Rat der
Europäischen Union

Brüssel, den 13. März 2025
(OR. en)

15941/2/24
REV 2

COSI 214
ENFOPOL 463
IXIM 234
CATS 109
COPEN 500
CYBER 342
DATAPROTECT 332

VERMERK

Absender:	Vorsitz
Empfänger:	Delegationen
Nr. Vordok.:	11281/24
Betr.:	Abschlussbericht der Hochrangigen Gruppe für den Zugang zu Daten für eine wirksame Strafverfolgung

Im Namen der Ko-Vorsitzenden der Hochrangigen Gruppe für den Zugang zu Daten für eine wirksame Strafverfolgung übermittelt der Vorsitz den Delegationen beiliegend den Abschlussbericht der Hochrangigen Gruppe.

Diese überarbeitete Fassung enthält redaktionelle Änderungen, die im Zuge der sprachlichen Überprüfung vorgenommen wurden.

ANLAGE

Abschlussbericht der Hochrangigen Gruppe für den Zugang zu Daten für eine wirksame Strafverfolgung

15. November 2024

Die geäußerten Meinungen sind ausschließlich die Meinungen der Experten der Hochrangigen Gruppe und sollten nicht als repräsentativ für die offiziellen Standpunkte der Europäischen Kommission oder des Rates betrachtet werden.

Bei der Umsetzung der Empfehlungen der Hochrangigen Gruppe für den Zugang zu Daten für eine wirksame Strafverfolgung müssen die Zuständigkeiten der Mitgliedstaaten in vollem Umfang gewahrt werden. Die Empfehlungen gelten nur für Strafverfolgungsmaßnahmen und kommerzielle Instrumente, die für justizielle Zwecke eingesetzt werden, und lassen die ausschließliche Zuständigkeit der Mitgliedstaaten für die nationale Sicherheit unberührt. Souveräne Instrumente und Instrumente, die ausschließlich für Zwecke der nationalen Sicherheit verwendet und/oder entwickelt werden, sind daher vom Anwendungsbereich dieser Empfehlungen ausgenommen.

Inhaltsverzeichnis

Zusammenfassung

Die Europäische Union bildet einen Raum der Freiheit, der Sicherheit und des Rechts, in dem die Grundrechte und die verschiedenen Rechtsordnungen und -traditionen der Mitgliedstaaten geachtet werden. Sie wirkt darauf hin, durch Maßnahmen zur Verhütung und Bekämpfung von Kriminalität und zur Erleichterung der Koordinierung und der Zusammenarbeit zwischen den Strafverfolgungs- und Justizbehörden sowie sonstigen zuständigen Behörden ein hohes Maß an Sicherheit[1] zu gewährleisten.

Technologische Entwicklungen und die Digitalisierung unserer Gesellschaften haben sowohl zu erheblichen Veränderungen im Alltag der Bürgerinnen und Bürger als auch zu neuen Herausforderungen für die Strafverfolgungs- und Justizbehörden bei der Gewährleistung eines hohen Sicherheitsniveaus auf nationaler Ebene und auf EU-Ebene geführt. Im heutigen digitalen Zeitalter haben fast alle strafrechtlichen Ermittlungen eine digitale Komponente. Dies wurde im April 2023 im Konzeptpapier für die Hochrangige Expertengruppe für den Zugang zu Daten für eine wirksame Strafverfolgung behandelt:

> Technologien und Instrumente [...] werden auch für kriminelle Zwecke missbraucht. Diese Entwicklung macht es zunehmend schwieriger, eine wirksame Strafverfolgung in der gesamten EU aufrechtzuerhalten, um die öffentliche Sicherheit zu schützen und Straftaten zu verhüten, aufzudecken, zu ermitteln und zu verfolgen und um den berechtigten Erwartungen der Opfer in Bezug auf Gerechtigkeit und Entschädigung gerecht zu werden. Wenn diese Entwicklung nicht richtig angegangen wird, besteht die reale Gefahr, dass dieser gegenwärtige Trend es den Kriminellen ermöglicht, „unter dem Radar zu fliegen“ [...]. Dies stellt eine ernsthafte Bedrohung für die Sicherheit des Einzelnen und der Gesellschaft dar und kann letztlich die positive Verpflichtung des Staates, die Rechtsstaatlichkeit und eine demokratische Gesellschaft weiterhin zu gewährleisten, behindern[2].

[1] Für die Zwecke dieses Dokuments bezeichnet der Begriff „Sicherheit“ die Bekämpfung von Kriminalität oder die Verhütung von Gefahren für die öffentliche Sicherheit.

[2] Dok. 8281/23 vom 13. April 2023.

Das Recht auf Achtung des Privat- und Familienlebens, der Wohnung und der Kommunikation sowie das Recht auf den Schutz personenbezogener Daten sind in der Charta der Grundrechte der EU garantiert. Die Vertraulichkeit der Kommunikation, sei es in schriftlicher Form oder telefonisch, ist eine wichtige Errungenschaft demokratischer Gesellschaften, die sicherstellt, dass weder der Staat noch private Akteure in die Meinungsfreiheit der Menschen eingreifen dürfen, und die die Entfaltung einer lebendigen Zivilgesellschaft ermöglicht. Die Ausübung dieser Rechte kann gesetzlich eingeschränkt werden, insbesondere in Bezug auf Maßnahmen zum Schutz der nationalen Sicherheit, der Landesverteidigung oder der öffentlichen Sicherheit und zur Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder der unerlaubten Nutzung elektronischer Kommunikationssysteme, sofern diese Maßnahmen in einer demokratischen Gesellschaft notwendig, angemessen und verhältnismäßig sind. Daher dürfen Strafverfolgungs- und Justizbehörden schriftliche Nachrichten öffnen und lesen, Telefonanrufe abfangen und Gespräche abhören, wenn dies für notwendig, verhältnismäßig und gerechtfertigt erachtet wird, wenn diese Maßnahmen mit den geltenden Rechtsvorschriften im Einklang stehen und wenn sie unter gebührender Achtung der Grundrechte durchgeführt werden. Diese Möglichkeit sollte allen zuständigen Behörden unabhängig von technologischen Entwicklungen offenstehen. Die Verbreitung neuer Formen der interpersonellen Kommunikation, die in den letzten Jahren stattgefunden hat, bedeutet, dass sich die gesamte Gesellschaft an die neuen Gegebenheiten anpassen muss. Wir müssen dafür sorgen, dass die Kommunikation zwischen den Bürgerinnen und Bürgern weiterhin geschützt wird und dass gleichzeitig die Strafverfolgungs- und Justizbehörden weiterhin in der Lage sind, ihrer Pflicht nachzukommen, die Bürgerinnen und Bürger durch die Verhütung und Bekämpfung von schwerer und organisierter Kriminalität und von Terrorismus zu schützen. Es besteht dringender Anpassungsbedarf, und die Experten fordern die politischen Entscheidungsträger auf, umgehend zu handeln, da die Strafverfolgungsbehörden bereits hinter dem Tempo der technologischen Entwicklungen zurückbleiben, was sich unmittelbar auf ihre Fähigkeit auswirkt, die Rechte der Bürgerinnen und Bürger zu wahren.

Auf der informellen Tagung der Ministerinnen und Minister für Justiz und Inneres vom 26. Januar 2023 haben die Innenministerinnen und -minister über die Herausforderungen der technologischen Entwicklungen für die Strafverfolgung im digitalen Zeitalter beraten. Sie äußerten ferner ihre Besorgnis darüber, dass die Arbeit der Strafverfolgungsbehörden aufgrund der geltenden Vorschriften und ihrer Auslegung durch die Rechtsprechung sowie aufgrund praktischer und operativer Hindernisse zunehmend schwieriger wird, insbesondere im Hinblick auf die Vorratsspeicherung von und den Zugang zu Daten, die für die Ermittlung und Verfolgung von Straftaten erforderlich sind[3].

[3] Siehe Dok. 7184/1/23 REV 1 vom 23. März 2023 für eine Zusammenstellung der Kommentare der Mitgliedstaaten.

Nach diesen Beratungen billigte der Rat die Einsetzung einer Arbeitsgruppe, die eine strategische und zukunftsorientierte Vision über den wirksamen und rechtmäßigen Zugang zu Daten, elektronischen Beweismitteln und Informationen für die Strafverfolgungs- und Justizbehörden im digitalen Zeitalter entwickeln sollte: die **Hochrangige Gruppe für den Zugang zu Daten für eine wirksame Strafverfolgung**[4].

Ziel der Hochrangigen Gruppe war es, Lösungen für die Herausforderung zu finden, die mit der Gewährung eines rechtmäßigen Datenzugangs verbunden ist, um ein hohes Maß an Sicherheit für alle in der EU lebenden Menschen zu wahren und gleichzeitig die Einhaltung der Grundrechte, einschließlich des Rechts auf Privatsphäre und auf Datenschutz, sowie ein hohes Maß an Cybersicherheit durch effiziente und zukunftssichere Lösungen zu gewährleisten.

Die **42 Empfehlungen**[5], die das wichtigste Ergebnis der Arbeit der Hochrangigen Gruppe sind, kommen zu einer Zeit, in der die Forderungen nach einer Rechenschaftspflicht im Internet zunehmen. Die Empfehlungen gehen aktuelle und zu erwartende Herausforderungen im Hinblick auf technologische Entwicklungen an und zielen darauf ab, ein umfassendes EU-Konzept zur Gewährleistung wirksamer strafrechtlicher Ermittlungen und Strafverfolgungsmaßnahmen zu ermöglichen. Die Empfehlungen sind in drei Cluster untergliedert: **Kapazitätsaufbau, Zusammenarbeit mit der Industrie und Normung sowie Gesetzgebungsmaßnahmen.** Darin werden die Herausforderungen hervorgehoben, mit denen die Strafverfolgungsbehörden beim Zugang zu Daten in einem lesbaren Format für strafrechtliche Ermittlungen konfrontiert sind, aufgrund fehlender harmonisierter Verpflichtungen zur Vorratsdatenspeicherung und fehlender strenger Anforderungen der EU-Rechtsprechung, der zunehmenden Nutzung der Ende-zu-Ende-Verschlüsselung und der mangelnden Zusammenarbeit bestimmter nicht herkömmlicher Telekommunikationsdienste. In den Empfehlungen werden die Vorschriften über elektronische Beweismittel begrüßt, jedoch deren Grenzen bei der Bewältigung der Herausforderungen im Zusammenhang mit der Verschlüsselung hervorgehoben, und es wird eine engere Zusammenarbeit zwischen Strafverfolgungs- und Justizbehörden und Diensteanbietern gefordert, um auf einen ständigen Dialog und ein gegenseitiges Verständnis der operativen, technischen und geschäftlichen Bedürfnisse hinzuarbeiten und Schwierigkeiten beim Zugang zu verschlüsselten Daten zu überwinden. Experten zufolge wird eine engere Zusammenarbeit zwischen Strafverfolgungsbehörden und Diensteanbietern die Situation bis zu einem gewissen Grad verbessern; aber eine zukunftssichere Lösung erfordert auch, dass die Verpflichtungen zur Zusammenarbeit, denen die Diensteanbieter unterliegen, mittels Rechtsvorschriften durchgesetzt werden, ohne dass die Verschlüsselung für die Nutzer eines Dienstes allgemein oder systematisch geschwächt wird.

