COMMISSION
EUROPÉENNE

Bruxelles, le 11.12.2025
COM(2025) 752 final

RAPPORT DE LA COMMISSION AU PARLEMENT EUROPÉEN ET AU CONSEIL

évaluant et analysant l'incidence opérationnelle de l'exécution des missions prévues par le règlement (UE) 2022/991, en particulier par l'article 4, paragraphe 1, point t), l'article 18, paragraphe 2, point e), l'article 18, paragraphe 6 *bis*, et les articles 18 *bis*, 26, 26 *bis* et 26 *ter*, en ce qui concerne les objectifs d'Europol, ainsi que l'incidence de ces missions sur les libertés et droits fondamentaux prévus par la charte, conformément à l'article 68, paragraphe 3, du règlement (UE) 2016/794

{SWD(2025) 404 final}

1. Portée de l'évaluation

Depuis son entrée en service en 1999, l'**Agence de l'Union européenne pour la coopération des services répressifs (Europol)** a joué **un rôle central dans la lutte contre les formes graves de criminalité transfrontière et le terrorisme**, devenant un moteur essentiel de la coopération des services répressifs en Europe. La situation en matière de sécurité a connu des changements radicaux au cours des 30 dernières années, transformant profondément la grande criminalité organisée[1]. Les États membres ont de nouveaux besoins opérationnels pour répondre efficacement aux menaces émergentes et leurs **attentes en ce qui concerne le soutien d'Europol ont** également **évolué**. Le mandat d'Europol a donc été remplacé ou modifié à plusieurs reprises pour maintenir et renforcer le rôle de l'Agence.

Le mandat d'Europol, tel qu'il est défini dans le règlement (UE) 2016/794[2] (ci-après le «règlement Europol» ou «RE»), a été modifié en dernier lieu en 2022 par le règlement (UE) 2022/991[3] afin de faire face aux nouvelles menaces pour la sécurité. Le règlement Europol n'était plus adapté à sa finalité dans une réalité nouvelle, dans laquelle les criminels exploitent les avantages de la **transformation numérique, des nouvelles technologies, de la mondialisation** et **de la mobilité**[4].

Les **objectifs spécifiques** du règlement (UE) 2022/991[5] étaient les suivants:

- permettre une coopération efficace entre les **parties privées** et les autorités répressives afin de lutter contre l'abus des services transfrontières par les criminels;
- permettre aux autorités répressives d'analyser des **ensembles de données vastes et complexes** afin de détecter les liens transfrontières, dans le strict respect des **droits fondamentaux**;
- permettre aux États membres d'utiliser les **nouvelles technologies** à des fins répressives.

En outre, le règlement (UE) 2022/991 a modifié les règles en matière de protection des données applicables à Europol afin de maintenir un **niveau élevé de protection des données**, en établissant un équilibre entre les nouveaux pouvoirs de l'Agence en matière de traitement des données à caractère personnel et la protection de la vie privée et des données à caractère personnel des personnes physiques. Il a largement aligné les règles en matière de protection des données applicables à Europol sur celles applicables aux autres agences et organes de l'UE chargés de la justice et des affaires intérieures (JAI) en vertu du chapitre IX du règlement (UE) 2018/1725 (ci-après le «règlement de l'UE sur la protection des données» ou «RPDUE»), ainsi que celles applicables aux autorités répressives des États membres (ci-après les «autorités compétentes») en vertu de leur droit national transposant la directive (UE) 2016/680 (la «directive en matière de protection des données dans le domaine répressif»)[6] afin de **faciliter la circulation des informations**.

---

1 Europol, 2025 EU Serious and Organised Crime Threat Assessment (SOCTA) — The changing DNA of serious and organised crime (Évaluation 2025 de la menace que représente la grande criminalité organisée dans l'Union européenne — La profonde mutation de la grande criminalité organisée), disponible en ligne à l'adresse https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf («SOCTA UE 2025»). Voir également l'évaluation de la menace douanière (CTA) 2025, disponible en ligne à l'adresse https://www.douane.gouv.fr/sites/default/files/2025-07/03/Livret-CTA-UE-public_0.pdf.

2 JO L 135 du 24.5.2016, p. 53, ELI: http://data.europa.eu/eli/reg/2016/794/oj.

3 JO L 169 du 27.6.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/991/oj.

4 SWD(2020) 543 final du 9 décembre 2020, p. 37, https://eur-lex.europa.eu/resource.html?uri=cellar:1a4d9f40-3b02-11eb-b27b-01aa75ed71a1.0001.02/DOC_1&format=PDF.

5 *Ibid.*

6 JO L 119 du 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj.

Le présent rapport a été adopté conformément à l'obligation qui incombe à la Commission en vertu de l'**article 68, paragraphe 3, du RE**, d'évaluer[7] et d'analyser l'incidence opérationnelle des missions d'Europol définies dans le règlement (UE) 2022/991 trois ans après son entrée en vigueur. Sur mandat des colégislateurs, la Commission a: premièrement, évalué et analysé l'**incidence opérationnelle** de certaines des nouvelles règles relatives au traitement des données à caractère personnel, par rapport aux objectifs d'Europol, en vertu de l'article 3 du RE (à savoir: soutenir et renforcer l'action des autorités compétentes des États membres et leur coopération mutuelle dans la prévention des infractions pénales relevant du mandat d'Europol et dans la lutte contre celles-ci); deuxièmement, évalué l'incidence de ces règles sur les **libertés et droits fondamentaux** (ci-après les «droits fondamentaux») tels qu'ils sont consacrés par la charte[8] et, troisièmement, procédé à une **analyse coûts-avantages** des tâches de traitement de données y afférentes.

Pour préparer le réexamen, les services de la Commission ont recueilli des informations et des retours d'information auprès de diverses sources et ont mené des consultations ad hoc avec Europol et les États membres. Le **document de travail des services de la Commission** qui accompagne le présent rapport fournit une description détaillée du contexte général et de la méthode de réexamen, ainsi qu'un compte rendu complet des sources probantes et des consultations corroborant les principales conclusions résumées dans le présent rapport.

2. Contexte général

Conformément à l'article 68, paragraphe 3, du RE, le présent rapport de la Commission couvre certaines dispositions du règlement (UE) 2022/991, en mettant l'accent sur cinq aspects essentiels des travaux d'Europol.

