ASSEMBLÉE NATIONALE

17ème législature

Danger des arnaques bancaires

Question écrite n° 6030

Texte de la question

Mme Tiffany Joncour interroge M. le ministre d'État, ministre de l'intérieur, sur la recrudescence alarmante des arnaques bancaires, un phénomène qui touche de plus en plus de Français et qui prend des formes de plus en plus diversifiées. Elle souhaite notamment attirer son attention sur un cas récemment révélé par la presse (*Le Progrès*) dans l'est lyonnais, dans lequel des malfaiteurs, se faisant passer pour des coursiers, ont trompé plusieurs victimes, souvent des personnes âgées, afin de leur dérober leurs cartes bancaires. Sous prétexte de livrer des colis, ces individus ont pu subtiliser une dizaine de cartes bancaires, provoquant un préjudice financier important pour les victimes. En France, selon la Fédération bancaire française, 57 % de la population indique avoir déjà été victime d'une tentative d'arnaque aux données bancaires. Face à cette situation, Mme la députée exprime son inquiétude quant à l'ampleur croissante de ces escroqueries, qui semblent exploiter les failles dans les systèmes de livraison et de transaction bancaire. Elle rappelle que ces pratiques, mêlant fraude et usurpation d'identité, créent un climat de méfiance et de vulnérabilité chez de nombreux Français. Au premier semestre 2024, le montant total de la fraude aux moyens de paiement s'élève à 584,6 millions d'euros selon l'OSMP (Observatoire de la sécurité des moyens de paiement). Mme la députée s'interroge donc sur les actions concrètes que le Gouvernement envisage pour endiguer ce phénomène, notamment en matière de prévention et de répression. Elle souhaiterait savoir si des mesures spécifiques sont envisagées pour renforcer la sécurité des transactions en ligne, mais aussi pour encadrer plus strictement les pratiques des entreprises de livraison, afin qu'elles prennent leurs responsabilités et évitent que des malfaiteurs ne puissent profiter de cette situation pour tromper les citoyens. Enfin, selon le rapport 2024 de Global Anti-Scam Alliance (GASA), seulement 16 % des Français ont pu récupérer l'intégralité de leurs pertes à la suite d'une arnaque et 46 % d'entre eux ont ressenti un fort impact émotionnel. Dès lors, Mme la députée soulève la question de l'accompagnement des victimes d'arnaques, qui se retrouvent souvent démunies face à la difficulté de récupérer leurs fonds et d'obtenir justice. Elle souhaite connaître son avis sur le sujet.

Texte de la réponse

La lutte contre la fraude constitue une priorité du ministère de l'intérieur, et des forces de sécurité intérieure. Le premier levier d'action est la présence de voie publique (PVP) : par une présence physique visible et dissuasive, directement auprès de la population, les patrouilles de gendarmes départementaux et de réservistes opérationnels sont au coeur de la lutte contre les faux courriers. La PVP de la gendarmerie a ainsi augmenté de 10% entre 2023 et 2024 pour atteindre 54 723 733 heures. Cela représente 44% de l'activité totale de la gendarmerie. Dans ce cadre, l'« opération tranquillité seniors » menée tant par la police que par la gendarmerie, permet de renforcer la surveillance du domicile des personnes âgées qui se sentent isolées, menacées ou tout simplement inquiètes pour leur sécurité. Plus de 1 500 opérations de ce type ont été réalisées par exemple par la gendarmerie en 2024 et 60 500 personnes de plus de 65 ans ont été sensibilisées aux risques liées aux fraudes et escroqueries. Le deuxième levier d'action est l'investigation judiciaire : par les signalements, et par les enquêtes, les gendarmes et les policiers recherchent, interpellent et présentent à la justice les auteurs d'escroqueries. Par exemple, une cellule nationale d'enquête créée sous l'égide de la direction générale de la

