COMMISSION
EUROPÉENNE

Bruxelles, le 14.4.2021
COM(2021) 170 final

COMMUNICATION DE LA COMMISSION AU PARLEMENT EUROPÉEN, AU CONSEIL, AU COMITÉ ÉCONOMIQUE ET SOCIAL EUROPÉEN ET AU COMITÉ DES RÉGIONS

relative à la stratégie de l'UE visant à lutter contre la criminalité organisée (2021-2025)

{SWD(2021) 74 final}

Introduction

Cachée au public en raison de l'opacité de ses activités, la criminalité organisée représente une menace importante pour les citoyens, les entreprises, les institutions publiques et l'économie de l'Europe dans son ensemble. Comme le relève la dernière **évaluation de la menace que représente la grande criminalité organisée dans l'Union européenne** (SOCTA UE 2021)[1], des groupes criminels organisés sont présents dans tous les États membres. Le paysage de la criminalité organisée se caractérise par un environnement en réseau dans lequel la coopération entre les criminels est fluide, systématique et tournée vers le profit. Les groupes criminels organisés utilisent leurs vastes profits illégaux pour infiltrer l'économie licite et les institutions publiques, notamment par la corruption, en affaiblissant l'état de droit et les droits fondamentaux et en sapant le droit des citoyens à la sécurité ainsi que leur confiance dans les pouvoirs publics. En 2019, les recettes d'origine criminelle dans les neuf principaux marchés criminels de l'Union européenne s'élevaient à 139 milliards d'euros [2], ce qui correspond à 1 % du produit intérieur brut de l'Union. Comme le souligne la stratégie de l'UE pour l'union de la sécurité[3], il convient de poursuivre et de renforcer les mesures prises au niveau de l'UE pour soutenir les États membres dans la lutte contre la criminalité organisée.

La complexité du modèle économique des groupes criminels organisés a été mise en lumière, en particulier, en 2020 dans le cadre de l'enquête menée conjointement par les autorités françaises et néerlandaises avec le soutien de l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et de l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust), afin de démanteler **EncroChat**, un réseau téléphonique crypté largement utilisé par les réseaux criminels. À ce jour, l'affaire EncroChat a abouti à plus de 1 800 arrestations et à plus de 1 500 nouvelles enquêtes. Elle a également montré dans quelle mesure les groupes criminels organisés opèrent au niveau transnational et en ligne dans tous les marchés criminels dans un environnement en réseau, en utilisant des modes opératoires de plus en plus sophistiqués et de nouvelles technologies. En mars 2021, une autre opération conjointe à la suite du crash de Sky CEC, un réseau crypté vers lequel de nombreux anciens utilisateurs d'Encrochat avaient migré, a permis de prévenir plus de 70 incidents violents, de saisir plus de 28 tonnes de substances médicamenteuses et d'arrêter plus de 80 suspects impliqués dans la criminalité organisée et le trafic de drogue en Belgique et

[1] Europol, rapport 2021 sur l'évaluation de la menace que représente la grande criminalité organisée dans l'Union européenne (SOCTA UE), 12 avril 2021, https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment. Le rapport SOCTA UE est une analyse exhaustive de la menace que représente la criminalité organisée et qui recense les domaines hautement prioritaires de la criminalité. Elle est réalisée tous les quatre ans par Europol, sur la base des contributions des États membres.

[2] Drogues illicites, traite des êtres humains, trafic de migrants, fraude (fraude intracommunautaire à l'opérateur défaillant, violations des droits de propriété intellectuelle, fraude alimentaire), criminalité environnementale (déchets illicites et espèces sauvages illicites), armes à feu illicites, tabac illicite, activités de cybercriminalité, criminalité organisée contre les biens — Mapping the risk of serious and organised crime infiltration in legitimate businesses (La cartographie des risques d'infiltration de la grande criminalité organisée dans les entreprises légitimes), mars 2021, DR0221244ENN, https://data.europa.eu/doi/10.2837/64101.

[3] Communication de la Commission relative à la stratégie de l'UE pour l'union de la sécurité, 24 juillet 2020, COM(2020) 605 final.

aux Pays-Bas. Plus de 400 nouvelles enquêtes ont été ouvertes contre des groupes criminels organisés à haut risque.

Le recours à la violence par les criminels impliqués dans la criminalité organisée est en augmentation dans l'UE, tout comme la menace que représentent les incidents violents dus à l'utilisation fréquente d'armes à feu ou d'explosifs dans l'espace public[4]. La capacité des groupes criminels organisés à s'adapter aux changements dans l'environnement dans lequel ils opèrent et à en tirer parti s'est confirmée au cours de la pandémie de COVID-19. Les groupes criminels se sont servis de la pandémie pour intensifier leurs activités criminelles en ligne[5] et pour commettre des fraudes, notamment en rapport avec des produits médicaux contrefaits. La demande élevée et soutenue de vaccins contre la COVID-19 est devenue un filon intéressant pour les criminels cherchant à produire et à fournir des vaccins contrefaits ou à escroquer des particuliers ou des autorités publiques. Jusqu'à présent, les gouvernements de l'UE ont détecté des tentatives d'escroqueries et de fausses offres de la part de fraudeurs tentant de vendre plus de 1,1 milliard de doses de vaccin pour un prix total de plus de 15,4 milliards d'euros[6]. La crise économique découlant de la pandémie renforce les risques liés aux activités de la criminalité organisée et la menace d'infiltration de la société et de l'économie par cette criminalité organisée.

Les menaces transnationales et l'évolution des modes opératoires des groupes criminels organisés actifs hors ligne et en ligne nécessitent une réponse coordonnée, plus ciblée et mieux adaptée. Si les autorités nationales opérant sur le terrain sont en première ligne dans la lutte contre la criminalité organisée, une action au niveau de l'Union et des partenariats mondiaux sont essentiels pour assurer une coopération efficace ainsi que l'échange d'informations et de connaissances entre les autorités nationales, en s'appuyant sur un cadre commun de droit pénal et sur des moyens financiers efficaces. Par ailleurs, la criminalité organisée est emblématique du lien entre la sécurité intérieure et la sécurité extérieure. L'engagement international en matière de lutte contre la criminalité organisée, comprenant de nouvelles mesures visant à établir des partenariats et une coopération avec les pays du voisinage immédiat et au-delà, est nécessaire pour relever ce défi transnational.

Tant le Parlement européen[7] que le Conseil[8] ont souligné que la criminalité organisée causait d'énormes préjudices et qu'une réponse forte de l'UE était nécessaire pour contrer toutes les formes d'activité criminelle organisée.

---

[4] Europol, rapport 2021 sur l'évaluation de la menace que représente la grande criminalité organisée dans l'Union européenne (SOCTA UE), 12 avril 2021, https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment.

[5] Dans le cadre d'une opération internationale menée entre mars et décembre 2020 et soutenue par Europol et par l'Office européen de lutte antifraude (OLAF), les services répressifs de 19 États membres et de 8 pays tiers ont saisi près de 33 millions de faux dispositifs médicaux, dont des masques, des tests et des kits de diagnostic, 8 tonnes de matières premières et 70 000 litres de désinfectant.

[6] Informations communiquées à l'OLAF par les autorités gouvernementales. Les services répressifs coopèrent avec Europol et l'OLAF pour déjouer ces tentatives de fraude.

[7] https://www.europarl.europa.eu/doceo/document/TA-9-2020-0378_FR.pdf. En octobre 2016, le Parlement européen a également adopté un rapport consacré spécifiquement à la lutte contre la corruption, https://www.europarl.europa.eu/doceo/document/A-8-2016-0284_FR.pdf

La présente stratégie s'appuie sur les réalisations passées, définit des axes de travail prioritaires pour mieux protéger les citoyens et l'économie contre les groupes criminels organisés et propose des actions concrètes à moyen et à long terme, qui seront mises en œuvre dans le plein respect des droits fondamentaux. Elle constitue la première stratégie spécifique en matière de lutte contre la criminalité organisée depuis l'entrée en vigueur du traité de Lisbonne[9].

1. Renforcer l'application du droit et la coopération judiciaire

Aujourd'hui, la criminalité organisée est une activité internationale. 65 % des groupes criminels actifs dans les États membres de l'UE comptent plusieurs nationalités parmi leurs membres[10]. Les itinéraires de transport de stupéfiants, d'armes à feu ou de produits contrefaits s'étendent sur tous les continents par l'intermédiaire d'une chaîne d'approvisionnement mondiale. Les groupes criminels organisés mobiles qui se livrent à la criminalité organisée contre les biens se déplacent rapidement à travers plusieurs territoires pour commettre leurs infractions. En étant actifs sur différents territoires, les groupes criminels évitent de se faire repérer et exploitent les différences entre les législations nationales applicables.

1.1.Échange fluide d'informations et accès en temps utile à ces informations

Dans une zone de liberté, de sécurité et de justice, au sein de laquelle il n'existe aucun contrôle aux frontières intérieures, il est possible d'assurer un niveau de sécurité élevé grâce à une solide coopération policière et judiciaire entre les États membres. Un accès en temps utile aux informations, dans le plein respect des droits fondamentaux et en particulier de la protection des données, est essentiel pour lutter contre toutes les formes de criminalité organisée. L'Union européenne a fourni aux services répressifs une large panoplie d'instruments pour faciliter l'échange d'informations qui se sont révélées cruciales pour mettre au jour les activités criminelles et les réseaux criminels.

Le **système d'information Schengen (SIS)** a permis aux agents de première ligne de détecter et de localiser rapidement des personnes et des objets impliqués dans la criminalité organisée et de prendre des mesures en conséquence. Les informations contenues dans cette base de données partagée peuvent aider les agents à arrêter une personne, à saisir un objet ou à définir les déplacements des personnes concernées par une enquête. Rien qu'en 2020, le SIS a été

[8] Conclusions du Conseil du 24 novembre 2020 sur la sécurité intérieure et le partenariat européen de police 13083/1/20 REV 1.

[9] La criminalité organisée est une priorité de l'UE depuis le milieu des années 90, comme le montre le programme de Tampere (qui a fixé les premiers objectifs stratégiques pluriannuels de l'UE dans le domaine de la justice et des affaires intérieures et les programmes pluriannuels ultérieurs en matière de justice et d'affaires intérieures, tels que le programme de La Haye de 2004, le programme de Stockholm de 2009, le programme de l'UE de 2015 en matière de sécurité et la stratégie de l'UE de 2020 pour l'union de la sécurité adoptée récemment). La dernière stratégie spécifique en matière de lutte contre la criminalité organisée date de 2005, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52005DC0232&from=FR.

[10] Europol, rapport 2021 sur l'évaluation de la menace que représente la grande criminalité organisée dans l'Union européenne (SOCTA UE), 12 avril 2021, https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment.

consulté près de 4 milliards de fois, ce qui a donné plus de 200 000 résultats positifs. La révision du cadre du SIS[11] en 2018 a considérablement renforcé les fonctionnalités du système et a mis en place un certain nombre de nouveaux outils, grâce auxquels les autorités nationales ont pu établir des signalements en rapport avec des personnes susceptibles de faire l'objet d'un enlèvement ou de traite des êtres humains, ou demander des contrôles d'investigation à l'encontre d'un suspect. La réforme permet également à Europol d'accéder aux signalements SIS et à l'échange d'informations supplémentaires, et d'utiliser plus efficacement les données biométriques, en introduisant la possibilité d'utiliser des images faciales à des fins d'identification et d'inclure des profils ADN afin de faciliter l'identification des personnes disparues. La mise en œuvre de ces nouveautés progresse rapidement, de sorte que le nouveau système sera pleinement opérationnel d'ici la fin de 2021, les actes d'exécution et la documentation technique étant achevés, les travaux sur le développement technique du SIS bien engagés et les premières mesures prises pour élaborer un manuel SIS et des activités de formation pour les utilisateurs du SIS.

Le nouveau cadre d'**interopérabilité** entre les systèmes d'information de l'UE dans le domaine de la justice et des affaires intérieures[12] renforcera encore le potentiel du SIS dans la lutte contre la criminalité organisée. Il est essentiel de consentir tous les efforts nécessaires pour parvenir à une interopérabilité totale d'ici la fin de 2023. Cela facilitera l'accès des services répressifs aux informations pertinentes dans les systèmes d'information centralisés de l'UE et permettra la détection d'identités multiples, essentielles pour lutter contre la fraude à l'identité souvent utilisée par les criminels pour commettre des infractions ou échapper à la justice. Au titre du cadre d'interopérabilité, un élément «**détecteur d'identités multiples**» est en cours d'élaboration. En vérifiant les données dans ces systèmes, cette fonction contribuera à lutter efficacement contre l'utilisation frauduleuse des identités.

[11]Règlement (UE) 2018/1860 du Parlement européen et du Conseil du 28 novembre 2018 relatif à l'utilisation du système d'information Schengen aux fins du retour des ressortissants de pays tiers en séjour irrégulier (JO L 312 du 7.12.2018), règlement (UE) 2018/1861 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine des vérifications aux frontières, modifiant la convention d'application de l'accord de Schengen et modifiant et abrogeant le règlement (CE) n° 1987/2006 (JO L 312 du 7.12.2018), et le règlement (UE) n° 2018/1862 du Parlement européen et du Conseil du 28 novembre 2018 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, modifiant et abrogeant la décision 2007/533/JAI du Conseil, et abrogeant le règlement (CE) n° 1986/2006 du Parlement européen et du Conseil et la décision 2010/261/UE de la Commission (JO L 312 du 7.12.2018).

