ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 21542	De **Mme Patricia Lemoine** (UDI et Indépendants - Seine-et-Marne)	**Question écrite**

Ministère interrogé > Intérieur	**Ministère attributaire** > Intérieur

Rubrique >Internet	**Tête d'analyse** >Lutte contre la cyberdélinquance	**Analyse** > Lutte contre la cyberdélinquance.

Question publiée au JO le : **16/07/2019**
Réponse publiée au JO le : **15/10/2019** page : **9020**

Texte de la question

Mme Patricia Lemoine interroge M. le ministre de l'intérieur sur l'augmentation de la cyberdélinquance et les moyens mis en œuvre pour lutter contre ce phénomène. Il y a quelques jours, la délégation ministérielle à la lutte contre les cybermenaces, rattachée au Ministère de l'intérieur, a rendu son rapport annuel sur la cyberdélinquance. Si l'année 2018 n'a pas été marquée par un bond spectaculaire de cette forme de criminalité comme ce fut le cas entre 2016 et 2017, il reste qu'elle est en augmentation de 7 %. Ce sont près de 68 000 infractions de ce type qui ont été recensées par les services de la gendarmerie nationale. Parmi les infractions qui font l'objet d'un dépôt de plainte, celles des « escroqueries liées à internet » sont les plus fréquentes, représentant 73 % de ces plaintes. Visant à la fois les particuliers et les entreprises, prenant des formes variées telles que les rançongiciels, les escroqueries *via* de faux profils sur des sites de rencontres ou encore les faux sites de *trading*, ces infractions représentent un préjudice total colossal de près d'un milliard d'euros. Afin de lutter contre cette criminalité numérique, différents dispositifs existent actuellement, tels que la plateforme Perceval. Cependant, elle apparaît insuffisante car tous les cas de fraude ne sont pas déclarés à la plateforme. De même, l'outil est parfois inadapté car il ne répertorie pas toutes les formes d'infractions. Les enquêteurs se retrouvent ainsi avec des informations parcellaires, d'autant que les parquets de tribunaux n'ouvrent des enquêtes qu'à partir d'un certain seuil de préjudice. Face à une forme criminalité qui n'aura de cesse de se développer durant les prochaines années, elle souhaite connaître ses intentions afin de renforcer les moyens de lutte contre cette cybercriminalité.

Texte de la réponse

La troisième édition du rapport annuel du ministère de l'Intérieur portant sur l'État de la menace liée au numérique, mis en ligne le 9 juillet 2019, rappelle quelques-uns des moyens dédiés à la lutte contre la cybercriminalité à venir : humains, financiers, matériels, juridiques, organisationnels, préventifs et répressifs, etc. Les moyens humains sont notamment renforcés avec la mise en place d'une politique innovante, à travers le recrutement de 800 agents supplémentaires affectés à la lutte contre les cybermenaces et à la sécurité des systèmes d'information au sein de l'ensemble des directions opérationnelles, sur la période 2018-2022. De nouveaux moyens organisationnels sont également à venir, comme le projet THESEE en 2020, portant sur la « plainte en ligne » pour les e-escroqueries. Il s'appuiera sur deux autres projets : le nouveau logiciel de rédaction de procédure (SCRIBE) et la signature électronique de l'officier de police judiciaire. Ces dispositifs viendront compléter utilement des outils récents, comme la plateforme PERCEVAL développée par la gendarmerie nationale et portant sur le signalement des fraudes à la carte bancaire. Le changement de paradigme de traitement, fondé sur les signalements en ligne et non plus uniquement sur les plaintes individuelles, permet en effet de mieux appréhender les phénomènes de

masse. Les moyens préventifs, à travers la mise en œuvre d'actions de sensibilisation auprès du grand public et du monde économique par l'ensemble des services du ministère, seront accrus. Le réseau des référents cybermenaces de la police nationale, lancé à titre expérimental en mars 2018 dans l'objectif de sensibiliser le tissu économique local au risque cyber, a vocation à être pérennisé et généralisé sur l'ensemble du territoire. Quant au programme gouvernemental « cybermalveillance.gouv.fr », qui assure un rôle de sensibilisation, de prévention et de soutien en matière de sécurité du numérique auprès de la population française, il montera encore en puissance dans les années à venir, avec l'appui du ministère de l'Intérieur. En complément de ces moyens préventifs, l'élaboration et la mise en œuvre de politiques pénales adaptées permettent de répondre à ce phénomène diffus, multiple et protéiforme que constitue la cyber délinquance. Grâce aux échanges avec les services centraux spécialisés du ministère (centre de lutte contre les criminalités numériques, office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, brigade d'enquêtes sur les fraudes aux technologies de l'information), le parquet F1 du tribunal de grande instance de Paris pilote l'activité des juridictions, au plus près de sa connaissance du phénomène, en particulier les rançongiciels. Il a entamé par ailleurs la nécessaire centralisation des affaires d'attaques informatiques. Enfin, si les moyens dédiés à la lutte contre la cybercriminalité sont mis en œuvre par chaque service concerné du ministère de l'Intérieur, ils ont également été pensés, de manière globale, par l'ensemble des directions opérationnelles : il s'agit de la « feuille de route cyber ». Ce document, classifié, décrit la projection de la lutte contre les cybermenaces à l'horizon 2022 et les réponses du ministère. Ces réponses sont au nombre de 7 : une connaissance affinée de la cybercriminalité, une augmentation des capacités opérationnelles, une montée en capacité en compétence des personnels cyber, une communauté cyber territoriale mieux organisée, un renforcement des capacités de gestion de crise, un renforcement des actions de R&D cyber, ainsi que l'affirmation de l'ancrage du ministère dans l'écosystème cyber, en mutation. Le renforcement de la délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces (qui a coordonné les travaux de la feuille de route et publié le rapport annuel mentionné supra) en constituera une première étape.