plateforme Perceval de la gendarmerie nationale offrent chacune des fonctions spécifiques pour faciliter ces démarches. En 2024, la plateforme THESEE a reçu 107 331 déclarations, qui se sont traduites par le dépôt de 71 765 plaintes et 27 342 signalements. 136 enquêtes ont été initiées et 4 individus ont été incarcérés pour avoir ouvert 6 faux sites de ventes sur internet ayant généré plus de 4 millions d'euros de préjudice pour plusieurs milliers de victimes. La ligne Info-Escroqueries de l'office anti-cybercriminalité a reçu 176 458 appels de particuliers en 2024. S'agissant de la plateforme PHAROS, elle a reçu 222 364 signalements de contenus illicites sur internet en 2024, qui se sont traduits par 87 410 demande de retraits et 599 demandes de blocage de contenus. Ces dispositifs sont renforcés depuis le 17 décembre 2024 avec la mise en place du « 17 cyber », qui permet aux internautes de recevoir des conseils adaptés aux faits rencontrés, de se connecter au téléservice adéquat ou de dialoguer avec un opérateur de la gendarmerie ou de la police par messagerie instantanée. Enfin, l'État développe des solutions innovantes pour renforcer la sécurité numérique. L'identité numérique certifiée, par l'intermédiaire de France Identité, facilite désormais les démarches à distance nécessitant une sécurité accrue. Depuis le 11 juillet 2024, grâce à FranceConnect+, il est possible d'effectuer des opérations sensibles telles que l'achat d'une formation sur MonCompteFormation, l'accès à MaPrimeRénov, ou la consultation de son dossier médical. Lancée en 2021, cette version renforcée de FranceConnect offre désormais une protection supplémentaire contre les fraudes, répondant aux exigences de sécurité accrues pour ces démarches. Aussi, poursuivre les actions de sensibilisation auprès des populations les plus vulnérables reste l'une des mesures les plus rapides à mettre en œuvre, car elles permettent d'adapter le message en fonction des évolutions des modes opératoires.  En partenariat avec l'ensemble des acteurs participant à diffuser une culture de la cybersécurité auprès de la population, notamment Cybermalveillance.gouv.fr, des acteurs économiques et des collectivités territoriales, il peut notamment être relevé que l'unité nationale cyber de la gendarmerie nationale élabore des contenus ciblés. Ces contenus sont destinés à générer une prise de conscience du risque lié à l'utilisation des technologies numériques pour s'en prémunir, diffuser une culture de la cybersécurité dans les foyers et améliorer le niveau de sécurité numérique des établissements publics comme privés. Par exemple, des actions de sensibilisation à la cybersécurité sont réalisées au profit des entreprises et des hôpitaux. Ces actions sont conçues à partir d'un outil de diagnostic opérationnel de la maturité cyber (dispositif Diagonal), et de nombreuses communications sont diffusées par la gendarmerie pour faire face aux cybermenaces. Ainsi, plus de 50 000 entreprises ont fait l'objet d'une action de prévention visant à lutter contre les cybermenaces. La police nationale s'est dotée d'un « plan cyber 2022-2027 » pour renforcer son action de prévention et d'investigation de la cybercriminalité. L'OFAC, créé par ce plan, est chargé de la coordination et de l'animation opérationnelle de la lutte contre la cybercriminalité. Il est également le point de contact central à l'international. L'office dispose d'un maillage de 11 antennes et de 8 détachements d'antennes, sur lesquels il s'appuie pour ses missions d'enquête et d'appui aux investigations numériques. Outre ce service hautement spécialisé, la police nationale dispose de plus de 12 000 agents formés aux investigations sur internet, dont les enquêteurs sous pseudonyme (plus de 500 habilités). Plus de 7 200 agents sont par ailleurs formés aux investigations informatiques, dont les investigateurs en cybercriminalité (plus de 580). La police nationale mène également des actions de cyber prévention au profit des entreprises, détentrices de volumes plus importants de données personnelles, en les sensibilisant aux risques et en diffusant les « bonnes pratiques ». Cette politique de prévention s'appuie en particulier sur le réseau des experts en cyber-menaces (RECyM), mis en place par l'office anti-cybercriminalité pour accompagner les entreprises et les collectivités territoriales face aux risques du cyberespace. À titre d'exemple, au cours de l'année 2024, le RECyM a mené 115 actions de sensibilisation, ayant bénéficié à plus de 2 400 entreprises. Plus globalement, l'OFAC cultive une approche à 360° en relation avec les acteurs de la cybersécurité, ainsi qu'avec les acteurs économiques et institutionnels. Cette approche permet de multiplier utilement les canaux d'échanges d'informations que l'OFAC peut notamment exploiter pour déjouer des cyberattaques. Sur ce volet préventif, cette sensibilisation est