[12] Le cadre d'interopérabilité couvre le SIS, le système d'information sur les visas (VIS), Eurodac, le système d'entrée/de sortie (EES), le système européen d'information et d'autorisation concernant les voyages (ETIAS) et le système européen d'information sur les casiers judiciaires pour les ressortissants de pays tiers (ECRIS-TCN). Règlement (UE) 2019/817 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine des frontières et des visas et modifiant les règlements (CE) nº 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726 et (UE) 2018/1861 du Parlement européen et du Conseil et les décisions 2004/512/CE et 2008/633/JAI du Conseil (JO L 135 du 22.5.2019), et règlement (UE) 2019/818 du Parlement européen et du Conseil du 20 mai 2019 portant établissement d'un cadre pour l'interopérabilité des systèmes d'information de l'UE dans le domaine de la coopération policière et judiciaire, de l'asile et de l'immigration et modifiant les règlements (UE) 2018/1726, (UE) 2018/1862 et (UE) 2019/816 (JO L 135 du 22.5.2019).

Les enquêteurs travaillant de manière isolée dans un État membre ne sont souvent pas en mesure d'établir la participation d'un groupe criminel organisé à une infraction spécifique. Le cadre **Prüm**[13] de 2008 permet aux services répressifs, au cours de leurs enquêtes, de rechercher de l'ADN et des empreintes digitales dans les bases de données d'autres États membres par l'intermédiaire d'un système de concordance/non-concordance («hit-no-hit») grâce à des connexions bilatérales, et de rechercher des données relatives à l'immatriculation de véhicules. Si le cadre Prüm s'est avéré utile pour résoudre de nombreuses infractions en Europe, sa nature décentralisée a pour conséquence que de nombreuses connexions bilatérales entre les bases de données nationales des États membres n'ont pas été établies en raison de la complexité technique et des importantes ressources financières et humaines que cela suppose. Par ailleurs, des semaines voire des mois peuvent être nécessaires pour que les autorités partagent les données à caractère personnel relatives à une correspondance. Afin d'accroître l'efficacité des enquêtes pénales et de renforcer l'échange automatisé d'informations sur les criminels, la Commission proposera de moderniser le **cadre Prüm afin de répondre aux besoins opérationnels** des services répressifs, dans le respect des droits fondamentaux et des exigences de nécessité et de proportionnalité, et d'aligner les dispositions relatives à la protection des données sur la directive en matière de protection des données dans le domaine répressif[14]. La Commission étudie actuellement les options permettant d'assurer la connexion des bases de données pertinentes entre tous les États membres et d'**accélérer l'échange d'informations** à la suite d'une correspondance. Elle évalue également la nécessité d'échanger des **catégories de données supplémentaires** importantes dans le cadre des enquêtes pénales, telles que les images faciales, les permis de conduire, les casiers judiciaires et la balistique, au titre du cadre Prüm, et d'inclure à ce cadre Europol en tant que nouveau partenaire.

Compte tenu de la dimension transfrontière et internationale de la criminalité organisée, les **informations concernant les voyages** sont essentielles pour identifier les voyageurs à haut risque qui ne sont au demeurant pas connus des services répressifs et pour établir des liens entre les membres de groupes criminels. Le traitement des **données des dossiers passagers (PNR)** aide les autorités compétentes à identifier les personnes impliquées dans des activités criminelles commises par des groupes organisés. Pour faire en sorte que cet outil soit pleinement exploité, la Commission continuera à suivre la mise en œuvre pleine et effective de la directive relative aux données des dossiers passagers[15] et soutiendra la coopération et l'échange de ces données entre les États membres, notamment en partageant les bonnes

[13] Décision 2008/615/JAI du Conseil relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière et décision 2008/616/JAI du Conseil concernant la mise en œuvre de la décision 2008/615/JAI (JO L 210 du 6.8.2008).

[14] Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016).

[15] Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière (JO L 119 du 4.5.2016).

pratiques, en organisant des formations et en développant les capacités nécessaires[16]. Les **informations préalables sur les passagers (données API)**, soit les données biographiques des passagers collectées par les transporteurs aériens lors de l'enregistrement, sont tout aussi précieuses[17], notamment en raison de leur complémentarité avec les données des dossiers passagers. Une révision du cadre juridique actuel[18] permettrait une série d'améliorations, notamment en ce qui concerne l'exactitude et l'exhaustivité des données. Plus important encore, la Commission analysera l'utilisation qui pourrait être faite des données API pour interroger systématiquement les données Europol aux fins de la lutte contre la criminalité organisée et, éventuellement, étendre leur utilisation aux mouvements intra-Schengen et aux transporteurs par voie d'eau et aux autocars. Dans cette optique, la Commission présentera une proposition de révision de la directive relative aux informations préalables sur les passagers au cours du premier semestre de 2022, sur la base d'une analyse d'impact dans laquelle les options susmentionnées et ses incidences seront analysées plus en détail.

1.2.Cadres de coopération avancée

Les principaux volets de la coopération en matière répressive dans l'ensemble de l'UE sont fondés sur la convention d'application de l'accord de Schengen de 1990. Ce socle est complété par d'autres instruments de l'Union, tels que la décision-cadre 2006/960/JAI du Conseil relative à la simplification de l'échange d'informations et de renseignements entre les services répressifs des États membres de l'Union européenne, ou par les chapitres 4 et 5 de la décision 2008/615/JAI du Conseil du 23 juin 2008 relative à l'approfondissement de la coopération transfrontalière, notamment en vue de lutter contre le terrorisme et la criminalité transfrontalière (Prüm).

Les États membres ont complété ce cadre par un ensemble complexe d'accords bilatéraux et multilatéraux. En conséquence, le niveau de coopération entre les États membres est inégal, ce qui crée des obstacles opérationnels empêchant une coopération transfrontière efficace.

La Commission élaborera une proposition législative relative à **un code de coopération policière européen**. Cette proposition s'appuiera sur les résultats d'une étude externe en cours et sera fondée sur un processus de consultation exhaustif, compte tenu de la compétence des États membres. L'objectif est de rationaliser et de développer les différents instruments de coopération en matière répressive, y compris la législation pertinente de l'UE, les lignes

[16] Telles que celles mentionnées dans le document de travail des services de la Commission accompagnant le rapport de la Commission sur le réexamen de la directive relative aux PNR, SWD(2020) 128 final, 24.7.2020, p 7 et 8.

[17] Des appels répétés en faveur d'une utilisation accrue des informations préalables sur les passagers fournies par les Nations unies [voir UNSCR 2178(2014), UNSCR 2309(2016), UNSCR 2482 (2019)], ainsi que l'engagement pris par les États participants de l'Organisation pour la sécurité et la coopération en Europe en faveur de la mise en place de systèmes d'informations préalables sur les passagers, confirment l'importance de ces données. En outre, depuis février 2018, la mise en place de systèmes nationaux d'informations préalables constitue une norme de l'Organisation de l'aviation civile internationale, qui la rend obligatoire pour tous les États parties à la convention de Chicago.

[18] Directive 2004/82/CE du Conseil concernant l'obligation pour les transporteurs de communiquer les données relatives aux passagers (JO L 261 du 6.8.2004) («directive relative aux informations préalables sur les passagers»).

directrices du Conseil et les bonnes pratiques des États membres découlant d'accords bilatéraux et multilatéraux, en un corpus réglementaire cohérent et moderne couvrant également les outils d'enquête.

En outre, afin de lever les obstacles potentiels à la coopération transfrontière spécifiquement en matière de lutte contre les structures de la criminalité organisée, la Commission a lancé une étude externe destinée à évaluer si la **décision-cadre du Conseil de 2008 relative à la lutte contre la criminalité organisée**[19] était toujours adaptée à son objectif.

Europol joue un rôle important en tant que **plaque tournante de l'information criminelle de l'UE**, qui soutient la coopération policière et l'échange d'informations et produit tous les quatre ans le rapport d'**évaluation de la menace que représente la grande criminalité organisée dans l'Union européenne** (SOCTA UE)[20]. Afin de répondre à des besoins opérationnels urgents, tels que la coopération avec des parties privées ou le traitement de grands ensembles de données, la Commission a proposé, en décembre 2020, de renforcer le mandat d'Europol[21]. Les nouvelles compétences et les nouveaux outils prévus dans la proposition permettront à Europol de renforcer son soutien en faveur de la lutte contre la criminalité organisée. Le Parlement européen et le Conseil travaillent sur leurs mandats en vue des négociations interinstitutionnelles à venir, qui devraient débuter plus tard cette année. La Commission facilitera les négociations et souhaite parvenir à un accord rapide des colégislateurs d'ici la fin de 2021.

La **plateforme pluridisciplinaire européenne contre les menaces criminelles (EMPACT)** est l'un des outils essentiels pour mettre en œuvre la présente stratégie et intensifier les efforts déployés dans la lutte contre les structures de la criminalité organisée au moyen d'opérations coordonnées. Depuis 2010, EMPACT permet aux États membres de déterminer les menaces criminelles prioritaires de l'UE pour lesquelles une action collective est nécessaire[22] et de lutter contre ces menaces au moyen d'une coopération structurée au niveau de l'UE entre les

[19]Décision-cadre 2008/841/JAI du Conseil du 24 octobre 2008 relative à la lutte contre la criminalité organisée (JO L 300 du 11.11.2008).

[20] Le rapport SOCTA UE est publié tous les quatre ans par Europol, sur la base d'informations détaillées fournies par les États membres et d'autres parties prenantes concernées. Il recense les principales menaces criminelles dans l'UE et propose des priorités pour l'UE en matière de criminalité pour les quatre prochaines années. Le rapport SOCTA UE est la première étape de chaque cycle EMPACT et sert de base à l'adoption par le Conseil des priorités de l'UE en matière de criminalité, sur lesquelles il se concentrera au cours des quatre prochaines années.

[21] Proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2016/794 en ce qui concerne la coopération d'Europol avec les parties privées, le traitement de données à caractère personnel par Europol à l'appui d'enquêtes pénales et le rôle d'Europol en matière de recherche et d'innovation, COM(2020) 796 final, et proposition de règlement du Parlement européen et du Conseil modifiant le règlement (UE) 2018/1862 sur l'établissement, le fonctionnement et l'utilisation du système d'information Schengen (SIS) dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale en ce qui concerne l'introduction de signalements par Europol, COM(2020) 791 final, 9 décembre 2020.

[22]Pour la période 2018-2021: la cybercriminalité, le trafic de drogue, l'aide à l'immigration clandestine, la criminalité organisée contre les biens, la traite des êtres humains (pour toutes les formes d'exploitation, y compris l'exploitation sexuelle et par le travail, ainsi que toutes les formes de traite des enfants), la fraude aux droits d'accises et la fraude intracommunautaire à l'opérateur défaillant, le trafic illicite d'armes à feu, la criminalité environnementale, les fonds d'origine criminelle et le blanchiment de capitaux ainsi que la fraude documentaire.

services répressifs, les douanes, les autorités fiscales, les magistrats, les institutions et agences européennes et, le cas échéant, les pays tiers, les organisations internationales et le secteur privé[23].

Dans le cadre d'EMPACT, les États membres et leurs partenaires mènent **chaque année plus de 200 actions opérationnelles conjointes** pour lutter contre la criminalité organisée, par exemple en dressant un tableau du renseignement criminel sur les priorités de l'UE en matière de criminalité, en renforçant les capacités répressives pour cibler des formes de criminalité spécifiques, en renforçant la coopération avec les partenaires internationaux, en menant des activités de prévention, en réalisant des enquêtes conjointes contre des phénomènes criminels spécifiques ou des groupes criminels spécifiques, et en abordant les méthodes utilisées par ces groupes pour blanchir des capitaux, commettre des infractions en ligne ou obtenir des documents frauduleux. Bien qu'EMPACT produise déjà des résultats opérationnels significatifs, par exemple en ce qui concerne les stupéfiants saisis ou les criminels arrêtés, elle n'est actuellement pas pleinement exploitée. Sa complexité, le manque de connaissance des agents de première ligne et son financement insuffisant ne garantissent pas toujours l'appropriation et la participation active des États membres et des partenaires extérieurs, et entravent le déroulement d'opérations plus complexes qui nuiraient davantage aux groupes criminels organisés.

En collaboration avec toutes les parties prenantes concernées d'EMPACT, la Commission travaillera à la mise en œuvre d'un certain nombre de mesures, décrites en détail dans le document de travail des services de la Commission accompagnant la présente stratégie, afin de tirer le meilleur parti du potentiel d'EMPACT et d'en faire un véritable **instrument phare de l'UE pour la coopération opérationnelle pluridisciplinaire et interservices** dans le cadre de la lutte contre la criminalité organisée au niveau de l'UE.

La Commission étudiera également la faisabilité d'inscrire EMPACT dans une législation spécifique de l'UE, ce qui ferait résolument de la plateforme un élément essentiel de l'UE permettant aux États membres et aux agences et organismes de l'UE de coopérer sur le plan opérationnel dans le cadre de la lutte contre la grande criminalité internationale organisée. EMPACT serait ainsi le vecteur permanent de la coopération structurelle entre les stratégies et les actions européennes et nationales en matière de criminalité, accompagné d'une méthode et d'une approche harmonisées, à titre de fondement juridique des partenariats conjoints ad hoc fondés sur les besoins opérationnels. La Commission s'efforcera également de renforcer sensiblement le financement d'EMPACT, afin de lui permettre de mettre au point des opérations plus complexes. La Commission étudiera également, en collaboration avec toutes les parties prenantes concernées, la possibilité de rationaliser EMPACT dans sa forme actuelle selon quatre piliers révisés et modernisés[24], complétés par des principes directeurs pour la

[23] Le «cycle politique de l'UE pour lutter contre la grande criminalité internationale organisée» est utilisé pour définir le cadre de coopération pour la définition de priorités communes, «EMPACT» étant la plateforme opérationnelle permettant la coopération entre les praticiens. «EMPACT» est devenu la seule dénomination pour désigner les deux concepts.

