COMMISSION
EUROPÉENNE

Bruxelles, le 24.6.2025
COM(2025) 349 final

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

Feuille de route pour un accès licite et effectif aux données à des fins répressives

Introduction

Comme indiqué dans la stratégie européenne de sécurité intérieure («ProtectEU»)[1], **la sécurité est le socle sur lequel se construisent toutes nos libertés**. La démocratie, l'état de droit, les droits fondamentaux, le bien-être des Européens, la compétitivité et la prospérité reposent tous sur notre capacité à garantir un niveau de sécurité élémentaire.

L'UE et les États membres ont le devoir de veiller à ce que les citoyens puissent jouir d'un **niveau élevé de sécurité dans leur vie quotidienne**. À cette fin, les services répressifs et les autorités judiciaires doivent disposer des outils nécessaires pour suivre les activités illicites, identifier les auteurs, démanteler les réseaux criminels et protéger les victimes, en garantissant en fin de compte la justice pénale, dans le plein respect des droits fondamentaux.

Le terrorisme, la criminalité organisée, la fraude en ligne, le trafic de drogues, les abus sexuels sur enfants, le chantage sexuel en ligne, les rançongiciels et de nombreuses autres formes de criminalité ont tous un point commun: ils laissent des **traces numériques**. Comme le relève Europol dans son évaluation de la menace que représente la grande criminalité organisée (SOCTA) pour 2025, presque toutes les formes de grande criminalité organisée ont une empreinte numérique[2]. **Aujourd'hui, environ 85 % des enquêtes pénales reposent sur des preuves électroniques**[3]. Les demandes de données adressées aux prestataires de services ont triplé entre 2017 et 2022, et la nécessité de disposer de telles données ne fait qu'augmenter[4].

Si nous avons récemment vu des exemples remarquables de démantèlement de réseaux de communication criminels spécialisés par des services répressifs et des autorités judiciaires[5], bien d'autres enquêtes sont **retardées ou infructueuses faute d'accès en temps utile à des preuves numériques**[6]. Au cours de la dernière décennie, les services répressifs et le pouvoir judiciaire ont perdu du terrain par rapport aux criminels, car ces derniers se procurent des outils et des produits fournis par des prestataires de services dont les mesures privent ces derniers des moyens de coopérer sur des demandes licites[7].

Les preuves essentielles en matière pénale restent inaccessibles pour les raisons suivantes[8]:

- **elles sont supprimées** par les fournisseurs de services dans un délai de quelques jours, conformément à leurs obligations en matière de protection des données à caractère personnel et de la vie privée ou à leurs besoins professionnels;

[1] EUR-Lex - 52025DC0148 - FR - EUR-Lex.
[2] Évaluation de la menace que représente la grande criminalité organisée dans l'Union européenne 2025, EU-SOCTA-2025.pdf.
[3] Analyse d'impact de la Commission concernant les propositions de règlement et de directive sur les preuves électroniques (17 avril 2018), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2018:0119:FIN:FR:PDF.
[4] Rapport Sirius 2023, https://www.eurojust.europa.eu/sites/default/files/assets/sirius-eueesr-2023.pdf, p. 69.
[5] Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized | Europol joint_ep_ej_third_report_of_the_observatory_function_on_encryption_en.pdf / Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe | Europol.
[6] Communiqué par le groupe de haut niveau sur l'accès aux données aux fins d'une répression efficace - Commission européenne.
[7] Rapport final du groupe de haut niveau sur l'accès aux données aux fins d'une répression efficace (15 novembre 2024).
[8] Common Challenges in Cybercrime, 2024 Review by Europol and Eurojust.

- **elles ne peuvent pas être obtenues** en raison de conflits de lois entre juridictions, divers pays ayant des lois et des réglementations différentes en matière d'accès aux données, ce qui rend difficile l'obtention de données stockées à l'étranger;
- **elles ne peuvent pas être récupérées à partir d'appareils saisis dans le cadre d'enquêtes pénales** parce que **la criminalistique numérique** est difficile, voire totalement impraticable;
- **elles ne peuvent pas être lues** parce que les données sont chiffrées;
- **elles ne peuvent pas être analysées de manière efficace et licite** faute de technologies appropriées ou de ressources humaines suffisantes pour filtrer et analyser efficacement de grandes quantités de données saisies sans empiéter sur les cadres juridiques de l'UE et des États membres.

En réponse à ces défis, un **groupe de haut niveau sur l'accès aux données à des fins répressives** (ci-après le «groupe de haut niveau») a été créé en 2023 et a formulé 42 recommandations en mai et novembre 2024. Le **Conseil «Justice et affaires intérieures» de l'UE** a approuvé les recommandations du groupe de haut niveau[9] le 13 juin 2024 et a ensuite, en décembre 2024, adopté des conclusions invitant la Commission à élaborer une feuille de route. Cette feuille de route devait se fonder sur les travaux du groupe de haut niveau et ses recommandations en vue de la mise en place de mesures destinées à garantir un accès licite et effectif aux données à des fins répressives[10]. La présente communication répond à cette demande.

Étant donné que la numérisation se généralise et fournit aux criminels une source croissante de nouveaux outils, un cadre régissant **l'accès licite aux données** est essentiel pour garantir que les criminels soient traduits en justice. L'«accès licite» auquel se réfère la présente feuille de route est l'accès, conformément à la loi, aux informations numériques dont les services répressifs ont besoin 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, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces.

Pour être licite, l'accès aux données doit être **nécessaire et proportionné et doit respecter les droits fondamentaux**, en garantissant que la vie privée et les données à caractère personnel sont protégées de manière adéquate; il doit se fonder sur des **règles claires, précises et accessibles prévues par la loi**, être soumis à des **mécanismes de contrôle** indépendants et prévoir des **voies de recours effectives** pour les personnes susceptibles d'être affectées par l'accès à leurs données. Il est tout aussi important de veiller à ce que les systèmes numériques restent **cybersécurisés** contre les accès non autorisés afin de se protéger contre les menaces en matière de cybersécurité.

I. Garantir la disponibilité de preuves numériques: conservation des données[11]

[9] Recommandations du groupe de haut niveau sur l'accès aux données en vue d'une répression efficace.

[10] Conclusions du Conseil sur l'accès aux données en vue d'une répression efficace (12 décembre 2024), https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/fr/pdf; conclusions du Conseil sur les priorités futures pour le renforcement des efforts conjoints de l'Union européenne et de ses États membres en matière de lutte contre le terrorisme (12 décembre 2024), https://data.consilium.europa.eu/doc/document/ST-16820-2024-INIT/fr/pdf.