(1) Dimension extérieure: article 4, paragraphe 1, point t), du RE sur les signalements pour information dans le système d'information Schengen (SIS) concernant des ressortissants de pays tiers, sur proposition d'Europol

Compte tenu de la **nature mondiale des formes graves de criminalité et du terrorisme**, les informations détenues par des pays tiers et des organisations internationales sur les auteurs et les personnes soupçonnées de tels crimes revêtent une importance croissante pour la sécurité intérieure de l'UE. La dimension extérieure de la coopération des services répressifs de l'UE est donc devenue cruciale pour les États membres, de même que le **rôle d'Europol aux côtés des États membres dans leurs partenariats avec des pays tiers** ou des entités situées dans ces pays. Des efforts supplémentaires seront **essentiels à l'avenir** pour renforcer la sécurité mondiale[9].

Le règlement (UE) 2022/991 a déjà apporté des modifications substantielles au règlement Europol afin de renforcer la **dimension extérieure des activités d'Europol**, notamment en facilitant l'échange d'informations avec les pays tiers[10] et en exigeant d'Europol qu'elle inclue

---

7 Cette évaluation effectuée conformément à l'article 68, paragraphe 3, du RE n'est pas celle prévue par les lignes directrices pour une meilleure réglementation en vue d'une éventuelle proposition de révision du règlement Europol. Voir à cet égard le point 4 ci-dessous.

8 Charte des droits fondamentaux de l'Union européenne, JO C 326 du 26.10.2012, p. 391, ELI: https://eur-lex.europa.eu/eli/treaty/char_2012/oj?locale=fr.

9 Voir ProtectEU: une stratégie européenne de sécurité intérieure, COM(2025) 148 final du 1er avril 2025, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52025DC0148.

10 Voir, par exemple, l'article 25, paragraphe 4 *bis*, du RE, qui prévoit la possibilité pour Europol de transférer des données vers des pays tiers sur la base d'une autoévaluation par Europol de l'ensemble des circonstances entourant le transfert de données à caractère personnel et concluant à l'existence de garanties appropriées en ce qui concerne la protection des données à caractère personnel, et l'article 25, paragraphe 5,

une stratégie pour les relations avec les pays tiers et les organisations internationales dans sa programmation pluriannuelle et ses programmes de travail annuels[11].

L'**article 4, paragraphe 1, point t), du RE** a confié une nouvelle mission à Europol: aider les États membres à traiter les données fournies par des pays tiers ou des organisations internationales sur les personnes impliquées dans le terrorisme ou dans la criminalité grave. Il s'agit notamment de **proposer aux États membres l'introduction éventuelle de signalements pour information concernant des ressortissants de pays tiers dans l'intérêt de l'Union dans le système d'information Schengen (SIS).** Cette nouvelle catégorie de signalements pour information a été introduite en 2022[12], à la suite d'une modification du règlement (UE) 2018/1862 sur l'utilisation du SIS dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale[13].

Certaines informations, en particulier lorsque la personne concernée n'est pas citoyenne de l'UE et qu'il n'y a pas de lien avec une affaire nationale, ne sont partagées par le pays tiers qu'avec Europol, qui traite les données et partage les résultats de ses analyses avec tous les États membres. L'objectif des nouvelles dispositions était de **maximiser l'exploitation des informations** reçues par Europol de la part des pays tiers en les rendant plus accessibles que si elles n'étaient disponibles que par l'intermédiaire du système d'Europol. Elles complétaient d'autres mesures, telles que le portail de recherche européen (ESP) et le cadre d'interopérabilité[14] entre les systèmes d'information de l'UE pour la sécurité, les frontières et la gestion des migrations, en remédiant aux lacunes structurelles des systèmes qui entravent le travail des autorités nationales, et notamment des garde-frontières.

Le **SIS** est considéré comme un **canal de diffusion supplémentaire essentiel:** il s'agit de la base de données la plus utilisée en Europe en matière répressive, de contrôle des frontières et de migration. En 2024, plus de 15 milliards de recherches ont été effectuées dans le SIS contre environ 14 millions de recherches dans le système d'information Europol (SIE) et moins de 3 milliards de recherches (dans le monde) dans les 19 bases de données d'Interpol, qui sont les deux autres systèmes d'information les plus utilisés par les autorités compétentes[15].

(2) Innovation: article 18, paragraphe 2, point e) et article 33 *bis* du RE sur le traitement des données à caractère personnel par Europol pour des projets d'innovation et de recherche

Les **évolutions technologiques** présentent à la fois d'énormes possibilités et des défis considérables pour la sécurité intérieure[16] de l'UE et ont eu une incidence si profonde sur la criminalité qu'elles en modifient même la nature profonde des menaces que représente la grande criminalité organisée[17]. Les criminels sont prompts à intégrer les nouvelles technologies

---

du RE qui étend le champ d'application des cas exceptionnels dans lesquels Europol peut transférer au cas par cas, dans des cas dûment justifiés, des (catégories de) données à des pays tiers et à des organisations internationales.

11 Article 12, paragraphe 2, du RE.

12 Règlement (UE) 2022/1190; JO L 185 du 12.7.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/1190/oj.

13 Règlement (UE) 2018/1862; JO L 312 du 7.12.2018, p. 56, ELI: http://data.europa.eu/eli/reg/2018/1862/oj.

14 Règlement (UE) 2019/818; JO L 135 du 22.5.2019, p. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj.

15 Rapport annuel 2024 d'eu-LISA sur le SIS, disponible en ligne sur https://www.eulisa.europa.eu/sites/default/ fichiers/documents/sis-annual-report-2024.pdf, Europol, rapport d'activité annuel consolidé (RAAC) 2024, disponible en ligne sur https://www.europol.europa.eu/cms/sites/default/files/documents/Consolidated_Annual_Activity_Report_2024.PDF et https://www.interpol.int/How-we-work/Databases.

16 Europol, Évaluation de la menace que représente la criminalité organisée sur l'internet (iOCTA) 2024, disponible en ligne sur Internet Organised Crime Threat Assessment (IOCTA) 2024 Europol.

17 Europol, SOCTA UE 2025, p. 19.

dans leurs activités, créant de nouveaux modèles commerciaux et affinant leurs tactiques. Dans le même temps, ces avancées offrent **aux services répressifs des possibilités sans précédent de renforcer leurs capacités**. Par conséquent, la recherche et l'innovation jouent un rôle crucial dans la sécurité intérieure en ce qu'elles contribuent à élaborer des solutions pour contrer les menaces émergentes et pour suivre l'évolution rapide des formes et des modes opératoires des réseaux criminels, y compris ceux résultant de l'utilisation abusive des technologies. L'Union a investi et continuera d'investir dans le développement d'outils innovants en finançant la recherche et l'innovation en matière de sécurité, dans le cadre de **ProtectEU**, la stratégie européenne de sécurité intérieure[18].