[24] Séquence de quatre piliers révisés: 1/ observer, détecter et orienter; 2/ décider et planifier ensemble; 3/ lutter, prévenir et désorganiser; 4/ apprendre et répéter.

lutte contre la criminalité organisée. En outre, elle s'efforcera de renforcer le rôle des réseaux et groupes d'experts européens dans l'appui aux actions relevant d'EMPACT. Enfin, la Commission, en collaboration avec le Service européen pour l'action extérieure (SEAE), encouragera également le renforcement de l'association de pays tiers aux activités d'EMPACT et encouragera le développement de la méthode d'EMPACT en dehors de l'UE, avec une adaptation aux besoins opérationnels.

Afin de traduire les criminels en justice, les services répressifs et les autorités judiciaires doivent travailler main dans la main: une réponse efficace à la criminalité organisée nécessite de nouvelles mesures afin de renforcer davantage la coopération judiciaire. Les recommandations du Parlement[25] et les conclusions du Conseil[26] préconisent une amélioration du fonctionnement pratique du **mandat d'arrêt européen**[27]. La Commission assure donc la bonne mise en œuvre, à la suite de son rapport sur la mise en œuvre du mandat d'arrêt européen[28], et fournira des orientations dans un manuel actualisé.

En outre, afin d'éviter des enquêtes parallèles sur les criminels opérant dans plusieurs États, des règles communes pourraient être nécessaires pour permettre aux États membres de transférer des procédures pénales vers un autre État membre, par exemple l'État membre dont le suspect a la nationalité, compte tenu de la décision-cadre relative à la prévention des conflits en matière de compétence[29]. La Commission étudie actuellement cette question de manière plus approfondie afin d'apprécier la nécessité d'une action de l'UE dans ce domaine. Elle examine également les problèmes qui se posent en matière de collecte, de transfert et d'utilisation des éléments de preuve dans le cadre des procédures transfrontières, ainsi que les pistes possibles[30].

La communication et le partage d'informations au sein des équipes communes d'enquête sont essentiels et la Commission travaillera donc à l'élaboration d'une plateforme de collaboration pour ces équipes communes d'enquête et à l'intensification de la coopération entre Eurojust et les pays tiers. En outre, comme annoncé dans la communication sur la numérisation de la justice au sein de l'UE[31], la Commission présentera, d'ici la fin de 2021, une proposition visant à assurer la sécurité des communications électroniques et des échanges d'informations et de documents entre les juridictions, les autorités nationales et, le cas échéant, les agences et organes relevant du domaine de la justice et des affaires intérieures. La Commission soutiendra également la modernisation du système de gestion des dossiers d'Eurojust afin

[25] https://www.europarl.europa.eu/doceo/document/TA-9-2021-0006_FR.html
[26] https://data.consilium.europa.eu/doc/document/ST-13214-2020-INIT/fr/pdf
[27] Cf. le manuel concernant l'émission et l'exécution d'un mandat d'arrêt européen (JO C 335 du 6.10.2017): https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52017XC1006(02)&from=DA.
[28] Rapport du 2 juillet 2020 de la Commission au Parlement européen et au Conseil sur la mise en œuvre de la décision-cadre du Conseil du 13 juin 2002 relative au mandat d'arrêt européen et aux procédures de remise entre États membres [COM(2020) 270 final du 2.7.2020].
[29] Décision-cadre 2009/948/JAI du Conseil du 30 novembre 2009 relative à la prévention et au règlement des conflits en matière d'exercice de la compétence dans le cadre des procédures pénales (JO L 328 du 15.12.2009).
[30] Une étude intitulée «Cross-border use of evidence» (Utilisation transfrontière des preuves) a été lancée en mars 2020.
[31] Communication de la Commission intitulée «Numérisation de la justice au sein de l'Union européenne - Une panoplie de possibilités» [COM(2020) 710 final du 2.12.2020].

d'aider Eurojust à fournir un retour d'information aux autorités nationales et à développer les liens judiciaires entre les enquêtes en cours. Cela devrait permettre à Eurojust de travailler efficacement avec ses partenaires, en particulier Europol et le Parquet européen, en contribuant à coordonner les enquêtes au niveau national et à éviter les enquêtes parallèles dans le but d'assurer l'efficacité des poursuites.

1.3. Coopération internationale

La coopération en matière répressive au-delà de l'Union est nécessaire pour désorganiser les réseaux criminels mondiaux et les itinéraires de transport. Il est indispensable de renforcer la coopération internationale notamment au moyen des activités des agences pertinentes du domaine de la justice et des affaires intérieures, en particulier en ce qui concerne les pays du voisinage et de l'élargissement.

Il est urgent de développer davantage le renseignement sur la grande criminalité organisée au sein d'Europol et de renforcer l'échange d'informations et les actions d'enquête avec les pays et régions tiers constituant des plaques tournantes majeures de la criminalité organisée à haut risque portant atteinte aux États membres de l'UE, y compris par l'intermédiaire des officiers de liaison bilatéraux des États membres détachés dans ces domaines critiques. La Commission a reçu des directives pour la négociation d'accords internationaux avec des pays tiers en vue d'échanger des données à caractère personnel avec Europol[32] et de permettre la coopération judiciaire avec Eurojust[33], et elle s'efforcera de progresser dans ces négociations difficiles.

En outre, les programmes et projets de coopération internationale de l'UE sont pertinents pour mettre en place des réseaux transcontinentaux de répression et de justice pénale. Le soutien de la Commission en faveur de ces réseaux et d'opérations conjointes continuera de s'intensifier.

L'approche de l'UE en matière de sécurité extérieure dans le cadre de la politique étrangère et de sécurité commune et de la politique de sécurité et de défense commune reste une composante essentielle des efforts de l'UE visant à lutter contre la criminalité organisée afin de renforcer la stabilité et de protéger les intérêts européens en matière de sécurité. Avec l'appui du SEAE, le haut-représentant/vice-président continuera à jouer un rôle clé dans le renforcement de la coopération stratégique et opérationnelle avec les pays tiers et les organisations internationales, en utilisant sans réserve les instruments externes dont il dispose, tels que les dialogues de haut niveau, le réseau d'experts en matière de lutte contre le terrorisme/sécurité au sein des délégations de l'UE et, le cas échéant, les missions et opérations menées dans le cadre de la politique de sécurité et de défense commune. En outre, la Commission et le SEAE continueront de donner la priorité aux projets de renforcement des capacités dans les pays tiers, et en particulier dans les pays du voisinage et de l'élargissement, tant pour soutenir la coopération opérationnelle avec les États membres et les agences de l'UE que pour doter les partenaires des outils leur permettant d'éradiquer des structures criminelles complexes susceptibles de nuire à l'UE.

[32] L'Algérie, l'Égypte, Israël, la Jordanie, le Liban, le Maroc, la Tunisie, la Turquie et la Nouvelle-Zélande.
[33] L'Algérie, l'Argentine, l'Arménie, la Bosnie-Herzégovine, le Brésil, la Colombie, l'Égypte, Israël, la Jordanie, le Liban, le Maroc, la Tunisie et la Turquie.

Interpol est un autre acteur clé en matière de coopération internationale contre la criminalité organisée. Ses 18 bases de données contiennent plus de 100 millions de documents en matière répressive, notamment sur des criminels recherchés, des terroristes présumés, des empreintes digitales, des véhicules volés, des documents de voyage volés et perdus, des armes et des armes à feu. Ces bases de données permettent aux services répressifs et aux autorités judiciaires de détecter les liens et, ainsi, de faciliter les enquêtes relatives à la criminalité transnationale organisée. La Commission est en train d'adopter, parallèlement à la présente stratégie, **une recommandation au Conseil visant à ouvrir des négociations avec Interpol** sur un accord de coopération UE-Interpol afin d'améliorer la coopération et de répondre aux besoins opérationnels.

Le principal instrument international permettant la coopération et l'entraide judiciaire dans le cadre des enquêtes sur la criminalité organisée est la **convention des Nations unies contre la criminalité transnationale organisée** (convention CTO), à laquelle l'UE et ses États membres sont parties. En 2021, la Commission actualisera la déclaration de compétence afin de l'aligner sur les modifications apportées au traité de Lisbonne[34] et de faire en sorte que le **Parquet européen** puisse s'appuyer sur les dispositions de la convention CTO en matière d'entraide judiciaire internationale pour coopérer avec des autorités de pays tiers. En outre, la Commission étudiera la possibilité de notifier le Parquet européen en tant qu'autorité responsable dans le cadre des accords de coopération existant au niveau de l'Union avec des pays tiers et, s'il y a lieu, envisagera l'ouverture de négociations avec certains pays tiers prioritaires. Comme indiqué dans la déclaration de Kyoto adoptée lors du 14e Congrès des Nations unies pour la prévention du crime et la justice pénale, l'Union et les États membres sont pleinement déterminés à renforcer le cadre international en faveur de l'état de droit, de la prévention du crime et de la justice pénale, notamment par une participation active aux processus d'examen en cours de l'application de la convention CTO et de la convention des Nations unies contre la corruption (CNUCC).

Actions clés:

La Commission:

- proposera de renforcer le **cadre Prüm** (4e trimestre 2021);
- proposera la création d'un **code de coopération policière** européen (4e trimestre 2021);
- proposera de réviser la directive relative aux **informations préalables sur les passagers** (1er trimestre 2022);
- mettra en place une **plateforme de collaboration** pour les équipes communes

[34] L'entrée en vigueur du traité de Lisbonne, le 1er décembre 2009, et la fin de la période de transition pour les instruments relevant de l'ancien troisième pilier, le 1er décembre 2014, ont modifié les limites des compétences de l'UE pertinentes pour la mise en œuvre de cette convention. L'UE a acquis de nouvelles compétences en vertu du titre V du TFUE (articles 82 et 83) et a exercé sa compétence en légiférant dans des domaines d'action pertinents. Par la suite, le processus d'examen de la convention des Nations unies contre la criminalité transnationale organisée devrait être fondé sur une déclaration de compétence actualisée.

d'enquête (4e trimestre 2021);

- travaillera avec toutes les parties prenantes en vue **de rationaliser, d'étendre et de moderniser** la plateforme pluridisciplinaire européenne contre les menaces criminelles (**EMPACT**) et d'en faire **l'instrument phare de l'UE dans la lutte contre la grande criminalité internationale organisée** au moyen d'une série d'actions et d'une proposition législative (2023);
- **renforcera sensiblement le financement** d'EMPACT par l'intermédiaire du Fonds pour la sécurité intérieure pour la période 2021-2027;
- entamera des négociations en vue de la conclusion d'accords de **coopération** entre **Eurojust** et les pays tiers;
- poursuivra les négociations sur la coopération entre **Europol** et les pays tiers;
- renforcera, conjointement avec le SEAE, la **coopération internationale** avec les pays tiers et les organisations internationales.

Le Parlement européen et le Conseil sont invités:

- à avancer dans les négociations législatives sur la **révision du règlement Europol**, y compris en ce qui concerne les modifications du règlement relatif au système d'information Schengen, en vue de parvenir à un **accord rapide**.

Le Conseil est invité:

- à adopter la recommandation d'ouvrir les négociations avec **Interpol** concernant un accord de coopération UE-Interpol.

2. Efficacité des enquêtes: désorganiser les structures de la criminalité organisée et lutter contre les formes de criminalité hautement prioritaires

2.1. Intensifier les efforts visant à lutter contre les structures de la criminalité organisée

Les enquêtes menées par les services répressifs ne devraient pas se limiter à la saisie d'objets illégaux ou à l'arrestation de petits criminels, mais viser des acteurs et des réseaux qui constituent l'épine dorsale des écosystèmes criminels.

La plupart des organisations criminelles étant structurées autour d'un noyau dur ou de manière hiérarchique[35], le paysage de la criminalité organisée se caractérise par un environnement en réseau dans lequel différents groupes et individus coopèrent systématiquement au moyen de «coentreprises» au sein de réseaux criminels informels et fluides. Les organisations criminelles qui orchestrent les chaînes d'approvisionnement sur les marchés criminels internationaux coopèrent avec des groupes plus petits spécialisés dans certaines activités et avec des individus occupant des rôles pivots fournissant des services à des criminels tels que la fraude documentaire, des conseils juridiques, des communications

[35] Selon le rapport SOCTA UE 2021, 43 % des groupes criminels organisés sont structurés autour d'un noyau dur, 40 % sont structurés de manière hiérarchique et 17 % sont des réseaux informels.

cryptées ou le transport. La capacité des groupes criminels à se connecter les uns aux autres sape les efforts des services répressifs, étant donné que chaque maillon de la chaîne criminelle peut facilement être remplacé en cas d'intervention des services répressifs.

Dans ce contexte, il est essentiel d'intensifier le **démantèlement des structures de la criminalité organisée**, en ciblant les groupes qui présentent un risque plus élevé pour la sécurité de l'Europe et les personnes aux échelons les plus élevés des organisations criminelles. À cette fin, certains États membres ont mis en place, à l'échelle nationale, des structures ou des organismes répressifs et judiciaires spécialisés pour lutter contre les organisations mafieuses. Ces expériences se sont avérées efficaces pour impulser une approche stratégique encourageant les efforts visant à désorganiser les infrastructures criminelles. En outre, la mise en place d'unités de police ou d'organes judiciaires spécialisés faciliterait une coopération transfrontière accrue. La Commission encouragera l'échange de bonnes pratiques afin de faciliter la reproduction de ces modèles dans tous les États membres, selon les spécificités nationales.

À l'échelle européenne, la coopération opérationnelle en matière de lutte contre les groupes criminels mafieux organisés menée par le truchement du **réseau @ON**[36] facilite le déploiement sur place d'enquêteurs spécialisés dans les États membres afin de contribuer aux enquêtes relatives aux groupes criminels organisés transfrontières. Une autre étape importante est le travail effectué par Europol en collaboration avec les États membres pour définir et mener des activités de renseignement et d'enquête au regard de certaines **cibles de grande importance**[37], à savoir des membres présumés d'organisations criminelles présentant un risque particulièrement élevé pour deux États membres ou plus.