[11] La «conservation des données» fait référence aux prestataires de services qui conservent certaines données non relatives au contenu traitées dans le cadre des services de communication qu'ils fournissent pendant une période donnée, afin de permettre aux autorités compétentes d'accéder, sous réserve de garanties appropriées, aux enquêtes pénales et de garantir la justice pénale.

En Espagne, une enquête pénale sur la disparition d'une jeune femme a été résolue en 2019 grâce aux données de localisation stockées par un fournisseur de services de communication conformément à une obligation légale nationale. Ces données ont permis aux enquêteurs de localiser la jeune femme disparue, de conclure que le suspect de l'enlèvement se trouvait également à cet endroit et d'exclure d'autres suspects[12]. Les données de communication non relatives au contenu (par exemple, les informations relatives à l'abonné, les données de localisation et la date, l'heure, la durée, l'expéditeur et le destinataire, ainsi que la taille de la communication) sont essentielles dans la plupart des enquêtes et poursuites pénales. Ces données peuvent être déterminantes pour identifier et localiser des victimes, des suspects et des personnes poursuivies, éclaircir une infraction commise, y compris aider à exclure des suspects.

Conformément à la législation de l'UE en matière de protection de la vie privée et des données, les fournisseurs de services de communications électroniques ne peuvent stocker des données de communication non relatives au contenu qui passent par leurs systèmes qu'aussi longtemps que cela est nécessaire à des fins professionnelles précises, explicites et légitimes. Toutefois, des obligations juridiques peuvent leur imposer de garder (ou de «conserver») ces données à d'autres fins, par exemple si elles sont nécessaires à des fins de prévention et de détection d'infractions pénales, ainsi que d'enquêtes et de poursuites en la matière.

Depuis que la directive de l'UE sur la conservation des données[13] a été invalidée en 2014[14], le paysage législatif de l'UE visant à obliger les fournisseurs de services à stocker des données s'est fragmenté et est devenu inégal. Les cadres des États membres régissant la conservation des données divergent en ce qui concerne les types de communications électroniques que les fournisseurs de services doivent conserver, les catégories de données qu'ils couvrent et les durées de conservation requises[15]. En outre, certains États membres ne disposent d'aucune législation sur la conservation des données. Les services répressifs et les autorités judiciaires sont confrontés à des obstacles juridiques et opérationnels dans l'exercice de leurs tâches. Les fournisseurs de communications électroniques, en particulier les petits fournisseurs, sont également confrontés à des coûts et à des obstacles supplémentaires lorsqu'ils fournissent leurs services dans l'ensemble de l'UE, car ils sont tenus de se conformer à des exigences juridiques différentes selon les États membres.

Le groupe de haut niveau a donc recommandé la mise en place d'**un cadre harmonisé au niveau de l'UE pour la conservation des données** afin de garantir la disponibilité des preuves numériques requises pour enquêter sur les infractions et engager des poursuites en la matière. Un régime harmonisé de l'UE viserait à limiter la fragmentation entre les États membres en ce qui concerne les règles relatives à la conservation des données et les garanties relatives aux droits fondamentaux, en particulier la protection de la vie privée et des données à caractère personnel et les droits de la défense, y compris le droit à un procès équitable. Un tel cadre

[12] La cobertura del móvil de Diana Quer desmonta la versión del Chicle: no la abordó donde él dijo que estaba robando gasolina | España.
[13] https://eur-lex.europa.eu/eli/dir/2006/24/oj.
[14] Arrêt de la Cour (grande chambre) du 8 avril 2014. Digital Rights Ireland Ltd contre Minister for Communications, Marine and Natural Resources e.a.
[15] Pour une vue d'ensemble, voir The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU | Eurojust | European Union Agency for Criminal Justice Cooperation et European Commission Study on the retention of electronic communications non-content data for law enforcement purposes.

juridique garantirait ainsi également la sécurité juridique pour les autorités compétentes, d'une part, et les fournisseurs de services, d'autre part[16].

Action clé

- **En 2025, la Commission réalisera une analyse d'impact en vue d'actualiser, s'il y a lieu, les règles de conservation des données au niveau de l'UE.**

Le groupe de haut niveau a mis en évidence la nécessité de **renforcer les synergies entre les professionnels des services répressifs et les fournisseurs de services**[17].

À cet effet, **l'Agence de l'Union européenne pour la coopération des services répressifs (Europol) et l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust)** sont invitées à poursuivre et à intensifier leurs efforts pour **faciliter la coopération, l'échange d'informations et de bonnes pratiques entre les professionnels des services répressifs et les fournisseurs de services** dans le cadre du **projet SIRIUS**[18], avec le soutien continu de la Commission. Le projet SIRIUS est devenu la principale source d'information **permettant aux professionnels des services répressifs et aux autorités judiciaires de l'UE et au-delà d'accéder aux preuves électroniques stockées par des fournisseurs de services en ligne** établis dans des pays tiers. La plateforme SIRIUS compte plus de 8 000 membres issus des services répressifs et des communautés judiciaires, représentant 47 pays dans le monde, et a soutenu directement près de 70 opérations de police.

Dans le même but, Europol et Eurojust devraient utiliser le projet SIRIUS pour élaborer, en coopération avec le **secteur privé, un catalogue des données que les services de communications électroniques traitent légitimement à des fins professionnelles**. Cela aidera les autorités compétentes à déterminer quelles données peuvent être disponibles pour leurs demandes d'accès licite, à identifier les fournisseurs de services concernés et à mieux cibler les demandes d'accès licite, ce qui permettra aux autorités publiques et aux fournisseurs de services de gagner du temps et de réaliser des économies.

