Rat der
Europäischen Union

Brüssel, den 24. Juni 2025
(OR. en)

10806/25

COSI 124
ENFOPOL 225
IXIM 137
CATS 36
COPEN 188
CYBER 188
DATAPROTECT 130
TELECOM 213
JAI 911

ÜBERMITTLUNGSVERMERK

Absender:	Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission
Eingangsdatum:	24. Juni 2025
Empfänger:	Frau Thérèse BLANCHET, Generalsekretärin des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2025) 349 final
Betr.:	MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN Fahrplan für den rechtmäßigen und wirksamen Zugang zu Daten für Strafverfolgungszwecke

Die Delegationen erhalten in der Anlage das Dokument COM(2025) 349 final.

Anl.: COM(2025) 349 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 24.6.2025
COM(2025) 349 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN RAT, DEN EUROPÄISCHEN WIRTSCHAFTS- UND SOZIALAUSSCHUSS UND DEN AUSSCHUSS DER REGIONEN

Fahrplan für den rechtmäßigen und wirksamen Zugang zu Daten für Strafverfolgungszwecke

Einführung

Wie in der Europäischen Strategie für die innere Sicherheit („ProtectEU“)[1] dargelegt, **ist Sicherheit das Fundament, auf dem alle unsere Freiheiten aufbauen**. Demokratie, Rechtsstaatlichkeit, Grundrechte, das Wohlergehen der Europäerinnen und Europäer, Wettbewerbsfähigkeit und Wohlstand – all dies hängt von unserer Fähigkeit ab, eine grundlegende Sicherheitsgarantie zu bieten.

Die EU und die Mitgliedstaaten haben die Pflicht, dafür zu sorgen, dass die Unionsbürgerinnen und Unionsbürger **in ihrem Alltag ein hohes Maß an Sicherheit** genießen können. Zu diesem Zweck müssen die Strafverfolgungs- und Justizbehörden über die erforderlichen Instrumente verfügen, um illegale Aktivitäten aufzuspüren, Täter zu ermitteln, kriminelle Netze zu zerschlagen und Opfer zu schützen und so letztlich das Strafrecht unter uneingeschränkter Achtung der Grundrechte sicherzustellen.

Terrorismus, organisierte Kriminalität, Online-Betrug, Drogenhandel, sexueller Missbrauch von Kindern, sexuelle Ausbeutung im Internet, Ransomware und viele andere Straftaten haben etwas gemein: Sie hinterlassen **digitale Spuren**. Wie Europol in seiner Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität (SOCTA) für 2025 feststellt, haben fast alle Formen der schweren und organisierten Kriminalität einen digitalen Fußabdruck[2]. **Heute stützen sich etwa 85 % der strafrechtlichen Ermittlungen auf elektronische Beweismittel**[3]. Die an Diensteanbieter gerichteten Datenanfragen haben sich zwischen 2017 und 2022 verdreifacht, und der Bedarf an diesen Daten nimmt immer weiter zu[4].

Wir haben zwar in jüngster Zeit bemerkenswerte Beispiele dafür gesehen, dass Strafverfolgungs- und Justizbehörden erfolgreich gegen spezielle kriminelle Kommunikationsnetze vorgegangen sind[5], aber viele weitere Ermittlungen **werden aufgrund des fehlenden zeitnahen Zugangs zu digitalen Beweismitteln verzögert oder bleiben erfolglos**[6]. Die Strafverfolgung und die Justiz haben in den letzten zehn Jahren gegenüber Kriminellen an Boden verloren, da Kriminelle Instrumente und Produkte von Diensteanbietern einsetzen, die Maßnahmen ergriffen haben, die eine Zusammenarbeit mit rechtmäßigen Ersuchen verhindern[7].

Wichtige strafrechtliche Beweismittel sind nach wie vor unzugänglich, weil sie[8]

---

[1] EUR-Lex – 52025DC0148 – DE – EUR-Lex.
[2] Bewertung der Bedrohungslage im Bereich der schweren und organisierten Kriminalität in der Europäischen Union 2025, EU-SOCTA-2025.pdf.
[3] Folgenabschätzung der Kommission zu den Vorschlägen für eine Verordnung über elektronische Beweismittel und eine Richtlinie über elektronische Beweismittel (17. April 2018), https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2018:0119:FIN:DE:PDF.
[4] SIRIUS-Bericht 2023, https://www.eurojust.europa.eu/sites/default/files/assets/sirius-eueesr-2023.pdf, S. 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] Berichtet von der Hochrangigen Gruppe für den Zugang zu Daten für eine wirksame Strafverfolgung – Europäische Kommission.
[7] Concluding report of the High-Level Group on access to data for effective law enforcement (15. November 2024).
[8] Common Challenges in Cybercrime, 2024 Review by Europol and Eurojust.

- von Diensteanbietern im Einklang mit ihren Verpflichtungen zum Schutz personenbezogener Daten und der Privatsphäre oder mit ihren Geschäftsanforderungen innerhalb von Tagen **gelöscht werden**;
- aufgrund von Rechtskollisionen zwischen verschiedenen Rechtsordnungen **nicht erlangt werden können**, da verschiedene Länder unterschiedliche Gesetze und Vorschriften über den Datenzugang haben, was die Erlangung von im Ausland gespeicherten Daten erschwert;
- **von Geräten, die bei strafrechtlichen Ermittlungen beschlagnahmt wurden, nicht abgerufen werden können**, da die **digitale Forensik** schwierig, wenn nicht sogar völlig undurchführbar ist;
- **nicht gelesen werden können**, weil die Daten verschlüsselt sind;
- **nicht wirksam und rechtmäßig analysiert werden können**, da es an geeigneten Technologien oder ausreichenden personellen Ressourcen mangelt, um große Mengen beschlagnahmter Daten wirksam zu filtern und zu analysieren, ohne gegen den Rechtsrahmen der EU und der Mitgliedstaaten zu verstoßen.

Als Reaktion auf diese Herausforderungen wurde 2023 eine **Hochrangige Gruppe für den Zugang zu Daten für die Strafverfolgung** (im Folgenden „Hochrangige Gruppe“) eingesetzt, die im Mai und November 2024 42 Empfehlungen abgab. Der **Rat „Justiz und Inneres“ der EU** hat die Empfehlungen der Hochrangigen Gruppe[9] am 13. Juni 2024 gebilligt und später im Dezember 2024 Schlussfolgerungen angenommen, in denen die Kommission aufgefordert wird, einen Fahrplan auszuarbeiten. Der Fahrplan sollte sich auf die Arbeit der Hochrangigen Gruppe und ihre Empfehlungen zur Einführung von Maßnahmen zur Sicherstellung eines rechtmäßigen und wirksamen Zugangs zu Daten für Strafverfolgungszwecke stützen[10]. Mit der vorliegenden Mitteilung wird dieser Aufforderung entsprochen.

Da die Digitalisierung immer weiter zunimmt und Kriminellen eine immer größere Quelle neuer Instrumente bietet, ist ein Rahmen für den **rechtmäßigen Zugang zu Daten** von entscheidender Bedeutung, um sicherzustellen, dass Kriminelle vor Gericht gestellt werden. Der „rechtmäßige Zugang“, auf den sich dieser Fahrplan bezieht, ist der im Einklang mit dem Gesetz erfolgende Zugang zu den digitalen Informationen, die Strafverfolgungsbehörden für die Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Durchführung der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, benötigen.

Um rechtmäßig zu sein, muss der Zugang zu den Daten **notwendig und verhältnismäßig sein und unter Wahrung der Grundrechte erfolgen**, wobei ein angemessener Schutz der Privatsphäre und personenbezogener Daten sicherzustellen ist; er muss **auf klaren, präzisen und zugänglichen Vorschriften beruhen, die gesetzlich festgelegt sind**, unabhängigen **Kontrollmechanismen** unterliegen und den Personen, die vom Zugang zu ihren Daten betroffen sein könnten, **wirksame Rechtsbehelfe** bieten. Für den Schutz vor Bedrohungen der

[9] Recommendations from the High-Level Group on Access to Data for Effective Law Enforcement.