gendarmerie nationale a mobilisé une centaine d'enquêteurs de la section de recherche de Rouen et d'une dizaine de groupements de gendarmerie départementale du Nord de la France. Avec la DGCCRF, le GIR de Rouen, la direction départementale de protection des populations de Seine-Maritime et le parquet de Rouen, les enquêteurs ont révélé une fraude d'ampleur nationale. Dans le cadre de démarchages à domicile, les commerciaux de trois sociétés (réparties en treize agences dans le Nord de la France) prétextaient divers motifs pour entrer chez des « clients », et recueillaient leurs coordonnées bancaires et leurs signatures. Ensuite, ils concluaient des contrats commerciaux à l'insu des victimes, pour un préjudice total de plusieurs dizaines de millions d'euros. L'action de la gendarmerie et de ses partenaires a permis de saisir plus de 3 millions d'euros d'avoirs criminels et de biens de luxe et de porter un coup d'arrêt à cette filière. Le troisième levier d'action doit être un renforcement de la communication des bonnes pratiques et de l'état de la menace à destination des populations, considérant que cette démarche doit permettre au plus grand nombre de se protéger de la majorité des escroqueries en adoptant des comportements adaptés (mots de passe sécurisés, évitement des liens frauduleux, réflexes de vigilance…). La gendarmerie nationale et la police nationale participent à cette action de prévention à plusieurs niveaux. Par l'organisation d'action de sensibilisations à l'échelon local par les référents de la gendarmerie, qualifiés au titre de « l'introduction aux cybermenaces » (ICM) ou spécialistes « nouvelles technologies » (NTECH). Par le déploiement d'actions de prévention de la division de la proximité numérique de l'unité nationale cyber (UNCyber) à destination des citoyens, des entreprises et des collectivités. Ainsi, par le biais de communications ciblées ou d'événements organisés sur des espaces privilégiés par les usagers concernés, elle entretient la vigilance de chacun et la confiance numérique. S'appuyant sur des infographies accessibles à tous les usagers et moyennant des diagnostics simples au profit des entreprises de toutes tailles et des collectivités territoriales, les actions de prévention conduites (en partenariat notamment avec le dispositif national de prévention et d'assistance Cybermalveillance.gouv.fr) visent à infuser une culture de la cybersécurité dans les foyers et à améliorer le niveau de sécurité numérique des établissements publics comme privés. A titre d'illustration, durant le « cyber mois » d'octobre 2024, l'UNCyber a intensifié ses efforts pour alerter le public sur les attaques de plus en plus sophistiquées : à travers de courtes vidéos pédagogiques diffusées sur les réseaux sociaux, elle a prodigué des conseils pratiques pour sécuriser les données des particuliers en illustrant des scénarios particulièrement réalistes. La police nationale mène des actions de cyber prévention, notamment au profit des entreprises et des collectivités 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'OFAC (Office anti-cybercriminalité) de la direction nationale de la police judiciaire (DNPJ) pour accompagner les entreprises et les collectivités territoriales face aux risques du cyberespace. 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 et par diverses actions de prévention menées par l'OFAC. La gendarmerie mène également des actions spécifiques au profit des TPE-PME, des collectivités ou des établissements de santé, mises en œuvre notamment par le réseau CyberGend. Plus de 50 000 entreprises ont fait l'objet d'une action de prévention visant à lutter contre les cybermenaces, conduites par des cyber-gendarmes régulièrement renforcés par des réservistes œuvrant dans la cyber-sécurité au quotidien. Aussi, un outil de diagnostic de la « maturité cyber » (appelé DIAGONAL) des entreprises, des collectivités territoriales et des établissements de santé est également mis en œuvre par le réseau Cybergend. Il permet d'identifier les failles techniques et organisationnelles face aux attaques. L'objectif est, dans un second temps, que ces structures puissent se mettre à niveau en investissant à bon niveau considérant le risque important de fermeture d'entreprises victimes d'une cyber-attaque (supérieur à 50 % dans les trois ans). Police et gendarmerie assurent aussi le développement et la mise à jour constante de l'application « M@Sécurité », qui emporte de nombreux conseils numériques contribuant également aux actions de sensibilisation de la gendarmerie et la police nationales. Cette application a déjà été téléchargée plus de 750 000 fois. L'agence nationale de sécurité des systèmes d'information (ANSSI) conduit des actions similaires avec « mon aide cyber » et les forces de sécurité intérieure s'y associent pleinement. Enfin, la directive NIS2 augmente considérablement le périmètre des entreprises et collectivités soumises à des obligations de résilience cyber. En cas d'attaque, les obligations d'information de l'ANSSI et de la CNIL permettent d'aider sans tarder les victimes et de partager des informations (via les CERT) afin d'améliorer la défense collective de l'économie française. D'importantes sanctions financières donnent le poids nécessaire à ces obligations. La collaboration avec le secteur bancaire est ancienne. Depuis le développement des faux ordres de virement (FOVI), les banques ont adapté leurs process tant pour vérifier la réalité des donneurs d'ordres que pour récupérer les fonds, a minima au sein de