---

4 High-Level Group (HLG) on access to data for effective law enforcement – European Commission (europa.eu) (Hochrangige Gruppe für den Zugang zu Daten für eine wirksame Strafverfolgung – Europäische Kommission).

5 High-Level Group Recommendations (Empfehlungen der Hochrangigen Gruppe).

Der **Rat führte** am 13. Juni 2024 **einen Gedankenaustausch** über die Empfehlungen der Hochrangigen Gruppe, begrüßte weitgehend die von den Experten der Hochrangigen Gruppe geleistete Arbeit und hob die Notwendigkeit hervor, die Arbeit am Zugang zu Daten für eine wirksame Strafverfolgung zügig voranzubringen[6]. Die Innenministerinnen und -minister legten folgende Prioritäten fest: 1. die Schaffung eines harmonisierten EU-Rechtsrahmens für die Vorratsspeicherung von Daten zu Strafverfolgungszwecken, 2. die Festlegung von Vorschriften für den wirksamen Zugang zu Daten aus interpersoneller elektronischer Kommunikation sowie 3. die Einführung rechtlich und technisch fundierter Lösungen für den Zugriff auf verschlüsselte elektronische Kommunikation in Einzelfällen und auf der Grundlage einer richterlichen Anordnung zu Zwecken der Prävention, Ermittlung und Verfolgung schwerer und organisierter Kriminalität sowie von Terrorismus.

Ferner traten die Ministerinnen und Minister für eine Stärkung der Wirkung der EU im Bereich der Normung von Protokollen und Technologien sowie für einen koordinierten Ansatz bei der Zertifizierung von Instrumenten und Verfahren der digitalen Forensik ein. Schließlich betonten sie die Notwendigkeit, einen Fahrplan zur Umsetzung der Empfehlungen mit klaren Fristen, einer Bewertung der Machbarkeit und angemessener Finanzierung aufzustellen. Die Koordinierung der Umsetzung einzelner Empfehlungen wurde ebenfalls als wichtig erachtet.

In diesem Abschlussbericht sollen die von den Experten ermittelten Herausforderungen im Einzelnen beschrieben und Optionen für die Fortsetzung der Arbeiten und die **Umsetzung der Empfehlungen** dargelegt werden. Es werden mehrere zentrale Fragen dargelegt, die von den Experten ermittelt und im Einklang mit dem Mandat der Hochrangigen Gruppe drei Arbeitsbereichen zugeordnet wurden.

Erstens ist der Zugang zu Daten für die **digitale Forensik** von entscheidender Bedeutung, damit die Strafverfolgungsbehörden Beweismittel aus elektronischen Geräten erheben und analysieren können. Diese Daten liefern zuverlässige Informationen über kriminelle Aktivitäten und zur Identifizierung von Straftätern. Angesichts des raschen Fortschritts und der weit verbreiteten Nutzung bestimmter Technologien wie Verschlüsselung müssen die Strafverfolgungsbehörden ihre Ressourcen, Kompetenzen und technischen Lösungen für den Zugang zu verschlüsselten Daten ausbauen. In diesem Zusammenhang und im Hinblick auf die Nutzung kommerzieller Lösungen kann eine wirksame grenzüberschreitende Zusammenarbeit durch den Austausch von Fachwissen, die Entwicklung standardisierter Instrumente und Verfahren und die Bündelung von Ressourcen Unterstützung leisten. Die Experten waren sich jedoch darin einig, dass der Kapazitätsaufbau allein die Strafverfolgungskapazitäten nicht verbessern wird. Die Ermöglichung des Zugangs zu Daten in einem lesbaren Format unter klar geregelten Umständen wurde von einigen Experten als eine nachhaltigere langfristige Lösung angesehen.

---

[6] Dok. 11281/24 vom 21. Juni 2024.

Zweitens sind harmonisierte und kohärente Rechtsvorschriften über die **Vorratsdatenspeicherung**, die voll und ganz im Einklang mit den Grundrechten stehen, erforderlich, damit die Strafverfolgungsbehörden Straftaten wirksam untersuchen und verfolgen können. Angesichts des raschen technologischen Fortschritts gewinnt der zeitnahe Zugang der Strafverfolgungsbehörden zu einschlägigen, von den Anbietern gespeicherten Daten zunehmend an Bedeutung. Insbesondere der Zugang zu Kommunikationsmetadaten, die von Diensteanbietern gespeichert werden, ist für die Identifizierung von Verdächtigen und die Aufdeckung ihrer Aktivitäten von wesentlicher Bedeutung und hat sich für den Fortschritt bei Ermittlungen als wichtig erwiesen.

Drittens ist die **rechtmäßige Überwachung** unerlässlich, um gegen organisierte Kriminalität und terroristische Gruppen wirksam zu ermitteln und sie strafrechtlich zu verfolgen. Sie ermöglicht es den Behörden, auf der Grundlage gerichtlicher Anordnungen und unter uneingeschränkter Achtung der Grundrechte, von Diensteanbietern die Bereitstellung des Inhalts einer Kommunikation zu verlangen, und dieser Inhalt bietet wertvolle Einblicke in kriminelle Aktivitäten. Angesichts der Verlagerung von herkömmlichen Kommunikationsanbietern zu Over-the-top-Diensten (OTT) im Sinne des Europäischen Kodex für die elektronische Kommunikation (EKEK)[7] und der Tatsache, dass Kriminelle zunehmend zu Ende-zu-Ende-verschlüsselten Plattformen[8] übergehen, erfordert der rechtmäßige Zugang zu Kommunikation in Echtzeit eine Bewertung der Notwendigkeit klarer Regeln für die Zusammenarbeit zwischen Strafverfolgungsbehörden und Technologieunternehmen sowie eine verstärkte Zusammenarbeit auf EU-Ebene, um grenzüberschreitende Ersuchen zu erleichtern.

Die Empfehlungen und der Inhalt dieses Abschlussberichts spiegeln **allein** die Erwartungen und Forderungen der **Experten der Hochrangigen Gruppe** wider.

Mit der Vorlage dieses Berichts **hat die Hochrangige Gruppe ihre Arbeit abgeschlossen** und ersucht die Kommission, die Mitgliedstaaten, das Europäische Parlament und alle einschlägigen Interessenträger, sich bei der Entwicklung von Maßnahmen zur Bewältigung des Problems des Zugangs zu Daten für eine wirksame Strafverfolgung an den Empfehlungen und dem Bericht zu orientieren. Diese Maßnahmen sollten mit einem klaren Narrativ einhergehen, das die Dringlichkeit verdeutlicht, mit der wichtige Maßnahmen ergriffen werden müssen, um einen wirksamen rechtmäßigen Zugang zu Daten zu gewährleisten. Die Experten fordern alle Organe und Einrichtungen der EU auf, diese Arbeit unverzüglich durch die Umsetzung konkreter Initiativen in einem speziellen Fahrplan weiterzuführen.

---

[7] Mit der Richtlinie (EU) 2018/1972 vom 11. Dezember 2018 über den europäischen Kodex für die elektronische Kommunikation wird der Teil des Rechtsrahmens, der für die herkömmliche Telekommunikation gilt, auf Unternehmen ausgeweitet, die internetgestützte Dienste über eine Telekommunikationsinfrastruktur anbieten, die sie nicht besitzen oder verwalten, einschließlich nummernunabhängiger interpersoneller Kommunikationsdienste (NI-ICS).

[8] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2024 (Bewertung der Bedrohungslage im Bereich der organisierten Kriminalität im Internet 2024).

Rechtmäßiger Zugang: die wichtigsten Herausforderungen

Unsere Fähigkeit, Kriminalität zu bekämpfen und die Sicherheit der EU zu gewährleisten, hat sich in den vergangenen Jahren in vielen Bereichen verbessert. Die Arbeit der Strafverfolgungsbehörden und die justizielle Zusammenarbeit sind wirksamer geworden, neue Rechtsvorschriften und Instrumente zur Bekämpfung von schwerer und organisierter Kriminalität wurden eingeführt, und die gemeinsamen Bemühungen zur Bekämpfung von Migrantenschleusung, Menschenhandel und unerlaubtem Handel mit Feuerwaffen und Drogen, Korruption sowie anderen schweren Straftaten wurden verstärkt.

Jedoch stehen die Strafverfolgungsbehörden tagtäglich vor neuen Herausforderungen, wenn es darum geht, die Sicherheit unserer Bürgerinnen und Bürger zu gewährleisten, insbesondere jenen, die sich durch die Digitalisierung unserer Gesellschaft ergeben.

Digitale Technologien verändern unser Leben – von der Art und Weise, wie wir kommunizieren, bis hin zur Art und Weise, wie wir leben und arbeiten –, und die gesellschaftlichen Aspekte dieses Wandels sind tiefgreifend. Die Digitalisierung hat das Potenzial, Lösungen für viele der Herausforderungen bereitzustellen, die sich Europa und den Europäerinnen und Europäern stellen, und sie bietet eine Vielzahl von Chancen – zur Schaffung von Arbeitsplätzen, zur Verbesserung der Bildung, zur Förderung von Wettbewerbsfähigkeit und Innovation, zur Bekämpfung des Klimawandels, zur Erleichterung des grünen Wandels und vieles mehr.

Die Digitalisierung schafft jedoch auch die Voraussetzungen für Kriminelle, den technologischen Fortschritt zu nutzen, um – sowohl online als auch offline – Straftaten zu begehen. Verschlüsselte Geräte und Anwendungen, neue Kommunikationsbetreiber, virtuelle private Netze (VPNs) usw. sind darauf ausgelegt, die Privatsphäre rechtmäßiger Nutzer zu schützen. Sie geben jedoch auch Kriminellen wirksame Mittel an die Hand, um ihre Identität zu verbergen, ihre kriminellen Produkte und Dienstleistungen zu vermarkten, Zahlungen zu kanalisieren und ihre Aktivitäten und Kommunikation zu verschleiern und so Aufdeckung, Ermittlung und Verfolgung effektiv zu vermeiden. Wenngleich es Instrumente und Dienste gibt, die eigens für illegale Aktivitäten entwickelt wurden und in erster Linie für deren Durchführung genutzt werden, so gibt es doch deutliche Hinweise darauf, dass Kriminelle zunehmend auf Maßnahmen zum Schutz der Privatsphäre zurückgreifen, die von rechtmäßigen elektronischen Kommunikationsdiensten zur Verfügung gestellt werden. ***Die Strafverfolgungsbehörden geraten in dieser Hinsicht oft ins Hintertreffen gegenüber Kriminellen, da sie nicht über ausreichend Personal sowie angemessene Instrumente und Mittel verfügen, um dieser Herausforderung wirksam zu begegnen.*** Infolge dieser Entwicklungen hat sich der Zugang zu Daten für Strafverfolgungszwecke in den letzten Jahren als eine der größten Herausforderungen für strafrechtliche Ermittlungen und Strafverfolgungen herausgestellt. Dennoch gab es bemerkenswerte Erfolge zu verzeichnen: So ist es beispielsweise Strafverfolgungsbehörden gelungen, verschlüsselte Kommunikationsnetzwerke krimineller Art wie EncroChat und SkyECC aufzulösen; ferner führen sie weiterhin Operationen wie „Desert Light“ durch, in deren Rahmen im November 2022 ein „Superkartell“ von Kokainhändlern zerschlagen wurde. Die Entschlüsselungsplattform von Europol hat in den letzten paar Jahren mehrere Ermittlungen auf hoher Ebene unterstützt und somit zu erfolgreichen Strafverfolgungsmaßnahmen gegen Terrorismus sowie schwere und organisierte Kriminalität beigetragen.