Créé fin 2019, lors du mandat des ministres JAI des États membres de l'UE, le **laboratoire d'innovation Europol (EIL)**[19] vise à renforcer l'engagement d'Europol en faveur de l'innovation en matière répressive. Le règlement (UE) 2022/991 a apporté des modifications substantielles au règlement Europol afin de renforcer le mandat d'Europol en matière d'innovation, afin à la fois de soutenir le potentiel de l'EIL et de promouvoir les synergies avec d'autres activités de recherche et d'innovation au niveau de l'UE, notamment au sein de la Commission, dans le cadre du **pôle d'innovation de l'UE** pour la sécurité intérieure[20].

L'article 18, paragraphe 2, du RE relatif aux finalités des activités de traitement de l'information a été modifié afin de permettre à Europol de **traiter des données opérationnelles à caractère personnel** également **pour des projets de recherche et d'innovation.** La disponibilité d'ensembles de données de haute qualité pour tester de manière empirique la validité des nouveaux outils est largement considérée comme une condition préalable essentielle au développement des technologies. En revanche, des ensembles de données non fiables ou biaisés dans le cadre de l'expérimentation peuvent conduire à la production de technologies médiocres[21].

Des garanties sur mesure en matière de protection des données pour ce type de traitement ont été prévues à l'article 18, paragraphe 3 *bis*, à l'article 30, paragraphes 2 et 3, et à l'**article 33 *bis* du RE**. Cette dernière disposition exigeait la mise en place d'un **environnement «bac à sable»** en prévoyant que toute donnée à caractère personnel traitée dans le cadre d'un projet doit être temporairement copiée dans un environnement de traitement de données distinct, isolé et protégé au sein d'Europol pour être utilisée uniquement pour ce projet.

(3) <u>Enquêtes pénales:</u> article 18, paragraphe 6 *bis*, et article 18 *bis* du RE sur les conditions de traitement des données à caractère personnel reçues sans catégorisation des personnes concernées

En tant que **pôle d'information sur la criminalité de l'UE**, Europol facilite non seulement la collecte et l'échange d'informations, mais contribue également à **accroître l'efficacité des enquêtes grâce à une analyse avancée des données** et à la détection de liens entre les infractions pénales et les réseaux criminels par-delà les frontières qui ne sont pas visibles au niveau national. Ces capacités soutiennent les États membres en enrichissant les informations disponibles pour leurs enquêtes pénales.

Avec l'utilisation intensive à grande échelle de la technologie, les **ensembles de données vastes et complexes sont devenus la norme dans tous les aspects de la vie**, y compris la

---

18 COM(2025) 148 final du 1er avril 2025, https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:52025DC0148, p. 9.

19 https://www.europol.europa.eu/how-we-work/innovation-lab.

20 Voir, en particulier, l'article 4, paragraphe 1, points v) et w), du RE.

21 SWD(2020) 543 final du 9 décembre 2020, p. 29.

criminalité[22]. Les enquêtes sur la criminalité organisée ou le terrorisme ont commencé à relever le défi de l'analyse de volumes importants de données stockées par voie électronique, qui se mesurent souvent en téraoctets, y compris les données audio, vidéo et générées par des machines saisies au cours des enquêtes. Par exemple, dans le cadre de l'enquête conjointe visant à démanteler le réseau EncroChat[23], les enquêteurs ont analysé des millions de messages échangés par des criminels pour planifier des crimes graves. Dans ce contexte, la disponibilité des outils, de l'expertise et des ressources des technologies de l'information et de la communication (TIC) nécessaires pour analyser des ensembles de données vastes et complexes (on parle de «mégadonnées» ou de «données massives» dans le jargon technique[24]) est essentielle pour les autorités répressives et judiciaires.

Bien que le règlement Europol adopté en 2016 n'impose pas de restrictions en tant que telles à l'analyse des mégadonnées, il manquait des dispositions structurées fixant les conditions de l'analyse de ce type de données. Le **point le plus critique** était l'**exigence relative à la catégorisation des personnes concernées**. La catégorisation des personnes concernées fait référence à la nécessité d'examiner les ensembles de données afin de trier les données à caractère personnel en fonction de différentes catégories, énumérées de manière exhaustive à l'annexe II.A et à l'annexe II.B. du règlement Europol, avant de procéder au traitement effectif des données à des fins d'enquête, y compris avant de recouper les données afin de détecter des liens ou de procéder à des analyses de nature stratégique ou thématique ou à des analyses opérationnelles[25]. Les catégories concernées sont liées à différents types de participation à des enquêtes pénales, y compris i) les suspects, les futurs contrevenants potentiels; ainsi que ii) les contacts, les associés, les victimes, les témoins et les informateurs associés à des activités criminelles. D'une manière générale, Europol ne peut pas traiter, ni même stocker, les données à caractère personnel de personnes qui ne relèvent d'aucune de ces catégories.

Les fournisseurs de données, tels que les **États membres** ou les **organes et agences de l'UE**, procèdent **généralement** déjà à une catégorisation des personnes concernées avant de transférer les données à caractère personnel à Europol[26]. En vertu du droit de l'Union, ils sont tous tenus de procéder à une catégorisation des personnes concernées dans le cadre de leurs propres traitements et enquêtes, indépendamment du transfert de données à Europol, et sur la base de règles équivalentes, mais non identiques, à celles d'Europol[27]. Toutefois, pour les ensembles de données vastes et complexes, la préparation manuelle des données est un exercice

---

22 Europol, SOCTA UE 2025, *passim*.

23 https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochatcommunications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized.

24 CEPD, avis nº 7/2015, p. 7, disponible à l'adresse https://www.edps.europa.eu/sites/default/files/publication/15-11-19_big_data_fr.pdf. «De façon générale, le dénominateur commun de toutes les définitions disponibles veut que les "**données massives**" fassent référence à la pratique qui consiste à combiner d'énormes volumes d'informations provenant de différentes sources et à les analyser en utilisant des algorithmes plus complexes pour mieux étayer les décisions. Les données massives dépendent non seulement de la capacité accrue de la technologie à supporter la collecte et le stockage de grandes quantités de données, mais également de sa capacité à analyser, comprendre et exploiter pleinement la valeur de ces données (en particulier, grâce à des applications d'analyse)».