l'Union Européenne. Au profit des particuliers, la généralisation de la double authentification pour accéder aux applications bancaires mais également pour réaliser les paiements en ligne est un gain majeur. L'utilisation de l'intelligence artificielle (IA) est un challenge nouveau, les auteurs disposant d'outils puissants pour tromper les victimes, mais l'IA peut également être utilisée à des fins de vérifications en masse des opérations. L'accompagnement des victimes se fait en premier lieu par la qualité de l'accueil physique dans les unités de la gendarmerie et les commissariats. Aussi, sur les thématiques cyber, il est complété par des dispositifs numériques. Ainsi, afin d'être au plus proche des citoyens, la brigade numérique (BNum) créée à Rennes est désormais renforcée depuis le début de l'année 2025 par une seconde unité implantée à Poitiers Ces unités permettent d'échanger par tchat, 7j/7 et 24h/24 avec un gendarme susceptible d'apporter des réponses immédiates et de prodiguer des conseils aux victimes potentielles. Les gendarmes de ces unités sont spécifiquement formés aux risques cyber du quotidien comme aux attaques de plus grande ampleur visant les entreprises ou collectivités, souvent accompagnées de demandes de rançons. Depuis sa création en 2018, la BNum a accompagné plus de 1,1 million de personnes venues au contact de la gendarmerie par ce biais innovant. Depuis le 17 décembre 2024, le dispositif 17-cyber, commun à la police et à la gendarmerie, complète l'accompagnement. Disponible 24h/24 et 7j/7, ce guichet unique permet aux victimes de comprendre rapidement, en répondant à quelques questions, à quel type de menace ils sont confrontés et ainsi recevoir des conseils personnalisés en fonction de l'atteinte subie. Si le diagnostic confirme la gravité de l'atteinte subie, les utilisateurs victimes peuvent échanger par tchat avec un policier ou un gendarme pour disposer des conseils de première urgence et engager les démarches de judiciarisation. Lorsque cela est nécessaire, les usagers peuvent également recevoir une assistance technique d'un prestataire référencé ou labellisé par Cybermalveillance.gouv.fr. En complément, la plate-formePerceval de la gendarmerie est dédiée depuis 2019 aux victimes de fraudes à la carte bancaire. Elle recueille les signalements des particuliers (plus de 200 000 par an) afin de collecter les informations pertinentes pour réaliser des rapprochements entre les faits et générer des enquêtes judiciaires. Elle a, par exemple, démontré son efficacité durant les jeux olympiques et paralympiques de Paris 2024 en stoppant une escroquerie visant des food trucks. Au total, ce sont plus de 500 procédures judiciaires diligentées. De même, la plateforme PHAROS, gérée par l'Office anti-cybercriminalité (OFAC) de la direction nationale de la police judiciaire (DNPJ), traite l'ensemble des signalements de contenus illicites sur internet (plus de 220 000 signalements reçus en 2024), tandis que la plateforme Thésée de l'OFAC est disponible pour certaines escroqueries commises sur internet par un auteur inconnu (plus de 107 000 déclarations reçues en 2024). Il convient de rappeler sur un plan plus général que les victimes d'escroquerie, personnes physiques ou morales, peuvent solliciter la plateforme téléphonique « Info Escroqueries » gérée par la DNPJ. La publicité de ces dispositifs est l'affaire de tous, acteurs publics et privés mais également représentation nationale grâce à son ancrage local au sein des circonscriptions. La coopération internationale varie fondamentalement dans et hors l'Union Européenne. Les dispositifs d'échanges d'informations entre forces de l'ordre (initiative suédoise transposée dans les articles 695-9-31 et suivant du CPP), la décision d'enquête européenne, le mandat d'arrêt européen ou l'action des agences Europol et Eurojust offrent dans l'UE une palette d'outils efficaces. En dehors de l'UE, la coopération existe. Toutefois, force est de constater que nombre d'enquêtes d'envergure en matière de fraudes et d'escroquerie cyber conduisent régulièrement vers des pays peu ou pas coopératifs : les organisations criminelles internationales dans ce domaine privilégient des zones géographiques dont les législations et la difficulté à faire accepter des demandes d'appui judiciaire les protègent (Asie du sud-est par exemple). De récentes actions avec le soutien d'Interpol dans cette partie du monde sont à souligner en matière de démantèlement de « call-center » d'escroqueries. Enfin, les moyens des forces de l'ordre afin de conduire les actions répressives contre les acteurs de la cyber-criminalité sont en constante évolution. La gendarmerie compte 10 000 cyber-gendarmes, parmi lesquels plus de 1 100 enquêteurs formés aux enquêtes sous pseudonyme (ESP), et des militaires hautement qualifiés dont 325 enquêteurs en technologies numériques (NTECH) et 248 enquêteurs spécialisés cryptoactifs (FINTECH) présents sur l'ensemble du territoire national. Ces enquêteurs hautement spécialisés enquêtent à plein temps dans le domaine cyber et notamment s'agissant des escroqueries commises sur internet, ils sont à même de conduire des investigations de premier niveau et les actes de criminalistique numérique associés, permettant une réponse rapide et adaptée face aux cyber-escroqueries. Les enquêteurs du haut du spectre sont de plus en plus nombreux et un plan est lancé en 2025 pour atteindre le nombre de 1 000 cyber-enquêteurs à l'horizon de 2030. Les formations à l'analyse des crypto-monnaie se multiplient également grâce à la création d'un centre de formation cyber à Lille en 2022. Ces forces s'inscrivent dans une organisation structurée, qui repose en