Hinter diesen Erfolgen verbergen sich jedoch zahlreiche verzögerte und erfolglose Ermittlungen – in der Tat berichten Praktiker über anhaltende Schwierigkeiten bei der fristgerechten Erfüllung des operativen Bedarfs.

Indem die Behörden rechtmäßigen Zugang erhalten, um kriminelle Kommunikation gezielt zu überwachen und abzufangen und die Handlungen von Straftätern zu unterbinden, wird die Nutzung von Technologie für kriminelle Zwecke erschwert. Ohne einen soliden Rechtsrahmen und angemessene Ressourcen hingegen werden die Strafverfolgungsbehörden weiterhin gegen unüberwindbare Schwierigkeiten ankämpfen müssen, und es besteht die Gefahr, dass kritische Beweismittel – aus unterschiedlichen Gründen – außer Reichweite bleiben.

- **Daten sind nicht immer verfügbar**, insbesondere wenn sie aufgrund uneinheitlicher und unzureichender Vorschriften über die Vorratsdatenspeicherung für Strafverfolgungszwecke gelöscht wurden. Diese Lücke stellt eine ernsthafte Behinderung von Ermittlungen zu schwerer und organisierter Kriminalität dar. Tatsächlich gaben fast die Hälfte der in der Studie von 2023 im Rahmen des SIRIUS-Projekts[9] befragten Ermittler das Fehlen einer harmonisierten Regelung für die Vorratsdatenspeicherung als Haupthindernis für ihre Arbeit an. Ohne harmonisierte Vorschriften besteht die Gefahr, dass wichtige Daten unzugänglich bleiben und somit eine wirksame Verbrechensbekämpfung untergraben wird.
- **Daten können nicht abgerufen werden**, insbesondere wenn die Extraktion von einem Gerät fehlschlägt. Der Mangel an notwendigen Kompetenzen, angemessenen Instrumenten und hinreichender Zusammenarbeit mit Geräteherstellern und durch diese macht die digitale Forensik beschwerlich, teuer und zeitaufwändig, wenn nicht sogar völlig undurchführbar. Dies führt zu einer erheblichen Behinderung wirksamer Ermittlungen. Ohne fortgeschrittene forensische Fähigkeiten und Kompetenzen und eine bessere Zusammenarbeit mit der Industrie und zwischen den nationalen Behörden bleiben wichtige digitale Beweismittel unzugänglich, was ernsthafte Auswirkungen auf die Bemühungen der Strafverfolgungsbehörden hat.
- **Daten können nicht immer gelesen werden**, z. B. weil sie verschlüsselt sind. Viele Dienste verwenden mittlerweile Ende-zu-Ende-Verschlüsselung, um die Vertraulichkeit der Kommunikation, die Privatsphäre und die Cybersicherheit zu schützen. Dies kann es jedoch für die Strafverfolgung äußerst schwierig machen, auf Kommunikationsdaten zuzugreifen. Das bedeutet, dass es oft unmöglich ist, legal abgefangene Daten zu entschlüsseln. Ohne die Fähigkeit, diese Daten zu lesen, bleiben wichtige Beweismittel verborgen, und somit werden die Ermittlungen zu Straftaten erheblich erschwert.

[9] SIRIUS Grenzüberschreitender Zugang zu elektronischen Beweismitteln (SIRIUS-Projekt), https://www.europol.europa.eu/operations-services-innovation/sirius-project.

- **Daten können nicht immer analysiert werden**, z. B. sind nicht immer die Technologien und/oder Humanressourcen verfügbar, um große Datenmengen zu durchsuchen oder Daten in einer wirksamen Weise zu filtern und zu analysieren, die mit den Grundwerten der EU und den Rechtsrahmen der EU und der Mitgliedstaaten vereinbar ist.

- **Daten können nicht erhalten werden**, aufgrund von Normenkollisionen zwischen Rechtsordnungen. Daten überschreiten oft internationale Grenzen, was zu komplexen Herausforderungen in Bezug auf die Gerichtsbarkeit führt. In den einzelnen Ländern gibt es unterschiedliche Gesetze und Vorschriften über den Zugang zu Daten, weshalb es schwierig ist, im Ausland gespeicherte Daten zu erhalten. Die neue Verordnung und Richtlinie der EU über elektronische Beweismittel sind wichtige Schritte, um dies zu erleichtern, aber es muss noch viel getan werden, um diese Maßnahmen vollständig umzusetzen – und ohne eine vollständige Umsetzung bleibt der Zugang zu wichtigen Daten aus anderen Ländern eine große Herausforderung für die Strafverfolgung.

Dies sind einige der Herausforderungen, mit denen die Strafverfolgungsbehörden im Alltag konfrontiert sind.

Kriminelle passen ihr Verhalten ständig an, um sich der Aufdeckung zu entziehen. Aus den verfügbaren Statistiken[10] geht hervor, dass Kriminelle zunehmend zu rechtmäßigen Plattformen mit Ende-zu-Ende-Verschlüsselung übergehen. Sobald jedoch wirksame Gegenmaßnahmen gefunden sind, werden sie voraussichtlich wieder auf andere Kommunikationskanäle umsteigen. Aus diesem Grund ist es von entscheidender Bedeutung, dass die Strafverfolgungsbehörden – mit Unterstützung durch Experten aus allen einschlägigen Gemeinschaften – in der Lage sind, technologische Entwicklungen zu überwachen und Veränderungen im kriminellen Verhalten zu antizipieren; dies gilt insbesondere im Zusammenhang mit 6G, dem Internet der Dinge (IoT) und der Satellitenkommunikation. Darüber hinaus müssen die Fähigkeiten, die erfolgreiche Operationen gegen spezielle kriminelle Kommunikationsdienste (z. B. EncroChat, Ghost ECC) ermöglicht haben, beibehalten und angepasst werden, damit sie für die Bewältigung künftiger ähnlicher Herausforderungen genutzt werden können.

[10] IOCTA 2024 von Europol.

Die Strafverfolgungsbehörden benötigen zunehmend rechtmäßigen Zugang zu digitalen Informationen. Da Kriminelle immer mehr auf Online-Dienste zurückgreifen, haben die Datenanfragen an Anbieter von Online-Diensten zugenommen; die Zahl solcher Anfragen hat sich zwischen 2017 und 2022 verdreifacht[11]. Kommunikationsdaten (sowohl Metadaten als auch Inhaltsdaten) sind für viele strafrechtliche Ermittlungen von entscheidender Bedeutung. Es wird davon ausgegangen, dass der Zugang zu digitalen Beweismitteln bei 85 % aller Ermittlungen eine zentrale Rolle spielt[12]. Die neuen Vorschriften über den grenzüberschreitenden Zugang zu elektronischen Beweismitteln werden die Fähigkeit der zuständigen Behörden, auf diese Daten zuzugreifen, erhöhen. Diese Vorschriften können jedoch nur funktionieren, wenn die Daten in einem lesbaren Format verfügbar sind. Gleichermaßen sind der Zugang zu in beschlagnahmten Geräten gespeicherten Daten und die rechtmäßige Überwachung von Kommunikationen mit erheblichen Herausforderungen verbunden, und zwar sowohl in rechtlicher als auch in praktischer Hinsicht. Wenn es darum geht, Daten auf dem Übermittlungsweg in grenzüberschreitenden Fällen wirksam abzufangen, können die Mitgliedstaaten im Wege des Übereinkommens über die Rechtshilfe in Strafsachen[13] und der Europäischen Ermittlungsanordnung[14] um justizielle Zusammenarbeit ersuchen; diese Instrumente wurden jedoch größtenteils für den Austausch physischer Beweismittel konzipiert, und ihre Wirksamkeit könnte im Kontext der technologischen Entwicklungen begrenzt sein.

Der rechtmäßige Zugang muss strengen Bedingungen unterliegen, die im nationalen, europäischen und internationalen Recht verankert sind, und es müssen auf Transparenz und Rechenschaftspflicht beruhende Verfahren vorhanden sein, um diesen Zugang zu regeln, unter anderem indem jede unrechtmäßige Offenlegung von Geschäftsgeheimnissen vermieden wird und indem im Fall einer rechtmäßigen Offenlegung sichergestellt wird, dass geeignete Maßnahmen ergriffen werden, um deren Vertraulichkeit zu wahren.

Der rechtmäßige Zugang muss den Grundsätzen der Notwendigkeit und Verhältnismäßigkeit in vollem Umfang entsprechen und erforderlichenfalls von einem Gericht oder einer unabhängigen Behörde genehmigt werden. Das Recht auf Zugang zu Daten muss im Gleichgewicht zu robusten Maßnahmen zum Schutz der Privatsphäre und zur Gewährleistung der Cybersicherheit stehen (z. B. Verschlüsselung, Firewalls sowie Antiviren- und Anti-Malware-Software). Dabei trägt es zur Wahrung der Privatsphäre der einzelnen Nutzer bei, wenn sichergestellt wird, dass der Datenzugang auf das für die Zwecke einer Ermittlung erforderliche Maß beschränkt ist.

---

11 SIRIUS-Projekt.

12 Folgenabschätzung der Kommission zu den Vorschlägen für eine Verordnung über elektronische Beweismittel und eine Richtlinie über elektronische Beweismittel (17. April 2018).

13 MLA - Council of Europe standards - PC-OC (coe.int).

14 https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex:32014L0041.

Während der rechtmäßige Zugang zu Daten für Strafverfolgungszwecke eine Grundvoraussetzung dafür ist, unseren Bürgerinnen und Bürgern ein Höchstmaß an Sicherheit zu bieten, darf dies nicht auf Kosten der Grundrechte oder der Cybersicherheit von Systemen und Produkten gehen. Es darf keinen Kompromiss zwischen dem Schutz der Unversehrtheit und Sicherheit der Menschen einerseits und ihren Rechten andererseits geben; vielmehr muss ein Gleichgewicht gefunden werden, mit dem sichergestellt wird, dass das eine das andere nicht beeinträchtigt. Die EU und die Mitgliedstaaten sind gleichermaßen verpflichtet, dafür zu sorgen, dass die Bürgerinnen und Bürger ein hohes Maß an Schutz ihrer Grundrechte genießen können und dass sie sich im Alltag sicher fühlen. Technologische Entwicklungen dürfen keine sicheren Zufluchtsorte für Kriminelle schaffen: Wenn ein begründeter Verdacht besteht, dass eine Straftat begangen wurde oder unmittelbar bevorsteht, müssen die Strafverfolgungsbehörden Zugang zu Instrumenten haben, die sie in die Lage versetzen, auf die entsprechenden Daten zuzugreifen.

In der Europäischen Menschenrechtskonvention, den nationalen Verfassungen und der EU-Grundrechtecharta wird jeweils anerkannt, dass jeder das Recht auf ein Privatleben hat und dass dazu auch die persönliche Kommunikation gehört. In der EU-Grundrechtecharta ist zudem das Recht auf Datenschutz festgelegt. Die Rechte auf Privatsphäre und auf Schutz personenbezogener Daten können keine uneingeschränkte Geltung beanspruchen, sondern müssen im Hinblick auf ihre gesellschaftliche Funktion gesehen werden[15]. Behörden dürfen nicht in die Ausübung dieser Rechte eingreifen, ***es sei denn dieses Eingreifen steht im Einklang mit dem Gesetz, achtet den Wesensgehalt der Rechte und ist in einer demokratischen Gesellschaft notwendig und verhältnismäßig***. Unter diesen Bedingungen können die Rechte auf Privatsphäre und auf Schutz personenbezogener Daten eingeschränkt werden, auch im Interesse der nationalen und öffentlichen Sicherheit und zur Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten.