Pour intensifier la lutte contre les organisations criminelles, il est plus que nécessaire de renforcer la coopération structurelle. L'élaboration de **critères communs** à tous les États membres afin de **déterminer les cibles de grande importance** et la facilitation de la coopération opérationnelle et de l'échange d'informations en temps réel permettraient de mener des enquêtes plus conjointes et plus systématiques sur les personnes jouant un rôle clé dans un réseau criminel. Le réseau @ON actuel devrait être renforcé par l'intégration de tous les États membres et l'élaboration de bonnes pratiques, ainsi que par un lien plus étroit avec EMPACT dans ses travaux de lutte contre les réseaux criminels.

Pour mettre davantage l'accent sur les enquêtes relatives à la criminalité organisée, il est également nécessaire de disposer d'**un tableau du renseignement** plus solide **des groupes criminels organisés** qui sont au cœur d'une toile complexe des réseaux criminels organisés. Europol et les États membres devraient poursuivre leurs travaux visant à élaborer des tableaux stratégiques et tactiques fondés sur le renseignement concernant les groupes qui représentent une menace accrue pour la sécurité de l'Europe, y compris par l'élaboration de rapports ad hoc qui complètent l'évaluation de la menace que représente la grande criminalité organisée

[36] Actuellement, 16 États membres participent au réseau @ON, qui existe depuis 2014.
[37] Depuis 2018, cette initiative a conduit à l'arrestation de 75 cibles de grande importance et de 2 529 de leurs associés, ainsi qu'à la saisie d'actifs d'une valeur de 310 millions d'euros.

dans l'Union européenne (SOCTA UE). L'échange d'informations stratégiques avec d'autres acteurs, y compris les missions et opérations relevant de la politique de sécurité et de défense commune, peut être bénéfique à cet égard. En outre, une meilleure vue d'ensemble de la dimension des activités criminelles et des mesures prises par les États membres est nécessaire. Compte tenu de l'opacité de la criminalité organisée, il est difficile de mesurer et de quantifier ces activités, et les données et statistiques dont dispose l'Union européenne sont fragmentées; elles sont collectées principalement au moyen d'obligations de déclaration répandues dans divers actes législatifs. Sur la base des résultats d'une étude approfondie déjà réalisée[38], la Commission évaluera la nécessité d'une collecte plus systématique de statistiques dans ce domaine.

2.2. Une réponse sur mesure aux formes spécifiques de criminalité

Selon le rapport SOCTA UE 2021, les groupes criminels organisés actifs en Europe participent à toute une série d'activités criminelles, la plupart d'entre eux étant impliqués dans le trafic de drogue et la criminalité organisée contre les biens, auxquels s'ajoutent la fraude (notamment douanière, aux droits d'accises et à la TVA), le trafic de migrants et la traite des êtres humains. Si certains groupes sont spécialisés dans un marché criminel particulier, d'autres sont de plus en plus **polycriminels** et utilisent les profits d'une activité criminelle pour financer leur expansion dans d'autres domaines criminels. Les formes spécifiques de criminalité nécessitent une réponse spécifique d'un point de vue législatif et politique.

L'UE a établi des règles relatives aux formes graves de criminalité telles que le trafic de migrants[39] et visant à détecter et interdire les nouvelles substances psychoactives[40], à contrôler la possession et le commerce d'armes à feu et à empêcher la réactivation d'armes neutralisées[41]. Le trafic de drogue demeure une source majeure de revenus pour les groupes criminels organisés et l'UE a défini les priorités pour les cinq prochaines années dans la **stratégie antidrogue de l'UE 2021-2025**, adoptée par le Conseil en décembre 2020[42]. Les discussions sur le **plan d'action antidrogue** s'y rapportant se poursuivent au Conseil, tandis que la Commission prépare les premières initiatives visant à mettre en œuvre la stratégie et le plan d'action[43].

[38] Étude intitulée «Availability, Comparability and Consistency of Administrative Statistical Data on Recorded Crime and on the Stages of the Criminal Justice Process in the EU» (Disponibilité, comparabilité et cohérence des données statistiques administratives relatives à la criminalité recensée et aux étapes des procédures pénales dans l'UE), mars 2021, DR0121067ENN, https://data.europa.eu/doi/10.2837/065004.

[39] Décision-cadre 2002/946/JAI du Conseil du 28 novembre 2002 visant à renforcer le cadre pénal pour la répression de l'aide à l'entrée, au transit et au séjour irréguliers (JO L 328 du 5.12.2002).

[40] Règlement (UE) 2017/2101 du Parlement européen et du Conseil du 15 novembre 2017 modifiant le règlement (CE) nº 1920/2006 en ce qui concerne l'échange d'informations, un système d'alerte rapide et une procédure d'évaluation des risques concernant les nouvelles substances psychoactives, (JO L 305 du 21.11.2017).

[41] https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/trafficking-in-firearms_en.

[42] Conclusions du Conseil sur la stratégie antidrogue de l'UE 2021-2025, 14178/20, 18 décembre 2020.

[43] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12854-Alternatives-to-coercive-sanctions-for-drug-using-offenders.

Les armes à feu sont un facteur essentiel de la montée de la violence par les groupes criminels. Elles leur permettent d'intimider leurs opposants et d'exercer un contrôle sur leurs membres et leurs marchés. Afin de limiter la disponibilité des armes à feu aux mains des criminels, la Commission a entamé la mise en œuvre du nouveau plan d'action de l'UE en matière de lutte **contre le trafic d'armes à feu** (2020-2025). Elle publiera le rapport sur l'application de la directive sur les armes à feu, en formulant des premiers outils en vue de l'amélioration du cadre juridique.

Le trafic de migrants demeure une activité essentielle pour les groupes criminels organisés qui mettent en danger les migrants et nuisent aux objectifs de l'UE en matière de gestion de la migration. En 2021, la Commission adoptera un **nouveau plan d'action contre le trafic de migrants** pour lutter contre les réseaux criminels impliqués dans cette forme de criminalité, soutenir la coopération entre services répressifs et entre agences et stimuler la coopération avec les pays tiers, ainsi qu'avec les missions et opérations menées dans le cadre de la politique de sécurité et de défense commune, lorsque cela s'avère nécessaire.

La **traite des êtres humains**, une forme particulièrement abjecte de criminalité, est souvent commise par des groupes criminels organisés, qui recrutent de plus en plus leurs victimes en ligne, créent des documents d'identité et des permis de travail et les exploitent à des fins sexuelles, de travail forcé, de criminalité forcée ou de mendicité. Bien que les priorités et les actions de la présente stratégie couvrent la traite des êtres humains, la Commission propose également, parallèlement au présent document, une stratégie spécifique de l'UE de lutte contre la traite des êtres humains pour la période 2021-2025 afin de tenir compte des spécificités de cette forme de criminalité.

La **cybercriminalité** devient plus agressive et plus hostile. La numérisation rapide de la société, qui a connu une accélération avec la pandémie de COVID-19, engendre de nouvelles vulnérabilités qui peuvent être exploitées par les criminels s'adonnant à la cybercriminalité. Les cyberattaques telles que la création et la diffusion de logiciels malveillants, le piratage destiné à voler des données personnelles ou industrielles sensibles, ou les attaques par déni de service ont augmenté au cours de l'année écoulée, tant en nombre qu'en degré de sophistication[44].

Le **Centre européen de lutte contre la cybercriminalité d'Europol (EC3)**, créé en 2013, a joué un rôle essentiel dans le suivi de l'utilisation de la pandémie de COVID-19 par la criminalité organisée, la création de matériel de sensibilisation et de rapports destinés à informer les États membres et le public, ainsi que le soutien aux enquêtes sur les escroqueries en ligne commises par des groupes criminels organisés. En outre, elle a publié ses rapports réguliers d'**évaluation de la menace que représente la criminalité organisée sur l'internet**

[44] Voir l'évaluation de la menace que représente la criminalité organisée sur l'internet (iOCTA) en 2020: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment, ainsi que les autres rapports d'Europol: https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know.

(iOCTA), qui constituent une source importante d'informations pour la définition des priorités dans les opérations et les politiques[45].

Conformément à la stratégie de l'UE de 2020 en faveur d'une lutte plus efficace contre les abus sexuels commis contre des enfants et à la stratégie globale de l'UE sur les droits de l'enfant (2021-2025), la Commission proposera, en 2021, une législation visant à améliorer la protection des enfants contre les **abus sexuels commis contre des enfants**, notamment en exigeant des prestataires de services en ligne concernés qu'ils détectent les contenus à caractère pédopornographique connus et qu'ils signalent ce matériel aux autorités publiques[46]. Cette législation assurera également la cohérence avec d'autres initiatives législatives, en particulier avec la proposition de législation sur les services numériques[47]. La Commission continue également d'appuyer le Parlement européen et le Conseil pour parvenir le plus rapidement possible à un accord sur la proposition de règlement concernant les efforts volontaires de certains prestataires de services dans la lutte contre les abus sexuels commis contre des enfants en ligne[48]. Parallèlement, Europol a soutenu le développement de sa campagne «Trace an Object», couronnée de succès, qui rassemble des informations sur des objets individuels sous forme d'images montrant des abus sexuels commis contre des enfants, ce qui peut aider à circonscrire la localisation géographique d'un abus et, ainsi, contribuer in fine à l'identification et au sauvetage des victimes.

La transition vers des économies sans espèces, accélérée par la pandémie, a donné des possibilités de fraude et de contrefaçon des **moyens de paiement autres que les espèces**, tels que les cartes de crédit et les outils de paiement en ligne[49], qui constituent une grave menace pour la sécurité de l'UE. Elles constituent une source importante de revenus pour la criminalité organisée et favorisent des activités criminelles telles que le trafic de drogue et la traite des êtres humains. En 2019, l'UE a adopté des règles plus strictes[50] que les États membres doivent mettre en œuvre au plus tard le 31 mai 2021. La Commission suivra de près les progrès accomplis afin de garantir la pleine efficacité des nouvelles règles.

La **fraude**, y compris la fraude douanière, la fraude aux droits d'accise et la fraude à la TVA, constitue un autre domaine de criminalité qui exerce un attrait croissant sur la criminalité organisée. Outre les efforts actuellement déployés par Europol et Eurojust dans ce domaine, le

[45] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment.
[46] Communication de la Commission sur une stratégie de l'UE en faveur d'une lutte plus efficace contre les abus sexuels commis contre des enfants [COM(2020) 607 final du 24.7.2020].
[47] Proposition de règlement du Parlement européen et du Conseil relatif à un marché intérieur des services numériques (Législation sur les services numériques) et modifiant la directive 2000/31/CE [COM(2020) 825 final du 15.12.2020].
[48] Proposition de règlement du Parlement européen et du Conseil concernant une dérogation temporaire à certaines dispositions de la directive 2002/58/CE du Parlement européen et du Conseil en ce qui concerne l'utilisation de technologies par des fournisseurs de services de communications interpersonnelles non fondés sur la numérotation pour le traitement de données à caractère personnel et d'autres données aux fins de la lutte contre les abus sexuels commis contre des enfants en ligne [COM(2020) 568 final du 10.9.2020].
[49] https://www.europol.europa.eu/newsroom/news/beyond-pandemic-what-will-criminal-landscape-look-after-covid-19.
[50] Directive (UE) 2019/713 du Parlement européen et du Conseil concernant la lutte contre la fraude et la contrefaçon des moyens de paiement autres que les espèces (JO L 123 du 10.5.2019).

Parquet européen enquêtera sur les infractions relatives à la participation à une organisation criminelle et poursuivra les auteurs de ces infractions, si les activités criminelles d'une telle organisation consistent essentiellement à commettre des infractions portant atteinte au budget de l'Union, y compris la fraude transfrontière grave à la TVA.

La **contrefaçon** de produits constitue une forme de criminalité à forte incidence. Les produits contrefaits représentent 6,8 % des importations de l'UE[51] et constituent une source de revenus importante pour les groupes criminels organisés. Les produits médicaux, de santé et sanitaires représentent une part considérable et croissante de la contrefaçon, un phénomène qui a gagné du terrain de manière alarmante avec la pandémie de COVID-19. La criminalité organisée s'est adonnée à la production et à la fourniture d'équipements de protection contrefaits, de kits de dépistage et de produits pharmaceutiques, et il existe un risque que des groupes criminels organisés tentent d'exploiter les possibilités que représente la forte demande de vaccins dans l'UE. Les services répressifs, conjointement avec Europol et l'OLAF, mènent avec succès d'importantes opérations conduisant à des arrestations et à des saisies importantes de produits contrefaits, y compris des produits médicaux, des jouets, des denrées alimentaires et des boissons[52]. Toutefois, des efforts supplémentaires doivent être réalisés pour renforcer la coopération opérationnelle en matière de lutte contre la contrefaçon. Les groupes criminels organisés interviennent de plus en plus dans les infractions telles que la contrefaçon de pesticides et l'utilisation frauduleuse du logo biologique de l'UE. Sur la base de ses contrôles officiels et du cadre d'application, la Commission continuera d'intensifier ses efforts pour lutter contre la fraude alimentaire et s'emploiera à doter les autorités nationales de moyens d'action, à instaurer une politique de tolérance zéro et à renforcer la prévention, les contrôles, la dissuasion et l'efficacité des sanctions.

À cette fin, en novembre 2020, la Commission a adopté le plan d'action en faveur de la propriété intellectuelle et établira en 2022 une **boîte à outils européenne de lutte contre la contrefaçon** définissant les principes d'action commune, de coopération et de partage de données entre les autorités répressives, les titulaires de droits et les intermédiaires[53]. Étant donné que la contrefaçon de produits médicaux a lieu principalement dans des pays tiers, il importe de renforcer la gouvernance mondiale, notamment par l'adhésion à la convention du Conseil de l'Europe sur la **contrefaçon des produits médicaux** («Convention Médicrime») et la ratification par les États membres de l'UE, et éventuellement par l'Union elle-même, de

[51] OCDE/EUIPO (2019), Trends in Trade in Counterfeit and Pirated Goods, Illicit Trade (Tendances dans le commerce des contrefaçons et des marchandises pirates – Commerce illicite), Éditions OCDE, Paris/Office de l'Union européenne pour la propriété intellectuelle. https://doi.org/10.1787/g2g9f533-en.