complétée par la recherche du développement des mécanismes d'alerte, en lien avec les différents prestataires du numérique. Cette disposition s'inscrit utilement au terme de l'action de déréférencement possible des sites principaux et miroirs lorsque ces escroqueries sont commises à partir de faux sites internet ou d'adresse électroniques de diffusion (décret n° 2023-454 du 12 juin 2023 relatif au blocage et déréférencement des « sites miroirs », pris en application de l'article 6-3 de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, dont la mise en œuvre incombe à la plateforme PHAROS de l'OFAC). Sur le plan répressif, les actions de la gendarmerie et de la police nationales mobilisent plusieurs composantes, en adéquation avec les différentes stratégies pour lutter contre ces escroqueries : suivi de la piste des concepteurs de sites internet frauduleux ; identification et localisation des auteurs, en France et à l'étranger (en coopération avec Europol et les pays concernés) ; traque du réseau de blanchiment en suivant les flux financiers et en recherchant les comptes rebonds ; action en réactivité dans les enquêtes et transmission rapide du renseignement pour bloquer les fonds. Les enquêtes judiciaires menées par les unités de la gendarmerie et les services de police sont régulièrement confiées à des enquêteurs spécialisés, qui donnent priorité aux circuits de blanchiment des sommes provenant de ces escroqueries. A titre d'exemple, les investigations menées dès novembre 2022 par les unités de gendarmerie de la région Grand-Est ont permis de matérialiser des pratiques commerciales frauduleuses visant à l'encaissement de primes énergétiques dont une partie est prise en charge sur des fonds européens. Le mode opératoire consiste à se substituer à des particuliers en vue de solliciter des aides par l'intermédiaire des différentes sociétés évoquées précédemment. Pour parfaire leurs escroqueries, les membres de l'organisation criminelle usent de subterfuges, sur internet notamment (courriel à en-tête trompeur), en vue d'obtenir de ces particuliers l'ensemble des documents justificatifs permettant l'octroi de la prime énergétique versée sur des comptes bancaires. Le produit infractionnel estimé dépasse les deux millions d'euros. L'opération judiciaire découlant de la traçabilité des fonds a permis en septembre 2024 de confondre 4 individus et la saisie de près de 400 000€ en avoirs criminels. L'ensemble des services de police judiciaire a également été mobilisé pour démanteler ces organisations criminelles. L'office central de lutte contre la grande délinquance financière de la DNPJ a interpellé dans le cadre de cette affaire une quarantaine de mis en cause, entre 2022 et 2024, ayant commis des actes représentant plusieurs millions d'euros de préjudice. Enfin, le dispositif du « filtre anti-arnaques », créé par la loi du 21 mai 2024 visant à sécuriser et à réguler l'espace numérique (dite loi SREN), pourrait permettre de compléter les actions judiciaires et préventives. Ce dispositif, actuellement en cours de développement, a vocation à améliorer les mécanismes de prévention existants, notamment au moyen de la mise en œuvre de pages d'avertissement à destination des internautes, ainsi que de mesures de blocage et de déréférencement visant les sites concernés.

## Données clés

**Auteur :** Mme Florence Goulet
**Circonscription :** Meuse (2e circonscription) - Rassemblement National
**Type de question :** Question écrite
**Numéro de la question :** 2584
**Rubrique :** Numérique
**Ministère interrogé :** Intérieur
**Ministère attributaire :** Intérieur

## Date(s) clée(s)

**Question publiée au JO le :** 3 décembre 2024, page 6375
**Réponse publiée au JO le :** 3 juin 2025, page 4513