[10] Schlussfolgerungen des Rates zum Zugang zu Daten für eine wirksame Strafverfolgung (12. Dezember 2024), abrufbar unter https://data.consilium.europa.eu/doc/document/ST-16448-2024-INIT/de/pdf; Schlussfolgerungen des Rates zu den künftigen Prioritäten zur Verstärkung der gemeinsamen Anstrengungen der Europäischen Union und ihrer Mitgliedstaaten zur Terrorismusbekämpfung (12. Dezember 2024) https://data.consilium.europa.eu/doc/document/ST-16820-2024-INIT/de/pdf.

Cybersicherheit ist es ebenso wichtig, dafür zu sorgen, dass digitale Systeme vor unbefugtem Zugriff geschützt bleiben.

I. Sicherstellung der Verfügbarkeit digitaler Beweismittel: Datenspeicherung[11]

In Spanien wurde 2019 eine strafrechtliche Untersuchung des Verschwindens einer jungen Frau mithilfe von Standortdaten abgeschlossen, die von einem Anbieter von Kommunikationsdiensten im Einklang mit einer nationalen rechtlichen Verpflichtung gespeichert wurden. Diese Daten ermöglichten es den Ermittlern, die vermisste Frau ausfindig zu machen, festzustellen, dass sich die Person, die der Entführung verdächtigt wurde, ebenfalls in diesem Gebiet befand, und andere Verdächtige auszuschließen[12]. Nichtinhalts-Kommunikationsdaten (z. B. Teilnehmerdaten, Standortdaten sowie Datum, Uhrzeit, Dauer, Absender und Empfänger sowie Größe der Nachricht) sind bei den meisten strafrechtlichen Ermittlungen und Strafverfolgungsmaßnahmen von entscheidender Bedeutung. Diese Daten können entscheidend dazu beitragen, Opfer, Verdächtige und beschuldigte Personen zu identifizieren und ausfindig zu machen, Informationen zu einer begangenen Straftat zu ermitteln und auch Verdächtige auszuschließen.

Im Einklang mit den EU-Rechtsvorschriften zum Schutz der Privatsphäre und zum Datenschutz dürfen Anbieter elektronischer Kommunikationsdienste Nichtinhalts-Kommunikationsdaten, die über ihre Systeme laufen, nur so lange speichern, wie dies für festgelegte, eindeutige und rechtmäßige Geschäftszwecke erforderlich ist. Aufgrund rechtlicher Verpflichtungen können sie jedoch verpflichtet sein, diese Daten für andere Zwecke aufzubewahren (oder „vorzuhalten“), z. B. wenn sie für die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten erforderlich sind.

Seit der Aufhebung der EU-Richtlinie über die Vorratsspeicherung von Daten[13] im Jahr 2014[14] ist das EU-Rechtssystem zur Verpflichtung von Diensteanbietern zur Speicherung von Daten fragmentiert und uneinheitlich geworden. Die Rahmen der Mitgliedstaaten für die Vorratsdatenspeicherung unterscheiden sich hinsichtlich der Arten der elektronischen Kommunikation, die die Diensteanbieter speichern müssen, der erfassten Datenkategorien und der vorgeschriebenen Speicherfristen[15]. Darüber hinaus gibt es in einigen Mitgliedstaaten überhaupt keine Rechtsvorschriften zur Datenspeicherung. Strafverfolgungs- und Justizbehörden stehen bei ihrer Arbeit vor rechtlichen und operativen Hindernissen. Anbieter elektronischer Kommunikationsdienste, insbesondere kleinere Anbieter, sind bei der Erbringung ihrer Dienste in der gesamten EU zudem mit zusätzlichen Kosten und Hindernissen konfrontiert, da sie in den einzelnen Mitgliedstaaten unterschiedliche rechtliche Anforderungen erfüllen müssen.

---

[11] Die Datenspeicherung bezieht sich darauf, dass Diensteanbieter bestimmte Nichtinhaltsdaten, die im Rahmen der von ihnen bereitgestellten Kommunikationsdienste verarbeitet werden, für einen bestimmten Zeitraum speichern, um den zuständigen Behörden bei strafrechtlichen Ermittlungen im Rahmen geeigneter Garantien den Zugang zu ermöglichen und die Umsetzung des Strafrechts sicherzustellen.

[12] La cobertura del móvil de Diana Quer desmonta la versión del Chicle: no la abordó donde él dijo que estaba robando gasolina | Spanien.

[13] https://eur-lex.europa.eu/eli/dir/2006/24/oj.

[14] Urteil des Gerichtshofs (Große Kammer) vom 8. April 2014. Digital Rights Ireland Ltd gegen Minister for Communications, Marine and Natural Resources u. a.

[15] Ein Überblick findet sich in The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU | Eurojust | Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen und European Commission Study on the retention of electronic communications non-content data for law enforcement purposes.

Die Hochrangige Gruppe empfahl daher die Schaffung eines **harmonisierten EU-Rahmens für die Datenspeicherung**, um sicherzustellen, dass die digitalen Beweismittel, die für die Ermittlung und Verfolgung von Straftaten erforderlich sind, zur Verfügung stehen. Eine harmonisierte EU-Regelung würde darauf abzielen, die Fragmentierung zwischen den Mitgliedstaaten in Bezug auf die Vorschriften über die Datenspeicherung und die Garantien in Bezug auf die Grundrechte, insbesondere den Schutz der Privatsphäre, den Datenschutz und die Verteidigungsrechte, einschließlich des Rechts auf ein faires Verfahren, zu begrenzen. Ein solcher Rechtsrahmen würde somit auch die Rechtssicherheit für die zuständigen Behörden einerseits und die Diensteanbieter andererseits sicherstellen[16].

Zentrale Maßnahme

- **Im Jahr 2025 wird die Kommission eine Folgenabschätzung erstellen, um die EU-Vorschriften über die Vorratsdatenspeicherung gegebenenfalls zu aktualisieren.**

Die Hochrangige Gruppe stellte fest, dass **die Synergien zwischen Strafverfolgungsbeamten und Diensteanbietern gestärkt werden müssen**[17].

Zu diesem Zweck werden **die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und die Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust)** ersucht, ihre Bemühungen zur **Erleichterung der Zusammenarbeit und des Austauschs von Informationen und bewährten Verfahren zwischen Strafverfolgungsbeamten und Diensteanbietern** im Rahmen des **SIRIUS-Projekts**[18] mit kontinuierlicher Unterstützung der Kommission fortzusetzen und auszuweiten. Das SIRIUS-Projekt ist zur wichtigsten Informationsquelle geworden, um **Strafverfolgungsbeamte und Justizbehörden in der EU und darüber hinaus beim Zugang zu elektronischen Beweismitteln zu unterstützen, die von Anbietern von Online-Diensten** mit Sitz in Drittländern **gespeichert werden**. Die SIRIUS-Plattform umfasst mehr als 8 000 Mitglieder aus den Bereichen Strafverfolgung und Justiz, die weltweit 47 Länder vertreten, und hat fast 70 Polizeieinsätze direkt unterstützt.

Mit demselben Ziel sollten Europol und Eurojust das SIRIUS-Projekt nutzen, um in Zusammenarbeit mit dem **Privatsektor einen Katalog der Daten zu erstellen, die Anbieter von elektronischen Kommunikationsdiensten rechtmäßig für ihre Geschäftszwecke verarbeiten**. Dies wird den zuständigen Behörden dabei helfen, zu identifizieren, welche Daten für ihre Anträge auf rechtmäßigen Zugang verfügbar sein können, relevante Diensteanbieter zu ermitteln und Anträge auf rechtmäßigen Zugang gezielter auszurichten, wodurch sowohl für Behörden als auch für Diensteanbieter Zeit und Kosten eingespart werden können.