25 Voir l'article 18, paragraphe 2, du RE.

26 Les États membres transfèrent des données à Europol par l'intermédiaire de son application de réseau d'échange sécurisé d'informations (SIENA), laquelle rend la catégorisation des personnes concernées obligatoire.

27 Voir, par exemple, l'article 6 de la directive (UE) 2016/680 (la «directive en matière de protection des données dans le domaine répressif» en ce qui concerne les autorités indirectement compétentes); JO L 119 du 4.5.2016, p. 89, ELI: http://data.europa.eu/eli/dir/2016/680/oj; l'article 51 du règlement (UE) 2017/1939 du Conseil («règlement sur le Parquet européen»); JO L 283 du 31.10.2017, p. 1, ELI: http://data.europa.eu/eli/reg/2017/1939/oj; l'article 27, paragraphe 3, du règlement (UE) 2018/1727 («règlement Eurojust»); JO L 295 du 21.11.2018, p. 138, ELI: http://data.europa.eu/eli/reg/2018/1727/oj.

exigeant en termes de ressources et de temps. L'analyse des données dans un seul téléphone portable peut prendre jusqu'à trois jours, si elle est semi-automatisée, et des centaines de téléphones portables peuvent être saisis au cours d'une enquête. La catégorisation des personnes concernées **pour les mégadonnées** n'est **pas toujours possible**, compte tenu du volume des ensembles de données, de la manière dont les données sont (non) structurées, du manque de ressources ou de l'**effort manuel excessif requis**. Dans la pratique, la seule possibilité est d'analyser d'abord les données de manière plus approfondie d'un point de vue opérationnel ou de détecter les liens, également de manière semi-automatisée, en recoupant les données disponibles.

Le règlement (UE) 2022/991 a clarifié les conditions dans lesquelles la catégorisation des personnes concernées contribue à la **sécurité juridique** du traitement des ensembles de données vastes et complexes. Europol et le Contrôleur européen de la protection des données (CEPD) avaient des interprétations divergentes de la lettre et de l'esprit du règlement Europol en ce qui concerne la durée de conservation des données applicable. Selon Europol, cette période devrait être de trois ans; selon le CEPD, elle devrait être de six mois[28]. De nouvelles dispositions ont également été nécessaires pour offrir une **flexibilité supplémentaire**, en établissant un juste équilibre entre les aspects liés à la protection des données et à la sécurité.

L'article 18, paragraphe 5 *bis*, du RE, lu en combinaison avec l'article 73 du RPDUE, a d'abord clarifié le principe général de la catégorisation des personnes concernées en vertu de l'article 18, paragraphe 2, et de l'annexe II. Europol a pour mission, le cas échéant et dans la mesure du possible, d'**attribuer clairement des données à caractère personnel à une catégorie spécifique de personnes concernées**. En pratique, en règle générale, Europol devrait déterminer le rôle précis dans l'activité criminelle (par exemple, si une personne est un suspect, une victime ou seulement un témoin) pour chaque personne dont les données à caractère personnel seront traitées, et non à un niveau agrégé pour toutes les personnes figurant dans un fichier de données à traiter, ou une partie de celui-ci (par exemple, en établissant simplement que toutes les personnes mentionnées sont impliquées dans une activité criminelle relevant de son mandat, sur la base d'un examen des circonstances générales qui ont généré le fichier de données) avant que les données à caractère personnel puissent être traitées.

L'article 18, paragraphe 6 *bis*, du RE autorise explicitement le traitement de données à caractère personnel reçues sans catégorisation des personnes concernées **pour une durée ne dépassant pas 18 mois**, qui peut être prolongée sans dépasser 36 mois dans des cas justifiés, uniquement **aux fins de l'achèvement de la catégorisation des personnes concernées**. L'article 18, paragraphe 6 *bis*, du RE ne fait pas explicitement référence à des ensembles de données vastes et complexes, mais, plus généralement, exige un critère de «**stricte nécessité**».

L'article 18 *bis* du RE prévoit une dérogation en permettant à Europol de traiter des données à caractère personnel reçues d'une **autorité compétente**, du **Parquet européen** ou d'**Eurojust**, lorsque cela est nécessaire pour soutenir une **enquête pénale en cours**, sans qu'il soit nécessaire de procéder à la catégorisation des personnes concernées, si cela n'a pas déjà été effectué, et au-delà des catégories de personnes concernées énumérées dans le règlement Europol. Europol peut traiter les données au moyen d'une **analyse opérationnelle** ou, dans des cas exceptionnels et dûment justifiés, en **effectuant des recoupements** afin de trouver des connexions ou d'autres liens pertinents. Cette dérogation visait à remédier aux différences entre les règles relatives à la catégorisation des personnes concernées applicables à Europol et celles applicables aux autorités compétentes, au Parquet européen et à Eurojust.

[28] https://www.edps.europa.eu/system/files/2022-01/22-01-10-edps-decision-europol_en.pdf.

(4) <u>Coopération avec des tiers:</u> articles 26, 26 *bis* et 26 *ter* du RE sur l'échange de données à caractère personnel entre Europol et des parties privées

Les criminels abusent de plus en plus des services (transfrontières) de parties privées – services de télécommunications basés sur l'internet, services financiers et services de télécommunications classiques. Par conséquent, **les parties privées détiennent un grand nombre de données à caractère personnel pertinentes pour les enquêtes pénales**. En particulier, l'internet a créé un espace public qui est effectivement aux mains des privés, ce qui rend difficile d'appliquer les règles <u>en ligne</u> aussi efficacement que <u>hors ligne</u> dans un contexte répressif[29].

Dans ce contexte, la **coopération entre les autorités répressives et les parties privées** est devenue **indispensable**. Comme indiqué dans **ProtectEU**, la stratégie européenne de sécurité intérieure, il sera essentiel de renforcer les partenariats avec le secteur privé afin de faciliter l'échange d'informations[30]. Les chefs de police ont également appelé, dans leur déclaration commune sur l'avenir d'Europol[31], à faire d'Europol un «**point d'accès essentiel pour l'obtention d'informations auprès d'entités privées**». La nature de cette collaboration va du partage d'informations à la fourniture de données commerciales libres, en passant par la participation à des projets de recherche et d'innovation et la prestation de services qui soutiennent le fonctionnement des entreprises[32]. Par exemple, en 2025, Europol a contribué au démantèlement de Lumma Stealer, la menace la plus importante au monde en matière de vol d'informations, grâce à la coopération de Microsoft, qui avait recensé plus de 394 000 ordinateurs Windows dans le monde infectés par le logiciel malveillant Lumma[33].

