ASSEMBLÉE NATIONALE

16ème legislature

Question N° : 7773	De **Mme Michèle Tabarot** (Les Républicains - Alpes-Maritimes)	**Question écrite**

Ministère interrogé > Intérieur et outre-mer	**Ministère attributaire** > Intérieur et outre-mer

Rubrique >crimes, délits et contraventions	**Tête d'analyse** >Moyens de lutte contre le « Darkweb »	**Analyse** > Moyens de lutte contre le « Darkweb ».

Question publiée au JO le : **09/05/2023**
Réponse publiée au JO le : **11/06/2024** page : **4828**
Date de changement d'attribution : **12/01/2024**

Texte de la question

Mme Michèle Tabarot appelle l'attention de M. le ministre de l'intérieur et des outre-mer sur l'opération internationale SpecTor coordonnée par Europol et engageant neuf pays, ayant permis l'arrestation de 288 utilisateurs du *Darkweb*, cette version parallèle d'internet où l'anonymat des utilisateurs est garanti. Au total, 51 millions d'euros en espèce et de monnaie virtuelle ont été saisis. Parmi les arrestations, cinq ont été effectuées en France. Malgré les efforts entrepris, nombreux sont les sites qui continuent à être accessibles aux concitoyens. Outre les ventes d'armes, de drogue et de tous types d'objets illégaux sur le *Darkweb*, se pose également la question de l'accès à la pédopornographie. Aussi, elle souhaiterait qu'il puisse préciser les moyens supplémentaires qui vont être développés pour continuer à amplifier la lutte contre les utilisateurs du *Darkweb*.

Texte de la réponse

La gendarmerie et la police nationales sont pleinement mobilisées dans la lutte contre la cybercriminalité, plus particulièrement contre les formes de criminalités issues du Darkweb, partie clandestine de l'internet accessible uniquement via des logiciels, protocoles ou configurations spécifiques, dont le plus connu est le réseau The Onion Router (TOR). Deux contraintes sont à prendre en compte pour les forces spécialisées de police et de gendarmerie. La première est d'ordre procédural en ce qu'il est indispensable, avant d'ouvrir une enquête, de caractériser la compétence judiciaire française. En effet, les enquêteurs devront démontrer que l'administrateur de cette plateforme est en France ou que l'hébergement informatique de cette plateforme est réalisé par une société française. La seconde contrainte relève de l'anonymat intrinsèque à l'utilisation des darkwebs par le réseau d'anonymisation TOR. La dernière loi d'orientation et de programmation du ministère de l'intérieur (LOPMI) de janvier 2023 a introduit dans le Code pénal deux nouvelles incriminations dédiées à la lutte contre ces plateformes illicites : le délit d'administration d'une plateforme en ligne pour permettre la cession de produits illicites et le délit d'intermédiation ou de séquestre pour faciliter la cession de produits illicites, lorsque cette plateforme restreint son accès aux personnes utilisant des techniques d'anonymisation des connexions ou lorsqu'elle contrevient aux obligations imposées par la loi pour la confiance dans l'économie numérique. Ce nouvel arsenal juridique va permettre aux enquêteurs de s'attaquer directement aux administrateurs de darkmarkets ou aux revendeurs présents sur ces darkmarkets. Pour ce qui concerne la gendarmerie nationale, l'Unité nationale cyber (UNC), bras armé numérique de la gendarmerie, traite des contentieux d'ordre cyber du haut spectre, en particulier sur le Darkweb. Dès lors, la lutte contre ces plateformes (darkmarkets) de ventes d'armes, de drogue, de logiciels malveillants, de bases de données, de matériels pédopornographiques ou d'autres types d'objets illégaux accessibles sur le Darkweb,