Actions clés

- **Avec le soutien continu de la Commission, Europol et Eurojust sont instamment invitées à s'appuyer sur le projet SIRIUS pour rationaliser la coopération avec les fournisseurs de services de communications électroniques.**

- **Europol et Eurojust sont instamment invitées à élaborer, en coopération avec le secteur privé, un catalogue des données que les fournisseurs de communications électroniques traitent à des fins professionnelles (à partir du quatrième trimestre 2025).**

II. Obtention de preuves dans l'ensemble des systèmes et des juridictions: interception licite

L'accès licite aux données de communication en temps réel est essentiel pour lutter contre les criminels en ligne et hors ligne. En 2020, une équipe commune d'enquête franco-néerlandaise a démantelé EncroChat, un réseau téléphonique crypté largement utilisé par les organisations

[16] Groupe de recommandations nº 6, rapport final du groupe de haut niveau.
[17] Groupe de recommandations nº 5, rapport final du groupe de haut niveau.
[18] Projet SIRIUS | Europol.

criminelles. Cette enquête commune a permis d'intercepter des millions de messages en temps réel entre des criminels qui projetaient de commettre des infractions graves, de partager ces messages avec d'autres autorités et de les analyser. Grâce aux informations obtenues, les services répressifs de toute l'Europe et d'autres régions du monde ont fait cesser des activités criminelles, notamment des attaques violentes, des faits de corruption, des tentatives d'assassinats et du trafic de drogues à grande échelle. Certains messages révélaient des projets de crimes violents imminents et ont ainsi permis aux services répressifs de les déjouer[19]. La décision d'enquête européenne (DEE) a facilité le partage efficace de ces éléments de preuve[20].

L'affaire EncroChat démontre que l'accès en temps réel aux données relatives au contenu des communications est un outil essentiel pour mener à bien les enquêtes et les poursuites à l'encontre des organisations criminelles. Toutefois, cette affaire reste l'une des rares réussites: le groupe de haut niveau a constaté que l'efficacité de l'interception licite[21] a considérablement diminué depuis que la communication est passée des appels téléphoniques et SMS traditionnels aux services de messagerie «par contournement» (OTT) fournis par l'intermédiaire d'applications. Actuellement, environ 97 % de l'ensemble des messages mobiles sont envoyés au moyen d'applications de messagerie, tandis que les SMS et les messages MMS traditionnels ne représentent plus que quelque 3 % des messages[22]. Le groupe de haut niveau a également relevé que, depuis 2020, à la suite de la perturbation de certains des principaux réseaux de communication criminels, de nombreuses organisations criminelles ont décidé de revenir à des services réguliers de messagerie OTT chiffrés de bout en bout[23].

Les règles nationales imposant des obligations en matière d'interception licite sont fragmentées dans l'UE[24]. Le groupe de haut niveau a noté que, si certains États membres imposent des obligations similaires pour tous les types de services de communications électroniques, y compris les OTT, d'autres les excluent. En outre, les fournisseurs de services ne sont souvent pas établis dans l'État membre de l'autorité requérante, ce qui peut entraîner des problèmes de compétence complexes, des conflits de lois et des difficultés d'application[25]. En conséquence, le contenu de ces services de messagerie est quasiment inaccessible.

La DEE et d'autres instruments de coopération peuvent contribuer à relever le défi de l'interception transfrontière dans certaines parties de l'UE. Toutefois, les autorités des États membres rencontrent encore des difficultés lorsqu'elles les utilisent: ces instruments ne peuvent appuyer l'interception lorsque le service est fourni soit à partir d'États membres qui ne participent pas à l'instrument concerné, soit à partir d'un pays tiers. Le groupe de haut niveau

[19] Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe | Europol; Retour sur l'affaire EncroChat, ou quand les cyber-gendarmes ont hacké la messagerie chiffrée utilisée par la criminalité organisée.
[20] Décision d'enquête européenne | Eurojust | Agence de l'Union européenne pour la coopération judiciaire en matière pénale.
[21] Dans le cadre de la présente communication, les technologies d'interception licite qui sont mises en œuvre pour obtenir un accès en temps réel aux données de communication dans le cadre d'enquêtes judiciaires par un opérateur de communication ainsi que les technologies qui peuvent être déployées de manière autonome par les services répressifs.
[22] Rapport final du groupe de haut niveau, p. 38.
[23] Évaluation de la menace que représente la criminalité organisée sur l'internet (iOCTA) 2024.
[24] Voir le livre blanc de l'UE sur les infrastructures numériques, p. 14; le rapport Letta sur le marché intérieur, p. 59; et le rapport Draghi sur la compétitivité de l'UE, p. 70, 74 et 76.
[25] Rapport final du groupe de haut niveau, p. 41.

a donc recommandé un certain nombre de mesures visant à garantir qu'un large éventail de fournisseurs, y compris les fournisseurs OTT, réponde aux demandes d'interception licite[26].

En réponse, **la Commission proposera des moyens d'améliorer les mesures visant à renforcer la coopération transfrontière en matière d'interception**, tant entre les autorités qu'entre les autorités et les fournisseurs de services. Suivant les recommandations du groupe de haut niveau, la Commission s'emploiera principalement à améliorer les instruments existants, en particulier la DEE, et la coopération volontaire (lorsqu'il n'y a pas de conflits de lois avec des pays tiers ou que ceux-ci ont été levés). En définitive, les États membres devraient être en mesure de faire respecter les obligations en matière d'interception licite à tous les fournisseurs de communications proposant des services au niveau national, comme le prévoient les législations nationales, qu'il s'agisse de services de télécommunications traditionnels ou fondés sur l'internet et indépendamment de leur localisation.

En outre, certains États membres ne disposent pas des capacités de réseau requises pour le partage de données dans le cadre de la coopération transfrontière. Par conséquent, **la Commission recensera les besoins des États membres** et soutiendra le déploiement de réseaux sécurisés disposant d'une bande passante suffisante entre les États membres concernés, ce qui permettra le transfert de grandes quantités de données en temps réel. Cette initiative pourrait être financée par des programmes de l'UE.

Actions clés

La Commission:

- **proposera des mesures visant à améliorer l'efficacité des demandes transfrontières d'interception licite au moyen des instruments existants, y compris en évaluant la nécessité de renforcer la décision d'enquête européenne (d'ici à 2027);**

- **étudiera des mesures visant à créer des conditions de concurrence équitables pour tous les types de fournisseurs de communications dans le cadre de l'application des obligations en matière d'interception licite;**

- **déterminera l'approche la plus efficace pour lutter contre les fournisseurs de communications non coopératifs;**

- **soutiendra le déploiement de capacités sécurisées de partage d'informations entre les États membres, Europol et d'autres organismes dans le domaine de la sécurité (de 2026 à 2028).**

Les États membres sont encouragés à mettre en œuvre des mesures d'interception licite transfrontière, en s'appuyant sur les mécanismes existants tels que la décision d'enquête européenne et les accords bilatéraux et multilatéraux.