Le règlement (UE) 2022/991 a introduit des **possibilités supplémentaires** pour Europol d'échanger des données à caractère personnel avec des parties privées. Auparavant, Europol ne pouvait recevoir des données à caractère personnel de parties privées que par l'intermédiaire d'une unité nationale Europol (UNE), ou par l'intermédiaire de points de contact désignés au préalable ou d'autorités de pays tiers ou d'organisations internationales. La finalité du traitement d'Europol se limitait à identifier l'UNE concernée, ou le point de contact ou l'autorité du pays tiers et de l'organisation internationale qui pourrait assumer la responsabilité de l'affaire.

L'**article 26 modifié du RE a élargi la mission d'Europol**, lui permettant de traiter de manière exhaustive les informations (y compris les données à caractère personnel) provenant de parties privées. L'une des finalités principales du traitement est restée l'identification de l'unité nationale Europol (UNE) concernée. Toutefois, Europol est désormais également autorisé à compléter les informations par sa propre analyse afin de faciliter le traitement ultérieur d'une affaire au niveau national.

Outre les dispositions horizontales de l'article 26 du RE, l'article 26 *bis* introduit des règles pour les **situations de crise en ligne** et l'article 26 *ter* traite de la **diffusion en ligne de matériel pédopornographique**. Dans ces cas, Europol peut aider les États membres en traitant

---

29 SWD(2020) 543 final du 9 décembre 2020, p. 16 et 17.

30 Voir ProtectEU: une stratégie européenne de sécurité intérieure, p. 6.

31 https://prezydencja.policja.pl/ppl/aktualnosci/260402,Wspolna-Deklaracja-Europejskich-Szefow-Policji-w-sprawie-przyszlosci-Europolu-Jo.html.

32 Europol, Coopération avec les parties privées, 31 mai 2023, EDOC #1306090v13. Voir également Milieu Consulting, Study on the Practice of direct exchanges with of personal data between Europol and Private Parties, rapport final, septembre 2020.

33 https://www.europol.europa.eu/media-press/newsroom/news/europol-and-microsoft-disrupt-world's-largest-infostealer-lumma. Plus d'exemples sont fournis dans le document de travail des services de la Commission qui accompagne la présente communication.

des données à caractère personnel reçues directement de parties privées. Europol peut également transmettre des données à caractère personnel à des parties privées au cas par cas.

Le règlement (UE) 2022/991 a introduit la possibilité d'utiliser l'infrastructure d'Europol pour l'échange d'informations entre les autorités compétentes et des parties privées, ainsi que la possibilité pour Europol de demander aux États membres d'obtenir, conformément à leur législation nationale, des données à caractère personnel auprès de parties privées.

Ces dispositions ont été adoptées en cohérence avec d'autres initiatives, telles que le règlement sur les contenus à caractère terroriste en ligne[34] et le règlement sur les services numériques[35]. D'autres mesures visant à renforcer la participation des parties privées à la lutte contre la criminalité et à faciliter l'accès légal aux données sont envisagées pour concrétiser «l'ambition d'un changement de culture en matière de sécurité» (**approche englobant l'ensemble de la société**) dans le cadre de **ProtectEU**, la stratégie européenne de sécurité intérieure[36].

(5) Contrôle interne et externe du respect des droits fondamentaux par Europol

Le règlement (UE) 2022/991 souligne l'obligation d'Europol de respecter les droits fondamentaux en vertu des dispositions définissant les missions d'Europol et les garanties connexes renforcées, notamment en **consolidant le contrôle interne et externe de l'Agence**.

Dans le domaine de la protection des données, l'alignement du règlement Europol sur les garanties en matière de protection des données prévues par le RPDUE a nécessité l'introduction de nouvelles règles pour le contrôle par le **délégué à la protection des données** (DPD) et le **Contrôleur européen de la protection des données** (CEPD). Par exemple, l'obligation de fournir une analyse d'impact relative à la protection des données (AIPD) et la consultation préalable du CEPD sont devenues systématiques pour tout nouveau type de traitement. Le règlement (UE) 2022/991 a également introduit une nouvelle compétence pour Europol en ce qui concerne les demandes de droits d'accès. Auparavant, les autorités nationales compétentes étaient chargées de traiter les demandes de droits d'accès si les États membres étaient les fournisseurs de données.

Le règlement (UE) 2022/991 a également créé un **nouveau poste d'officier aux droits fondamentaux** au sein d'Europol, qui est notamment chargé d'informer le directeur exécutif d'Europol d'éventuelles violations des droits fondamentaux dans le cadre des activités de l'Agence.

En outre, le **contrôle démocratique et la responsabilité** ont été **renforcés** grâce au contrôle politique des activités d'Europol par le **Parlement européen et les parlements nationaux**, comme le prévoit l'article 88, paragraphe 2, deuxième alinéa, du traité sur le fonctionnement de l'Union européenne (TFUE). Le règlement (UE) 2022/991 a renforcé le suivi assuré par le **groupe de contrôle parlementaire conjoint**[37]. Par exemple, il a prévu la consultation obligatoire du groupe sur le projet de programmation pluriannuelle et le programme de travail annuel d'Europol, la possibilité pour le groupe d'adresser des recommandations spécifiques non contraignantes à Europol et de les soumettre au Parlement européen et aux parlements nationaux, ainsi que la création d'un forum consultatif pour assister le groupe, sur demande, en fournissant des conseils en toute indépendance dans les matières concernant les droits fondamentaux.

3. Principales conclusions de l'évaluation

[34] Règlement (UE) 2021/784; JO L 172 du 17.5.2021, p. 79. ELI: http://data.europa.eu/eli/reg/2021/784/oj.
[35] Règlement (UE) 2022/2065; JO L 277 du 27.10.2022, p. 1. ELI: http://data.europa.eu/eli/reg/2022/2065/oj.
[36] Voir ProtectEU: une stratégie européenne de sécurité intérieure, p. 2.
[37] Voir https://www.europarl.europa.eu/relnatparl/en/eu-agencies-oversight/jpsg-on-europol.

3.1. État d'avancement de la mise en œuvre opérationnelle des nouvelles compétences et missions d'Europol en matière de traitement des données à caractère personnel

Le règlement (UE) 2022/991 est entré **en vigueur le 28 juin 2022**. Toutefois, sa mise en œuvre opérationnelle dépendait de diverses mesures de gouvernance, techniques et administratives, ainsi que d'exigences opérationnelles, telles que la mise en place de nouvelles structures TIC dans certains cas.