[52] Voir par exemple les opérations Pangea XIII (articles médicaux), LUDUS (jouets) et Opson IX (denrées alimentaires et boissons). Au cours de l'opération coordonnée d'Europol «Shield», conclue en septembre 2020, près de 33 millions de dispositifs médicaux contrefaits liés à la COVID-19 ont été saisis: il s'agissait notamment de 8 tonnes de matières premières, de masques, de tests et de kits de diagnostic.

[53] Communication de la Commission «Exploiter au mieux le potentiel d'innovation de l'Union européenne: Un plan d'action en faveur de la propriété intellectuelle afin de soutenir la relance et la résilience de l'Union européenne» [COM (2020) 760 final du 25.11.2020].

ladite convention, qui a été signée par quatorze États membres, dont seulement six l'ont ratifiée[54].

La **criminalité environnementale** mérite une attention particulière en raison de ses effets néfastes sur la biodiversité et sur l'environnement, ainsi que sur la santé et la cohésion sociale au sein de l'UE et dans les pays tiers. Toutes sortes d'espèces sauvages - plantes, animaux et produits dérivés - continuent d'être commercialisées illégalement, souvent à grande échelle, ce qui a des conséquences potentiellement dévastatrices. La gestion illégale des déchets et leurs transferts illicites compromettent l'activité des industries légitimes de traitement et de recyclage des déchets. L'UE a adopté une législation visant à réglementer le commerce légal d'espèces sauvages[55] et de déchets[56] et a demandé aux États membres d'ériger en infraction une vaste gamme d'actes portant atteinte à l'environnement et de sanctionner ceux-ci[57]. Ces instruments législatifs ont été complétés par le plan d'action de 2016 contre le trafic d'espèces sauvages et le plan d'action de 2018 sur le respect de la législation environnementale et la gouvernance environnementale. L'OLAF a développé significativement ses activités opérationnelles dans la lutte contre le commerce illicite de biens qui portent préjudice à l'environnement.

Malgré ces efforts, les services d'inspection, les services répressifs et les autorités judiciaires ne disposent souvent pas des capacités et des ressources nécessaires pour détecter efficacement la criminalité environnementale, enquêter sur ce type de criminalité et engager des poursuites en la matière. C'est particulièrement le cas dans les États membres qui ne sont pas dotés de services répressifs spécialisés ou d'organes chargés des poursuites et où il n'existe pas d'approche stratégique établie en matière de lutte contre la criminalité environnementale. Il est nécessaire de renforcer la capacité répressive à l'échelle nationale et de l'UE. Les sanctions infligées ne sont pas suffisamment dissuasives et la coordination et l'échange d'informations au sein des États membres et entre ceux-ci, en particulier entre les autorités administratives et les services répressifs, sont insuffisants[58]. La Commission examine actuellement le **règlement de l'UE sur les transferts de déchets** et le **plan d'action contre le trafic d'espèces sauvages**. La **directive sur la criminalité environnementale** sera révisée afin de clarifier le champ d'application des infractions liées à la criminalité

[54] Convention CET nº 211. La convention a été ratifiée par la Belgique, la Croatie, l'Espagne, la France, la Hongrie et le Portugal. Elle a été signée mais pas encore ratifiée par l'Autriche, Chypre, l'Allemagne, le Danemark, la Finlande, l'Italie, le Luxembourg et la Slovénie. Outre la Convention Médicrime, la directive 2011/62/UE du Parlement européen et du Conseil du 8 juin 2011 modifiant la directive 2001/83/CE instituant un code communautaire relatif aux médicaments à usage humain, en ce qui concerne la prévention de l'introduction dans la chaîne d'approvisionnement légale de médicaments falsifiés (JO L 174 du 1.7.2011), établit des règles et des mécanismes visant à renforcer les exigences de vérification qui sont applicables à cet effet au fabricant du médicament.

[55] https://ec.europa.eu/environment/cites/legislation_en.htm.

[56] Voir l'article 50 du règlement (CE) n° 1013/2006 du Parlement européen et du Conseil du 14 juin 2006 concernant les transferts de déchets (JO L 190 du 12.7.2006).

[57] Directive 2008/99/CE du Parlement européen et du Conseil du 19 novembre 2008 relative à la protection de l'environnement par le droit pénal (JO L 328 du 6.12.2008 - directive sur la criminalité environnementale).

[58] Évaluation de la directive 2008/99/CE du Parlement européen et du Conseil du 19 novembre 2008 relative à la protection de l'environnement par le droit pénal (directive sur la criminalité environnementale - SWD(2020) 259 final du 28.10.2020).

environnementale, d'apporter une plus grande précision en ce qui concerne les sanctions et de faciliter l'utilisation d'outils d'enquête efficaces. En outre, la coopération assurée par l'intermédiaire des réseaux européens de contrôle de l'application de la législation environnementale sera renforcée. Enfin, la dimension internationale du trafic d'espèces sauvages étant primordiale, la Commission encouragera l'adoption d'un protocole additionnel dans le cadre de la convention CTO.

Le trafic de **biens culturels** a une incidence dévastatrice sur le patrimoine culturel des pays, fournit des moyens de financement aux organisations criminelles et joue un rôle déterminant dans le blanchiment de capitaux. L'amélioration du suivi et de l'échange d'informations, le renforcement de la coopération entre les services répressifs et la coopération douanière, le renforcement de la coopération dans le domaine de la justice et des affaires intérieures ainsi que de la politique de sécurité et de défense commune sur le terrain et le recours à l'expertise des différents acteurs publics et privés sont nécessaires pour apporter une réponse efficace à cette forme de criminalité. La communication rapide avec des archéologues et des historiens de l'art peut apporter une contribution précieuse aux enquêtes relatives au trafic de biens culturels. Afin de lutter contre cette forme unique de criminalité, la Commission continuera de soutenir le renforcement des capacités des experts en matière de patrimoine culturel, ainsi qu'un réseau constitué de tels experts auquel les États membres pourront faire appel dans le cadre de EMPACT. Leur coopération structurée avec les services répressifs sera favorisée afin de faciliter les enquêtes ainsi que le financement de projets relatifs au trafic de biens culturels. En outre, la Commission examinera d'autres mesures nécessaires pour lutter contre ce phénomène, y compris par l'amélioration de la traçabilité en ligne et hors ligne des biens culturels sur le marché intérieur et la coopération avec les pays tiers où les biens culturels sont pillés. À cette fin, la Commission proposera en 2022 un plan d'action sur la lutte contre le commerce illicite de biens culturels.

Actions clés:

La Commission:

- proposera des modifications de la **directive sur la criminalité environnementale** (4e trimestre de 2021);
- renforcera les dispositions relatives à la lutte contre les transferts illicites de déchets dans le cadre de sa proposition de modification du **règlement sur les transferts de déchets** (2e trimestre de 2021);
- mettra en place une **boîte à outils européenne de lutte contre la contrefaçon** définissant les principes d'action commune, de coopération et de partage de données entre les **autorités répressives**, les titulaires de droits et les intermédiaires (2022);
- proposera un **plan d'action sur la lutte contre le commerce illicite de biens culturels** (2022);
- évaluera la possibilité pour l'Union d'accéder à la **Convention Médicrime** du Conseil de l'Europe.

Les États membres sont instamment invités:

- **à rejoindre et à renforcer le réseau @ON** sur les groupes criminels mafieux organisés et à envisager une intégration plus structurée d'une **approche ciblée contre les réseaux criminels dans EMPACT**;
- à mettre en place ou à développer davantage des structures de coordination au niveau national ou des **services répressifs spécialisés** et des autorités judiciaires axées sur la lutte contre la criminalité organisée;
- à adhérer à la **Convention Médicrime** du Conseil de l'Europe et à la ratifier;

Les États membres et Europol sont instamment invités:

- à élaborer des critères communs d'identification pour sélectionner et enquêter sur les **cibles de grande importance** et à donner la priorité aux enquêtes portant sur des individus et des réseaux criminels présentant le risque le plus élevé pour la sécurité dans l'UE;
- à dresser un **tableau stratégique et tactique du renseignement** sur les groupes criminels organisés à haut risque;
- à renforcer la **coopération** stratégique et opérationnelle dans la lutte contre la **contrefaçon des produits médicaux**, notamment avec l'OLAF et l'Office de l'Union européenne pour la propriété intellectuelle et à l'échelle mondiale.

3. Éliminer les profits générés par la criminalité organisée et prévenir l'infiltration de l'économie légale et de la société

3.1. Renforcer le recouvrement des avoirs et les mesures de lutte contre le blanchiment de capitaux en promouvant les enquêtes financières

La criminalité organisée dans l'UE repose fondamentalement sur la capacité de blanchir d'importants profits issus de la criminalité. Si trois quarts des groupes criminels utilisent toujours des méthodes élémentaires pour dissimuler leurs gains illicites, tels que l'investissement dans des biens immobiliers ou d'autres biens de grande valeur, d'autres recourent à des méthodes de plus en plus sophistiquées et bénéficient de l'aide de blanchisseurs en col blanc[59]. Les circuits financiers empruntés par les criminels constituent des indicateurs clés de leur activité et fournissent des indices utiles aux enquêteurs et des éléments de preuve inestimables pour incriminer les auteurs. Par conséquent, il est essentiel de lutter contre les fonds d'origine criminelle afin de mettre au jour les activités illicites, de décourager les pratiques criminelles et de prévenir l'infiltration de l'économie légale et de la société.

Malgré le développement des cadres juridiques de lutte contre le blanchiment de capitaux et le recouvrement des avoirs, seule une petite partie des activités de blanchiment de capitaux est

[59] Rapport Europol du 12 avril 2021 sur l'évaluation de la menace que représente la grande criminalité organisée dans l'Union européenne (SOCTA UE), https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment.

détectée, et seule une part de 1 % des avoirs d'origine criminelle est confisquée[60]. Cette situation a été aggravée par l'utilisation croissante de canaux financiers dont la surveillance est plus limitée que dans le secteur bancaire, comme les **monnaies virtuelles**.

Il convient de renforcer la lutte contre les fonds d'origine criminelle. Comme souligné dans le plan d'action contre le blanchiment de capitaux de 2020[61], le cadre de l'UE en matière de lutte contre le blanchiment de capitaux doit être nettement amélioré afin de remédier aux divergences majeures qu'on peut observer dans ses modalités d'application, mais aussi aux graves lacunes relevées dans l'exécution des règles. Les enquêtes financières ne sont pas pleinement exploitées, en partie en raison de la capacité insuffisante des services répressifs à mener à bien ces enquêtes complexes et fastidieuses.

Par ailleurs, la capacité à priver les criminels de leurs avoirs obtenus illégalement est encore davantage entravée par la portée restreinte du cadre juridique prévu en matière de confiscation pour ce qui concerne les avoirs et les agissements criminels couverts. En outre, les bureaux de recouvrement des avoirs sont actuellement confrontés à des difficultés lors du dépistage des avoirs car ils ne disposent pas, par exemple, de pouvoirs de gel temporaire qui leur permettraient d'écarter le risque de disparition des avoirs, ni d'un accès direct et immédiat à certains registres publics, tels que les registres fonciers centraux ou les registres centraux des entreprises[62]. À cela s'ajoute que les avoirs recouvrés ne sont pas toujours gérés de manière efficace et ne sont pas suffisamment utilisés pour indemniser les victimes ou au bénéfice de la société.

Comme annoncé dans le plan d'action contre le blanchiment de capitaux de 2020, veiller à la mise en œuvre effective du cadre existant en matière de lutte contre le blanchiment de capitaux est une priorité. Outre les efforts en cours pour assurer une mise en œuvre adéquate, la Commission prépare actuellement des propositions législatives visant à renforcer et à développer le **cadre de l'UE en matière de lutte contre le blanchiment de capitaux** et proposera, durant le deuxième trimestre de 2021, d'établir un corpus réglementaire unique directement applicable, de renforcer la surveillance au niveau de l'UE et de mettre en place un mécanisme de coordination et de soutien de l'UE pour les cellules de renseignement financier.

Il est également nécessaire de continuer à promouvoir une culture des **enquêtes financières précoces** dans tous les États membres et de renforcer la capacité des enquêteurs à prendre en compte la dimension financière de la criminalité organisée. Dans ses conclusions de 2020 sur le renforcement des enquêtes financières[63], le Conseil invite les États membres à veiller à ce que les enquêtes financières fassent partie des enquêtes pénales de tout type portant sur la

[60] Europol, Does crime still pay? Criminal Asset Recovery in the EU – Survey of statistical information 2010-2014, 2016, disponible à l'adresse suivante: https://www.europol.europa.eu/publications-documents/does-crimestill-pay.

[61] Communication de la Commission «Plan d'action pour une politique globale de l'Union en matière de prévention du blanchiment de capitaux et du financement du terrorisme» [C(2020) 2800 final du 7.5.2020].

[62] Conclusions du Conseil sur le renforcement des enquêtes financières en vue de lutter contre la grande criminalité organisée, document du Conseil nº 8927/20 du 17 juin 2020.

[63] Conclusions du Conseil sur le renforcement des enquêtes financières en vue de lutter contre la grande criminalité organisée, document du Conseil nº 8927/20 du 17 juin 2020.

criminalité organisée. En outre, grâce à la création du Centre européen de la criminalité financière et économique, Europol a renforcé ses capacités pour aider les États membres à mener des enquêtes financières.