Zentrale Maßnahmen

- **Europol und Eurojust werden nachdrücklich aufgefordert, mit anhaltender Unterstützung der Kommission auf dem SIRIUS-Projekt aufzubauen, um die Zusammenarbeit mit Anbietern elektronischer Kommunikationsdienste zu straffen.**

[16] Empfehlungscluster 6, Abschlussbericht der Hochrangigen Gruppe.
[17] Empfehlungscluster 5, Abschlussbericht der Hochrangigen Gruppe.
[18] SIRIUS-Projekt | Europol.

- **<u>Europol und Eurojust</u> werden nachdrücklich aufgefordert, in Zusammenarbeit mit dem Privatsektor einen Katalog der Daten zu erarbeiten, die die Anbieter elektronischer Kommunikationsdienste für ihre Geschäftszwecke verarbeiten (mit Beginn im vierten Quartal 2025).**

II. Erhebung von Beweismitteln in verschiedenen Systemen und Rechtsordnungen: rechtmäßige Überwachung des Telekommunikationsverkehrs

Der rechtmäßige Zugang zu Kommunikationsdaten in Echtzeit ist von entscheidender Bedeutung für die Bekämpfung Krimineller online und offline. Im Jahr 2020 zerschlug eine gemeinsame Ermittlungsgruppe aus Frankreich und den Niederlanden EncroChat, ein verschlüsseltes Telefonnetz, das weithin von organisierten kriminellen Gruppen genutzt wurde. Im Rahmen der gemeinsamen Ermittlungen wurden Millionen von Nachrichten zwischen Straftätern, die die Durchführung schwerer Straftaten planten, in Echtzeit abgefangen, an andere Behörden weitergegeben und analysiert. Dank der erhaltenen Informationen haben Strafverfolgungsbehörden in ganz Europa und in anderen Teilen der Welt kriminelle Aktivitäten wie gewaltsame Angriffe, Korruption, Mordversuche und großflächigen Drogenhandel verhindert. Bestimmte Nachrichten wiesen auf Pläne hin, in unmittelbarer Zukunft Gewaltverbrechen zu begehen, und ermöglichten es den Strafverfolgungsbehörden, diese Straftaten zu verhindern[19]. Die Europäische Ermittlungsanordnung (EEA) erleichterte den effizienten Austausch dieser Beweismittel[20].

Der Fall EncroChat zeigt, dass der Echtzeit-Zugang zu Inhaltsdaten der Kommunikation ein wesentliches Instrument für die wirksame Ermittlung und Verfolgung organisierter krimineller Gruppen ist. Dieser Fall ist jedoch nur eine von wenigen Erfolgsgeschichten: Die Hochrangige Gruppe stellte fest, dass die Wirksamkeit der rechtmäßigen Überwachung des Telekommunikationsverkehrs[21] drastisch abgenommen hat, da die Kommunikation von herkömmlichen Telefonanrufen und SMS zu „Over-the-top"-Nachrichtenübermittlungsdiensten (OTT) über Apps verlegt wurde. Derzeit werden rund 97 % aller mobilen Nachrichten über Messaging-Apps gesendet, während herkömmliche SMS- und MMS-Nachrichten nur etwa 3 % der Nachrichten ausmachen[22]. Die Hochrangige Gruppe stellte ferner fest, dass seit 2020 nach der Störung einiger der großen kriminellen Kommunikationsnetze viele kriminelle Gruppen wieder zu regelmäßigen, durchgängig verschlüsselten OTT-Nachrichtenübermittlungsdiensten zurückgekehrt sind[23].

Die nationalen Vorschriften, mit denen Verpflichtungen zur rechtmäßigen Überwachung des Telekommunikationsverkehrs auferlegt werden, sind in der EU fragmentiert[24]. Die

[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] Europäische Ermittlungsanordnung | Eurojust | Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen.

[21] Im Zusammenhang mit dieser Mitteilung bezeichnet dies Technologien zur rechtmäßigen Überwachung des Telekommunikationsverkehrs, die eingeführt werden, um bei gerichtlichen Untersuchungen Echtzeitzugang zu Kommunikationsdaten durch einen Kommunikationsbetreiber zu erhalten, sowie Technologien, die von Strafverfolgungsbehörden autonom eingesetzt werden können.

[22] Abschlussbericht der Hochrangigen Gruppe, S. 38.

[23] Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet (IOCTA), 2024.

[24] Siehe EU-Weißbuch zur digitalen Infrastruktur, S. 14; Letta-Bericht über den Binnenmarkt, S. 59, und Draghi-Bericht über die Wettbewerbsfähigkeit der EU, S. 70, 74, 76.

Hochrangige Gruppe stellte fest, dass einige Mitgliedstaaten zwar ähnliche Verpflichtungen für alle Arten von elektronischen Kommunikationsdiensten, einschließlich OTT-Diensten, auferlegen, andere diese jedoch ausschließen. Darüber hinaus sind die Diensteanbieter oft nicht im Mitgliedstaat der ersuchenden Behörde niedergelassen, was zu komplexen Zuständigkeitsfragen, Rechtskollisionen und Herausforderungen bei der Durchsetzung führen kann[25]. Infolgedessen ist der Inhalt solcher Nachrichtenübermittlungsdienste praktisch unzugänglich.

Die EEA und andere Instrumente der Zusammenarbeit können dazu beitragen, die Herausforderung der grenzüberschreitenden Überwachung des Telekommunikationsverkehrs in Teilen der EU zu bewältigen. Die Behörden der Mitgliedstaaten sind bei ihrer Nutzung jedoch nach wie vor mit Schwierigkeiten konfrontiert: Diese Instrumente können die Überwachung des Telekommunikationsverkehrs nicht unterstützen, wenn der Kommunikationsdienst entweder von Mitgliedstaaten, die nicht an dem betreffenden Instrument beteiligt sind, oder von einem Drittland aus erbracht wird. Die Hochrangige Gruppe empfahl daher eine Reihe von Maßnahmen, um sicherzustellen, dass ein breites Spektrum von Anbietern, einschließlich OTT-Anbietern, rechtmäßigen Überwachungsanfragen nachkommt[26].

Als Reaktion auf diese Empfehlung **wird die Kommission Vorschläge dazu vorlegen, wie die Maßnahmen zur Verbesserung der grenzüberschreitenden Zusammenarbeit bei der Überwachung des Telekommunikationsverkehrs** sowohl zwischen den Behörden als auch zwischen Behörden und Diensteanbietern verbessert werden können. Entsprechend den Empfehlungen der Hochrangigen Gruppe wird die Kommission in erster Linie daran arbeiten, bestehende Instrumente, insbesondere die EEA, und die freiwillige Zusammenarbeit (sofern keine Rechtskollisionen mit Drittländern bestehen bzw. diese gelöst wurden) zu verbessern. Letztlich sollten die Mitgliedstaaten in der Lage sein, allen Kommunikationsanbietern, die Dienste im Inland anbieten, Pflichten der rechtmäßige Überwachung aufzuerlegen, wie sie in den nationalen Rechtsvorschriften vorgesehen sind, unabhängig davon, ob es sich um traditionelle Telekommunikationsdienste oder internetgestützte Dienste handelt und wo die Anbieter ansässig sind.

Darüber hinaus verfügen einige Mitgliedstaaten nicht über die erforderlichen Netzkapazitäten für den Datenaustausch im Rahmen der grenzüberschreitenden Zusammenarbeit. Daher wird die **Kommission den Bedarf der Mitgliedstaaten ermitteln** und den Aufbau gesicherter Netze mit ausreichender Bandbreite, die die Übertragung großer Datenmengen in Echtzeit ermöglichen, zwischen den betreffenden Mitgliedstaaten unterstützen. Diese Initiative könnte aus EU-Programmen finanziert werden.

[25] Abschlussbericht der Hochrangigen Gruppe, S. 41.
[26] Empfehlungscluster 8, Abschlussbericht der Hochrangigen Gruppe.