III. Récupérer des éléments de preuve à partir d'appareils saisis dans le cadre d'enquêtes: criminalistique numérique

Pour mener des enquêtes pénales, les services répressifs et les autorités judiciaires doivent être en mesure d'accéder aux preuves numériques stockées sur des appareils électroniques, de les

[26] Groupe de recommandations nº 8, rapport final du groupe de haut niveau.

collecter, de les analyser et de les conserver. Ces preuves numériques peuvent, par exemple, aider à identifier des membres d'organisations criminelles ou à exclure des personnes en tant que suspects[27].

Le groupe de haut niveau s'est penché sur un certain nombre de problèmes qui entravent l'accès à ces preuves numériques. Les autorités nationales souffrent d'un grave manque de ressources et de capacités pour mener des expertises technico-légales numériques. Elles peinent à répondre à la nécessité de développer en permanence de nouvelles compétences et de nouveaux outils pour suivre le rythme des nouvelles technologies (par exemple, les nouveaux types d'appareils et de systèmes d'exploitation, l'internet des objets et l'informatique en nuage). La coopération transfrontière entre les États membres est compromise par le manque de capacités comparables et par l'absence de mécanismes de reconnaissance des compétences et de l'expertise des experts en criminalistique numérique. Les solutions commerciales existantes deviennent rapidement obsolètes, sont inabordables et sont souvent développées en dehors de l'UE. Elles peuvent également être mal adaptées aux besoins des autorités des États membres ou ne pas satisfaire aux normes de responsabilité de l'UE en matière de criminalistique numérique ou à d'autres exigences juridiques.

En conséquence, afin de renforcer la capacité des services répressifs européens à effectuer des expertises technico-légales numériques sur les appareils saisis, le groupe de haut niveau a recommandé de fournir un financement ciblé pour des projets visant à la fois la recherche et le développement d'outils de criminalistique numérique et leur adoption. Le groupe de haut niveau s'est félicité des efforts actuellement déployés par la Commission pour soutenir ces projets au moyen d'un financement au titre de certains instruments de l'UE (Horizon Europe, le programme pour une Europe numérique et le Fonds pour la sécurité intérieure) et des instruments correspondants dans le cadre du prochain budget à long terme de l'UE (cadre financier pluriannuel).

En réponse à ces recommandations[28], **la Commission, avec le concours d'Europol, coordonnera une analyse des lacunes et des besoins en matière de recherche, de développement, de déploiement, de maintenance et d'adoption de solutions techniques communes pour la criminalistique numérique**.

Il convient de maximiser l'utilisation des ressources en créant des synergies entre les projets de criminalistique numérique, y compris en intégrant ceux financés au titre des programmes des États membres dans les mécanismes ou réseaux existants. Cela devrait inclure le financement de partenariats public-privé afin de fournir des outils logiciels entièrement testés et prêts à l'emploi sans frais de licence[29].

Dans le cadre de sa mission consistant à mener des enquêtes administratives, l'OLAF a acquis une expérience considérable dans les processus et outils de criminalistique numérique et peut

[27] Un cas examiné au sein du groupe de haut niveau portait sur l'analyse d'un appareil qui a contribué à prouver qu'un suspect n'était pas impliqué dans un assassinat. Rapport final du groupe de haut niveau, p. 12.
[28] Groupe de recommandations nº 1, rapport final du groupe de haut niveau.
[29] Par exemple, l'Association européenne pour le développement de technologies de lutte contre la cybercriminalité (EACTDA) (www.eactda.eu) fournit des outils logiciels entièrement testés et prêts à l'emploi, sans frais de licence ni accès au code source, aux services répressifs de l'UE. En plus des huit outils mis au point à ce jour, l'EACTDA développe actuellement 16 outils d'enquête numériques supplémentaires, qui doivent être fournis d'ici la mi-2025.

aider les autorités des États membres à renforcer leurs capacités au moyen du programme de l'Union en matière de lutte contre la fraude.

Le **répertoire d'outils d'Europol** est une plateforme en ligne sécurisée, exclusivement accessible aux services répressifs, qui permet de partager gratuitement des logiciels non commerciaux développés par Europol, les services répressifs européens et les universités européennes. Les autorités nationales chargées des enquêtes utilisent largement les outils du répertoire pour soutenir des domaines liés à la grande criminalité organisée, y compris la traite des êtres humains, la cybercriminalité et les abus sexuels commis contre des enfants en ligne. Ce répertoire devrait rester le canal de distribution privilégié pour les outils d'enquête numériques mis au point par les projets de l'UE, et les États membres, qui seront encouragés à partager les outils de criminalistique numérique à code source ouvert développés au niveau national au sein des mécanismes ou réseaux existants. **Europol peut poursuivre le développement et la promotion de son répertoire d'outils** afin de mettre à la disposition des services répressifs de l'UE des outils d'enquête fiables, sûrs, gratuits, faciles à installer et modulables.

La Commission **soutiendra** également **l'adoption de solutions innovantes par les services répressifs des États membres au moyen de mécanismes existants, tels que l'EMPACT[30], et d'appels spécifiques du Fonds pour la sécurité intérieure**.

Le groupe de haut niveau a souligné que les **licences concernant les outils de criminalistique numérique** sont coûteuses et parfois inabordables pour certains services répressifs. Les outils de criminalistique numérique peuvent fournir des données dans des formats qui ne sont pas compatibles avec les systèmes utilisés pour le traitement ultérieur. En outre, la confiance est fondamentale pour les activités de criminalistique numérique, qui ne devraient pas s'appuyer sur des outils de type «boîte noire» (c'est-à-dire des outils qui traitent des données sans que les autorités de confiance soient en mesure de vérifier leur fonctionnement). Le partage d'outils de criminalistique numérique devrait être soutenu par des systèmes d'évaluation et, le cas échéant, par la certification des outils commerciaux au niveau de l'UE afin de garantir qu'ils respectent les normes en matière de fiabilité et de police scientifique sans imposer de charges excessives. Un soutien devrait également être apporté au moyen de mécanismes communs de passation de marchés, garantissant la coopération entre les unités opérationnelles et les points de contact au sein des autorités chargées des marchés publics[31].

Par conséquent, **la Commission aidera les unités opérationnelles des États membres et leurs autorités chargées des marchés publics à mettre en place des achats conjoints de licences pour les outils de criminalistique numérique, en commençant par une phase pilote**.