Il est tout aussi essentiel d'intensifier les efforts en matière **de gel et de confiscation** en renforçant encore le cadre juridique au niveau de l'UE et en consolidant les capacités opérationnelles des **bureaux de recouvrement des avoirs**. Il convient d'envisager des mesures de confiscation en l'absence de condamnation car elles peuvent contribuer à augmenter le montant des avoirs confisqués lorsque, par exemple, il n'est pas possible de lier les avoirs obtenus à une condamnation pénale[64]. Afin de renforcer le régime de confiscation et de doter les bureaux nationaux de recouvrement des avoirs d'un mandat plus efficace, la Commission proposera en 2022 une révision de la **directive de 2014 relative à la confiscation** et de la décision du Conseil de 2007 relative aux **bureaux de recouvrement des avoirs**[65] dans le but d'élargir la liste des infractions pénales couvertes et d'introduire des règles plus efficaces en matière de confiscation en l'absence de condamnation; d'assurer une gestion efficace, une réutilisation sociale des avoirs confisqués et une indemnisation des victimes d'infraction, et de renforcer la capacité des bureaux de recouvrement des avoirs à dépister et à identifier les avoirs illicites[66].

En outre, la Commission examinera les options possibles en ce qui concerne le **lancement systématique d'enquêtes financières** et d'enquêtes financières postérieures à une condamnation. Un accès rapide aux informations financières est essentiel à la réalisation d'enquêtes financières efficaces et à la réussite du dépistage et de la confiscation des avoirs. La transposition en temps utile, par les États membres, de la **directive visant à faciliter l'accès aux informations financières,** qui donne aux services répressifs un accès aux registres centralisés des comptes bancaires et qui renforce la coopération entre les services répressifs et les cellules de renseignement financier, revêt donc une importance capitale. La Commission révisera également la directive ainsi que le cadre de lutte contre le blanchiment de capitaux afin de permettre aux autorités répressives d'accéder à la future plateforme qui assure l'interconnexion des comptes bancaires dans l'ensemble de l'Union.

Dans le même temps, il sera nécessaire de renforcer la coopération internationale en matière de répression contre le blanchiment de capitaux. Les États membres devraient exploiter pleinement les possibilités offertes par le **réseau opérationnel de lutte contre le blanchiment de capitaux (AMON)**, un réseau international informel de l'unité chargée de la lutte contre le blanchiment de capitaux, et par **CARIN (Camden Asset Recovery Inter-Agency Network)**, un réseau informel de praticiens de la justice spécialisés dans le dépistage, le gel, la saisie et la confiscation des avoirs. La Commission proposera également la

[64]Voir aussi l'analyse des mesures de confiscation prises en l'absence de condamnation dans l'Union européenne [SWD (2019) 1050 final du 12.4.2019].

[65] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12725-Freezing-and-confiscation-of-the-proceeds-of-crime.

[66] Rapport de la Commission au Parlement européen et au Conseil intitulé «Recouvrement et confiscation d'avoirs: Garantir que le crime ne paie pas» [COM(2020) 217 final du 2.6.2020].

ratification, au nom de l'UE, de la **convention de Varsovie** du Conseil de l'Europe relative au blanchiment, au gel et à la confiscation des capitaux.

3.2. Renforcement des mesures de lutte contre la corruption

La corruption est un élément central du mode opératoire des groupes criminels organisés. Ils soudoient et intimident les fonctionnaires et le personnel d'entités déterminantes comme les ports, et recourent à la force à leur encontre, pour ne pas se faire remarquer, obtenir des informations ou faciliter leurs activités. En vertu des règles actuelles de l'UE en matière de lutte contre la corruption, les États membres sont tenus d'ériger en infraction les actes de corruption active et passive dirigés contre les fonctionnaires, d'établir des sanctions adéquates et de veiller à ce que les entrepreneurs corrompus soient tenus pénalement responsables. Toutefois, ces instruments ne couvrent pas certaines infractions liées à la corruption, telles que le trafic d'influence, l'abus de pouvoir, l'enrichissement illicite, le détournement ou tout autre détournement de biens par un agent public. Plus récemment, l'Union a mis en place une nouvelle législation protégeant les lanceurs d'alerte et exigeant la création de canaux sûrs pour signaler les pratiques de corruption. Le rapport annuel sur l'état de droit examine également la situation des États membres du point de vue des politiques de lutte contre la corruption.

Afin de redoubler d'efforts au niveau de l'UE, la Commission **évaluera les règles existantes de l'UE en matière de lutte contre la corruption**[67], qui ont été adoptées il y a vingt ans, afin de déterminer si elles sont à jour avec l'évolution des pratiques criminelles et de veiller à ce qu'elles couvrent toutes les infractions pertinentes liées à la corruption.

Les différentes formes de corruption liées à la criminalité organisée dans un contexte transnational justifient également la nécessité d'améliorer le partage d'expertise, de bonnes pratiques, de données et d'informations entre les États membres et avec la société civile. Afin de soutenir efficacement les enquêtes pénales grâce à l'échange de données, il est essentiel de disposer d'une vue d'ensemble et d'une bonne compréhension des menaces et des risques causés par la corruption avant qu'ils ne se traduisent par des formes de criminalité liées à ce phénomène.

La pandémie de COVID-19 vient ajouter toute une série de risques sérieux de corruption: la mobilisation à grande échelle de ressources pour faire face à la crise sanitaire et économique a indirectement créé de nouvelles possibilités de corruption. Il est nécessaire de renforcer la capacité des autorités nationales à traiter les affaires de corruption très complexes liées à la criminalité organisée, notamment en mettant en place des structures spécialisées en matière de lutte contre la corruption. Il importe que les États membres utilisent davantage les fonds disponibles et les instruments de soutien technique fournis par la Commission afin de renforcer leur approche structurelle et stratégique, leurs outils réglementaires et opérationnels

[67] Décision-cadre 2003/568/JAI du Conseil du 22 juillet 2003 relative à la lutte contre la corruption dans le secteur privé et Convention de 1997 relative à la lutte contre la corruption impliquant des fonctionnaires des Communautés européennes ou des fonctionnaires des États membres de l'Union européenne (JO L 192 du 31.7.2003).

et leurs capacités dans le domaine de la lutte contre la corruption. En outre, compte tenu du rôle essentiel que jouent les médias dans la mise au jour des affaires de corruption, il est primordial de garantir la sécurité des journalistes d'investigation dans toute l'Union, notamment contre les recours abusifs. Comme annoncé dans le plan d'action pour la démocratie européenne, la Commission publiera en 2021 une recommandation sur la sécurité des journalistes et présentera une initiative visant à lutter contre les recours abusifs dirigés contre les journalistes et les défenseurs des droits.

L'UE est partie à la **Convention des Nations unies contre la corruption** depuis 2008 et l'application qu'elle fait de la convention fera l'objet d'un examen conformément aux dispositions prévues par cet instrument. L'UE et ses États membres œuvrent, dans le cadre du Groupe d'États contre la corruption du Conseil de l'Europe (GRECO) et du G20, à la réalisation de nouveaux progrès en matière de prévention et de lutte contre la corruption. La session extraordinaire de l'Assemblée générale des Nations unies, prévue pour juin 2021, sera une occasion majeure de faire progresser la lutte contre la corruption à l'échelle mondiale.

Les États membres sont également tenus d'ériger en infraction les actes de corruption commis par des citoyens et des entreprises de l'UE dans les pays en développement et de poursuivre leurs auteurs, conformément aux obligations découlant de la **Convention de l'OCDE sur la lutte contre la corruption d'agents publics étrangers dans les transactions commerciales internationales**. Le déroulement cohérent des poursuites et des procès dans les affaires d'actes de corruption commis à l'étranger jouera un rôle important dans la lutte contre la corruption au niveau mondial.

3.3. Lutter contre l'infiltration de l'économie et de la société

Les groupes criminels investissent une partie de leurs revenus considérables dans des entreprises légales qui sont actives dans des secteurs aussi variés que l'immobilier et la construction, le transport ou l'hôtellerie[68]. En contrôlant les entreprises de ces secteurs, les organisations criminelles sont en mesure de blanchir leurs avoirs illégaux et de maximiser leurs profits. L'infiltration de la criminalité organisée nuit à l'économie légale et fausse les règles du marché. En raison de la situation économique engendrée par la pandémie de COVID-19, il existe un risque accru que la criminalité organisée s'empare d'entreprises affaiblies et infiltre des secteurs d'activité entiers. Preuve a déjà été faite de tentatives criminelles de fraude visant les différents mécanismes financiers mis en place pour soutenir la reprise économique[69]. Afin de contrer cette menace et de déterminer les points clés nécessitant une intervention et une sensibilisation, les États membres et Europol doivent dresser un tableau du renseignement sur l'ampleur et le degré des investissements criminels, les méthodes d'infiltration et les secteurs à risque.

[68] Étude intitulée «Mapping the risk of serious and organised crime infiltration in legitimate businesses» (La cartographie des risques d'infiltration de la grande criminalité organisée dans les entreprises légitimes), mars 2021, DR0221244ENN, https://data.europa.eu/doi/10.2837/64101.

[69] Rapport Europol du 12 avril 2021 sur l'évaluation de la menace que représente la grande criminalité organisée dans l'Union européenne (SOCTA UE), https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment.

Des enseignements pourraient être tirés de l'échange de bonnes pratiques favorisé par l'intermédiaire du réseau européen sur l'**approche administrative**[70], méthode par laquelle les autorités locales, en collaboration avec les services répressifs et la société civile, utilisent des outils administratifs tels que les procédures d'obtention de permis, les appels d'offres et des subventions pour prévenir l'infiltration par la criminalité organisée des entreprises et des infrastructures administratives. Les autorités locales devraient être habilitées, dans le plein respect des droits fondamentaux, à créer des barrières assurant la protection du tissu économique contre la criminalité organisée.

La **dimension locale** joue également un rôle essentiel dans les efforts visant à réduire la marge de manœuvre dont disposent les groupes criminels pour renforcer leurs rangs. Les personnes élevées dans un environnement où règne la criminalité organisée et dans des régions défavorisées sur le plan socio-économique sont les plus susceptibles d'être recrutées à des fins criminelles. Elles commencent par s'adonner à de la petite criminalité ou par endosser des rôles mineurs au sein de l'organisation pour devenir les membres et les dirigeants des organisations criminelles de demain. Des actions ciblées menées dans certains quartiers et dans certaines communautés se sont avérées efficaces pour offrir des alternatives aux jeunes et les empêcher ainsi de s'engager dans une vie empreinte de violence et de criminalité. En outre, les activités de prévention de la criminalité telles que les patrouilles de la police de proximité ou les campagnes de sensibilisation dans les zones particulièrement touchées par les activités criminelles sont essentielles pour accroître la résilience de la société face aux agissements des groupes criminels organisés. La Commission renforcera l'échange de connaissances et de bonnes pratiques en matière de prévention de la criminalité par l'intermédiaire du **réseau européen de prévention de la criminalité**.

Actions clés:

La Commission:

- proposera de réviser la **directive relative à la confiscation** et la décision du Conseil relative aux **bureaux de recouvrement des avoirs** (2022);
- évaluera les **règles existantes de l'UE en matière de lutte contre la corruption** (2022);
- favorisera la **coopération** et l'échange d'informations sur le **lien entre la corruption et la criminalité organisée**, notamment grâce à Europol.

Les États membres sont instamment invités:

- **à conduire systématiquement des enquêtes financières** dans le cadre d'investigations sur la criminalité organisée et, dès que l'environnement financier

[70] L'approche administrative de la grande criminalité organisée est complémentaire des activités répressives traditionnelles. Elle offre des outils supplémentaires pour prévenir et combattre l'utilisation abusive de l'infrastructure juridique grâce à la coopération interservices en partageant des informations et en prenant des mesures afin de mettre en place des obstacles à l'infiltration.

indique la présence d'avoirs d'origine criminelle, à mener systématiquement des enquêtes en matière de recouvrement des avoirs;

- à transposer dans les meilleurs délais la **directive visant à faciliter l'accès aux informations financières** avant août 2021;
- **à échanger des informations stratégiques** avec les **secteurs qui présentent un risque** d'être infiltrés par des groupes criminels organisés (partenariats public-privé);
- à renforcer la **spécialisation** des services répressifs et à renforcer les organes chargés des enquêtes, des poursuites et des procédures judiciaires dans les affaires de **corruption** à haut niveau.

Les États membres et Europol sont instamment invités:

- à améliorer le **tableau du renseignement** sur la menace d'**infiltration** de l'économie légale, en évaluant les risques et les méthodes utilisées par les groupes criminels organisés.

4. Adapter les services répressifs et l'appareil judiciaire à l'ère numérique

4.1. Accès aux preuves et aux indices numériques

La recherche de preuves et d'indices, notamment l'accès aux données de communication, est la pierre angulaire des enquêtes et des poursuites en matière répressive et permet de traduire les criminels en justice. Étant donné que nos vies et nos activités se déroulent plus que jamais en ligne, les empreintes criminelles sont elles aussi numériques. Les membres de groupes criminels organisés planifient, exécutent et dissimulent leurs actes en ligne. Ils commercialisent des substances et des produits illégaux et trouvent des moyens ingénieux de blanchir leurs profits, sans être entravés par les frontières physiques. L'ampleur du problème est décuplée par l'évolution rapide des technologies. Le transfert de certaines preuves et de certains indices d'un espace physique vers un espace en ligne pose toute une série de défis, notamment la rapidité avec laquelle les données peuvent être transférées d'un pays à l'autre, ou la possibilité de se cacher derrière le cryptage. En outre, certains **instruments de collecte de preuves et mesures conçus pour les preuves physiques ne sont pas encore entièrement adaptés au monde numérique**[71]. Cet état de fait peut entraver ou ralentir les enquêtes et les poursuites pénales parce que les données ne sont pas disponibles ou ne sont pas accessibles en temps utile.