Eine solide Rechenschaftspflicht ist von entscheidender Bedeutung. In unseren demokratischen Gesellschaften liegt es in der Verantwortung der Gesetzgeber, die Voraussetzungen für eine solche Rechenschaftspflicht zu schaffen und somit für ein hohes Maß an Privatsphäre und Sicherheit zu sorgen. ***Privatsphäre und Sicherheit schließen sich nicht gegenseitig aus.***

Lösungen für die Gewährleistung eines rechtmäßigen Zugangs in begründeten Fällen müssen in Zusammenarbeit mit allen einschlägigen Interessenträgern, einschließlich der Industrie, erarbeitet werden, damit Innovation und eine starke Cybersicherheit gefördert werden. ***Bei der Gestaltung dieser Lösungen müssen alle einschlägigen Bedürfnisse und Anforderungen berücksichtigt werden, und sie dürfen nicht dem alleinigen Ermessen der Technologieunternehmen überlassen werden.***

---

[15] Urteil vom 30. April 2024, *La Quadrature du Net u. a.*, Rechtssache C-470/21 EU:C:2024:370, Rd. 70.

Technische Bewertungen müssen durchgeführt werden, bevor weitere Schritte ergriffen werden können, um den Bedenken einiger Cybersicherheitsexperten zu entsprechen, die es für äußerst komplex halten, einen rechtmäßigen Zugang zu gewährleisten und gleichzeitig eine starke Cybersicherheit aufrechtzuerhalten. ***Sowohl die Cybersicherheit von Produkten und Dienstleistungen als auch der rechtmäßige Zugang zu Daten ergeben sich aus rechtlichen Verpflichtungen und müssen daher nebeneinander bestehen können.*** Die Anforderungen des rechtmäßigen Zugangs müssen auf der Grundlage klarer Standards umgesetzt werden, die von allen einschlägigen Interessenträgern (einschließlich Vertretern der Industrie, Datenschutz- und Cybersicherheitsexperten und Strafverfolgungspraktikern) entwickelt wurden; ihre Umsetzung muss die einschlägigen rechtlichen Anforderungen widerspiegeln und sie muss auf der Grundlage hinreichend geprüfter potenzieller Lösungen erfolgen, damit gewährleistet ist, dass der rechtmäßige Zugang die Sicherheit von Produkten und Dienstleistungen nicht beeinträchtigt.

Viele Unternehmen und Diensteanbieter zögern, mit Strafverfolgungsbehörden zusammenzuarbeiten; Grund dafür ist die Rechtsunsicherheit im Zusammenhang mit freiwilligen Maßnahmen und die Gefahr einer Gegenreaktion seitens der Nutzer. Dieser Widerwille behindert die Ermittlungen. Darüber hinaus kann die Wahrnehmung, dass Nutzer ihre Privatsphäre über die öffentliche Sicherheit stellen, dazu führen, dass Industrieakteure weniger bereit sind, Kanäle für die Kommunikation mit den Strafverfolgungsbehörden zu öffnen und angepasste Mechanismen zu schaffen, die einen rechtmäßigen Zugang gewährleisten. Um dieses Problem anzugehen, ist ein klarer Rechtsrahmen für den rechtmäßigen Zugang zu Daten vonnöten. Nach den geltenden Rechtsvorschriften gibt es erhebliche Hindernisse, die die Bereitstellung eines solchen Zugangs – insbesondere auf freiwilliger Basis – erschweren.

Die Zusammenarbeit zwischen Unternehmen und Strafverfolgungsbehörden ist unzureichend und mangelhaft und muss durch klare Regeln ergänzt werden. ***Ohne klare und durchsetzbare rechtliche Verpflichtungen sind Unternehmen häufig nicht in der Lage, die Strafverfolgungsbehörden beim Zugang zu Daten zu unterstützen.***

In Ermangelung wirksamer Lösungen für die Gewährleistung des rechtmäßigen Zugangs ***werden auf Schwachstellen gestützte Lösungen oft als die einzige Option angesehen***.

Wenn abgefangene Daten (und möglicherweise andere aus einem Gerät extrahierte Daten) mit Instrumenten verarbeitet werden, die von privaten Unternehmen konzipiert wurden, haben die nationalen Behörden – ungeachtet etwaiger Zusicherungen dieser Unternehmen – keine wirkliche Sicht darauf, welche Daten durchsucht werden und wie sie durchsucht werden, und sie sind gezwungen, sich ausschließlich auf Bescheinigungen zu verlassen, die von der Regierung des Landes vorgelegt werden, in dem die Unternehmen, die die Abfangdienste anbieten, ansässig sind. Die Notwendigkeit, die genutzte Schwachstelle geheim zu halten, um die Wirksamkeit der Instrumente/Dienste zu bewahren, verschärft dieses Problem. Dies ist besonders problematisch, wenn der Anbieter außerhalb der EU ansässig ist.

Nicht zuletzt haben private Unternehmen, die Dienstleistungen für in die Privatsphäre eingreifende Ermittlungsmethoden anbieten, ein Interesse daran, ihre Gewinne zu maximieren, und können daher beschließen, ihre Instrumente an nicht-demokratische Regime zu verkaufen (wie es beim Skandal um die Firma Hacking Team der Fall war[16]).

Alternativ können Herausforderungen beim Zugang zu Daten ***die Strafverfolgungsbehörden dazu bewegen, noch einschneidendere Ermittlungsmaßnahmen anzuwenden***. In diesen Fällen sehen die Strafverfolgungsbehörden sich gezwungen, auf stärker in die Privatsphäre eingreifende Maßnahmen zurückzugreifen, wie etwa physische Überwachung anstatt Zugriff auf Geolokalisierungsdaten oder Hausdurchsuchungen anstatt rechtmäßiger Überwachung.

Die Tatsache, dass Strafverfolgungsbehörden nicht auf Daten zugreifen können, kann zu einem erheblichen Vertrauensverlust seitens der Öffentlichkeit gegenüber dem Justizsystem führen. Die Verzögerung oder Beeinträchtigung von Ermittlungen kann dazu führen, dass die Bürgerinnen und Bürger das System als unwirksam betrachten. Diese Aushöhlung des Vertrauens kann Recht und Ordnung untergraben und die Bereitschaft der Öffentlichkeit verringern, die Strafverfolgungsbehörden in ihren Bemühungen zu unterstützen.

Letztendlich ***versetzt der rechtmäßige Zugang die Strafverfolgungsbehörden in die Lage, den Opfern Gerechtigkeit zu verschaffen und sie vor weiterem Schaden zu schützen***. Daten können wichtige Anhaltspunkte für die Aufdeckung und Verfolgung aller Arten von Straftaten, sowohl offline als auch online, bieten. Einzelpersonen können schweren Formen von Cybermobbing, Identitätsdiebstahl, Betrug usw. ausgesetzt sein, die auf den kriminellen Missbrauch digitaler Technologien, Dienste und Kommunikation zurückzuführen sind. Diese Erfahrungen können schwerwiegende emotionale und psychische Folgen für die Opfer haben, die bestehende Ungleichheiten und Schwachstellen verschärfen.

[16] Siehe https://www.cbsnews.com/news/italy-hacking-team-breach-suggest-spy-software-sold-fbi-russia-vatican/.

Bei allen strafrechtlichen Ermittlungen sind Beweismittel erforderlich, um den Täter zu identifizieren oder seine Verantwortung vor einem Richter nachzuweisen. Sie können auch dazu beitragen, eine zu Unrecht beschuldigte Person zu entlasten. Können Ermittler und Staatsanwälte nicht auf die erforderlichen Informationen zugreifen, so sind sie möglicherweise nicht in der Lage, ihre Ermittlungen voranzubringen und die Täter zu identifizieren, was zu zusätzlichen Belastungen und finanziellen Verlusten für die Opfer führt und das Vertrauen in das Justizsystem untergräbt. Herkömmliche physische Beweismittel allein reichen nicht immer aus, um Verbindungen herzustellen und Anhaltspunkte zu finden. ***Die Strafverfolgung und die Justiz müssen für das digitale Zeitalter gerüstet sein. Nur dann werden sie in der Lage sein, unsere Gesellschaften und Volkswirtschaften vollständig*** vor den zunehmenden Bedrohungen ***zu schützen***, die von Cyberangriffen und hybriden Bedrohungen sowie von Aktivitäten der organisierten Kriminalität ausgehen.

Zusammenfassend lässt sich sagen, dass die Fähigkeit der Strafverfolgungsbehörden, für Sicherheit zu sorgen und die Urheber der schwersten Straftaten zu fassen, erheblich geschwächt wird, wenn sie keinen wirksamen Zugang zu Daten haben. ***Den Strafverfolgungsbehörden sollte ein rechtmäßiger und streng kontrollierter wirksamer Zugang zu Daten – mit robusten Sicherheiten für den Schutz der Privatsphäre und für Cybersicherheit – gewährt werden, um Straftaten zu verhüten, aufzudecken, zu ermitteln und zu verfolgen, damit sie in der Lage sind, für Sicherheit zu sorgen, und damit die Bürgerinnen und Bürger der EU ihr Leben in Sicherheit führen und Gerechtigkeit für gegen sie begangene Straftaten erlangen können.***

Kapitel I: Digitale Forensik

WAS SIND DIE ZUGRUNDE LIEGENDEN PROBLEME?

Digitale Forensik bezeichnet die Erhebung, Analyse und Sicherung digitaler Beweismittel (sowohl Metadaten als auch Inhaltsdaten von Kommunikationen), die in einer beliebigen digitalen Form auf einem elektronischen Gerät gespeichert sind, einschließlich Informationen aus Computer-Festplatten, Mobiltelefonen, intelligenten Geräten, Fahrzeugnavigationssystemen, elektronischen Türschlössern, in der Cloud gespeicherten Daten und sonstigen digitalen Geräten.

Da der Zugang zu Kommunikationsdaten immer schwieriger wird, gewinnt die Extraktion von Informationen aus beschlagnahmten Geräten (oder aus Netzwerken vernetzter Geräte) für strafrechtliche Ermittlungen zunehmend an Bedeutung. Der Zugang zu in Geräten gespeicherten Daten kann den Strafverfolgungsbehörden qualitativ bessere Informationen z. B. zur Identität von Mitgliedern organisierter krimineller Gruppen als andere Methoden wie etwa die rechtmäßige Überwachung liefern. Einige Experten führen an, dass es nicht möglich ist, im Voraus zu wissen, welche Daten für konkrete Ermittlungen wichtig sind: Auch Informationen, die anfangs irrelevant erscheinen mögen, könnten sich im Laufe der Ermittlungen als entscheidend erweisen. Der Zugang zu allen in einem Gerät gespeicherten Daten kann auch wichtig sein, um die Unschuld einer verdächtigen Person zu bestätigen und die Rechte einer beschuldigten Person zu schützen[17]. Darüber hinaus müssen die Ermittlungsmethoden immer verhältnismäßig sein.