est une mission pleinement prise en compte par la gendarmerie. La division des opérations de l'UNC (Centre de lutte contre les criminalités numériques – C3N) dispose en effet de 49 militaires spécialisés dans les investigations numériques, dont un groupe dédié aux investigations relatives aux darkmarkets. Ce dernier a été renforcé de 2 enquêteurs supplémentaires au cours des derniers mois. En parallèle, les 20 antennes régionales (métropole et outre-mer) sont également amenées à diligenter des enquêtes sur le darkweb au plus proche des victimes d'infractions. Plusieurs techniques d'enquête sont maîtrisées et utilisées par les militaires de l'UNC comme l'enquête sous pseudonyme, couplée avec le coup d'achat ou l'achat de confiance. Cela permet à l'enquêteur de se connecter à un darkmarket et se faire passer pour un individu désirant acheter des produits illicites et de commander un produit illicite afin de sécuriser le vendeur et de tracer le processus d'achat et de livraison. Aujourd'hui la gendarmerie compte près de 900 enquêteurs sous pseudonyme, chiffre en constante augmentation grâce aux formations décentralisées mises en œuvre. En parallèle, un travail technique de précision est réalisé par la division technique pour essayer de désanonymiser les points d'accès du réseau TOR (ces points d'accès sont appelés des nœuds TOR et de nombreux nœuds TOR sont hébergés en France ou dans l'Union européenne). La coopération internationale avec d'autres services d'enquête européens, initiée et suivie activement par le C3N, permet de mettre en place des projets d'ampleur sur cette désanonymisation. Dans le cadre de la lutte contre l'exploitation sexuelle des mineurs par le biais du Darkweb, la gendarmerie s'appuie sur le département du C3N dédié à ce contentieux. Ce département traque continuellement les prédateurs et cherchent à développer des techniques innovantes pour conjuguer les évolutions technologiques et surmonter les obstacles liés à l'anonymat que procure ce réseau. Il est néanmoins constaté que si nombre de trafics illicites et échanges se déroulent sur le darkweb ces derniers ont un lien avec l'internet et les réseaux sociaux, le plus souvent ceux procurant le plus de garanties sur la préservation de l'anonymat. En effet la plupart des prédateurs se trouvent généralement sur des canaux plus ouverts et accessibles que le darkweb. Aussi les efforts doivent être portés simultanément sur l'ensemble des réseaux. C'est pour cela que la Gendarmerie fait le choix de mener régulièrement, de manière centralisée et déconcentrée, des opérations nationales et régionales de lutte contre la pédopornographie (Horus) ou contre les trafics de produits stupéfiants. Les mis en cause utilisent de moins en moins de services « law enforcement friendly ». Cet état de fait rend les investigations plus fastidieuses et plus longues en raison d'un besoin de coopération internationale qui n'est pas évident avec certaines zones du globe. Pour ce qui concerne la police nationale, le darkweb fait l'objet d'un suivi attentif et expert de la part de la Direction nationale de la police judiciaire (DNPJ). La numérisation constatée de la criminalité organisée justifie l'engagement de l'ensemble des offices spécialisés de la DNPJ dans la lutte contre le darkweb, mais appelle aussi une surveillance des criminels sur d'autres supports de communication que sont notamment les messageries chiffrées de type « Telegram ». En sa qualité d'expert de la lutte contre la cybercriminalité, l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) de la DNPJ lutte contre toutes les formes d'activités criminelles se développant sur le Darkweb. Les activités judiciaires de l'OCLCTIC le conduisent à démanteler très régulièrement les structures et forums criminels du darkweb. Entre 2018 et 2023, les enquêtes de l'office ont, par exemple, conduit au démantèlement des forums Black Hand, French Deeb Web, Liberty Hackers, etc., qui proposaient toutes sortes de services criminels (faux papiers, armes, stupéfiants, etc.). L'office a mis en place une section d'enquête dédiée à la répression de ces plateformes criminelles. La haute technicité requise pour lutter contre la criminalité sur le darkweb explique la composition particulière de l'OCLCTIC où des policiers, des ingénieurs et des contractuels travaillent de concert. À l'instar de la gendarmerie, des techniques d'enquête spécifiques y sont quotidiennement déployées, en particulier les enquêtes sous pseudonyme. L'OCLCTIC est également le point d'entrée, pour la France, de toutes les informations reçues des partenaires internationaux pour signaler les activités cybercriminelles. Des coopérations avec le FBI, Interpol et Europol conduisent ainsi régulièrement les enquêteurs à démanteler des structures et forums du darkweb. Au-delà de la répression des activités cybercriminelles consistant à mettre à disposition de la criminalité organisée des marchés illégaux, dits « dark markets », il convient de lutter contre la numérisation de la criminalité organisée. Les nouveaux utilisateurs du darkweb sont en effet des acteurs habituels de la criminalité organisée, trafiquants de stupéfiants ou d'armes, proxénètes, faussaires, qui étendent leurs activités vers la sphère cyber. La diversité des activités criminelles développées ou proposées sur le darkweb justifie donc que l'ensemble des offices centraux spécialisés de la DNPJ soient quotidiennement impliqués dans cette lutte aux côtés de l'OCLCTIC. Chaque office dispose, à ce titre, d'enquêteurs voire de groupes spécialement formés à la lutte