Les enquêtes portant sur la criminalité organisée nécessitent généralement l'accès aux données de communications électroniques pour établir un lien entre l'infraction, l'auteur et ses victimes, ainsi que pour repérer les réseaux criminels. Compte tenu de l'ampleur et de la structure d'un réseau de criminalité organisée, il est difficile pour les services répressifs de détecter ces communications sans accès rétroactif aux métadonnées de communication. En l'absence de telles données, la tâche consistant à identifier les acteurs centraux qui tirent les

[71] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en#internaleurulesproposaloneevidence.

ficelles en coulisse est particulièrement ardue. L'identification et l'arrestation ne touchent donc souvent que les membres les moins haut placés de ces réseaux, ceux qui se trouvaient sur le lieu de l'infraction, plutôt que les acteurs centraux[72]. En outre, les groupes criminels organisés utilisent les technologies modernes pour organiser la prochaine livraison de drogue, partager des cibles prometteuses pour un prochain cambriolage, convenir du point de rendez-vous pour un vol à main armée ou, dans le cas de groupes cybercriminels organisés, perpétrer des attaques bancaires à l'aide de logiciels malveillants.

Pour garantir l'accès aux preuves et aux indices d'enquête numériques, les États membres ont établi des **cadres de conservation des données**. Compte tenu du principe de confidentialité des communications électroniques, il se peut que les fournisseurs de services de communication aient effacé les métadonnées au moment où les services répressifs demandent l'accès à celles-ci. Dans de tels cas, des preuves importantes peuvent être perdues, à moins que les fournisseurs ne soient légalement tenus de stocker les métadonnées de communications pendant une durée raisonnablement plus longue conformément à un cadre législatif prévoyant la conservation des données. Par conséquent, des infractions pourraient ne pas faire l'objet d'une enquête fructueuse ou certaines victimes pourraient ne pas être identifiées. Les métadonnées de communication revêtent, par exemple, une importance particulière dans le cadre des enquêtes et des poursuites en matière de cybercriminalité, constituent souvent le principal moyen de détecter l'infraction et sont des éléments de preuve essentiels. Elles peuvent également représenter un moyen important de corroborer (ou de réfuter) d'autres types de preuves relatives aux faits d'une affaire. En outre, la complexité de la criminalité organisée, telle que le trafic illicite de stupéfiants, la traite des êtres humains ou le blanchiment de capitaux, et le temps nécessaire pour enquêter sur ce type de criminalité, de nouveaux suspects n'apparaissant qu'au cours de l'enquête, témoignent de l'importance que revêt la conservation des données.

Dans le même temps, les mesures de conservation des données soulèvent des questions importantes en ce qui concerne leur ingérence dans les droits fondamentaux, notamment le droit au respect de la vie privée et à la protection des données à caractère personnel. Dans ses récents arrêts relatifs à la conservation des données[73], la Cour de justice de l'Union européenne a confirmé sa jurisprudence antérieure selon laquelle les données de communications électroniques sont confidentielles et, en principe, les données relatives au trafic et à la localisation ne peuvent pas être conservées de manière générale et indifférenciée. La portée de ces mesures ne peut être justifiée du point de vue de l'ingérence dans les droits fondamentaux que si elles sont nécessaires et proportionnées par rapport à l'objectif poursuivi. La Cour a énoncé des exceptions circonscrites à cette règle en ce qui concerne la sécurité nationale, la défense publique et la sécurité ou la prévention de la criminalité, les

[72]https://www.bka.de/SharedDocs/Kurzmeldungen/DE/Kurzmeldungen/180611_MINDESTSPEICHERFRISTEN.html.

[73] Arrêts dans l'affaire C-623/17, *Privacy International*, dans les affaires jointes C-511/18, C-512/18 et C-520/18, *La Quadrature du Net e.a.*, du 6 octobre 2020 et dans l'affaire C-746/18 *H.K./Prokuratuur* du 2 mars 2021.

enquêtes, la détection et les poursuites pénales[74]. La Commission analysera et définira les approches et solutions envisageables, conformément aux arrêts de la Cour, qui répondent aux besoins des services répressifs et judiciaires d'une manière qui soit utile sur le plan opérationnel, techniquement possible et juridiquement solide, notamment en respectant pleinement les droits fondamentaux. Elle consultera les États membres avant la fin du mois de juin 2021 afin de définir la voie à suivre.

Une réponse répressive efficace requiert également un accès rapide aux preuves numériques lorsqu'elles sont détenues par des fournisseurs dans un autre État. En 2018, la Commission a proposé le **train de mesures sur les preuves électroniques** dans le but de faciliter l'accès aux preuves électroniques par-delà les frontières sur la base des injonctions européennes de production et de conservation. Le Parlement européen et le Conseil entament à présent des discussions interinstitutionnelles, avec l'appui de la Commission, afin de trouver le terrain d'entente nécessaire pour aboutir à l'adoption rapide de ces propositions. En outre, dans le cadre des efforts visant à accélérer la numérisation des services répressifs et judiciaires[75], tous les États membres devraient participer au système d'échange électronique de preuves numériques (eEDES). Dans le même temps, des progrès rapides sont nécessaires dans les négociations internationales multilatérales et bilatérales afin de faciliter la coopération avec les partenaires internationaux et d'établir des règles compatibles au niveau international pour l'accès transfrontière aux preuves électroniques[76].

Compte tenu des attaques de plus en plus massives qui sont menées, la collecte de preuves électroniques au stade le plus précoce possible et avant la réparation demeure essentielle à la réussite des enquêtes, ce qui facilite la dissuasion. À cette fin, les services répressifs et la communauté de la cybersécurité devraient coopérer étroitement afin de garantir une réponse collective et globale. En outre, les enquêtes nécessitent un accès rapide et fiable aux données WHOIS, notamment pour aider à identifier les groupes criminels organisés qui abusent régulièrement du système de noms de domaines (DNS) et d'autres protocoles internet dans le cadre de leurs cyberattaques ou d'autres infractions telles que des escroqueries ou la diffusion de produits et services illicites.

Le **cryptage** est essentiel pour le monde numérique, en ce qu'il permet de sécuriser les systèmes et les transactions numériques et de protéger une série de droits fondamentaux, notamment la liberté d'expression, la protection de la vie privée et la protection des

[74] La Cour a notamment autorisé la conservation généralisée et indifférenciée de l'identité civile des utilisateurs aux fins de la lutte contre toutes les infractions, ainsi que la conservation généralisée et indifférenciée des adresses IP attribuées à la source d'une connexion internet aux fins de la lutte contre les infractions graves. Le raisonnement de la Cour repose sur la charte des droits fondamentaux et sur l'analyse de la nécessité et de la proportionnalité de l'ingérence dans ces droits.

[75] Communication de la Commission sur la numérisation de la justice au sein de l'Union européenne: «Une panoplie de possibilités» [COM (2020) 710 final du 2.12.2020].

[76] En particulier, le deuxième protocole additionnel à la convention de Budapest sur la cybercriminalité du Conseil de l'Europe et un accord entre l'Union européenne et les États-Unis sur l'accès transfrontière aux preuves électroniques.

données[77]. Toutefois, si cette technologie est utilisée à des fins délictueuses, elle masque l'identité des criminels et dissimule le contenu de leurs communications. Dans son 11e rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective[78], la Commission a proposé un ensemble de six mesures concrètes visant à soutenir les services répressifs et le pouvoir judiciaire lorsqu'ils sont confrontés au chiffrement de données stockées sur des dispositifs (tels que des téléphones ou des disques durs) dans le cadre d'enquêtes pénales, sans interdire, limiter ni affaiblir le chiffrement. Dans le cadre de ces mesures, le nouveau dispositif de déchiffrement d'Europol, lancé par la Commission en décembre 2020, contribuera à relever ces défis. Des modules de formation ont été élaborés et des cours pilotes ont été dispensés par le groupe européen de formation et d'enseignement sur la cybercriminalité (ECTEG), financé par l'intermédiaire du volet «police» du Fonds pour la sécurité intérieure. Ces cours figureront dans l'offre de formation régulière de l'Agence de l'Union européenne pour la formation des services répressifs (CEPOL).

Au-delà des dispositifs classiques, le marché de niche des dispositifs de communication cryptés, qui sont largement acquis et utilisés par les groupes criminels organisés, est en plein essor. Comme le montrent les récentes opérations relatives à Encrochat et à Sky ECC, les autorités répressives de l'UE doivent constamment renforcer leur capacité à lutter contre le cryptage dans le contexte de certaines enquêtes pénales, conformément à la législation applicable.

En décembre 2020, le Conseil a adopté une résolution[79] plaidant en faveur d'une discussion active avec le secteur des technologies et de l'élaboration d'un cadre réglementaire approprié qui permettrait aux autorités compétentes de s'acquitter efficacement de leurs tâches opérationnelles tout en protégeant la vie privée, les droits fondamentaux et la sécurité des communications. En outre, le Conseil a demandé un renforcement de la coordination des efforts des États membres et des institutions et organes de l'Union européenne. Comme annoncé dans le Programme de lutte antiterroriste[80], la Commission s'emploie à trouver des solutions techniques, opérationnelles et juridiques pour garantir un accès légal aux informations cryptées, tout en maintenant l'efficacité du cryptage dans la protection de la vie privée et de la sécurité des communications.

En 2020, la Commission, en collaboration avec des experts du secteur, des spécialistes de la cryptographie, des membres d'organisations de la société civile et des autorités compétentes, a mené un processus d'expertise visant à recenser les solutions techniques susceptibles d'aider les entreprises à détecter spécifiquement les abus sexuels commis contre des enfants dans les communications électroniques cryptées de bout en bout. La Commission soutiendra la

[77] Communication de la Commission relative à la stratégie de l'UE pour l'union de la sécurité [COM(2020) 605 final du 24.7.2020]. Communication de la Commission relative au premier rapport sur l'état d'avancement de la stratégie de l'UE sur l'union de la sécurité [COM (2020) 797 final du 9.12.2020].

[78] Onzième rapport sur les progrès accomplis dans la mise en place d'une union de la sécurité réelle et effective [COM(2017) 608 final du 18.10.2017].

[79] Résolution du Conseil sur le chiffrement - La sécurité grâce au chiffrement et malgré le chiffrement, 13084/1/20 REV 1, 24.11.2020.

[80] Communication de la Commission intitulée «Programme de lutte antiterroriste pour l'UE: anticiper, prévenir, protéger et réagir [COM (2020) 795 final du 9.12.2020].

recherche afin de déterminer les solutions techniques les plus réalisables et susceptibles d'être renforcées et mises en œuvre de manière pratique par les entreprises.

Plus généralement, la Commission orientera le processus d'analyse, avec les parties prenantes concernées, les capacités et les approches existantes pour permettre un accès légal et ciblé aux informations cryptées dans le cadre d'enquêtes et de poursuites pénales. Ces approches ne devraient pas entraîner un affaiblissement général du chiffrement ou une surveillance aveugle. Non seulement cette analyse se concentrera sur la levée des obstacles actuels, mais elle anticipera également l'évolution probable des technologies de cryptage et la coopération nécessaire avec le monde universitaire et le secteur privé à cet effet. En outre, la Commission intensifie ses efforts dans le domaine de la normalisation afin de maintenir des capacités d'interception légales dans le contexte de la 5G et au-delà. À l'issue de ce processus, la Commission proposera, en 2022, une **voie à suivre** pour permettre un accès légal et ciblé aux informations cryptées dans le cadre d'enquêtes et de poursuites pénales, sur la base d'une cartographie détaillée de la manière dont les États membres traitent le cryptage, ainsi que d'un processus multipartite visant à explorer et à évaluer les options concrètes (juridiques, éthiques et techniques).

4.2. Outils et technologies efficaces

Souvent, les autorités répressives n'ont pas les moyens d'acquérir les bons outils nécessaires à la conduite d'enquêtes en ligne. Aujourd'hui, plus de 80 % des infractions ont une composante numérique; même lorsque des infractions sont commises hors ligne, chaque agent des services répressifs et chaque procureur, ou presque, doit connaître les notions de base relatives à la conduite d'enquêtes sur les infractions en ligne[81]. Pour détecter les actes de criminalité organisée et intenter des poursuites contre leurs auteurs, les enquêteurs doivent mettre au jour les activités en ligne suspectes, suivre les transactions criminelles en monnaies virtuelles, comprendre ce qu'ils ont trouvé (les données peuvent être cryptées ou doivent être mises en relation avec d'autres données), conserver les données et les utiliser comme preuves électroniques devant les tribunaux.

Il est urgent d'accroître les capacités et les compétences des services répressifs non spécialisés et des ministères publics[82]. En outre, l'expertise en matière d'enquêtes numériques dans des domaines spécifiques tels que la criminalistique de l'internet des objets[83] fait défaut. Les services répressifs et les autorités judiciaires doivent suivre le rythme de l'évolution rapide des technologies utilisées par les criminels et de leurs activités transfrontières. Cela requiert

[81] Document de travail des services de la Commission – Analyse d'impact accompagnant les documents: Proposition de règlement du Parlement européen et du Conseil relatif aux injonctions européennes de production et de conservation de preuves électroniques en matière pénale et Proposition de directive du Parlement européen et du Conseil établissant des règles harmonisées concernant la désignation de représentants légaux aux fins de la collecte de preuves en matière pénale [SWD(2018) 118 final].

[82] Voir la communication de la Commission intitulée «Assurer la justice dans l'UE - Une stratégie européenne de formation judiciaire pour la période 2021-2024» [COM (2020) 713 final du 2.12.2020], qui souligne la nécessité de permettre aux professionnels de relever de nouveaux défis.