Zentrale Maßnahmen

Die Kommission wird

- **Vorschläge für Maßnahmen zur Verbesserung der Effizienz grenzüberschreitender Anträge auf rechtmäßige Überwachung des Telekommunikationsverkehrs durch bestehende Instrumente machen, einschließlich der Bewertung der Notwendigkeit einer weiteren Stärkung der Europäischen Ermittlungsanordnung (bis 2027);**

- **Maßnahmen zur Schaffung gleicher Wettbewerbsbedingungen für alle Arten von Kommunikationsanbietern bei der Durchsetzung der Pflichten der rechtmäßigen Überwachung prüfen;**

- **den effizientesten Ansatz für den Umgang mit nicht kooperativen Kommunikationsanbietern ermitteln;**

- **den Aufbau gesicherter Kapazitäten für den Informationsaustausch zwischen den Mitgliedstaaten, Europol und anderen Sicherheitsbehörden unterstützen (von 2026 bis 2028).**

Die Mitgliedstaaten werden aufgefordert, Maßnahmen für die grenzüberschreitende rechtmäßige Überwachung des Telekommunikationsverkehrs durchzuführen und dabei auf bestehenden Mechanismen wie der Europäischen Ermittlungsanordnung und bilateralen und multilateralen Übereinkünften aufzubauen.

III. Abrufen von Beweismitteln von Geräten, die bei Ermittlungen beschlagnahmt wurden: digitale Forensik

Um strafrechtliche Ermittlungen durchführen zu können, müssen die Strafverfolgungs- und Justizbehörden in der Lage sein, auf elektronischen Geräten gespeicherte digitale Beweismittel abzurufen, zu sammeln, zu analysieren und aufzubewahren. Diese digitalen Beweismittel können beispielsweise dazu beitragen, Mitglieder organisierter krimineller Gruppen zu identifizieren oder Personen als Verdächtige auszuschließen[27].

Die Hochrangige Gruppe erörterte eine Reihe von Herausforderungen, die den Zugang zu diesen digitalen Beweismitteln behindern. Die nationalen Behörden leiden an einem gravierenden Mangel an Ressourcen und Kapazitäten für die Durchführung digitaler Forensik. Es fällt ihnen schwer, ständig neue Kompetenzen und Instrumente entwickeln zu müssen, um mit neuen Technologien Schritt zu halten (z. B. neue Gerätetypen und Betriebssysteme, das Internet der Dinge und Cloud-Computing). Die grenzüberschreitende Zusammenarbeit zwischen den Mitgliedstaaten wird durch den Mangel an vergleichbaren Kapazitäten und das Fehlen von Mechanismen zur Anerkennung der Fähigkeiten und des Fachwissens von Experten für digitale Forensik beeinträchtigt. Bestehende kommerzielle Lösungen sind schnell überholt, sind kostspielig und werden oft außerhalb der EU entwickelt. Sie sind möglicherweise auch schlecht auf die Bedürfnisse der Behörden der Mitgliedstaaten zugeschnitten oder erfüllen

[27] Ein in der Hochrangigen Gruppe erörterter Fall betraf die Analyse eines Geräts, die entscheidend dazu beigetragen hat, nachzuweisen, dass ein Verdächtiger nicht an einem Mord beteiligt war. Abschlussbericht der Hochrangigen Gruppe, S. 12.

möglicherweise hinsichtlich der Rechenschaftspflicht oder anderer rechtlicher Anforderungen nicht die Standards der digitalen Forensik der EU.

Um die Fähigkeit der europäischen Strafverfolgungsbehörden zur Durchführung von Maßnahmen der digitalen Forensik an beschlagnahmten Geräten zu stärken, empfahl die Hochrangige Gruppe daher die Bereitstellung gezielter Mittel für Projekte, sowohl für die Forschung und Entwicklung im Hinblick auf digitale forensische Instrumente als auch für deren Einführung. Die Hochrangige Gruppe begrüßte die laufenden Bemühungen der Kommission, dies durch Finanzierung im Rahmen bestimmter EU-Instrumente (Horizont Europa, Programm „Digitales Europa“ und Fonds für die innere Sicherheit) und entsprechender Instrumente im Rahmen des nächsten langfristigen EU-Haushalts (Mehrjähriger Finanzrahmen) zu unterstützen.

Als Reaktion auf diese Empfehlungen[28] **wird die Kommission mit Unterstützung von Europol eine Lücken- und Bedarfsanalyse zu Forschung, Entwicklung, Wartung und Einführung gemeinsamer technischer Lösungen für die digitale Forensik koordinieren**.

Die Ressourcen müssen optimal genutzt werden, indem Synergien zwischen Projekten der digitalen Forensik geschaffen werden, unter anderem durch die Integration der im Rahmen der Programme der Mitgliedstaaten finanzierten Projekte in bestehende Mechanismen oder Netze. Dies sollte auch die Finanzierung öffentlich-privater Partnerschaften umfassen, um vollständig erprobte und gebrauchsfertige Software-Tools ohne Lizenzkosten bereitzustellen[29].

Im Rahmen des Mandats des OLAF zur Durchführung von Verwaltungsuntersuchungen hat das Amt umfangreiche Erfahrungen mit digitalen forensischen Verfahren und Instrumenten gesammelt und kann die Behörden der Mitgliedstaaten im Rahmen des Betrugsbekämpfungsprogramms der Union beim Ausbau ihrer Kapazitäten unterstützen.

Das **Instrumentenarchiv von Europol** ist eine sichere, ausschließlich Strafverfolgungsbehörden zur Verfügung stehende Online-Plattform für den Austausch kostenloser, nicht kommerzieller Software, die von Europol, europäischen Strafverfolgungsbehörden und Hochschulen entwickelt wurde. Nationale Ermittlungsbehörden haben die Instrumente des Archivs umfassend genutzt, um Ermittlungen in den Bereichen der schweren und organisierten Kriminalität, einschließlich Menschenhandel, Cyberkriminalität und sexuellen Missbrauchs von Kindern im Internet, zu unterstützen. Dieses Archiv sollte der bevorzugte Verteilungskanal für digitale Ermittlungsinstrumente, die im Rahmen von EU-Projekten und von Mitgliedstaaten entwickelt werden, bleiben, und die Mitgliedstaaten werden ermutigt, quelloffene digitale Open-Source-Forensiktools, die auf nationaler Ebene im Rahmen bestehender Mechanismen oder Netze entwickelt wurden, auszutauschen. **Europol kann sein Instrumentenarchiv weiterentwickeln und bekannt machen**, um den Strafverfolgungsbehörden der EU vertrauenswürdige, sichere, kostenlose, leicht zu installierende und skalierbare Ermittlungsinstrumente zur Verfügung zu stellen.

[28] Empfehlungscluster 1, Abschlussbericht der Hochrangigen Gruppe.

[29] So stellt die European Anti-Cybercrime Technology Development Association (EACTDA) (www.eactda.eu) beispielsweise vollständig erprobte und operativ gebrauchsfertige Software-Tools ohne Lizenzkosten und mit Zugang zum Quellcode für Strafverfolgungsbehörden in der EU bereit. Zusätzlich zu den acht bisher fertiggestellten Instrumenten entwickelt die EACTDA derzeit 16 weitere digitale Ermittlungsinstrumente, die bis Mitte 2025 bereitgestellt werden sollen.

Die Kommission wird auch **die Einführung innovativer Lösungen bei den Strafverfolgungsbehörden der Mitgliedstaaten durch bestehende Mechanismen wie EMPACT[30] und spezielle Aufforderungen zur Einreichung von Vorschlägen aus dem Fonds für die innere Sicherheit unterstützen**.