Der chronische **Mangel an Ressourcen** und Fähigkeiten, mit dem die Strafverfolgungsbehörden in diesem Bereich konfrontiert sind, wird durch die Entwicklung neuer Technologien (z. B. neue Arten von Geräten, Internet der Dinge und Cloud-Computing) verschärft, die neue Kompetenzen und Instrumente erfordern. Auch wenn in den Agenturen und Institutionen der Mitgliedstaaten bereits ein umfangreiches Fachwissen im Bereich der digitalen Forensik vorhanden ist, so ist dieses Wissen doch breit verstreut und es gibt keine klaren Mechanismen für die gemeinsame Nutzung und die Verbreitung von Fähigkeiten, was bedeutet, dass es in „getrennten Silos“ verbleibt.

[17] Ein Experte erwähnte einen Fall, in dem die Analyse der Aktivität eines Geräts wesentlich war, um nachzuweisen, dass der Verdächtige nicht an einem Mord beteiligt gewesen sein konnte.

Der Mangel an vergleichbaren Kapazitäten der Labors für digitale Forensik und der allgemeine Mangel an **standardisierten forensischen Verfahren** und an Mechanismen für die **Anerkennung von Kompetenzen und Fachkenntnissen der Experten für digitale Forensik** könnten die grenzüberschreitende Zusammenarbeit behindern.

Die Experten der Hochrangigen Gruppe waren sich einig: Die standardmäßige **Verschlüsselung** von Daten auf Geräten ist eine zentrale Herausforderung für die Strafverfolgungsbehörden. Daten, die auf bestimmten Arten moderner Geräte gespeichert sind, die durch Krypto-Chips[18] oder durch starke Verschlüsselungsalgorithmen und komplexe Passwörter geschützt sind, können von Strafverfolgungsbehörden nicht abgerufen werden, selbst wenn diese auf die leistungsfähigsten Entschlüsselungsplattformen zurückgreifen. Verschlüsselung und andere Maßnahmen zum Schutz der Cybersicherheit und der Privatsphäre sind notwendig, um Informationssysteme sowie Kommunikationsdaten und personenbezogene Daten zu schützen, aber diese Maßnahmen – und insbesondere die zunehmende Verwendung der standardmäßigen Verschlüsselung – verringern die Fähigkeit der Strafverfolgungsbehörden, Beweismittel zu erheben.

Die Mitgliedstaaten verfügen über begrenzte **Fachkenntnisse und Fähigkeiten** in diesem Bereich: Nahezu alle geben an, dass sie nicht die technischen Lösungen haben, um den Bedarf der Praktiker zu decken, und die überwiegende Mehrheit von ihnen halten ihre Kompetenzen und Finanzmittel für unzulänglich. Die Fähigkeiten der Strafverfolgungsbehörden für die Entschlüsselung der auf beschlagnahmten Geräten gespeicherten Informationen unterscheiden sich von Mitgliedstaat zu Mitgliedstaat erheblich: Sie reichen von einer Erfolgsquote von 15-20 % in einigen Fällen bis zu über zwei Drittel in anderen. Auch wenn Fähigkeiten vorhanden sind, sind sie in der Regel unwirksam, wenn es darum geht, Daten zu entschlüsseln, die durch starke Passwörter gesichert sind, oder Dateien zu entschlüsseln, die in speziellen verschlüsselten Behältern gesichert sind. Selbst wenn die Entschlüsselung gelingt, erfolgt dies häufig nicht rechtzeitig. Entschlüsselungsausrüstung ist teuer und hochspezialisiert, und die Hardware ist kapazitätsintensiv.

Die meisten Abteilungen für digitale Forensik der Strafverfolgungsbehörden stützen sich für den Zugang zu Daten auf Geräten auf kommerzielle Lösungen, was zusätzliche Herausforderungen mit sich bringt: Diese Lösungen können nur schwer mit den technologischen Entwicklungen Schritt halten und sind rasch überholt, die hohen Lizenzkosten führen zu einer wesentlichen Verringerung der Zahl der zugelassenen Nutzer, und diese Lösungen werden oft außerhalb Europas entwickelt und sind möglicherweise nicht an die Bedürfnisse der Strafverfolgungsbehörden der EU angepasst oder entsprechen möglicherweise nicht den EU-Standards für Rechenschaftspflicht im Bereich der digitalen Forensik.

[18] Wie der T2-Sicherheitschip auf den jüngsten Apple-Laptops.

Oftmals haben die Strafverfolgungsbehörden keine andere Wahl als **Schwachstellen** auszunutzen, um Zugang zu den Entschlüsselungsschlüsseln auf Geräten zu erhalten. Die auf diesem Ansatz beruhenden Ermittlungsmethoden müssen jedoch mit dem Ziel in Einklang gebracht werden, für sicherere Hard- und Software zu sorgen, das in der Cyberresilienz-Verordnung verankert ist; Systeme für das Management und die Offenlegung von Schwachstellen würden die unbeabsichtigten Folgen solcher Methoden mindern. Die Experten haben alternative Lösungen geprüft, wie etwa die Verpflichtung von Verdächtigen, den Ermittlungsbehörden die Elemente auszuhändigen, die für den Zugang zu einschlägigen Geräten erforderlich sind (z. B. Passwörter). Die in diesen Fällen anwendbaren nationalen Rechtsrahmen unterscheiden sich erheblich voneinander, und nur drei Mitgliedstaaten haben angegeben, dass sie über spezifische Rechtsvorschriften verfügen, die einen Verdächtigen dazu verpflichten, Zugang zu Verschlüsselungsschlüsseln oder zu entschlüsselten Daten zu gewähren[19]. Einige Mitgliedstaaten verpflichten Verdächtige dazu, bestimmte biometrische Daten (z. B. einen Fingerabdruck) zur Verfügung zu stellen, um den Zugang zu einem Gerät zu gewähren; in anderen Fällen müssen Verdächtige ihr Passwort bekanntgeben. Im Allgemeinen ist dies nach wie vor ein Bereich, der weiter evaluiert werden muss.

Einige der vorstehend dargelegten Probleme können durch eine **gemeinsame Nutzung der Kapazitäten der Mitgliedstaaten** gemindert werden, wobei ihre ausschließliche Zuständigkeit in Fragen der nationalen Sicherheit zu achten ist. Diese Lösung wird jedoch vernachlässigt, mitunter aufgrund rechtlicher Zwänge (in sieben Mitgliedstaaten gibt es Beschränkungen für die Weitergabe von Instrumenten, während fünf Mitgliedstaaten Beschränkungen bei der Nutzung von von anderen Mitgliedstaaten bereitgestellten Instrumenten meldeten), aber häufiger aufgrund eines Mangels an etablierten Mechanismen für den Austausch von Instrumenten oder den gemeinsamen Erwerb von Lizenzen.

In der Vergangenheit verfügten die Strafverfolgungsbehörden über klare **Kanäle für die Kommunikation mit Herstellern, Anbietern und Lieferern**. Dadurch konnten sie Protokolle für die Zusammenarbeit erstellen, die ihnen wiederum ein besseres Verständnis von neu eingeführten technologischen Entwicklungen ermöglichten und folglich Strafverfolgungsmaßnahmen bei gleichzeitiger Gewährleistung von Cybersicherheit erleichterten. Angesichts der Geschwindigkeit, mit der neue Technologien eingeführt werden und neue Unternehmen auf den Markt kommen, haben die Bedingungen sich geändert, und die Zusammenarbeit mit der Industrie ist nicht mehr gegeben.

Die Annahme geeigneter Standards könnte es ermöglichen, dass Produktprotokolle und die technische Architektur so gestaltet werden, dass sie eine frühzeitige Berücksichtigung der Bedenken und technischen Anforderungen der Strafverfolgungsbehörden gewährleisten. Die **Einbeziehung der Strafverfolgungsbehörden in die einschlägigen Normungsgremien** ist jedoch nicht ausreichend, was ihre Fähigkeit beeinträchtigt, sich wirksam in die Entwicklung künftiger technologischer Standards einzubringen.

---

[19] Eurojust: Cybercrime Judicial Monitor (Ausgabe 4), Dezember 2018, S. 34, https://www.eurojust.europa.eu/sites/default/files/assets/eurojust_cybercime_judicial_monitor_4_2018.pdf.

MÖGLICHE LÖSUNGEN

I. Verstärkung und Straffung der Bemühungen um einen Ausbau der Kapazitäten im Bereich der Instrumente der digitalen Forensik

Die Mitgliedstaaten verfügen bereits über das Fachwissen und die Kapazität für die Durchführung von Aufgaben der digitalen Forensik; indem sie ihre technischen Lösungen austauschen und gemeinsam nutzen, können die einschlägigen nationalen Institutionen und Behörden jedoch von der Erfahrung anderer Agenturen profitieren und erhebliche Größenvorteile erzielen, was zu einer Verringerung der benötigten Finanzmittel führt. Die Mitgliedstaaten können diesbezügliche Lösungen weiter sondieren, sowohl im Bereich der Instrumente der digitalen Forensik als auch hinsichtlich Ausbildung und Entwicklung von Kompetenzen.

Empfehlungen Cluster 1

Für die Verbesserung der Zusammenarbeit und den Aufbau einer stärkeren kollektiven Kapazität im Bereich der digitalen Forensik empfehlen die Experten Folgendes:

1. *Bestandsaufnahme und Vernetzung der bestehenden Netzwerke für digitale Forensik und Einrichtung eines Sekretariats [Empfehlung 1];*
2. *bessere Zugänglichkeit von Wissen und Verbreitung unter Experten [Empfehlung 1];*
3. *Überlegungen zu Mechanismen für die Bündelung von Wissen [Empfehlung 2];*
4. *mehr Finanzmittel für Forschung und Entwicklung, mit klaren Zielvorgaben [Empfehlung 4];*
5. *Förderung des Instrumentenregisters von Europol (Europol Tool Repository – ETR) als zentrale Plattform für den Austausch von Instrumenten [Empfehlung 4];*
6. *Erleichterung des Austauschs von Lösungen und Instrumenten der digitalen Forensik zwischen Mitgliedstaaten in einem vertrauensvollen Umfeld (unter Berücksichtigung der nationalen Vorschriften) [Empfehlung 2];*
7. *Entwicklung eines Mechanismus auf EU-Ebene für die gemeinsame Beschaffung von Lizenzen für Instrumente der digitalen Forensik, zur gemeinsamen Nutzung durch die Mitgliedstaaten [Empfehlung 3];*
8. *Förderung der Zusammenarbeit mit Herstellern und Entwicklern von Instrumenten der digitalen Forensik, zur Vereinheitlichung der Struktur und des Formats der von Strafverfolgungsbehörden durch die Nutzung dieser Instrumente erhaltenen Daten, idealerweise nach vereinbarten Standards [Empfehlung 12];*
9. *Schaffung eines Mechanismus/Systems für die Evaluierung und – sofern relevant – die Zertifizierung kommerzieller Instrumente der digitalen Forensik auf EU-Ebene, unter Beachtung etwaiger negativer Auswirkungen auf Ermittlungen und Strafverfolgung, wie z. B. zusätzlicher unnötiger Aufwand [Empfehlung 5].*

Mehrere Organisationen, Netzwerke, Verbände und Projekte bringen Praktiker und verschiedene Kategorien von Partnern zusammen, um die Kapazitäten der EU-Strafverfolgung im Bereich digitaler Ermittlungen zu verbessern:

- Das *Europäische Netz der kriminaltechnischen Institute* (European Network of Forensic Science Institutes – ENFSI)[20] ist das wichtigste europäische Netzwerk für (unter anderem) digitale Forensik; es hat 73 Mitglieder aus 39 Ländern, die an Arbeitsgruppen zu – unter anderem – kriminologischer Informationstechnologie und digitaler Bilddarstellung teilnehmen;
- in der *Europäischen Vereinigung zur Entwicklung von Technologien zur Bekämpfung der Cyberkriminalität* (European Anti-Cybercrime Technology Development Association – EACTDA)[21] sind Strafverfolgungsbehörden, Forschungs- und Technologieorganisationen, Partner aus der Industrie und Hochschulen aus zahlreichen Mitgliedstaaten vereint; ihr Ziel ist es, die Umsetzung der Ergebnisse von Forschungsprojekten im Bereich Sicherheit zu erleichtern und vollständig erprobte und betriebsfähige Software-Instrumente bereitzustellen, ohne Lizenzkosten und mit Zugang zum Quellcode für Organisationen der öffentlichen Sicherheit in der EU;
- das Europäische Amt für Betrugsbekämpfung (OLAF) bietet seit 2007 gezielte *Schulungen für digitale Forensik und Analysten (DFAT)* für nationale Strafverfolgungsbehörden an, mit besonderem Schwerpunkt auf Betrug, Korruption und sonstigen illegalen Aktivitäten zum Nachteil der finanziellen Interessen der Europäischen Union; pro Jahr erhalten etwa 175 Experten für digitale Forensik entsprechende Schulungen, womit eine solide Gemeinschaft in diesem Kriminalitätsbereich aufgebaut wird;
- andere Projekte wie *CYCLOPES*[22] und *I-LEAD*[23] sind keine permanenten Strukturen, aber sie bringen dennoch Experten zusammen und liefern einschlägige Lückenanalysen.

Die bestehenden permanenten Netze sind jedoch nicht darauf ausgelegt, Einheiten für digitale Forensik der Strafverfolgungsbehörden der EU und Organisationen zusammenzubringen, die eng mit ihnen zusammenarbeiten (z. B. das Zentrum für Cybersicherheit und Ermittlung von Cyberstraftaten (Centre for Cybersecurity and Cybercrime Investigation) des University College Dublin (UCD) oder das litauische Exzellenzzentrum für Schulung, Forschung und Ausbildung im Bereich Cyberkriminalität).

---

20 https://enfsi.eu/.
21 https://www.eactda.eu/index.html.
22 https://www.cyclopes-project.eu/.
23 https://cordis.europa.eu/project/id/740685/de.

Europol (insbesondere das Europol-Innovationslabor, zusammen mit dem Europäischen Zentrum zur Bekämpfung der Cyberkriminalität) arbeitet bereits in gewissem Umfang mit allen oben aufgeführten Netzwerken zusammen und hat bewiesen, dass es in der Lage ist, eine beträchtliche Zahl von Praktikern zusammenzubringen, z. B. in Form der Kerngruppen des Europäischen Clearinggremiums für Innovation (European Clearing Board for Innovation – EuCB), das *Forum für Forensik-Experten*[24] zu organisieren und Experten mit einschlägigen Partnern in Kontakt zu bringen, z. B. durch das *Cyber-Innovationsforum*[25].

Europol bietet darüber hinaus mit der Europol-Expertenplattform (Europol Platform for Experts – EPE) eine fertige Infrastruktur, die Zusammenarbeit und Wissensaustausch zwischen Experten zu bestimmten Themen ermöglicht.

Wichtigste Maßnahme: Die Experten der Hochrangigen Gruppe fordern die Ausweitung der Fähigkeiten von Europol im Bereich der digitalen Forensik

Akteure: Europol, Europäische Kommission, Mitgliedstaaten	*Zeitrahmen: 2028*	*Mittelausstattung: wird zu einem späteren Zeitpunkt erörtert, je nach Ergebnis der laufenden Beratungen über den nächsten MFR*

- Im Rahmen der in den politischen Leitlinien für die Europäische Kommission 2024-2029 angekündigten wesentlichen Verstärkung von Europol fordern die Experten der Hochrangigen Gruppe eine Aufstockung der Kapazitäten von Europol, um den Mitgliedstaaten dabei zu helfen, **Ressourcen, Wissen und Fachkenntnisse zu bündeln sowie Lösungen und Instrumente der digitalen Forensik** in einem vertrauensvollen Umfeld **auszutauschen**. Souveräne Instrumente und Instrumente, die ausschließlich für Zwecke der nationalen Sicherheit verwendet und/oder entwickelt werden, sollten davon ausgenommen sein.

- Die Experten der Hochrangigen Gruppe fordern Europol auf, **die Rolle einer Plattform** für den Zugang zu einschlägigem operativem Fachwissen in diesem Bereich **zu übernehmen** und möglicherweise **ein Projekt nach dem Modell von SIRIUS im Bereich der digitalen Forensik einzurichten**, um die gemeinsame Nutzung von Wissen und Fachkenntnissen sowie den Austausch bewährter Verfahren zu erleichtern.

- Die Experten der Hochrangigen Gruppe fordern Europol auf, seine Rolle bei der **Koordinierung von Organisationen und Projekten**, die zur Schaffung von Wissen im Bereich der digitalen Forensik auf EU-Ebene beitragen, zu stärken, und zwar unter der Leitung des EuCB und unter Berücksichtigung der Beiträge anderer einschlägiger Agenturen.

[24] https://www.europol.europa.eu/publications-events/events/forensic-experts-forum-2024-conference.
[25] https://www.europol.europa.eu/publications-events/events/ec3-cyber-innovation-forum-2024.

Es gibt mehrere Finanzierungsinstrumente zur Unterstützung der Forschung und der Entwicklung von Instrumenten im Bereich der digitalen Forensik.

- Im Rahmen des *Fonds für die innere Sicherheit (ISF)* veröffentlicht die Kommission regelmäßig offene Aufforderungen zur Einreichung von Vorschlägen im Bereich Cyberkriminalität und digitale Ermittlungen. Trotz der eher begrenzten Mittelausstattung (im Rahmen des derzeitigen MFR wurden ca. 15 Mio. EUR für diese Maßnahmen zugeteilt) haben sich die im Rahmen dieser Aufforderungen ausgewählten Projekte als zielgerichtet und erfolgreich erwiesen.

  Etwa zwei Drittel der ISF-Mittel werden im Rahmen der geteilten Mittelverwaltung zugewiesen, wobei die Mitgliedstaaten entscheiden, welche Projekte sie finanzieren, und die Verantwortung für die laufende Verwaltung übernehmen. Somit haben die Mitgliedstaaten die Möglichkeit, Projekte im Bereich der digitalen Forensik im Rahmen ihrer jeweiligen nationalen Programme zu unterstützen.

- Mit einer Mittelausstattung von insgesamt 1,596 Mrd. EUR über sieben Jahre ist das *Cluster „Zivile Sicherheit für die Gesellschaft" von Horizont Europa* darauf ausgelegt, sichere europäische Gesellschaften vor dem Hintergrund eines beispiellosen Wandels und wachsender globaler Interdependenzen und Bedrohungen unter Verstärkung der europäischen Kultur der Freiheit und des Rechts zu fördern. In den vergangenen Jahren wurden damit mehrere einschlägige Forschungsprojekte unterstützt, wie FORMOBILE[26] und EXFILES[27], die ihrerseits die Praktiker bei ihrer täglichen Arbeit unterstützt haben.

- Das *Programm „Digitales Europa"* ist das Hauptfinanzierungsinstrument der EU für die Verbesserung der digitalen Infrastruktur der EU durch eine Vielzahl von Initiativen. Das Programm, das über eine Mittelausstattung von insgesamt 7,5 Mrd. EUR für den Zeitraum 2021 bis 2027 verfügt, stellt erhebliche Mittel insbesondere für Cybersicherheit bereit und deckt auch die digitale Forensik ab.

---

[26] FORMOBILE – From mobile phones to court – A complete FORensic investigation chain targeting MOBILE devices (Vom Mobiltelefon zum Gericht – Eine vollständige forensische Ermittlungskette für mobile Geräte): https://cordis.europa.eu/project/id/832800.

[27] EXFILES – Europe fights against crime and terrorism (Europa bekämpft Kriminalität und Terrorismus): https://exfiles.eu/.

Die Entschlüsselungsplattform von Europol ist ein Vorzeigeprojekt im Rahmen des ISF. Diese Plattform, die 2020 von Europol in enger Zusammenarbeit mit der Gemeinsamen Forschungsstelle (JRC) der Europäischen Kommission eingerichtet wurde, unterstützt die nationalen Strafverfolgungsbehörden bei der Entschlüsselung ihrer digitalen Beweismittel. Sie soll den Strafverfolgungsbehörden eine nachhaltige Lösung für den Zugang zu den technischen und IT-Ressourcen, die sie benötigen, bieten. In den letzten paar Jahren wurde die Plattform in zahlreichen wichtigen Fällen genutzt; sie hat in knapp der Hälfte davon wichtige Ergebnisse geliefert, die zu einigen Erfolgen geführt haben. Im Jahr 2023 unterstützte die Plattform erfolgreich 37 Ermittlungen (zu sexueller Ausbeutung von Kindern, Terrorismus, Cyberkriminalität, organisierter Kriminalität, Drogenschmuggel und Betrug, sowie hochkarätige Finanzermittlungen), einschließlich Ermittlungen mit hoher Priorität wie etwa zu SkyECC und EncroChat. Die Plattform hat sich zu einem unverzichtbaren Instrument für die Strafverfolgungsbehörden entwickelt, aber sie reicht nicht aus, um alle Probleme im Zusammenhang mit der Entschlüsselung anzugehen, mit denen die EU-Behörden konfrontiert sind.

Wichtigste Maßnahme: Die Experten der Hochrangigen Gruppe fordern die Weiterentwicklung und Förderung des Einsatzes der Entschlüsselungsfähigkeiten der EU

Akteure: Europäische Kommission, Europol	*Zeitrahmen: 2028*	*Mittelausstattung: von den Mitgliedstaaten festzulegen (z. B. im Rahmen nationaler ISF-Programme)*

- Die Experten der Hochrangigen Gruppe fordern die Europäische Kommission auf, die Fähigkeit der nationalen Behörden zur Erhebung hochwertiger Kontextinformationen zu unterstützen, wobei die ausschließliche Zuständigkeit der Mitgliedstaaten im Bereich der nationalen Sicherheit zu wahren ist, durch gezielte Finanzierung (beispielsweise im Rahmen der nationalen ISF-Programme) und den Austausch bewährter Verfahren, damit sie einen Beitrag zur Förderung der Effizienz der Entschlüsselungsplattform von Europol leisten können.
- Die Experten der Hochrangigen Gruppe fordern die Europäische Kommission auf, die Investitionen von Europol in die Aufrechterhaltung der technischen Fähigkeiten und die Verbesserung der Entschlüsselungsfähigkeiten zu unterstützen, um mit den technologischen Entwicklungen Schritt zu halten und unter Berücksichtigung der Forschung zur Quantenkryptografie.
- Die Experten der Hochrangigen Gruppe fordern die Europäische Kommission auf, die Mitgliedstaaten bei der Entwicklung **nationaler und regionaler Entschlüsselungsfähigkeiten** finanziell zu unterstützen, um die Bemühungen von Europol zu ergänzen.