contre la criminalité sur le darkweb. En matière de pédopornographie sur le darkweb par exemple, le Groupe central des mineurs victimes (GCMV, rattaché à l'Office central pour la répression des violences aux personnes), dont les missions seront reprises par le nouvel Office des mineurs (OFMIN) en cours de mise en place, initie des enquêtes sous pseudonyme sur différents forums et sites, hébergés sur le darkweb, dédiés à l'exploitation sexuelle des enfants. Le GCMV est la première unité de police en France à avoir formé ses enquêteurs à l'enquête sous pseudonyme (ESP) et à avoir initié, dès 2009, des investigations de cette nature. Actuellement, 17 enquêteurs du GCMV sont habilités auprès de la cour d'appel de Paris à effectuer des enquêtes sous pseudonymes. Ce groupe hautement spécialisé mène diverses enquêtes en lien avec le darkweb, notamment aux fins d'identification d'internautes susceptibles d'être Français, postant des photos ou des vidéos d'exploitation sexuelle d'enfants, parfois également producteurs de ces photos et vidéos. La lutte contre la pédopornographie en ligne suppose une forte coopération internationale. Le GCMV travaille en coopération avec EUROPOL et INTERPOL, aux fins de localisation de serveurs et d'identification de leurs administrateurs. Par ailleurs, le GCMV représente la France au sein d'une taskforce dédiée à l'enquête sous pseudonyme qui regroupe des enquêteurs spécialisés de près de 30 pays. La création de l'OFMIN, et en son sein d'une unité dédiée à l'enquête sous pseudonyme, devrait permettre de lutter encore plus efficacement contre la pédocriminalité sur les réseaux du Darknet. La lutte contre les activités criminelles développées ou proposées en ligne ne se limite cependant pas à la seule lutte contre les structures et forums criminels du Darkweb. Les coups portés aux « dark markets », tant nationaux qu'en coopération internationale, ont conduit les criminels à faire évoluer leurs pratiques. L'OCLCTIC a observé, à la faveur des nombreuses enquêtes élucidées sur le darkweb, que les criminels les plus jeunes utilisaient désormais plus volontiers des réseaux anonymes (Telegram, Snapchat, etc.). La mise en place de « salons numériques fermés très spécialisés » diminue l'exposition et, espèrent-ils, la détection. En matière de lutte contre la pédopornographie comme pour les autres formes de cybercriminalité, le suivi attentif de ces réseaux apparaît comme une priorité judiciaire pour les prochaines années. La lutte contre la criminalité véhiculée par le darkweb fait partie des enjeux pris en compte dans le cadre du plan cyber 2022-2027 de la police nationale. Le plan prévoit notamment d'accroître les capacités d'exploitation de données de masse issues du démantèlement des cyber-services criminels, par l'intermédiaire d'un plateau technique spécialisé. Le plan prévoit également le renforcement des compétences cyber des services territoriaux de police judiciaire, par la création de nouvelles antennes territoriales spécialisées placées sous l'autorité fonctionnelle de l'OCLCTIC et de 45 détachements d'antennes, ainsi que par le recrutement de 220 agents spécialisés. L'offre de formation destinée à tous les policiers en matière de recherches en sources ouvertes, darknet, crypto-monnaies et enquête sous pseudonyme sera parallèlement renforcée. Il doit par ailleurs être notée la très prochaine mise en place d'un nouvel Office anti-cybercriminalité (OFAC), rattaché au directeur national de la police judiciaire. Il se substituera à la sous-direction de la lutte contre la cybercriminalité de la DNPJ et à son OCLCTIC. Cette réorganisation va permettre aux services spécialisés de la « PJ » de gagner encore en efficacité, en adaptabilité et en capacités de coordination opérationnelle des services, pour faire face au développement de la cybercriminalité de haut niveau, de plus en plus complexe, et à la généralisation des cyberinvestigations dans les enquêtes. Enfin, la création récente du Commandement du ministère de l'intérieur dans le cyberespace (ComCyberMi), service à compétence nationale du ministère, permet d'offrir un appui significatif aux unités de police judiciaire des différentes forces de sécurité intérieure. La division des enquêtes spécialisées, de la donnée et des investigations techniques offre plusieurs technicités en matière d'analyse de grands volumes de données (science de la donnée), de suivi et de désanonymisation des transactions sur la « blockchain » ou encore en matière de recueil de données des supports chiffrés ou dégradés.