Die Hochrangige Gruppe betonte, dass **Lizenzen für digitale forensische Instrumente** kostspielig und manchmal für einige Strafverfolgungsbehörden unerschwinglich sind. Digitale forensische Instrumente können Daten in Formaten bereitstellen, die nicht mit den Systemen kompatibel sind, die für die Weiterverarbeitung verwendet werden. Darüber hinaus ist Vertrauen von grundlegender Bedeutung für Tätigkeiten der digitalen Forensik, die sich nicht auf „Black Box"-Instrumente stützen sollten (d. h. Instrumente, die Daten verarbeiten, ohne dass vertrauenswürdige Behörden in der Lage sind, zu überprüfen, wie sie funktionieren). Der Austausch digitaler forensischer Instrumente sollte durch Evaluierungssysteme und gegebenenfalls die Zertifizierung kommerzieller Instrumente auf EU-Ebene unterstützt werden, um sicherzustellen, dass sie den Standards der Vertrauenswürdigkeit und der Forensik entsprechen, ohne übermäßige Belastungen zu verursachen. Die Unterstützung sollte auch durch gemeinsame Beschaffungsprogramme erfolgen, die die Zusammenarbeit zwischen den operativen Einheiten und den Kontaktstellen in den Vergabebehörden sicherstellen[31].

Daher **wird die Kommission die operativen Einheiten der Mitgliedstaaten und ihre Vergabebehörden bei der gemeinsamen Beschaffung von Lizenzen für digitale forensische Instrumente unterstützen, beginnend mit einer Pilotphase.**

Zentrale Maßnahmen

Die Kommission wird mit Unterstützung von Europol

- **vor dem zweiten Quartal 2026 eine Lücken- und Bedarfsanalyse in Bezug auf Forschung, Entwicklung, Wartung und Einführung gemeinsamer technischer Lösungen für die digitale Forensik koordinieren;**

- **die Entwicklung technischer Lösungen für die digitale Forensik durch geeignete Finanzierungs- und Koordinierungsmechanismen weiterhin unterstützen;**

- **die Mitgliedstaaten und die Vergabebehörden (vor dem zweiten Quartal 2027) bei der gemeinsamen Beschaffung von Lizenzen für digitale forensische Instrumente unterstützen, beginnend mit einer Pilotphase.**

Europol wird ersucht, sein Instrumentenarchiv weiterzuentwickeln und bekannt zu machen, um den Strafverfolgungsbehörden den Zugang zu nicht kommerziellen digitalen Instrumenten zu ermöglichen (ab dem dritten Quartal 2025).

Die Mitgliedstaaten werden aufgefordert, sich an der Entwicklung, Validierung und Einführung digitaler forensischer Instrumente zu beteiligen, diese zu unterstützen und zu steuern.

[30] EMPACT (Europäische multidisziplinäre Plattform gegen kriminelle Bedrohungen) ist eine von den EU-Mitgliedstaaten geleitete Sicherheitsinitiative zur Ermittlung, Priorisierung und Bewältigung von Bedrohungen durch organisierte und schwere internationale Kriminalität.

[31] Aufbauend auf dem Projekt iProcureNet (www.iprocurenet.eu/), das im Rahmen des EU-Programms „Horizont Europa" für Forschung und Innovation finanziert wurde und in dessen Rahmen eine Methodik für die gemeinsame Auftragsvergabe im Sicherheitsbereich sowie ein Netz von Vergabebehörden in den Mitgliedstaaten entwickelt wurde.

Die Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL) führt Schulungen für auf dem Gebiet der digitalen Forensik tätige Ermittler durch, unter anderem zur mobilen Forensik und Live-Daten-Forensik. Entsprechend der Empfehlung der Hochrangigen Gruppe[32] **sollte die Kommission weiterhin die Schaffung von Schulungsmaterialien und -ressourcen** durch bestehende Mechanismen unterstützen, an denen Strafverfolgungsbeamte und Hochschulen beteiligt sind[33]. Darüber hinaus sollten CEPOL und die Mitgliedstaaten **vorrangig Schulungen im Bereich der digitalen Forensik anbieten**.

Die Hochrangige Gruppe betonte ferner, dass auf EU-Ebene ein Zertifizierungssystem für Sachverständige für digitale Forensik geschaffen werden könnte. Ein solches System würde die Qualität der Arbeiten im Bereich digitale Forensik sicherstellen, zu transparenteren Gerichtsverfahren beitragen und das Vertrauen zwischen den Strafverfolgungsbehörden über Grenzen hinweg stärken.

Im Einklang mit den Empfehlungen der Hochrangigen Gruppe[34] **könnte die CEPOL Strafverfolgungsbeamte und Hochschulen bei der Schaffung eines Zertifizierungssystems für Sachverständige für digitale Forensik auf EU-Ebene unter umfassender Nutzung bestehender Netze und Mechanismen[35] unterstützen**.

Zentrale Maßnahmen

Die <u>Kommission</u> wird

- **die Erstellung von Schulungsmaterialien und -ressourcen weiter unterstützen.**

<u>Die CEPOL und die Mitgliedstaaten</u> werden aufgefordert,

- **der Durchführung von Schulungen zur digitalen Forensik Vorrang einzuräumen (ab dem dritten Quartal 2025);**

- **die Entwicklung und Umsetzung eines Zertifizierungssystems auf EU-Ebene für Sachverständige für digitale Forensik zu unterstützen (zwischen dem ersten Quartal 2026 und dem vierten Quartal 2028).**

Die Hochrangige Gruppe gab Empfehlungen zur Erleichterung des Austauschs von Lösungen und digitalen forensischen Instrumenten zwischen den Mitgliedstaaten in einem vertrauensvollen Umfeld ab[36]. Als Reaktion darauf **<u>sollte Europol seine Rolle als Kompetenzzentrum der EU für die Strafverfolgung in Bezug auf digitales operatives Fachwissen im Bereich der digitalen Forensik weiterentwickeln</u>**. Dies könnte die Einrichtung eines Projekts nach dem Vorbild von SIRIUS[37] umfassen, um in einem

[32] Empfehlungscluster 3, Abschlussbericht der Hochrangigen Gruppe.

[33] Die ECTEG (European Cybercrime Training and Education Group, www.ecteg.eu) ist zum Beispiel ein Verband, der eng mit Europol und CEPOL zusammenarbeitet, um den Strafverfolgungsbehörden kostenlose Schulungsressourcen im Bereich der digitalen Ermittlungen zur Verfügung zu stellen. Sie wird derzeit aus dem EU-Fonds für die innere Sicherheit finanziert.

[34] Empfehlungscluster 3, Abschlussbericht der Hochrangigen Gruppe.

[35] Insbesondere die ECTEG.

[36] Empfehlungscluster 1, Abschlussbericht der Hochrangigen Gruppe.

[37] Das von Europol und Eurojust geleitete Projekt SIRIUS unterstützt die Strafverfolgungs- und Justizbehörden der EU, indem es den effizienten grenzüberschreitenden Zugang zu elektronischen Beweismitteln, die von Online-Diensteanbietern gespeichert werden, erleichtert. Es bietet praktische Instrumente, Schulungen und Ressourcen für mehr als 9 000 Strafverfolgungsbeamte, fördert die Zusammenarbeit zwischen Anbietern von Online-Diensten und unterstützt durch internationale Veranstaltungen und Partnerschaften den Wissensaustausch.

vertrauensvollen Umfeld den Austausch von Wissen, Fachwissen, technischen Lösungen, Instrumenten der digitalen Forensik und bewährten Verfahren zu erleichtern. Europol sollte auch seine Koordinierungsfunktion bei der Schaffung von Kenntnissen im Bereich der digitalen Forensik auf EU-Ebene erweitern und dabei auf den in den letzten Jahren geschaffenen Mechanismen aufbauen[38]. Einige dieser Maßnahmen kann Europol im Rahmen seines derzeitigen Mandats einleiten. Europol wird jedoch ein erweitertes Mandat und zusätzliche Ressourcen benötigen, um diese Maßnahmen vollständig durchzuführen und den operativen Erfordernissen der Mitgliedstaaten wirksam gerecht zu werden.

Anknüpfend an die in den politischen Leitlinien für die Europäische Kommission 2024-2029 eingegangene Verpflichtung und wie in der Europäischen Strategie der inneren Sicherheit angekündigt, **wird die Kommission eine ambitionierte Überarbeitung des Mandats von Europol vorschlagen**. Um dies vorzubereiten, wird die Kommission in enger Zusammenarbeit mit den Mitgliedstaaten prüfen, wie das technologische Fachwissen und die Kapazitäten von Europol zur Unterstützung der nationalen Strafverfolgungsbehörden im digitalen Raum gestärkt werden können. Die Stärkung der digitalen forensischen Fähigkeiten von Europol auf der Grundlage eines erweiterten Mandats und mit zusätzlichen Ressourcen wird bei diesen Bemühungen von entscheidender Bedeutung sein.