Die bestehenden EU-Finanzierungsprogramme bieten eine wesentliche Unterstützung für die Strafverfolgung. Eine weitere Straffung dieser Möglichkeiten würde ihren Beitrag zur Verbesserung der Kapazitäten der Abteilungen für digitale Forensik erhöhen und die Abhängigkeit von bestimmten Anbietern sowie die Nutzung von außerhalb der EU entwickelten sogenannten Black-Box-Instrumenten (d. h. Instrumenten, die Daten verarbeiten, ohne dass vertrauenswürdige Behörden ihre Funktionsweise überprüfen können) durch die Strafverfolgungsbehörden verringern.

Die Schritte im Zyklus der Tätigkeiten (Forschung, Entwicklung, Einsatz), die ergriffen werden sollten, um einen spürbaren Mehrwert für die Strafverfolgungsbehörden zu erzielen, werden durch verschiedene Programme unterstützt. Um die Vorteile der auf EU-Ebene verfügbaren Möglichkeiten voll auszuschöpfen, sollten die nationalen Verwaltungen, die Strafverfolgungsbehörden und die Praktiker Kenntnis der Funktionen und Ziele der einzelnen spezifischen Programme und Mechanismen haben.

Im Rahmen von Horizont Europa wurden verschiedene erfolgreiche Projekte unter aktiver Beteiligung von Praktikern der Strafverfolgungsbehörden unterstützt. Bei Horizont Europa handelt es sich jedoch um ein Forschungsprogramm, und die Erwartungen in Bezug darauf, wie einsatzbereit die entwickelten Instrumente sind, sollten angepasst werden.

Mit dem Projekt *Tools4LEAs* (Instrumente für die Strafverfolgungsbehörden), das durch den ISF finanziert und von der EACTDA betrieben wird, sollen die Übernahme von Ergebnissen von Forschungsprojekten im Bereich Sicherheit erleichtert und einsatzbereite Software-Instrumente bereitgestellt werden, und zwar ohne Lizenzkosten und mit Zugang zum Quellcode für die EU-Behörden für die öffentliche Sicherheit. Das Projekt *Tools4LEAs* ist am besten geeignet, auf den Ergebnissen von Forschungsprojekten aufzubauen, um zur Bereitstellung operativer Instrumente beizutragen. Europol ist am Projekt *Tools4LEAs* beteiligt und leitet – zusammen mit allen Endnutzern, die Mitglieder der EACTDA sind – seine Arbeit.

Das EuCB hat über 15 Kerngruppen von Mitgliedstaaten gebildet, um neue Technologien zu erforschen und gemeinsam innovative Instrumente zu schaffen. Die Mitgliedstaaten haben die Kerngruppen des EuCB genutzt, um einen Teil der Entwicklung innovativer Instrumente, die durch ISF-Finanzhilfen finanziert werden, zu koordinieren (z. B. MARIT-D, ProfID und Webcrawler). Die Kerngruppen sind ein idealer Rahmen, über den die Mitgliedstaaten die gemeinsame Schaffung von Instrumenten für digitale Ermittlungen koordinieren können.

Die Europäische Kommission finanziert weiterhin durch gezielte *Aufforderungen zur Einreichung von Vorschlägen im Rahmen des ISF* Projekte, die einen wesentlichen Beitrag zum Erfolg operativer Maßnahmen geleistet haben. Beispielsweise wurden mit dem Projekt CERBERUS die Schwachstellen im EncroChat-System ermittelt, die es der französischen Gendarmerie in der Folge ermöglicht haben, es – mit Unterstützung des niederländischen Nationalen Instituts für Forensik und des UCD – aufzulösen. Daneben hat das Projekt FREETOOL[28] unter der Leitung des UCD-Zentrums für Cybersicherheit und Ermittlungen zu Cyberkriminalität die Entwicklung einer Reihe kostenloser Instrumente für Ermittlungen zu Cyberkriminalität[29] ermöglicht, die auf die spezifischen Anforderungen der Strafverfolgungsbehörden für digitale Ermittlungen und Analysen zugeschnitten sind. Diese Instrumente wurden in Partnerschaft mit den Strafverfolgungsbehörden entwickelt und stehen der Strafverfolgungsgemeinschaft kostenlos zur Verfügung. 3 000 Nutzer aus über 100 Strafverfolgungsbehörden, die über Dutzende von Gerichtsbarkeiten verteilt sind, haben sich für den Zugang zu den Instrumenten angemeldet, die auch von mehreren Strafverfolgungsbehörden auf organisatorischer Ebene übernommen und in öffentlichkeitswirksamen Ermittlungen eingesetzt wurden. Das *Programm „Justiz“* deckt auch die justizielle Zusammenarbeit in Strafsachen ab und könnte möglicherweise die grenzüberschreitende Zusammenarbeit beim Einsatz von Instrumenten für digitale Ermittlungen fördern.

---

28 https://www.ucd.ie/cci/projects/freetool/.

29 Die Instrumente decken die verschiedenen Phasen von Ermittlungen ab: Informationsgewinnung aus frei zugänglichen Quellen (OSINT) vor Durchsuchungen; forensische Untersuchung von Live-Daten; Speicheranalyse; OSINT nach Durchsuchungen und Bewahrung von Online-Ressourcen; automatisches Abrufen von Dateien/Artefakten; forensische Berichterstattung; Medienverarbeitung; und Geolokalisierung von Artefakten.

Seit seiner Einrichtung wurde das Instrumentenregister von Europol (*Europol Tool Repository – ETR*) weiterentwickelt und umfasst mittlerweile mehr als 40 fortgeschrittene Instrumente, die direkten Zugang zu modernsten Technologien für die europäischen Strafverfolgungsbehörden bieten. Jeden Monat kommen neue Instrumente dazu, und das Register hat sich zur Hauptquelle für EU-Praktiker entwickelt, die nach Software zur Unterstützung ihrer Ermittlungen suchen. Das ETR hat derzeit über 2 700 Nutzer, mit mehr als 7 800 Downloads der verschiedenen Instrumente. Die Instrumente wurden von nationalen Ermittlungsstellen in großem Umfang zur Unterstützung von zahlreichen Operationen genutzt, unter anderem in verschiedenen Kriminalitätsbereichen wie Menschenhandel, schwere und organisierte Kriminalität, Cyberkriminalität und sexueller Missbrauch von Kindern im Internet. Das ETR bietet eine direkte Nutzungsmöglichkeit für von der EU finanzierte Projekte, die zu konkreten und ausgereiften Ergebnissen führen und deren Urheber bereit sind, sie an Europol zur Verbreitung an alle europäischen Strafverfolgungsbehörden zu lizenzieren. Ausgewählte Partner der Projekte INSPECTr, Tools4LEAs und FORMOBILE haben bereits Instrumente in das ETR eingestellt. Europol koordiniert zusammen mit der EU-Agentur für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL) das Angebot von Schulungen zu ETR-Instrumenten für die Nutzer.

Darüber hinaus sollte das Programm „Digitales Europa“ zunehmend Synergien und Komplementaritäten zwischen Cybersicherheit und der Bekämpfung von Cyberkriminalität fördern, die oft auf dieselben Instrumente und Methoden der digitalen Forensik angewiesen sind.

Derzeit gibt es keinen Mechanismus, mit dem sichergestellt werden könnte, dass Instrumente der digitalen Forensik den innerhalb der EU geltenden Standards für Rechenschaftspflicht und Forensik entsprechen. Ein derartiger Mechanismus sollte eine technische Evaluierung bieten, mit der sichergestellt wird, dass Verhältnismäßigkeit (d. h. Nachweis, dass das Instrument Zugang zu gezielten Informationen ermöglicht und somit die Analyse auf das Notwendige beschränkt), Transparenz und die Rechte der Beschuldigten (d. h. Nachweis, dass das Instrument authentische und genaue Informationen abruft und somit Verteidigern und unabhängigen forensischen Experten, die vor Gericht aussagen, Sicherheit bietet) sowie andere gesetzliche Anforderungen (z. B. Einhaltung der KI-Verordnung) uneingeschränkt geachtet werden. Dies würde die Vertrauenswürdigkeit von Beweismitteln vor Gericht sowohl auf nationaler Ebene als auch grenzüberschreitend stärken und somit die grenzüberschreitende Zusammenarbeit fördern.

Wichtigste Maßnahme: Die Experten der Hochrangigen Gruppe fordern eine gezielte Finanzierung von Projekten zu Forschung, Entwicklung und Einsatz für Instrumente der digitalen Forensik

Akteure: Europäische Kommission, Europol, Mitgliedstaaten, EACTDA, ENFSI	*Zeitrahmen: ab 2024*	*Mittelausstattung:*

- Die Experten der Hochrangigen Gruppe fordern die Mitgliedstaaten auf, **Projekte der digitalen Forensik, die im Rahmen ihrer jeweiligen nationalen ISF-Programme finanziert werden, in bestehende Mechanismen** (z. B. EMPACT) oder Netze (z. B. ECTEG, EACTDA) **zu integrieren**, damit sie von der Erfahrung der Praktiker aus anderen Mitgliedstaaten profitieren und gleichzeitig die Verbreitung und Verwendung der Ergebnisse durch andere Strafverfolgungsbehörden fördern können.

- Die Experten der Hochrangigen Gruppe begrüßen die anhaltenden Bemühungen der Europäischen Kommission zur Unterstützung von Forschung, Entwicklung und Einsatz für Instrumente der digitalen Forensik durch Mittelzuweisungen im Rahmen einschlägiger Finanzierungsprogramme: **Horizont Europa**, **Digitales Europa** und **ISF**. Je nach den verfügbaren Ressourcen wird die Europäische Kommission alle zwei Jahre **offene Aufforderungen zur Einreichung von Vorschlägen** im Bereich Cyberkriminalität und digitale Ermittlungen im Rahmen des ISF veröffentlichen.

- Die Experten der Hochrangigen Gruppe begrüßen die anhaltenden Bemühungen der Europäischen Kommission zur Finanzierung der **EACTDA** im Rahmen des ISF, sodass die EACTDA vollständig erprobte und einsatzbereite Software-Instrumente ohne Lizenzkosten und mit Zugang zum Quellcode für EU-Behörden der öffentlichen Sicherheit bereitstellen kann.

- Die Experten der Hochrangigen Gruppe begrüßen die anhaltenden Bemühungen der Europäischen Kommission zur Förderung – im Rahmen der Finanzierungsmöglichkeiten – der Nutzung des **Europol-Instrumentenregisters** als zentrale Plattform für die Verbreitung von Instrumenten; sie ermutigen das **Europol-Innovationslabor**, seine Bemühungen zur Bereitstellung vertrauenswürdiger, sicherer, kostenloser, einfach zu installierender und skalierbarer Ermittlungsinstrumente für die europäischen Strafverfolgungsbehörden fortzusetzen.

- Die Experten der Hochrangigen Gruppe fordern, die **Einrichtung von Systemen zur Evaluierung und gegebenenfalls Zertifizierung** kommerzieller Instrumente der digitalen Forensik auf EU-Ebene weiter zu prüfen. Dies kann beispielsweise **im Rahmen des Europäischen Netzes der kriminaltechnischen Institute** erfolgen.