gendarmerie sur l'Unité nationale cyber, qui concentre ses moyens opérationnels en matière cyber au niveau national. L'UNCyber capitalise sur 20 années d'investissements dans ce domaine. Elle est articulée autour d'un état-major, d'un détachement implanté au sein du centre national des opérations de la gendarmerie nationale, d'une division des opérations (C3N), d'une division technique et d'une division de la proximité numérique, et coordonne le dispositif cybergend, comprenant les unités élémentaires, les unités de recherches, les 105 sections opérationnelles de lutte contre les cybermenaces (SOLC) des groupements de gendarmerie départementale (GGD) et commandements de la gendarmerie outre-mer (COMGEND) et les 20 antennes du centre de lutte contre la criminalité numérique (12 AC3N en métropoles et 8 outre-mer). Son action couvre le champ de la prévention, la fonction contact, et des moyens d'investigation. Aussi, la gendarmerie contribue massivement au Commandement du ministère de l'intérieur dans le cyberespace (ComCyber-Mi), dont elle assure le pilotage, et qui aide au quotidien à définir l'état de la menace et à identifier les acteurs malveillants grâce à de nombreux capteurs. La police nationale s'est pour sa part dotée d'un « plan cyber 2022-2027 » pour renforcer son action de prévention et d'investigation de la cybercriminalité. Sur le plan opérationnel, l'Office anti-cybercriminalité assume un rôle de coordination et d'animation opérationnelle dans la lutte contre la cybercriminalité. Cet office central est également le point de contact central à l'international. Il assure, outre ses missions judiciaires, des actions de prévention, un travail de recueil et d'analyse du renseignement criminel et la production d'états de la menace.il s'appuie pour ses missions d'enquête et d'appui aux investigations numériques menées par les services déconcentrés de police. Outre ce service hautement spécialisé, la police nationale dispose de plus de 15 000 personnels formés aux investigations sur internet, dont les enquêteurs sous pseudonyme. Plus de 8 000 agents sont par ailleurs formés aux investigations techniques, dont les investigateurs en cybercriminalité (plus de 600).

Données clés

Auteur : Mme Tiffany Joncour
Circonscription : Rhône (13e circonscription) - Rassemblement National
Type de question : Question écrite
Numéro de la question : 6030
Rubrique : Sécurité des biens et des personnes
Ministère interrogé : Intérieur
Ministère attributaire : Intérieur

Date(s) clée(s)

Question publiée au JO le : 15 avril 2025, page 2666
Réponse publiée au JO le : 1er juillet 2025, page 5815