Die Hochrangige Gruppe empfahl, dass der Zugang zu Wissen für Sachverständige durch spezielle Mechanismen verbessert wird und dass die Sachverständigen mit Herstellern und Entwicklern digitaler forensischer Instrumente zusammenarbeiten[39]. Ab 2026 **sollte Europol mit eigenen Mitteln die Zusammenarbeit zwischen den zuständigen nationalen Behörden und Sachverständigen fördern, um die öffentlich-private Zusammenarbeit bei der digitalen Forensik zu erleichtern**. Europol sollte die Mitgliedstaaten bei der Entwicklung digitaler Instrumente und gemeinsamer Verfahren unterstützen und unter anderem gemeinsame Datenformate für die Zwecke der digitalen Forensik festlegen[40].

Zentrale Maßnahmen

Europol wird aufgefordert,

- **sich zu einem Exzellenzzentrum für operatives Fachwissen in der digitalen Forensik zu entwickeln und seine Rolle bei der EU-weiten Koordinierung der Schaffung von Wissen in diesem Bereich zu stärken (ab 2026);**

- **die Zusammenarbeit zwischen Strafverfolgungsbehörden und privaten Parteien, einschließlich Diensteanbietern, im Bereich der digitalen Forensik zu erleichtern und die Festlegung gemeinsamer Datenformate für digitale forensische Zwecke zu unterstützen (ab 2026).**

[38] Spezielle Gemeinschaften auf der Europol-Expertenplattform (Europol Platform for Experts, https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/europol-platform-for-experts); Forum für Forensiksachverständige (Forensic Experts Forum, https://www.europol.europa.eu/publications-events/events/forensic-experts-forum-2024-conference); Europol-Industrie- und Forschungstage (Europol Industry and Research Days, https://www.europol.europa.eu/publications-events/events/europol-industry-and-research-days-2025).

[39] Empfehlungscluster 1, Abschlussbericht der Hochrangigen Gruppe.

[40] Diese Bemühungen sollten durch eine geeignete EU-Finanzierungsquelle (Forschungs- oder Entwicklungsprogramme, je nach Reifegrad der geplanten Systeme) unterstützt werden.

IV. Sicherstellung der Lesbarkeit von Beweismitteln: Entschlüsselung von Daten

Verschlüsselung und andere Cybersicherheitsmaßnahmen spielen eine wichtige Rolle beim Schutz von Informationssystemen vor Spionage und Störungen sowie beim Schutz von Nachrichten, Privatsphäre und personenbezogenen Daten. Zwischen 60 % und 80 % der Nachrichtenübermittlungsanwendungen arbeiten mit Ende-zu-Ende-Verschlüsselung, darunter auch etablierte Anwendungen wie WhatsApp, Messenger, Signal und iMessage; dagegen nimmt die Nutzung von SMS und herkömmlichen Telefonanrufen weltweit drastisch ab[41].

Die Hochrangige Gruppe betonte, dass sich diese Entwicklungen auf die Fähigkeit der Strafverfolgungs- und Justizbehörden auswirken, Beweismittel bei strafrechtlichen Ermittlungen und Strafverfolgungsmaßnahmen zu sammeln, da die abgefangenen Daten aus der rechtmäßigen Überwachung des Telekommunikationsverkehrs unbrauchbar werden. Die Hochrangige Gruppe unterstrich, dass die Mitgliedstaaten nur über begrenztes Fachwissen und begrenzte Fähigkeiten verfügen, um gespeicherte Daten („Data at Rest“) zu entschlüsseln, wobei es erhebliche Unterschiede bei den Erfolgsquoten gibt, die von 15 bis 20 % in einigen Mitgliedstaaten bis zu mehr als 66 % in anderen reichen.

Entschlüsselungsvorrichtungen sind teuer und hochspezialisiert, und die Hardware nimmt ein hohes Maß an Ressourcen in Anspruch. Die meisten Abteilungen für digitale Forensik der Strafverfolgungsbehörden nutzen beim Zugriff auf Daten, die auf Geräten gespeichert sind, kommerzielle Lösungen. Diese Lösungen können mit den technologischen Entwicklungen nur schlecht Schritt halten und sind schnell überholt; durch die hohen Lizenzkosten verringert sich die Zahl der zugelassenen Nutzer erheblich; und diese Lösungen werden häufig außerhalb der EU entwickelt und entsprechen daher möglicherweise nicht den Bedürfnissen der EU-Behörden oder den Standards der digitalen Forensik. Daher werden sie nur in sehr wenigen Ermittlungen erfolgreich eingesetzt.

Darüber hinaus hat der Rückgriff auf diese Instrumente weitere Nachteile. Bei ihren Ermittlungen nutzen die Behörden häufig Schwachstellen aus, um Zugang zu Entschlüsselungsschlüsseln auf Geräten zu erhalten, was in einigen Fällen zu Spannungen mit dem politischen Ziel führen könnte, standardmäßig für Cybersicherheit zu sorgen. Darüber hinaus wird der Zugang zu verschlüsselten Daten immer komplexer. Die Hochrangige Gruppe stellte fest, dass die Behörden Daten, die auf bestimmten Arten moderner Geräte gespeichert sind und durch Kryptochips oder starke Verschlüsselungsalgorithmen und komplexe Passwörter geschützt sind, selbst über die leistungsfähigsten Entschlüsselungsplattformen nicht abrufen können.

Die Entwicklung und Einführung einer **quantensicheren Kryptografie** ist notwendig, um Daten vor künftigen Quantencomputerangriffen zu schützen, durch die sensible Kommunikation, Finanztransaktionen und Staatsgeheimnisse anfällig für Entschlüsselung und Ausbeutung würden. Wie in der Empfehlung der Kommission zu einem koordinierten Umsetzungsfahrplan für den Übergang zur **Post-Quantum-Kryptografie (PQC)**[42] und in der Europäischen Strategie für die innere Sicherheit (ProtectEU) dargelegt, werden die Einführung von PQC-Lösungen und die Entwicklung der Quantum Key Distribution für den Schutz von Daten im neuen Quantenzeitalter von entscheidender Bedeutung sein. Wie Europol

[41] Der genannte Prozentsatz bezieht sich auf die Ende-zu-Ende-Verschlüsselung während der Übermittlung.
[42] Empfehlung zu einem koordinierten Umsetzungsfahrplan für den Übergang zur Post-Quantum-Kryptographie.

hervorgehoben hat, wird dies jedoch den rechtmäßigen Zugang zu digitalen Beweismitteln in den kommenden Jahren erschweren, und die Strafverfolgungsbehörden müssen investieren, um mit der raschen technologischen Entwicklung Schritt zu halten[43].