Actions clés
La Commission, avec le concours d'Europol:

[30] La plateforme EMPACT (plateforme pluridisciplinaire européenne contre les menaces criminelles) est une initiative en matière de sécurité menée par les États membres de l'UE dans le but d'identifier, de hiérarchiser et de combattre les menaces que représente la grande criminalité internationale organisée.

[31] En s'appuyant sur le projet iProcureNet (www.iprocurenet.eu/), qui, financé au titre du programme «Horizon Europe» pour la passation conjointe de marchés dans le domaine de la recherche et de l'innovation, a mis au point une méthodologie pour la passation conjointe de marchés dans le domaine de la sécurité, ainsi qu'un réseau d'autorités chargées des marchés publics dans les États membres.

- **coordonnera une analyse des lacunes et des besoins en matière de recherche, de développement, de déploiement, de maintenance et d'adoption de solutions techniques communes pour la criminalistique numérique avant le deuxième trimestre 2026;**

- **continuera à soutenir le développement de solutions techniques pour la criminalistique numérique au moyen de mécanismes de financement et de coordination appropriés;**

- **aidera les États membres et les autorités chargées des marchés publics à mettre en place des achats conjoints de licences pour les outils de criminalistique numérique (avant le deuxième trimestre 2027), en commençant par une phase pilote.**

<u>Europol</u> est invitée à poursuivre le développement et la promotion de son répertoire d'outils afin de permettre aux services répressifs d'accéder à des outils numériques non commerciaux (à partir du troisième trimestre 2025).

<u>Les États membres</u> sont invités à participer, à soutenir et à piloter le développement, la validation et l'adoption d'outils de criminalistique numérique.

L'Agence de l'Union européenne pour la formation des services répressifs (CEPOL) dispense des formations aux enquêteurs en criminalistique numérique, y compris sur la criminalistique mobile et la criminalistique des données en temps réel. Suivant la recommandation du groupe de haut niveau[32], la **Commission devrait continuer à soutenir la création de matériel et de ressources de formation** au moyen de mécanismes existants associant les professionnels et le monde universitaire[33]. En outre, le CEPOL et les États membres devraient **donner la priorité à la formation à la criminalistique numérique**.

Le groupe de haut niveau a également souligné qu'un système de certification pourrait être créé au niveau de l'UE pour les experts en criminalistique numérique. Un tel système garantirait la qualité des travaux de criminalistique numérique, contribuerait à une plus grande transparence des procédures judiciaires et renforcerait la confiance entre les services répressifs par-delà les frontières.

Conformément aux recommandations du groupe de haut niveau[34], le CEPOL **pourrait aider les professionnels et le monde universitaire à créer un système de certification au niveau de l'UE pour les experts en criminalistique numérique, en tirant pleinement parti des réseaux et mécanismes existants**[35].

Actions clés

<u>La Commission</u>:

- **continuera à soutenir la création de matériel et de ressources de formation.**

[32] Groupe de recommandations nº 3, rapport final du groupe de haut niveau.
[33] Par exemple, le groupe européen de formation et d'enseignement sur la cybercriminalité (ECTEG) (www.ecteg.eu) est une association travaillant en étroite coopération avec Europol et le CEPOL, dans le but de fournir des ressources de formation gratuites aux services répressifs dans le domaine des enquêtes numériques. Il est actuellement financé par le Fonds de l'UE pour la sécurité intérieure.
[34] Groupe de recommandations nº 3, rapport final du groupe de haut niveau.
[35] En particulier l'ECTEG.

Le CEPOL et les États membres sont encouragés:

- **à donner la priorité à la formation à la criminalistique numérique (à partir du troisième trimestre 2025);**

- **à soutenir l'élaboration et la mise en œuvre d'un système de certification au niveau de l'UE pour les experts en criminalistique numérique (à préparer entre le premier trimestre 2026 et le quatrième trimestre 2028).**

Le groupe de haut niveau a formulé des recommandations visant à faciliter le partage de solutions et d'outils de criminalistique numérique entre les États membres dans un climat de confiance[36]. En réponse, **Europol devrait continuer à renforcer son rôle de centre d'excellence des services répressifs de l'UE pour l'expertise opérationnelle numérique dans le domaine de la criminalistique numérique**. Il pourrait s'agir notamment de mettre en place un projet similaire à SIRIUS[37] pour faciliter le partage de connaissances, d'expertise, de solutions techniques, d'outils de criminalistique numérique et de bonnes pratiques dans un climat de confiance. Europol devrait également renforcer son rôle de coordination dans la création de connaissances en matière de criminalistique numérique au niveau de l'UE, en s'appuyant sur les mécanismes créés ces dernières années[38]. Europol peut commencer à mettre en œuvre certaines de ces mesures dans le cadre de son mandat actuel. Toutefois, Europol aura besoin d'un mandat renforcé et de ressources supplémentaires pour concevoir pleinement ces mesures et répondre efficacement aux besoins opérationnels des États membres.

Dans le prolongement de l'engagement pris dans les orientations politiques à l'intention de la Commission européenne pour son mandat 2024-2029 et comme annoncé dans la stratégie européenne de sécurité intérieure, **la Commission proposera une révision ambitieuse du mandat d'Europol**. À cette fin, en étroite coopération avec les États membres, la Commission étudiera les moyens de renforcer l'expertise technologique et la capacité d'Europol à soutenir les services répressifs nationaux dans l'espace numérique. Il sera essentiel, dans le cadre de cet effort, de renforcer les capacités d'Europol en matière de criminalistique numérique, sur la base d'un mandat renforcé et de ressources supplémentaires.

Le groupe de haut niveau a recommandé d'améliorer l'accès des experts aux connaissances au moyen de mécanismes spécifiques et de permettre aux experts de collaborer avec les producteurs et les développeurs d'outils de criminalistique numérique[39]. À partir de 2026, **Europol devrait, à l'aide de ses propres ressources, encourager la coopération entre les autorités nationales compétentes et les experts afin de faciliter la coopération public-privé en matière de criminalistique numérique**. Europol devrait aider les États membres à mettre

[36] Groupe de recommandations nº 1, rapport final du groupe de haut niveau.

[37] Le projet SIRIUS, dirigé par Europol et Eurojust, soutient les services répressifs et les autorités judiciaires de l'UE en permettant un accès transfrontière efficace aux preuves électroniques stockées par les fournisseurs de services en ligne. Il fournit des outils pratiques, des formations et des ressources à plus de 9 000 professionnels, favorise la coopération entre les fournisseurs de services en ligne et encourage le partage des connaissances au moyen d'événements et de partenariats internationaux.

