ASSEMBLÉE NATIONALE

17ème législature

Industrialisation des escroqueries par l'intelligence artificielle

Question écrite n° 17731

Texte de la question

Mme Sophie Blanc attire l'attention de M. le ministre de l'intérieur sur l'industrialisation des escroqueries transnationales rendue possible par l'intelligence artificielle. Dans sa question écrite n° 2697 relative à la hausse des escroqueries et des fraudes aux moyens de paiement, Mme la députée avait déjà alerté le Gouvernement sur la sophistication croissante de cette criminalité, sur son caractère transfrontalier et sur la nécessité de renforcer tant les capacités des forces de l'ordre que la coopération avec les établissements bancaires, les acteurs du numérique et les autorités étrangères. Dans sa réponse publiée le 10 juin 2025, M. le ministre de l'intérieur reconnaissait que l'intelligence artificielle constituait un défi nouveau en fournissant aux escrocs des outils particulièrement puissants pour tromper leurs victimes. Il mettait principalement en avant les dispositifs généraux de prévention, de signalement et d'enquête alors existants. Or depuis cette première alerte, la menace a changé de nature et d'échelle. Le nouveau rapport d'Interpol publié le 3 août 2026 indique que l'intelligence artificielle intervient désormais dans 55 % des escroqueries attribuées aux réseaux criminels étudiés en Afrique. Entre 2024 et 2025, les pertes recensées seraient passées de 192 à 484 millions de dollars, tandis que le nombre de victimes africaines identifiées aurait progressé de 35 000 à 87 000. Ces données ne rendent en outre compte que des faits connus des autorités, alors que de nombreuses victimes ne signalent jamais l'escroquerie dont elles ont fait l'objet, soit par honte, soit parce qu'elles demeurent sous l'emprise de leurs interlocuteurs. L'intelligence artificielle ne sert plus seulement à rédiger des messages vraisemblables ou à produire de fausses photographies. Associée aux données personnelles provenant de fuites informatiques massives, elle permet d'analyser la situation d'une cible, d'adapter instantanément le scénario frauduleux à sa vie personnelle, de cloner la voix ou l'image d'un proche et d'entretenir simultanément des milliers de conversations individualisées. Ces outils permettent également la création d'« identités synthétiques », composées de données appartenant à plusieurs personnes réelles et d'éléments entièrement fictifs. De telles identités peuvent être utilisées pour contourner les procédures de vérification, ouvrir des comptes bancaires ou des portefeuilles de paiement, obtenir des crédits, enregistrer des cartes SIM et organiser la réception puis la dispersion des fonds détournés. Cette technique fragilise les mécanismes traditionnels de détection. À la différence d'une usurpation classique, l'identité synthétique ne correspond pas nécessairement à une personne déterminée susceptible de constater l'atteinte et de la signaler. Les documents présentés peuvent être cohérents entre eux, les contrôles biométriques trompés par des hypertrucages et les comptes frauduleux utilisés puis abandonnés avant même que les victimes aient compris la nature des faits. La réponse publique ne peut donc plus reposer principalement sur la vigilance individuelle et sur le signalement effectué après le transfert des fonds. Face à des campagnes automatisées, internationales et capables de changer très rapidement d'identité, de compte bancaire, de numéro téléphonique ou de plateforme, l'efficacité de l'action publique dépend désormais de la capacité à rapprocher immédiatement les alertes, à préserver les données techniques, à suspendre les moyens de communication utilisés et à interrompre les flux financiers avant leur dissémination. Elle lui demande par conséquent s'il dispose d'une évaluation du nombre d'escroqueries commises en France au moyen de contenus générés par intelligence artificielle ou d'identités synthétiques, ainsi que du préjudice financier correspondant. Elle lui demande quelles capacités techniques spécifiques ont été déployées depuis sa précédente question écrite afin de permettre aux forces de l'ordre de détecter ces procédés et d'identifier les infrastructures utilisées par les réseaux criminels. Elle souhaite enfin savoir si le Gouvernement entend mettre en place un mécanisme national de coordination en temps réel entre les services d'enquête, les établissements bancaires, les prestataires de paiement, les opérateurs de télécommunications et les plateformes numériques afin de détecter les identités

synthétiques, de suspendre rapidement les comptes et les lignes frauduleux, de geler les fonds détournés et de renforcer la coopération opérationnelle avec Interpol et les États depuis lesquels agissent ces réseaux.

Données clés

Auteur : Mme Sophie Blanc
Circonscription : Pyrénées-Orientales (1re circonscription) - Rassemblement National
Type de question : Question écrite
Numéro de la question : 17731
Rubrique : Banques et établissements financiers
Ministère interrogé : Intérieur
Ministère attributaire : Intérieur

Date(s) clée(s)

Question publiée au JO le : 18 août 2026, page 7556