[83] Analyse criminalistique des dispositifs connectés et des données relatives aux systèmes de l'internet des objets.

une coordination dans la mise au point d'outils et de formations, entre les États membres et entre les secteurs, dans des domaines tels que la cybercriminalistique, le renseignement de source ouverte, les cryptomonnaies et les enquêtes sur le «dark web», par exemple pour accéder aux forums de vente de biens et services illicites et, si possible, les fermer. En outre, les autorités nationales ne sont pas toujours en mesure de recourir aux solutions techniques «open source» en raison d'une méconnaissance des solutions qui ont été mises au point et qui sont disponibles, des différences qui existent en matière d'exigences et de niveaux d'expertise, et d'un manque de soutien en faveur de la poursuite du développement et de la maintenance. Dans le même temps, une absence de coordination entre les différentes autorités et les États membres risque d'entraîner un chevauchement des initiatives. Les mécanismes existants de l'UE (EMPACT, agences de l'UE telles qu'Europol, le CEPOL et Eurojust, réseaux de praticiens, programmes de financement tels que le Fonds pour la sécurité intérieure) peuvent jouer un rôle clé dans la promotion d'une approche plus efficace des enquêtes en ligne, grâce à des actions coordonnées et bien ciblées visant à renforcer les capacités et les compétences.

Les besoins des enquêteurs en ligne doivent être recensés de manière fiable. Europol, conformément à son mandat, et le pôle d'innovation de l'UE pour la sécurité[84] devraient coordonner une **analyse complète des lacunes et des besoins technologiques dans le domaine des enquêtes numériques**, ainsi que des analyses prospectives, qui sont essentielles pour orienter les programmes de recherche, d'innovation et de développement et les instruments d'action contribuant au renforcement des capacités. Il est important que les entités et réseaux concernés[85] soutiennent ces travaux. Sur cette base, Europol et le pôle d'innovation de l'UE pour la sécurité devraient définir des priorités en matière de recherche et de développement qui seront validées par les États membres[86]. Pour fournir une vision claire des mécanismes pratiques en place et des ressources disponibles pour soutenir les capacités des services répressifs dans le domaine des enquêtes numériques, et pour clarifier les rôles et responsabilités des entités concernées, la Commission consultera les États membres et d'autres parties prenantes d'ici la fin 2021 et effectuera un suivi si nécessaire.

La **recherche et l'innovation** sont nécessaires, tant pour les technologies d'enquête que pour la lutte contre la criminalité facilitée par la technologie. Le programme de recherche et d'innovation de l'UE, Horizon 2020, a financé l'élaboration de solutions technologiques innovantes dans le but de renforcer la capacité des autorités nationales à lutter contre la criminalité organisée. Ces travaux seront encore renforcés par le nouveau programme Horizon Europe, qui financera des projets de recherche visant à améliorer le tableau du renseignement sur la criminalité organisée, à élaborer des outils et des programmes de formation et à renforcer la coopération interservices.

[84] Le pôle d'innovation de l'UE pour la sécurité intérieure est un réseau collaboratif destiné à apporter un soutien aux laboratoires d'innovation des agences de l'UE, des États membres, du Centre commun de recherche de la Commission européenne et d'autres entités concernées dans la fourniture de produits innovants de pointe.
[85] ENFSI, ENLETS, i-LEAD, ILEAnet.
[86] Le comité de compensation d'Europol et l'EUCTF (Task Force «cybercriminalité» de l'Union européenne, le groupe rassemblant les responsables des unités de lutte contre la cybercriminalité au sein des services répressifs de l'UE) constitueraient les formats de consultation choisis pour des États membres.

La Commission facilitera l'**accès aux ensembles de données de haute qualité nécessaires pour mettre au point des outils d'enquête**, notamment l'intelligence artificielle, qui répondent aux besoins des services répressifs dans le cadre des enquêtes pénales, comme pour l'analyse de grandes quantités de données ou pour les enquêtes sur le «dark web». À cette fin, la Commission soutiendra, dans le cadre du programme DIGITAL, la création d'un espace européen des données de sécurité[87] qui sera essentiel au développement, à la formation et à l'évaluation des outils de répression, et qui contribuera à la stratégie européenne pour les données dans le plein respect des droits fondamentaux. En outre, la Commission soutiendra les États membres en ce qui concerne les projets pilotes sur les solutions d'intelligence artificielle[88] qui contribueraient à favoriser l'adoption de l'innovation par les services répressifs. Les services répressifs, les entreprises et les milieux universitaires devraient coopérer au sein d'un réseau soutenu par des fonds de l'UE dans le but de **mettre au point des outils et des solutions au niveau de l'UE qui répondent aux besoins des services répressifs de l'UE**[89], soutenant ainsi les travaux d'Europol dans la fourniture de services et de solutions techniques aux services répressifs de l'UE. Ce réseau devrait garantir la pérennité des projets au titre d'«Horizon Europe» et du Fonds pour la sécurité intérieure et appuyer Europol à cet égard.

Le réseau devrait fournir gratuitement ses résultats aux services répressifs par l'intermédiaire d'Europol et améliorer en permanence les solutions existantes. À cette fin, Europol devrait devenir le guichet unique pour l'accès aux outils et services, tels que l'analyse des logiciels malveillants, pour les autorités répressives nationales.

4.3. Améliorer l'accès aux compétences, aux connaissances et à l'expertise opérationnelle

Si la recherche et l'analyse des preuves numériques sont au cœur de la majorité des enquêtes, le niveau des compétences nécessaires dans le domaine de la procédure pénale, de la tactique et des techniques d'enquête numérique ou de cybercriminalistique n'est toujours pas disponible dans certains États membres et doit être élargi et approfondi dans la plupart des États membres. En outre, l'accès à une expertise opérationnelle de pointe dans des domaines

[87] Dans le programme de travail 2021-2022 de DIGITAL, une action est prévue pour définir le cadre d'une architecture des données fédérée pour l'innovation en matière de sécurité en finançant la création des composantes nationales d'un espace européen des données de sécurité pour l'innovation. Il serait ainsi possible de favoriser l'innovation et le développement en mettant en place un écosystème à l'échelle de l'UE pour le partage, le développement, les tests, la formation et la validation d'algorithmes pour les outils d'IA à des fins répressives et de sécurité, sur la base de différents types d'ensembles de données, y compris de pseudo-ensembles de données opérationnels et anonymisés, conformément à la stratégie européenne pour les données (Communication de la Commission - Une stratégie européenne pour les données [COM/2020/66 final du 19.2.2020]). Un appel à propositions sera lancé au premier trimestre de 2022 pour la participation d'au moins six services répressifs et de deux entreprises pour un montant compris entre 5 et 10 millions d'euros sous la forme d'une subvention nécessitant un cofinancement de 50 %.

[88] Conformément à l'initiative sur l'intelligence artificielle présentée par la Commission dans le livre blanc sur l'intelligence artificielle [COM(2020) 65 final du 19.2.2020].

[89] À cette fin, la Commission européenne finance par exemple l'Association européenne pour le développement de technologies de lutte contre la cybercriminalité (https://www.eactda.eu/) dans le cadre du programme de travail annuel 2020 du Fonds pour la sécurité intérieure (volet «police»).

spécifiques tels que la criminalistique de l'internet des objets reste un problème pour un certain nombre d'États membres.

Le développement de la formation devrait reposer sur une définition des compétences requises pour mener des enquêtes numériques et des profils professionnels associés (par exemple analyste de données, enquêteur en ligne ou expert en cybercriminalistique). À cette fin, Europol et le CEPOL devraient collaborer avec les États membres[90] pour définir et mettre à jour périodiquement un «**cadre des compétences en matière de formation**». Sur cette base, la Commission devrait soutenir l'élaboration de matériaux de formation, par l'intermédiaire du groupe européen de formation et d'enseignement sur la cybercriminalité (ECTEG), et soutenir la formation au niveau national au moyen des instruments disponibles[91].

Le CEPOL et le Réseau européen de formation judiciaire (REFJ) devraient évaluer régulièrement les besoins de formation et donner la priorité à la formation en conséquence, notamment en vue de développer davantage la compétence numérique générale des autorités répressives et judiciaires. Sur la base du cadre des compétences de formation, le CEPOL devrait également coopérer étroitement avec les praticiens[92] et les États membres afin de créer **des systèmes de certification/d'accréditation pour les experts en enquêtes numériques**. Ces programmes 1) augmenteraient le nombre d'experts capables de dispenser des formations dans des domaines spécifiques; 2) faciliteraient la coopération transfrontière, étant donné que la certification/l'accréditation fournirait des garanties quant à la collecte et au traitement des preuves, en garantissant leur recevabilité devant les juridictions également dans d'autres États; et 3) faciliterait l'identification des enquêteurs spécialisés.

Les enquêtes numériques peuvent nécessiter une expertise rare dans l'UE, par exemple en ce qui concerne les cryptomonnaies, les rançongiciels[93] ou les enquêtes sur le «dark web». Les États membres devraient recenser les experts qui ont développé des compétences de pointe dans ces domaines afin de se soutenir mutuellement dans les opérations où cette expertise est nécessaire. La Commission aidera Europol à mettre en place des mécanismes visant à faire en sorte que les autorités et les experts des États membres soient dûment incités à faire partie d'un groupe d'experts.

Actions clés:

La Commission:

- analysera et définira les approches et solutions possibles en matière de **conservation**

[90] Dans le cadre de la Task Force «cybercriminalité» de l'Union européenne (EUCTF), créée en 2010 et composée des chefs des unités nationales de lutte contre la cybercriminalité des différents États membres, ainsi que de représentants d'Europol, de la Commission européenne et d'Eurojust. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/euctf.

[91] Par exemple, par l'intermédiaire du Fonds pour la sécurité intérieure et de l'instrument d'appui technique.

[92] Le groupe européen de formation et d'enseignement sur la cybercriminalité (ECTEG) a déjà réalisé d'importants travaux sur ce sujet, dans le cadre de son projet mondial de certification de la cybercriminalité (https://www.ecteg.eu/running/gcc/).

[93] Europol a collaboré avec le secteur pour mettre en place le projet «No More Ransom» (https://www.nomoreransom.org/), qui fournit des conseils en matière de prévention et des outils de déchiffrement.

des données pour les services répressifs et judiciaires et consultera les États membres à ce sujet d'ici la fin du mois de juin 2021;

- proposera une voie à suivre pour permettre aux services répressifs d'accéder de manière licite et ciblée aux **informations cryptées** dans le cadre des enquêtes pénales. Cette approche devra reposer sur une cartographie détaillée de la manière dont les États membres traitent le chiffrement et sur un processus associant des parties prenantes multiples pour explorer et évaluer les options concrètes;
- encouragera et facilitera la **participation pleine et rapide des États membres au système d'échange électronique de preuves numériques** (e-EDES);
- mettra au point, par l'intermédiaire de son Centre commun de recherche, un outil de suivi permettant de recueillir des renseignements sur les activités illégales qui se développent sur le **«dark web»**;
- soutiendra l'**élaboration de modules et de matériels de formation** et appuiera la formation dispensée par le CEPOL et les établissements nationaux de formation.

Europol est invité:

- à coordonner une **analyse complète** des lacunes et des besoins technologiques dans le domaine des enquêtes numériques;
- à créer un **répertoire d'outils** permettant aux services répressifs de recenser les solutions les plus avancées et d'y accéder;
- à créer et à tenir à jour une base de données d'**experts en enquêtes et en criminalistique** dans des domaines spécialisés tels que l'internet des objets ou les cryptomonnaies.

Le CEPOL est invité:

- à créer des systèmes de **certification/d'accréditation** pour les experts en enquêtes numériques;
- à fournir et à mettre régulièrement à jour un **cadre de compétences de formation**, en collaboration avec Europol.

Le Parlement européen et le Conseil sont instamment invités:

- à adopter d'urgence les propositions relatives aux **preuves électroniques** afin de garantir aux autorités un accès rapide et fiable à ces preuves.

Conclusion

La présente stratégie définit les priorités, les actions et les objectifs à atteindre au cours des cinq prochaines années afin de renforcer la position de l'UE dans la lutte contre la criminalité organisée. Toutefois, ce phénomène criminel est en constante évolution et il est essentiel de

détecter les nouvelles tendances et de réagir rapidement aux nouvelles évolutions. L'Union et ses États membres doivent garder une longueur d'avance sur les organisations criminelles.

Il est donc temps d'intensifier l'action collective de l'Union à l'encontre de la criminalité organisée en renforçant les instruments existants pour soutenir la coopération transfrontière, y compris par l'intermédiaire d'agences chargées de la justice et des affaires intérieures, en luttant contre les crimes hautement prioritaires et en désorganisant les structures qui les sous-tendent, en réprimant le financement d'origine criminelle et ses méthodes corrompues visant à infiltrer l'économie et en s'attaquant à l'utilisation des nouvelles technologies par les criminels. Toute législation n'a de sens qu'à condition d'être mise en œuvre. Il est donc important que les États membres mettent pleinement et correctement en œuvre les instruments existants de l'UE. La Commission continuera à jouer son rôle; elle soutiendra les États membres, leur fournira en permanence des orientations et sera prête à prendre rapidement des mesures en cas de violation du droit de l'UE.

Les autorités présentes sur le terrain doivent être en mesure d'exploiter pleinement le potentiel des outils existants afin de désorganiser les activités criminelles et le modèle économique des organisations criminelles. Pour atteindre cet objectif, les mesures relevant de la présente stratégie doivent s'accompagner d'une nouvelle culture dans laquelle les services répressifs et les autorités judiciaires vérifient systématiquement les éventuels liens transfrontières et internationaux lors des enquêtes sur les affaires de criminalité organisée. L'échange d'agents des services répressifs, de procureurs et de juges, y compris avec des pays tiers, ainsi que de nouvelles possibilités de formation peuvent contribuer à y parvenir.

La Commission est résolue à contribuer à cette nouvelle dynamique de lutte contre la criminalité organisée et invite le Parlement européen et le Conseil à s'engager dans cet effort commun, qui est essentiel pour garantir la sécurité dans l'UE, protéger l'économie européenne et préserver l'état de droit et les droits fondamentaux.