[38] Communautés spécialisées sur la plateforme d'experts Europol (https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-platform-for-experts); le forum d'experts légistes (https://www.europol.europa.eu/publications-events/events/forensic-experts-forum-2024-conference); les Journées de l'industrie et de la recherche Europol (https://www.europol.europa.eu/publications-events/events/europol-industry-and-research-days-2025).

[39] Groupe de recommandations nº 1, rapport final du groupe de haut niveau.

au point des outils numériques et des procédures communes, notamment en établissant des formats de données communs à des fins de criminalistique numérique[40].

Actions clés

<u>Europol</u> est invitée:

- **à devenir un centre d'excellence pour l'expertise opérationnelle en criminalistique numérique et à renforcer son rôle dans la coordination de la création de connaissances dans ce domaine au niveau de l'UE (à partir de 2026);**

- **à faciliter la coopération entre les services répressifs et les parties privées, y compris les fournisseurs de services, en matière de criminalistique numérique et à contribuer à la mise en place de formats de données communs à des fins de criminalistique numérique (à partir de 2026).**

IV. <u>Veiller à ce que les éléments de preuve puissent être lus: déchiffrement des données</u>

Le chiffrement et d'autres mesures de cybersécurité jouent un rôle important dans la protection des systèmes d'information contre l'espionnage et les perturbations et dans la sécurisation des communications, de la vie privée et des données à caractère personnel. Entre 60 % et 80 % des applications de messagerie sont chiffrées de bout en bout, y compris des fournisseurs traditionnels tels que WhatsApp, Messenger, Signal et iMessage, tandis que l'utilisation des SMS et des appels téléphoniques traditionnels est en net recul dans le monde entier[41].

Le groupe de haut niveau a souligné que ces évolutions ont une incidence sur la capacité des services répressifs et des autorités judiciaires à recueillir des preuves dans le cadre d'enquêtes et de poursuites pénales, étant donné que la plupart des interceptions licites de communications deviennent inutilisables. Il a également précisé que les États membres disposent d'une expertise et de capacités limitées pour déchiffrer les données au repos, avec des écarts importants dans les taux de réussite, allant de 15 à 20 % dans certains États membres à plus de 66 % dans d'autres.

Les équipements de déchiffrement sont coûteux et hautement spécialisés, et le matériel consomme beaucoup de ressources. La plupart des unités de criminalistique numérique des services répressifs s'appuient sur des solutions commerciales pour accéder aux données sur les appareils. Ces solutions peinent à suivre le rythme des évolutions technologiques et deviennent rapidement obsolètes; le coût élevé des licences réduit considérablement le nombre d'utilisateurs autorisés; enfin, ces solutions sont souvent développées en dehors de l'UE et risquent donc de ne pas répondre aux besoins des autorités de l'UE ou aux normes en matière de criminalistique numérique. En conséquence, elles ne sont utilisées avec succès que dans un très petit nombre d'enquêtes.

En outre, le recours à ces outils présente d'autres inconvénients. Dans leurs enquêtes, les autorités exploitent souvent des vulnérabilités pour accéder aux clés de déchiffrement des appareils, ce qui pourrait, dans certains cas, créer des tensions eu égard à l'objectif stratégique consistant à garantir la cybersécurité par défaut. En outre, l'accès aux données chiffrées devient

[40] Ces efforts devraient être soutenus par la source de financement appropriée de l'UE (programmes de recherche ou de développement, en fonction du niveau de maturité des systèmes envisagés).
[41] Les pourcentages mentionnés concernent le chiffrement de bout en bout pendant la transmission.

de plus en plus complexe. Le groupe de haut niveau a noté que les données stockées sur certains types d'appareils modernes, protégés par des cryptoprocesseurs ou des algorithmes de chiffrement solides et des mots de passe complexes, ne peuvent pas être consultées par les autorités, même en utilisant les plateformes de déchiffrement les plus puissantes.

Le développement et le déploiement d'une **cryptographie quantique sûre** sont une nécessité pour protéger les données contre de futures attaques informatiques quantiques qui rendraient les communications sensibles, les transactions financières et les secrets d'État vulnérables au décryptage et à l'exploitation. Comme indiqué dans la recommandation de la Commission relative à une feuille de route pour la mise en œuvre coordonnée de la transition vers la **cryptographie post-quantique (PQC)**[42] et dans la stratégie européenne de sécurité intérieure (ProtectEU), le déploiement de solutions PQC et le développement de la distribution quantique de clés seront essentiels pour préserver les données à l'ère quantique nouvelle. Toutefois, comme l'a souligné Europol, cela rendra l'accès licite aux preuves numériques plus difficile dans les années à venir, et les services répressifs doivent investir pour suivre le rythme d'une évolution technologique rapide[43].

Le groupe de haut niveau[44] a recommandé d'élaborer une feuille de route technologique afin de mettre en œuvre, le cas échéant, un accès licite ciblé dès la phase de conception, tout en garantissant une sécurité et une cybersécurité solides et en respectant pleinement les obligations juridiques en matière d'accès licite. En réponse, **la Commission charge actuellement un groupe d'experts d'apporter son soutien à l'élaboration d'une feuille de route technologique sur le chiffrement**. Ce groupe recensera et évaluera les solutions technologiques qui permettraient aux services répressifs d'accéder à des données chiffrées de manière licite, tout en préservant la cybersécurité et les droits fondamentaux. Ce groupe comprendra des experts des services répressifs, de la cybersécurité, du chiffrement, des technologies de communication, de la normalisation et des droits fondamentaux. Des études technologiques et des preuves de concepts soutiendront ces travaux. L'objectif de ces travaux est de recenser:

- **les outils dont les services répressifs ont actuellement besoin et dont ils auront besoin à l'avenir** pour trouver, récupérer et analyser de manière licite des données chiffrées; ces outils doivent faciliter les activités de criminalistique numérique, de déchiffrement, de collecte de données à distance et d'analyse de la criminalité;
- **les technologies qui garantissent que les futures technologies de l'information et de la communication**, telles que la sixième génération de réseaux cellulaires (6G) et le chiffrement post-quantique, ne nuisent pas à la capacité des services répressifs à accéder de manière licite aux données, tout en veillant au respect des droits fondamentaux et de la cybersécurité.