Trois ans plus tard, **presque toutes les dispositions** énumérées à l'article 68, paragraphe 3, du règlement (UE) 2022/991 **sont devenues opérationnelles.** Les dispositions relatives à l'analyse d'ensembles de données vastes et complexes (article 18, paragraphe 6 *bis*, et article 18 *bis* du RE) et à la coopération avec des parties privées (articles 26, 26 *bis* et 26 *ter* du RE) ont commencé à s'appliquer à partir du 28 juin 2022, ou peu après. Le traitement des données à caractère personnel pour des projets de recherche et d'innovation [article 18, paragraphe 2, point e), du RE] a débuté en 2023 après que l'environnement «bac à sable», dénommé ODIN, a été mis en place pour satisfaire aux exigences spécifiques en matière de protection des données prévues à l'article 33 *bis* du RE. Au 29 juin 2025, la possibilité pour Europol de proposer aux États membres des **signalements pour information dans le SIS** conformément à l'article 4, paragraphe 1, point t), du RE n'était pas encore devenue opérationnelle, étant donné que la mise en œuvre technique du nouveau type de signalement est toujours en cours. La mise en service est **prévue pour 2026**.

3.2. Évaluation de l'incidence opérationnelle des nouvelles compétences et missions d'Europol en matière de traitement des données à caractère personnel sur les objectifs de l'Agence au titre de l'article 3 du RE

En ce qui concerne l'incidence opérationnelle des nouvelles compétences et missions d'Europol en matière de traitement des données à caractère personnel, il est ressorti de la consultation que **les États membres conservent une opinion globalement favorable** quant à leur pertinence, leur efficacité et leur valeur ajoutée, ainsi qu'au soutien d'Europol à leurs autorités compétentes dans les domaines connexes[38].

Les pouvoirs d'enquête couverts par cette évaluation ne sont pas utilisés de manière continue ou systématique pour traiter des données à des fins de contrôle; certains ont même un caractère exceptionnel, tandis que d'autres sont utilisés plus régulièrement en fonction des besoins dans les enquêtes. L'**utilisation opérationnelle des nouvelles dispositions** au cours de la période de référence a **considérablement varié** sur le **plan quantitatif**, en fonction des caractéristiques techniques et des conditions juridiques différentes associées aux nouvelles dispositions.

Europol a reçu un nombre **non négligeable** de **nouvelles contributions sans catégorisation des personnes concernées** de la part des États membres au titre de l'article 18, paragraphe 6 *bis*, du RE, soit 653 en 2023 et 597 en 2024. Il n'y a pas eu d'augmentation à court terme des contributions sans catégorisation des personnes concernées, et le nombre de cas dans lesquels l'article 18, paragraphe 6 *bis*, a été appliqué est resté **stable** par rapport à des cas équivalents au cours de la période antérieure au 28 juin 2022. Les nouvelles dispositions n'ont pas non plus eu d'incidence négative sur l'engagement des États membres à procéder à la catégorisation des personnes concernées[39]. Entre 2023 et 2024, la part des contributions sans

[38] Voir les éléments de preuve présentés à la section 5 du document de travail des services de la Commission accompagnant le présent rapport, et en particulier les observations d'Europol et les réponses des États membres aux questions 2, 4 et 5 du questionnaire succinct du 2 juin 2025, à l'annexe III du document de travail des services de la Commission.

[39] Comme l'a souligné un État membre au cours de la consultation, «[les États membres] peuvent clairement distinguer le type de données qu'[ils] traitent, lesquelles peuvent être très importantes dans le cadre de l'enquête elle-même».

catégorisation des personnes concernées représentait **moins de 1 % de l'ensemble des contributions** acceptées par Europol de la part des États membres (0,85 % en 2023 et 0,71 % en 2024). Depuis juin 2022, Europol a toujours achevé la catégorisation des personnes concernées dans un délai de 18 mois, sans utiliser le délai prolongé de 36 mois. Europol et six États membres ont souligné que, malgré l'amélioration de la sécurité juridique, la **charge administrative restait importante** tant pour Europol que pour les autorités compétentes en raison des efforts requis pour se conformer à la catégorisation des données à caractère personnel selon la participation de chacun à l'infraction pénale. Cette exigence est mise en œuvre de manière très stricte par Europol[40].

Europol a indiqué que l'échange d'informations avec des **parties privées** était encore négligeable en 2023, étant donné que seuls 26 cas de mise en œuvre de l'article 26 du RE ont été enregistrés (en plus des cas relevant de la législation sur les services numériques)[41]. Toutefois, en **2024**, les statistiques ont **fortement augmenté pour atteindre 284 cas** (près de + 1 000 %) de coopération avec des parties privées au titre de l'article 26 du RE. Étaient particulièrement concernées les données provenant d'entreprises privées pour enquêter sur la **criminalité financière et économique**. Europol a également fait un usage important de l'article 26 *ter* du RE dans la lutte contre l'exploitation sexuelle des enfants, où la coopération avec des parties privées était déjà très importante auparavant. Dans les deux cas, les données incluent également la coopération qui était possible dans le cadre juridique précédent. Les données disponibles ne révèlent pas dans quelle mesure ces nouveaux cas relèvent des nouvelles dispositions, pas plus qu'elles ne font état d'un recours accru aux possibilités existantes.

En **2025**, Europol a adopté une **nouvelle stratégie** visant à renforcer encore la coopération avec les parties privées. En outre, des mesures ont été prises pour moderniser l'infrastructure TIC d'Europol à la disposition des autorités compétentes pour l'échange d'informations avec des parties privées. En **2023**, Europol a lancé la *Plateforme européenne de retraits de contenus illégaux sur Internet* (**PERCI**) afin de faciliter la mise en œuvre du règlement sur les contenus à caractère terroriste en ligne et potentiellement, à l'avenir, de l'article 18 du règlement sur les services numériques, ainsi que le *service européen de signalement des abus sexuels sur enfants* (**EU CARES**). PERCI n'est pas intégré dans le système d'information Europol (SIE)[42].

D'autres dispositions n'ont **pas été utilisées** du tout (article 26 *bis* du RE), bien qu'elles soient opérationnelles, **ou** n'ont été appliquées **qu'à titre exceptionnel** [un cas dans lequel l'article 18 *bis* du RE a été utilisé en 2024 et un projet réalisé avec le traitement de données à caractère personnel au titre de l'article 18, paragraphe 1, point t), du RE en 2025, trois nouveaux projets étant déjà en préparation].