Die Hochrangige Gruppe empfahl[44] die Ausarbeitung eines Technologiefahrplans, um gegebenenfalls einen konzeptionsintegrierten rechtmäßigen Zugang umzusetzen und gleichzeitig für eine hohe Sicherheit und Cybersicherheit zu sorgen und die rechtlichen Verpflichtungen in Bezug auf den rechtmäßigen Zugang in vollem Umfang einzuhalten. Als Reaktion darauf **beauftragt die Kommission eine Expertengruppe, Unterstützung bei der Ausarbeitung eines Technologiefahrplans für Verschlüsselung zu leisten**. Die Gruppe wird technologische Lösungen ermitteln und bewerten, die es den Strafverfolgungsbehörden ermöglichen würden, rechtmäßig auf verschlüsselte Daten zuzugreifen und gleichzeitig die Cybersicherheit und die Grundrechte zu wahren. Der Gruppe werden Sachverständige in den Bereichen Strafverfolgung, Cybersicherheit, Verschlüsselung, Kommunikationstechnologien, Normung und Grundrechte angehören. Technische Studien und Konzeptnachweise werden diese Arbeiten unterstützen. Mit diesen Arbeiten soll Folgendes ermittelt werden:

- **Instrumente, die die Strafverfolgungsbehörden derzeit benötigen und in Zukunft benötigen werden**, um verschlüsselte Daten rechtmäßig aufzufinden, abzurufen und zu analysieren; diese Instrumente müssen die digitale Forensik, die Entschlüsselung, die Fernerfassung von Daten und die Kriminalitätsanalyse erleichtern;
- **Technologien, mit denen sichergestellt wird, dass künftige Informations- und Kommunikationstechnologien**, wie z. B. die sechste Generation von Mobiltelefonnetzen (6G) und quantenresistente Verschlüsselung, nicht die Fähigkeit der Strafverfolgungsbehörden beeinträchtigen, rechtmäßig auf Daten zuzugreifen, und gleichzeitig für die Einhaltung der Grundrechte und der Cybersicherheit sorgen.

In den Fällen, in denen es derzeit keine Instrumente gibt, wird erwartet, dass der Technologiefahrplan Empfehlungen zu deren Entwicklung und dazu enthält, wie sowohl für die Vereinbarkeit mit dem EU-Rechtsrahmen als auch für die Cybersicherheit gesorgt werden kann. Die Ergebnisse des Technologiefahrplans können auch in spezifische Maßnahmen zur Förderung eines koordinierten Ansatzes für die Normung einfließen.

Die Entschlüsselungsplattform von Europol hat sich als maßgeblich für die Unterstützung wichtiger Strafsachen erwiesen, einschließlich solcher, die aus den Fällen Sky ECC[45] und EncroChat hervorgegangen sind. Verbesserte Entschlüsselungsfähigkeiten, die unter anderem durch weitere Investitionen in künstliche Intelligenz (KI) und Hochleistungsrechnen vorangebracht werden, sind erforderlich, um sicherzustellen, dass die Strafverfolgungsbehörden in der Lage sind, immer komplexere Algorithmen zu entschlüsseln.

Die Hochrangige Gruppe empfahl[46], die Mittel aufzustocken, um Innovationen beim Zugang zu Daten zu unterstützen. Als Reaktion darauf **wird die Kommission die Forschung und Entwicklung neuer Entschlüsselungskapazitäten unterstützen**, um sicherzustellen, dass Europol nach 2030 gut gerüstet ist, um die Mitgliedstaaten angesichts neuer technologischer

[43] The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement | Europol.
[44] Empfehlungscluster 10, Abschlussbericht der Hochrangigen Gruppe.
[45] New major interventions to block encrypted communications of criminal networks | Europol.
[46] Empfehlungscluster 10, Abschlussbericht der Hochrangigen Gruppe.

Entwicklungen und der fortschrittlichsten Forschung in diesem Bereich zu unterstützen. Diese Initiative könnte eine Aufstockung der Mittel zur Unterstützung der Entschlüsselungsforschung sowie die Entwicklung und Implementierung von Instrumenten durch die Mitgliedstaaten umfassen. Die Mitgliedstaaten werden eng einbezogen, um ihre spezifischen Anforderungen zu teilen und um ihre Kapazitäten, Kompetenzen und technischen Ressourcen zu erhöhen, indem sie auf Technologien aufbauen, die auf EU-Ebene konzipiert wurden, und möglicherweise eine gemeinsame Beschaffung in Erwägung ziehen.

Zentrale Maßnahmen

Die Kommission wird

- **einen Technologiefahrplan für Verschlüsselung vorlegen (im zweiten Quartal 2026);**
- **die Forschung und Entwicklung neuer Entschlüsselungskapazitäten unterstützen, um Europol mit Entschlüsselungsfähigkeiten der nächsten Generation auszustatten (ab 2030).**

V. Technologie und rechtmäßigen Zugang miteinander in Einklang bringen: Normung

Normen sind für die digitale Kommunikation von wesentlicher Bedeutung. Sie werden von einer Vielzahl von Akteuren, hauptsächlich in der Industrie, entwickelt, sorgen für die Interoperabilität zwischen Systemen und Geräten, die von Technologieanbietern entwickelt werden, und erleichtern die Einhaltung der rechtlichen Verpflichtungen, auch in Bezug auf den rechtmäßigen Zugang zu Strafverfolgungszwecken. Das Europäische Institut für Telekommunikationsnormen (ETSI) hat mehrere Normen im Bereich der rechtmäßigen Überwachung und der rechtmäßigen Offenlegung erarbeitet. Es bestehen jedoch Lücken, z. B. bei der fünften Generation von Mobiltelefonnetzen (5G), wo eine fehlende angemessene Berücksichtigung des rechtmäßigen Zugangs bei ihrer Entwicklung die Strafverfolgungs- und Justizbehörden daran gehindert hat, Zugang zu den Beweismitteln zu erhalten, die erforderlich sind, um Straftäter zu identifizieren und vor Gericht zu bringen[47].

Die Hochrangige Gruppe empfahl, bei der Entwicklung von Lösungen für den rechtmäßigen Zugang zu Systemen einen vorsichtigen Ansatz zu verfolgen und die Industrie nicht aufzufordern, Systeme zu integrieren, die die Verschlüsselung für alle Nutzer eines Dienstes allgemein oder systemisch schwächen könnten. Der rechtmäßige Zugang zu Daten muss zielgerichtet bleiben und fallweise auf bestimmte Nachrichten beschränkt sein.

Grundsätzlich sollten alle Lösungen auf der Grundlage klarer Normen umgesetzt werden, die unter Mitwirkung aller Interessenträger entwickelt werden, einschließlich Vertretern der Industrie und Sachverständigen aus den Bereichen Datenschutz, Privatsphäre und Cybersicherheit sowie Strafverfolgungsbeamten. Allerdings ist Vorsicht geboten, wenn es um Verschlüsselung geht, wie die Hochrangige Gruppe betont hat. Auf der Grundlage der im Technologiefahrplan ermittelten Lösungen werden spezifische Maßnahmen zur Förderung eines koordinierten Ansatzes für die Normung ins Auge gefasst.

[47] Siehe First report on Encryption from the EU Innovation Hub on Internal Security, 11. Juni 2024.

Jede Normung sollte den geltenden rechtlichen Anforderungen entsprechen und auf bewerteten Lösungen beruhen. Sie muss sicherstellen, dass der rechtmäßige Zugang weder mit den geltenden Cybersicherheitsnormen, wie sie im Rahmen der Cyberresilienz-Verordnung entwickelt wurden, noch mit den Normen, die die Umsetzung der NIS-2-Richtlinie unterstützen, kollidiert oder die Sicherheit von Produkten und Diensten anderweitig beeinträchtigt.

In Bezug auf die Empfehlungen der Hochrangigen Gruppe[48] **wird die Kommission ein EU-Konzept für die Normung im Bereich der inneren Sicherheit erarbeiten und straffen, wobei der Schwerpunkt auf der digitalen Forensik, der rechtmäßigen Offenlegung und der rechtmäßigen Überwachung des Telekommunikationsverkehrs liegen wird**. Dieses Konzept wird sich auf eine fortlaufende Situationsanalyse stützen, die von Strafverfolgungsbeamten durchgeführt wird, insbesondere im Rahmen der von Europol geleiteten Europäischen Arbeitsgruppe zur Normung für die innere Sicherheit. Diese Maßnahme wird zudem die Ressourcen und den Umfang der Arbeitsgruppe erhöhen und eine weitere Zusammenarbeit mit anderen Normungsinitiativen, insbesondere in den Bereichen KI und digitale Forensik, mit sich bringen. Damit soll sichergestellt werden, dass Sicherheitsbelange in die Normungspolitik einbezogen werden. Darüber hinaus umfasst diese Initiative die Erarbeitung und Organisation von Schulungen zur Normung im Bereich der Sicherheit und die Bereitstellung finanzieller Unterstützung aus dem Fonds für die innere Sicherheit für Sachverständige, die an einschlägigen Normungsforen teilnehmen. Außerdem wird sie einschlägige Governance-Mechanismen umfassen.