S'il n'existe actuellement aucun outil, la feuille de route technologique devrait formuler des recommandations sur leur développement et sur la manière d'assurer la compatibilité avec le cadre juridique de l'UE et de garantir la cybersécurité. Les résultats de la feuille de route

[42] Recommandation relative à une feuille de route pour la mise en œuvre coordonnée de la transition vers la cryptographie post-quantique.
[43] The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement | Europol.
[44] Groupe de recommandations nº 10, rapport final du groupe de haut niveau.

technologique peuvent également éclairer des actions spécifiques visant à favoriser une approche coordonnée de la normalisation.

La plateforme de déchiffrement d'Europol s'est révélée déterminante dans le cadre d'enquêtes criminelles importantes, y compris celles liées aux affaires Sky ECC[45] et EncroChat. Il est nécessaire de renforcer les capacités de déchiffrement, notamment grâce à de nouveaux investissements dans l'intelligence artificielle (IA) et le calcul à haute performance, pour faire en sorte que les services répressifs aient la capacité de déchiffrer des algorithmes de plus en plus complexes.

Le groupe de haut niveau a formulé une recommandation[46] visant à augmenter le financement pour soutenir l'innovation en matière d'accès aux données. En réaction, **la Commission soutiendra la recherche et le développement de nouvelles capacités de déchiffrement** afin de faire en sorte qu'Europol soit bien équipée après 2030 pour soutenir les États membres, à la lumière des nouvelles évolutions technologiques et des recherches les plus avancées dans ce domaine. Cette initiative pourrait impliquer une augmentation des fonds destinés à soutenir la recherche sur le déchiffrement, ainsi que l'élaboration et la mise en œuvre d'outils par les États membres. Les États membres seront étroitement associés à cette initiative afin de partager leurs besoins spécifiques, en vue de renforcer leurs capacités, leurs compétences et leurs ressources techniques, en s'appuyant sur les technologies conçues au niveau de l'UE et, éventuellement, en envisageant la passation conjointe de marchés.

Actions clés

La Commission:

- **élaborera une feuille de route technologique sur le chiffrement (au deuxième trimestre 2026);**
- **soutiendra la recherche et le développement de nouvelles capacités de déchiffrement afin de doter Europol de capacités de déchiffrement de nouvelle génération (à partir de 2030).**

V. Concilier technologie et accès licite: normalisation

Les normes sont essentielles dans les communications numériques. Développées par un large éventail d'acteurs, principalement par le secteur, elles assurent l'interopérabilité entre les systèmes et les dispositifs mis au point par les fournisseurs de technologies et facilitent la conformité des technologies avec les obligations juridiques, y compris en ce qui concerne l'accès licite à des fins répressives. L'Institut européen de normalisation des télécommunications (ETSI) a élaboré plusieurs normes dans le domaine de l'interception licite et de la divulgation licite. Toutefois, des lacunes subsistent, notamment en ce qui concerne la cinquième génération de réseaux cellulaires (5G), où l'absence de prise en compte appropriée de l'accès licite dans son développement a entravé la capacité des services répressifs et des

[45] New major interventions to block encrypted communications of criminal networks | Europol.
[46] Groupe de recommandations nº 10, rapport final du groupe de haut niveau.

autorités judiciaires à accéder aux éléments de preuve nécessaires pour identifier les criminels et les traduire en justice[47].

Le groupe de haut niveau a recommandé d'adopter une approche prudente dans la conception de solutions permettant un accès licite aux systèmes, selon laquelle le secteur ne devrait pas avoir à intégrer des systèmes susceptibles d'affaiblir le chiffrement de manière généralisée ou systémique pour tous les utilisateurs d'un service. L'accès licite aux données doit rester ciblé et limité à certaines communications déterminées au cas par cas.

En règle générale, toute solution devrait être mise en œuvre sur la base de normes claires élaborées avec la contribution de toutes les parties prenantes, y compris les représentants du secteur, les experts en matière de protection des données, de respect de la vie privée et de cybersécurité, ainsi que les professionnels des services répressifs. Toutefois, il convient de faire preuve de prudence en ce qui concerne le chiffrement, comme l'a souligné le groupe de haut niveau. Sur la base des solutions recensées dans la feuille de route technologique, des mesures spécifiques seront envisagées pour favoriser une approche coordonnée de la normalisation.

Toute normalisation devrait refléter les exigences légales applicables et se fonder sur des solutions évaluées. Elle doit faire en sorte que l'accès licite soit conforme aux normes de cybersécurité applicables, telles que celles élaborées en vertu du règlement sur la cyberrésilience, aux normes soutenant la mise en œuvre de la directive SRI 2 ainsi qu'aux autres exigences en matière de sécurité des produits et services.

En ce qui concerne les recommandations du groupe de haut niveau[48], **la Commission élaborera et rationalisera une approche de l'UE en matière de normalisation pour la sécurité intérieure, en mettant l'accent sur la criminalistique numérique, la divulgation licite et l'interception licite**. Cette approche sera fondée sur une analyse continue du paysage menée par les professionnels des services répressifs, en particulier par l'intermédiaire du groupe de travail européen sur la normalisation en matière de sécurité intérieure, dirigé par Europol. Cette action permettra également d'accroître les ressources et d'élargir le mandat du groupe de travail et impliquera une collaboration supplémentaire avec d'autres initiatives en matière de normalisation, en particulier en ce qui concerne l'IA et la criminalistique numérique. L'objectif est de veiller à ce que les questions de sécurité soient intégrées dans la politique de normalisation. En outre, cette initiative comprendra la mise au point et l'organisation de formations sur la normalisation dans le domaine de la sécurité ainsi que l'octroi d'un soutien financier au titre du Fonds pour la sécurité intérieure aux experts participant aux forums de normalisation concernés. Elle intégrera également les mécanismes de gouvernance pertinents.

[47] Voir le premier rapport sur le chiffrement du pôle d'innovation de l'UE pour la sécurité intérieure, 11 juin 2024.
[48] Groupe de recommandations nº 10, rapport final du groupe de haut niveau.