En raison de la période limitée de mise en œuvre opérationnelle des dispositions introduites par le règlement (UE) 2022/991 et de la longueur des enquêtes pénales et des procédures judiciaires, les États membres n'ont pas été en mesure de fournir des données quantitatives sur l'incidence de ces dispositions sur le plan opérationnel. Ils ont plutôt proposé quelques exemples d'enquêtes réussies qui démontrent les **avantages tangibles des nouvelles possibilités d'enquête en situation réelle** pour les dispositions déjà utilisées, telles que les enquêtes concernant EncroChat, Sky ECC, les réseaux criminels basés dans les Balkans impliqués dans le trafic de cocaïne ou Lumma Stealer.

---

40 Voir la sous-section 7.1.3 du document de travail des services de la Commission accompagnant le présent rapport et les réponses des États membres à la question 9 du questionnaire succinct du 2 juin 2025, à l'annexe III du document de travail des services de la Commission.

41 Europol, rapport 2023 présenté conformément à l'article 16, paragraphe 11, du RE.

42 Règlement (UE) 2019/818; JO L 135 du 22.5.2019, p. 85, ELI: http://data.europa.eu/eli/reg/2019/818/oj.

Europol et huit États membres ont également signalé **quelques points à améliorer** afin de maximiser l'utilisation efficace et cohérente du nouveau cadre juridique et de renforcer le rôle d'Europol à l'avenir. Il existe des craintes, notamment de la part d'Europol, que la complexité, la fragmentation et la longueur excessives des dispositions juridiques ne découragent les praticiens ou les parties privées d'utiliser les nouveaux instruments disponibles. Les observations des États membres portent plutôt sur la manière dont Europol met en œuvre de manière restrictive les garanties en matière de protection des données sous le contrôle du CEPD, ce qui risque de compromettre l'efficacité et la valeur ajoutée de certaines dispositions.

3.3. Évaluation de l'incidence des nouvelles compétences et missions d'Europol en matière de traitement des données à caractère personnel sur les droits fondamentaux

La Commission n'a trouvé **aucune** preuve d'une incidence négative sur les **droits fondamentaux** résultant de l'utilisation opérationnelle des nouvelles compétences en matière de traitement des données à caractère personnel en raison de l'utilisation limitée faite jusqu'à présent desdites compétences.

Outre la mise en œuvre des exigences spécifiques en matière de protection des données associées aux nouvelles compétences en matière de traitement des données à caractère personnel, Europol a progressivement pris toutes les mesures nécessaires pour mettre en œuvre les nouveaux mécanismes de contrôle horizontal liés aux droits fondamentaux.

En 2024, le conseil d'administration d'Europol a adopté les modalités d'application révisées du DPD, qui constituent l'un des derniers actes d'exécution nécessaires liés au nouveau régime de protection des données. Les éléments recueillis laissent entendre qu'Europol et son conseil d'administration ont également assuré, en coopération avec le DPD d'Europol et le CEPD, une **mise en œuvre rigoureuse des nouvelles garanties en matière de protection des données** introduites en 2022. Cette approche, à première vue, a effectivement empêché toute incidence négative ou ingérence causée par l'utilisation initiale des nouvelles compétences en matière de traitement des données à caractère personnel avec les droits des personnes au respect de la vie privée et à la protection des données à caractère personnel. Selon les États membres, Europol dispose actuellement d'un **cadre juridique solide en matière de protection des données**, qui apporte des garanties suffisantes en cas de recours accru à ses nouvelles compétences. Sept États membres ont également souligné que ce cadre **facilite la circulation des informations** en renforçant la confiance, même si des améliorations sont encore possibles. Un seul État membre a exprimé un avis négatif[43].

Outre les **défis** spécifiques liés à la catégorisation des personnes concernées, Europol et quatre États membres ont mentionné les coûts et le temps associés à l'**analyse d'impact relative à la protection des données** (AIPD) et à la **consultation préalable** du CEPD, qui sont en pratique réalisées par défaut, parmi les points à améliorer. Un autre défi soulevé par six États membres est le traitement par Europol des **demandes d'accès des personnes concernées,** pour lesquelles elle est désormais compétente, même lorsqu'un État membre est le propriétaire des données.

Le **premier officier aux droits fondamentaux** a été nommé en décembre **2022**. Au cours des deux premières années de son mandat, il n'a reçu ni présenté **aucune plainte** au directeur exécutif. Le groupe de contrôle parlementaire conjoint a continué de suivre de près les activités d'Europol et n'a formulé aucune recommandation depuis l'entrée en vigueur des nouvelles

[43] Voir les réponses des États membres à la question 9 du questionnaire succinct du 2 juin 2025, à l'annexe III du document de travail des services de la Commission.

dispositions. Le Parlement européen a créé le **forum consultatif du groupe de contrôle parlementaire conjoint sur les droits fondamentaux** en février **2024**.

3.4. Analyse coûts-avantages des nouvelles compétences et missions d'Europol en matière de traitement des données à caractère personnel

Compte tenu du stade précoce de la mise en œuvre des dispositions introduites par le règlement (UE) 2022/991 et de l'expérience limitée acquise avec celles-ci, il est **prématuré** que la Commission tire des conclusions utiles sur les nouvelles dispositions à partir d'une **analyse coûts-avantages**.

Les services de la Commission ont recueilli auprès d'Europol des informations sur les coûts supportés à ce jour dans le cadre de la mise en œuvre opérationnelle du règlement (UE) 2022/991, pour les dispositions faisant l'objet du réexamen. Ces coûts se sont élevés à environ **25 millions d'EUR** (environ 5 % de l'enveloppe totale allouée à Europol[44]) entre 2022 et 2025, comprenant principalement des coûts ponctuels. À ce jour, les États membres n'ont supporté aucun nouveau coût spécifiquement lié au règlement (UE) 2022/991 digne d'être pris en considération.

La plupart des coûts (près de 17 millions d'EUR) consistaient en des investissements importants dans le **développement de nouvelles structures TIC**, dans la mise en œuvre des dispositions relatives à la recherche et à l'innovation (le bac à sable ODIN) et dans l'échange de données à caractère personnel avec des parties privées (PERCI et EU CARES). Les coûts des **ressources humaines (RH)**, liés à la fois aux TIC et aux opérations, représentaient environ un tiers des dépenses totales (environ 8 millions d'EUR). Les RH représenteront les **principaux coûts récurrents à long terme**.