Zentrale Maßnahmen

- **Die Kommission wird in enger Zusammenarbeit mit Europol Normungstätigkeiten für den rechtmäßigen Zugang entwickeln und straffen, die durch geeignete Governance-Mechanismen unterstützt werden (vom zweiten Quartal 2025 bis zum zweiten Quartal 2027).**

- **Die Mitgliedstaaten werden aufgefordert, ausreichende Ressourcen bereitzustellen, um sicherzustellen, dass Sicherheitsfachkräfte an den einschlägigen Normungsforen für den rechtmäßigen Zugang teilnehmen.**

VI. Wirksame und rechtmäßige Analyse von Beweismitteln: KI

Europol und Eurojust haben kürzlich festgestellt, dass bei immer mehr Ermittlungen sehr große Datenmengen zu verarbeiten sind[49]. In einem standardmäßigen Fall in Verbindung mit dem sexuellen Missbrauch von Kindern erfordern die Ermittlungen häufig eine Analyse von zwischen 1 und 3 Terabyte Datenmaterial, das 1 Million bis 10 Millionen Bilder und Tausende Stunden Videoaufnahmen umfassen kann[50]. Im Jahr 2023 wurden über das System Large File Exchange (LFE) von Europol 1 553 822 große Dateien ausgetauscht[51]. Im Fall EncroChat wurden mehr als 115 Millionen Gespräche zwischen Verdächtigen der organisierten Kriminalität abgefangen. In den folgenden Monaten konnten Europol und

[48] Empfehlungscluster 10, Abschlussbericht der Hochrangigen Gruppe.
[49] Common Challenges in Cybercrime, 2024 Review by Europol and Eurojust.
[50] Europol, Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet (IOCTA).
[51] Konsolidierter jährlicher Tätigkeitsbericht 2023 von Europol.

Strafverfolgungsbehörden mithilfe fortgeschrittener Analysetechniken und -mittel wie maschinellem Lernen Muster, Verbindungen und Hotspots ermitteln, was zur Festnahme von 6 558 Verdächtigen führte. Die niederländischen und französischen Behörden haben diese Informationen an ihre Amtskollegen in den EU-Mitgliedstaaten und Drittländern weitergegeben, was dazu führte, dass allein im Vereinigten Königreich mehr als 200 Mordanschläge vereitelt wurden[52].

Die kontinuierliche Zunahme der im Rahmen von Ermittlungen verarbeiteten Daten hat zur Folge, dass es schwierig wird, die Daten ohne umfangreiches Fachwissen, Rechenressourcen und spezialisierte Instrumente zu speichern, zu verwalten und wirksam zu analysieren. Europol und Eurojust bestätigten, dass das Datenvolumen für Ermittler überwältigend sein und zu höheren Bearbeitungszeiten sowie zu Problemen mit der Speicherkapazität führen kann. Häufig fehlt es den Mitgliedstaaten auch an den Mechanismen und der Infrastruktur, die für die Übermittlung großer Datenmengen an andere Mitgliedstaaten und Europol erforderlich sind.

Daher ist der Einsatz von KI für die Strafverfolgungsbehörden von entscheidender Bedeutung, um Straftaten zu verhüten, aufzudecken und zu untersuchen und so unsere Gesellschaften im digitalen Zeitalter zu schützen. KI-gestützte Lösungen können einfache Aufgaben wie maschinelle Übersetzung oder die Umwandlung von Sprache in Text oder komplexere Aufgaben wie das Filtern von Daten, die Korrelation von Beweismitteln aus massiven Datenmengen oder die Bekämpfung des böswilligen Einsatzes von KI ausführen. KI-gestützte Instrumente für Strafverfolgungsbehörden müssen präzise und transparent sein und vollständig mit dem EU-Rechtsrahmen für KI, Datenschutz und Privatsphäre im Einklang stehen, um vertrauenswürdige und ethische datengesteuerte Ermittlungen sicherzustellen. KI und Hochleistungsrechnen sind von größter Bedeutung, wenn es darum geht, Zugang zu verschlüsselten Daten zu erhalten sowie Ermittlungen und forensische Analysen zu unterstützen.

Als Reaktion auf die Empfehlungen der Hochrangigen Gruppe zur Aufstockung der Mittel für die Forschung und Entwicklung von Instrumenten für die KI-gestützte Datenanalyse und zur Festlegung klarer Arbeitsergebnisse[53] **wird die Kommission die Entwicklung und Einführung von KI-Lösungen fördern**. Dies umfasst gezielte Investitionen in die Entwicklung von Schlüsselfähigkeiten, wie z. B. Lösungen zur Identifizierung von Ermittlungsansätzen aus sehr großen Datenmengen unter uneingeschränkter Einhaltung der Grundsätze des Datenschutzes und der Privatsphäre oder Verbesserungen bei der Rückverfolgung von Transaktionen in Kryptowährungen. Ebenso könnte es möglich sein, Gelegenheiten für das Training, die Erprobung und die Bewertung von KI-Instrumenten in einem KI-Reallabor, wie in der KI-Verordnung[54] vorgesehen, mit Unterstützung und Anleitung der zuständigen Aufsichtsbehörden zu nutzen. Darüber hinaus könnten KI-Fabriken und künftige Gigafabriken die Entwicklung KI-gestützter Instrumente und Dienste für die Strafverfolgung unterstützen. Die Kommission sollte diese Bemühungen auf der Grundlage einer Bedarfsanalyse mit Interessenträgern, einschließlich des Innovationslabors von Europol

[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.
[53] Empfehlung 4, Empfehlungen der Hochrangigen Gruppe.
[54] Siehe Artikel 57 der KI-Verordnung.

und des Innovationszentrums für innere Sicherheit der EU-Agenturen im Bereich Justiz und Inneres, unterstützen.

Die Mitgliedstaaten können zu geringen Kosten oder kostenfrei Zugang zu einschlägigen Fähigkeiten haben, um die Vereinbarkeit mit den Anforderungen der KI-Verordnung sicherzustellen. Ein umfassendes KI-Konzept ist von entscheidender Bedeutung, einschließlich der Schaffung standardisierter Datenformate für jeden Austausch und der Ausarbeitung von Leitlinien für die Nutzung solcher Systeme im Einklang mit der KI-Verordnung und den geltenden EU-Datenschutzvorschriften. Diese Maßnahme könnte durch Mittel aus dem Fonds für die innere Sicherheit, dem Programm „Digitales Europa“ und Horizont Europa unterstützt werden. Ebenfalls gehört dazu die Unterstützung von Europol und der EMPACT-Gemeinschaft, um eine angemessene Anpassung an die operativen Erfordernisse sicherzustellen und die Einführung und durchgängige Berücksichtigung durch Strafverfolgungsbeamte zu fördern.

Zentrale Maßnahmen

Die <u>Kommission</u> wird

- **die Schaffung und Einführung neuer KI-Lösungen fördern und bestehende Lösungen für die Filterung und Analyse digitaler Beweismittel verbessern, unter anderem durch die umfassende Nutzung von KI-Reallaboren für ihre Entwicklung, Erprobung und Bewertung im Einklang mit der KI-Verordnung (von 2025 bis 2028);**

- **aufbauend auf der Arbeit des Innovationszentrums von Europol und des Labors der EU-Agenturen im Bereich Justiz und Inneres einen Dialog mit Strafverfolgungsbehörden und anderen Interessenträgern aufnehmen, um deren Bedarf zu ermitteln;**

- **die Ausarbeitung klarer Leitlinien für den Einsatz von KI in der Strafverfolgung unterstützen;**

- **Pilotprojekte zur Entwicklung und zum Training rechtlich und technisch fundierter KI-Lösungen für digitale Forensik, Datenanalyse und andere Ermittlungsinstrumente für die Strafverfolgung unterstützen.**