Actions clés

- **La Commission, en étroite coopération avec Europol, élaborera et rationalisera des activités de normalisation pour un accès licite, soutenues par des mécanismes de gouvernance appropriés (du deuxième trimestre 2025 au deuxième trimestre 2027).**

- **Les États membres sont encouragés à consacrer des ressources suffisantes pour garantir que les professionnels de la sécurité participent aux forums de normalisation pertinents sur l'accès licite.**

VI. Analyser les éléments de preuve de manière efficace et licite: IA

Europol et Eurojust ont récemment constaté qu'un nombre croissant d'enquêtes contiennent de très grandes quantités de données[49]. Dans une affaire classique d'abus sexuels sur enfants, les enquêtes nécessitent souvent d'analyser entre 1 et 3 téraoctets de données, ce qui peut comprendre 1 à 10 millions d'images et des milliers d'heures d'enregistrements vidéo[50]. En 2023, 1 553 822 fichiers volumineux ont été échangés au moyen de l'outil LFE (Large File Exchange) d'Europol[51]. Dans l'affaire EncroChat, plus de 115 millions de conversations entre suspects appartenant à des organisations criminelles ont été interceptées. Au cours des mois qui ont suivi, grâce à des techniques et des moyens d'analyse de pointe, tels que l'apprentissage automatique, Europol et les services répressifs ont été en mesure d'établir des schémas, des liens et des points chauds («hotspots»), ce qui a conduit à l'arrestation de 6 558 suspects. Les autorités néerlandaises et françaises ont partagé ces informations avec leurs homologues des États membres de l'UE et de pays tiers, permettant ainsi de déjouer plus de 200 projets d'assassinat rien qu'au Royaume-Uni[52].

L'augmentation continue du volume des données traitées au cours des enquêtes rend difficile leur stockage, leur gestion et leur analyse efficace sans expertise significative, ressources informatiques et outils spécialisés. Europol et Eurojust ont confirmé que le volume de données à traiter pouvait représenter une tâche considérable pour les enquêteurs et entraîner ainsi des délais de traitement plus longs et des problèmes de capacité de stockage. Les États membres ne disposent souvent pas non plus des mécanismes et de l'infrastructure nécessaires pour gérer le transfert de grandes quantités de données vers d'autres États membres et Europol.

Par conséquent, l'utilisation de l'IA est essentielle pour permettre aux services répressifs de prévenir et de détecter les infractions, ainsi que d'enquêter sur celle-ci, et donc de protéger nos sociétés à l'ère du numérique. Les solutions fondées sur l'IA peuvent effectuer des tâches simples, telles que la traduction automatique ou la conversion de la parole en texte, ou des tâches plus complexes, telles que le filtrage de données, la mise en corrélation de preuves extraites de quantités massives de données ou la lutte contre l'utilisation malveillante de l'IA. Les outils fondés sur l'IA destinés aux services répressifs doivent être précis, transparents et pleinement conformes au cadre juridique de l'UE en matière d'IA, de protection des données

[49] Common Challenges in Cybercrime, 2024 Review by Europol and Eurojust.
[50] IOCTA d'Europol.
[51] Rapport d'activité annuel consolidé d'Europol 2023.
[52] Retour sur l'affaire EncroChat, ou quand les cyber-gendarmes ont hacké la messagerie chiffrée utilisée par la criminalité organisée; Dismantling encrypted criminal EncroChat communications leads to over 6 500 arrests and close to EUR 900 million seized | Europol. EncroChat.

et de la vie privée afin de garantir la fiabilité et l'éthique des enquêtes fbasées sur les données. L'IA et le calcul à haute performance sont d'une importance capitale pour accéder aux données chiffrées et pour soutenir les enquêtes et l'analyse technico-légale.

Suivant les recommandations du groupe de haut niveau visant à accroître le financement de la recherche et du développement d'outils d'analyse des données fondés sur l'IA et à définir des éléments livrables clairs[53], **la Commission encouragera le développement et l'adoption de solutions d'IA**. Cela comprend des investissements ciblés dans le développement de capacités clés, telles que des solutions permettant de trouver des pistes d'enquête à partir de très grandes quantités de données, dans le plein respect des principes de protection des données et de la vie privée, ou des améliorations du traçage des transactions en cryptomonnaie. Il pourrait également être possible de tirer parti des possibilités offertes pour former à l'utilisation d'outils d'IA et tester et évaluer de tels outils dans un bac à sable réglementaire de l'IA, comme le prévoit le règlement sur l'IA[54], avec le soutien et sous la direction des autorités de contrôle compétentes. En outre, les fabriques d'IA et les futures gigafabriques d'IA pourraient soutenir le développement d'outils et de services fondés sur l'IA à des fins répressives. La Commission devrait faciliter ces efforts, sur la base d'une analyse des besoins avec les parties prenantes, y compris le laboratoire d'innovation d'Europol et le pôle d'innovation pour la sécurité intérieure des agences de l'UE compétentes en matière de justice et d'affaires intérieures.

Les États membres peuvent avoir accès aux capacités nécessaires à un coût faible voire nul, ce qui est conforme aux exigences du règlement sur l'IA. Il est essentiel d'adopter une approche globale de l'IA, notamment en créant des formats de données normalisés pour tout échange et en élaborant des lignes directrices sur l'utilisation de ces systèmes dans le respect du règlement sur l'IA et de la législation de l'UE applicable en matière de protection des données. Cette initiative pourrait être soutenue par un financement au titre du Fonds pour la sécurité intérieure, du programme pour une Europe numérique et d'Horizon Europe. Il conviendra de soutenir Europol et la communauté EMPACT afin de répondre de manière adéquate aux besoins opérationnels et de promouvoir l'adoption et l'intégration par les professionnels.

Actions clés

La Commission:

- **favorisera la création et l'adoption de nouvelles solutions d'IA et améliorera les solutions existantes pour le filtrage et l'analyse des preuves numériques, y compris en utilisant pleinement les bacs à sable réglementaires de l'IA pour leur mise au point, leur expérimentation et leur évaluation, conformément au règlement sur l'IA (de 2025 à 2028);**

- **engagera un dialogue avec les services répressifs et d'autres parties prenantes afin de recenser leurs besoins, en s'appuyant sur les travaux du laboratoire d'innovation d'Europol et du pôle d'innovation des agences de l'UE compétentes en matière de justice et d'affaires intérieures;**

- **soutiendra l'élaboration de lignes directrices claires pour l'utilisation de l'IA à des fins répressives;**

[53] Recommandation nº 4, recommandations du groupe de haut niveau.
[54] Voir l'article 57 du règlement sur l'IA.

- **soutiendra des projets pilotes visant à développer, et à former à leur utilisation, des solutions d'IA juridiquement et techniquement solides pour la criminalistique numérique, l'analyse de données et d'autres outils d'enquête à des fins répressives.**