Il convient de noter que les 8 millions d'EUR susmentionnés ne comprennent pas les coûts des ressources humaines pour l'unité de gestion de l'information ni les ressources associées aux mesures de contrôle (précédentes et nouvelles) qui ont un caractère horizontal et pour lesquelles une ventilation au niveau de la mise en œuvre des dispositions spécifiques n'est pas possible. Les coûts de ces ressources ne sont pas négligeables. Par exemple, en 2023, on a estimé que **60 équivalents temps plein (ETP)** (près de **5 %** du personnel d'Europol) participaient à des activités au sein des **organes d'assurance/de contrôle et des entités de contrôle/consultatives**. Europol a affecté 25 ETP aux travaux consacrés au contrôle de la protection des données et aux actions d'assurance correspondantes. Il s'agit notamment du suivi des recommandations du CEPD, ainsi que des travaux générés dans le cadre des consultations préalables pour le traitement opérationnel des données. Seize de ces 25 ETP sont spécifiquement engagés dans des activités liées aux exigences du CEPD. Depuis juin 2025, Europol dispose d'une équipe spécialisée de huit personnes travaillant à temps plein dans le domaine de la protection des données, dont le DPD.

Selon Europol et quinze États membres, les **avantages** des nouvelles compétences et missions en matière de traitement des données à caractère personnel, en particulier l'analyse d'ensembles de données vastes et complexes, ainsi que la coopération avec des parties privées, devraient être importants et **largement compenser les coûts associés**. Aucun État membre n'a exprimé un point de vue différent. Certains gains d'efficacité sont raisonnablement attendus à long terme, grâce aux économies d'échelle et à la diminution des coûts marginaux. Un État membre a souligné qu'«il est important qu'Europol apporte les ressources informatiques

[44] Au cours de la même période, le budget alloué à Europol s'élevait globalement à environ **860 millions d'EUR** (passant progressivement de 192 millions d'EUR en 2022 à 241 millions d'EUR en 2025). Pour de plus amples informations, voir document de travail des services de la Commission accompagnant le présent rapport.

nécessaires pour fournir et développer les outils nécessaires à la mise en œuvre des nouvelles possibilités prévues par le règlement (UE) 2022/991», un constat auquel se sont ralliés deux autres États membres et d'autres parties prenantes[45].

De l'avis d'Europol et de cinq États membres, les éventuels **problèmes d'efficacité** dans la mise en œuvre doivent également être résolus dans le **cadre existant en matière de gouvernance, d'administration et de protection des données** afin d'éviter de compromettre l'incidence opérationnelle des nouvelles missions de traitement des données à caractère personnel en retardant ou en restreignant leur utilisation. Cinq États membres ont mis en cause une mise en œuvre trop prudente des règles en matière de protection des données par Europol et son conseil d'administration, sous la direction du CEPD. Ils suggèrent que la flexibilité accordée par les colégislateurs soit utilisée de manière adéquate pour maximiser l'efficacité et l'efficience des missions d'Europol et garantir leur pertinence et leur rentabilité à long terme.

Une évaluation des méthodes de travail d'Europol et des domaines de simplification potentiels sort du champ d'application du rapport prévu à l'article 68, paragraphe 3, du RE et sera effectuée dans le cadre de l'évaluation prévue à l'article 68, paragraphe 1, dudit règlement.

4. Conclusions et perspectives

Dans l'ensemble, les principales conclusions préliminaires de la Commission sont que les États membres maintiennent **leur soutien au rôle joué par Europol** dans les domaines clés où elle assiste actuellement les États membres avec ses **nouvelles missions de traitement des données à caractère personnel.** Toutefois, pour **maximiser les avantages** des nouvelles compétences en matière de traitement des données à caractère personnel, il est nécessaire, de l'avis de certaines parties prenantes, de **remédier à d'éventuels problèmes d'efficacité**, notamment dans le cadre existant en matière de gouvernance, d'administration et de protection des données. Il serait également utile d'atténuer la **complexité et la fragmentation** du cadre juridique, qui pourraient dissuader les praticiens d'exploiter les nouvelles possibilités.

D'une manière générale, la Commission n'a pas trouvé d'éléments prouvant que les nouvelles règles avaient une **incidence négative sur les droits fondamentaux**, un constat qu'elle doit notamment aux garanties solides en matière de protection des données mises en place et qui facilitent également la circulation des informations en renforçant la confiance des partenaires. Pour certains États membres, l'Agence a privilégié la prudence, alors qu'elle devrait **exploiter de manière appropriée la flexibilité accordée par les colégislateurs** en ce qui concerne la catégorisation des personnes concernées, l'analyse d'impact relative à la protection des données, la consultation préalable du Contrôleur européen de la protection des données, le traitement des demandes de droits d'accès.

Compte tenu de la période généralement courte de mise en œuvre des nouvelles règles en matière de protection des données à caractère personnel prévues par le règlement (UE) 2022/991, les éléments recueillis ne sont toutefois pas concluants sur toutes les questions.

Dans **ProtectEU**, sa stratégie européenne de sécurité intérieure[46], la Commission a annoncé qu'elle proposerait une révision ambitieuse du mandat d'Europol afin de relever les défis croissants en matière de sécurité. Conformément à ses lignes directrices pour une meilleure

---

45 Voir les éléments de preuve présentés à la section 5 du document de travail des services de la Commission accompagnant le présent rapport, et en particulier les observations d'Europol et les réponses des États membres aux questions 2, 4 et 5 du questionnaire succinct du 2 juin 2025, à l'annexe III du document de travail des services de la Commission et la déclaration commune des chefs de police européens sur l'avenir d'Europol.

46 ProtectEU: une stratégie européenne de sécurité intérieure, p. 10.

réglementation[47], la Commission a entamé des préparatifs en vue de l'évaluation du règlement Europol et des méthodes de travail d'Europol, ouvrant ainsi la voie à une **proposition de la Commission en 2026 visant à rendre l'Agence plus opérationnelle, comme indiqué dans les orientations politiques**[48]. En juillet 2025, la Commission a publié l'appel à contributions[49] et a commandé une étude externe à l'appui de l'évaluation du règlement Europol et de l'analyse d'impact de la nouvelle proposition. L'évaluation du règlement Europol effectuée aux fins de la préparation du présent rapport vise à contribuer à cette évaluation.

47 Voir https://commission.europa.eu/law/law-making-process/better-regulation/better-regulation-guidelines-and-toolbox_en.

48 Ursula von der Leyen, Orientations politiques pour la prochaine Commission européenne 2024-2029, https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_fr?filename=Political%20Guidelines%202024-2029_FR.pdf.

49 https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/14638-Law-enforcement-cooperation-new-Europol-Statu-proposal-en.