Lizenzen für Instrumente der digitalen Forensik sind kostspielig und mitunter für einige Strafverfolgungsbehörden unbezahlbar. Für den gemeinsamen Erwerb von Lizenzen, die dann zwischen Behörden in verschiedenen Mitgliedstaaten geteilt werden können, können möglicherweise niedrigere Preise ausgehandelt werden.

Mit dem im Rahmen von Horizont Europa finanzierten Projekt *iProcureNet*[30] wurde eine Methodik für gemeinsame Beschaffungen im Bereich der Sicherheit sowie ein Netz von Vergabebehörden in den Mitgliedstaaten errichtet. Aufgrund seiner Zusammensetzung und der Organisation seiner Arbeit wäre das *EU-Innovationszentrum für die innere Sicherheit* gut dafür geeignet, die Bestimmung des gemeinsamen Bedarfs durch die Mitgliedstaaten zu begleiten und zu ermitteln, welche Instrumente am nützlichsten wären, sofern ein spezieller Arbeitsbereich für digitale Forensik eingerichtet wird.

Häufig sind mit Instrumenten der digitalen Forensik neben den Kosten noch weitere Probleme verbunden. So können die von diesen Instrumenten abgerufenen Daten beispielsweise in einem Format strukturiert oder dargestellt sein, das nicht den für die Weiterverarbeitung (z. B. Datenanalyse oder -weitergabe) verwendeten bestehenden inländischen Informationssystemen entspricht. Daher müssen gemeinsame Anforderungen der Mitgliedstaaten bezüglich der Struktur und des Formats von Daten, die durch Instrumente der digitalen Forensik erhalten werden, formuliert werden. Auf dieser Grundlage wären die Behörden der Mitgliedstaaten in der Lage, Verhandlungen mit den Anbietern von Instrumenten der digitalen Forensik zu führen, damit ihre Anforderungen gebührend berücksichtigt werden können, beispielsweise im Rahmen gemeinsamer Vergabeverfahren wie oben angegeben.

Wichtigste Maßnahme: Die Experten der Hochrangigen Gruppe betonen die Notwendigkeit eines besseren Kosten-Nutzen-Verhältnisses beim Erwerb von Instrumenten der digitalen Forensik

Akteure: Mitgliedstaaten, Europäische Kommission, EU-Innovationszentrum für die innere Sicherheit, Europol	*Zeitrahmen: ab 2025 (gemeinsame Beschaffung)*	*Mittelausstattung: keine Angabe*

- Die Experten der Hochrangigen Gruppe fordern die Europäische Kommission auf,
  - die Mitgliedstaaten bei der **Bestimmung der** für wirksame Ermittlungen am dringendsten benötigten **Instrumente der digitalen Forensik** zu unterstützen (möglicherweise im Rahmen des EU-Innovationszentrums für die innere Sicherheit);
  - die **Zusammenarbeit zwischen operativen Einheiten und den Kontaktstellen in den Vergabebehörden** zu unterstützen, die im Rahmen von iProcureNet zusammengeführt werden;
  - **Pilotprojekte für die gemeinsame Beschaffung von Lizenzen für Instrumente der digitalen Forensik** einzurichten.
- Die Experten der Hochrangigen Gruppe sind der Auffassung, dass **Europol** dazu geeignet ist, den Mitgliedstaaten bei der Bestimmung der **gemeinsamen Anforderungen bezüglich der Struktur und des Formats der** durch Instrumente der digitalen Forensik **erhaltenen Daten** zu helfen und – auf dieser Grundlage – die Zusammenarbeit zwischen den einschlägigen nationalen Behörden und Experten zu fördern, um es ihnen zu ermöglichen, mit den Herstellern und Entwicklern dieser Produkte in Kontakt zu treten, damit sie Standards vereinbaren können und die Anforderungen der Mitgliedstaaten berücksichtigt werden können.

[30] https://www.iprocurenet.eu/.

II. Austausch von Kapazitäten und gemeinsame Nutzung empfindlicher Instrumente

Angesichts der begrenzten Verfügbarkeit von Entschlüsselungsfähigkeiten (z. B. die Europol-Entschlüsselungsplattform) und des Fehlens einer wirksamen Zusammenarbeit mit der Industrie oder eines speziellen Rechtsrahmens zur Gewährleistung des rechtmäßigen Zugangs zu Informationen auf digitalen Geräten bleibt die Ausnutzung von Schwachstellen für den Zugriff auf Entschlüsselungsschlüssel auf Geräten derzeit die Hauptoption der Strafverfolgungsbehörden für den Zugang zu verschlüsselten Inhalten.

Selbst wenn diese Voraussetzungen – oder einige davon – bis zu einem gewissen Grad erfüllt sein mögen, werden Kriminelle in der Regel auf spezielle verschlüsselte Geräte zurückgreifen, um Informationen oder illegale Inhalte zu verbergen. Deshalb wird es auch in absehbarer Zeit weiterhin erforderlich sein, dass die Strafverfolgungsbehörden empfindliche Instrumente[31] und Kapazitäten einsetzen und möglicherweise gemeinsam nutzen.

Empfehlungen Cluster 2

Für die gemeinsame Nutzung empfindlicher Instrumente und die verantwortungsvolle Verwaltung damit verbundener Kapazitäten empfehlen die Experten Folgendes:

1. *Sondierung von Mechanismen, mit denen sichergestellt wird, dass empfindliche Instrumente unter uneingeschränkter Achtung nationaler Vorschriften gemeinsam genutzt werden können [Empfehlung 1];*

2. *Einrichtung eines speziellen Verfahrens für den Austausch von Kapazitäten unter potenzieller Nutzung von Schwachstellen, das die Bündelung von Wissen und Ressourcen ermöglichen und gleichzeitig die Wahrung der Vertraulichkeit und Sensibilität der Informationen gewährleisten würde [Empfehlung 6];*

3. *möglicherweise Erforschung eines europäischen Ansatzes für die Verwaltung und Offenlegung von Schwachstellen durch die Strafverfolgungsbehörden, auf der Grundlage bestehender bewährter Verfahren [Empfehlung 2].*

Die Kommission hat im Rahmen von Horizont Europa und des ISF Projekte (*EXFILES* und *ForRES*[32]) unterstützt, die auf die Nutzung von Schwachstellen und Software ausgelegt sind und den Praktikern der Strafverfolgungsbehörden Instrumente und Protokolle für eine rasche und einheitliche, aber dennoch allen einschlägigen Rechtsvorschriften entsprechende Datenextraktion bieten.

---

31 „Empfindliche Instrumente“ bezieht sich sowohl auf Instrumente der digitalen Forensik als auch auf Instrumente für taktisches Abfangen.

32 https://forres.eu.

Die gemeinsame Nutzung empfindlicher Instrumente und damit verbundener Kapazitäten unter vertrauenswürdigen europäischen Partnern erleichtert die operative Zusammenarbeit, ermöglicht die gemeinsame Nutzung von Wissen und schafft Skaleneffekte, was zu einer Verringerung der erforderlichen Ressourcen führt.

Auch wenn die Nutzung von Schwachstellen nach wie vor mitunter von zentraler Bedeutung für Ermittlungen ist, muss sie mit äußerster Vorsicht und in Übereinstimmung mit dem einschlägigen innerstaatlichen Rechtsrahmen gehandhabt werden, da sie Auswirkungen auf die Sicherheitslage von Hard- und Software hat.

Wichtigste Maßnahme: Die Experten der Hochrangigen Gruppe fordern Unterstützung für die gemeinsame Nutzung empfindlicher Instrumente und die verantwortungsvolle Verwaltung damit verbundener Kapazitäten

Akteure: Mitgliedstaaten, Europäische Kommission	*Zeitrahmen: ab 2024*	*Mittelausstattung: keine Angabe*

- Die Experten der Hochrangigen Gruppe ersuchen die Europäische Kommission, weiterhin Projekte, die auf die gemeinsame Nutzung empfindlicher Instrumente (sowohl Instrumente der digitalen Forensik als auch Instrumente für taktisches Abfangen) und auf die Bündelung von Ressourcen ausgelegt sind, im Rahmen der einschlägigen Finanzierungsprogramme zu unterstützen; die Kommission könnte ferner die **Schaffung einer transnationalen Plattform für die Strukturierung und die gemeinsame Nutzung von Wissen** unterstützen.

- Die Experten der Hochrangigen Gruppe ersuchen die Gemeinsame Forschungsstelle der Europäischen Kommission, zu erforschen, ob auf der Grundlage bestehender bewährter Verfahren ein **europäischer Ansatz für die Verwaltung und Offenlegung von Schwachstellen**, der von den Strafverfolgungsbehörden befolgt wird, entwickelt werden kann.

III. Gemeinsame Investitionen zur Entwicklung von Kompetenzen und zum Ausbau von Fachwissen im Bereich der digitalen Forensik

Die zuständigen Mitarbeiter der Strafverfolgungsbehörden sollten für den Einsatz von Ermittlungsinstrumenten und -methoden im Rahmen ihrer Ermittlungen geschult werden, und ihr Fachwissen sollte zertifiziert werden. Ihre geforderten und dokumentierten Kompetenzen sollten ihrer Rolle entsprechen und mindestens allgemeine digitale Forensik für mobile Geräte (unabhängig von Instrumenten), Themen der Beweismittelkette/Beweismittel sowie Grundkenntnisse zu Arten des Erwerbs, Analysen, Berichterstattung und Erscheinen vor Gericht umfassen. Aus der Dokumentation sollte hervorgehen, ob diese Kompetenzen durch Schulungen oder am Arbeitsplatz erworben wurden.

Empfehlungen Cluster 3

Zur Unterstützung der Entwicklung von Kompetenzen und Fachwissen im Bereich der digitalen Forensik, einschließlich Entschlüsselung und Normung, empfehlen die Experten Folgendes:

1. *Steigerung der Zahl von Schulungsmöglichkeiten für Experten [Empfehlung 7];*
2. *Schaffung eines Zertifizierungssystems auf EU-Ebene für Experten der digitalen Forensik, um die Qualität und Einheitlichkeit der fachlichen Schulungen zu garantieren [Empfehlung 7];*
3. *Investitionen zur Schließung der Lücke bei den technischen Kompetenzen im Bereich der Normung und Sensibilisierung durch Schließung von Vereinbarungen mit Hochschulen und anderen einschlägigen Institutionen [Empfehlung 8].*

Die CEPOL führt Schulungen zu mehreren einschlägigen Themenbereichen durch[33]. Die Europäische Gruppe für Schulung und Ausbildung in Bezug auf Cyberkriminalität (ECTEG)[34] entwickelt Kurse zu Cyberkriminalität und digitaler Forensik und stellt sie der CEPOL und den nationalen Strafverfolgungsbehörden kostenlos zur Verfügung.

Die ECTEG hat mit *Decrypt* eine Schulungsressource entwickelt, um die Fähigkeiten der Strafverfolgungsbehörden der EU-Mitgliedstaaten zur rechtmäßigen Entschlüsselung durch ausgefeilte Strategien für den rechtmäßigen Umgang mit verschlüsselten Beweismitteln zu verbessern. *Decrypt* kann von der CEPOL sowie von nationalen Stellen eingesetzt werden, wobei die von der Gemeinsamen Forschungsstelle bereitgestellte Infrastruktur genutzt werden kann.

---

[33] Schulung im Bereich digitale Forensik für Ermittler, mobile Forensik, Live-Daten-Forensik und Mac-Forensik.

[34] Die ECTEG ist eine Organisation ohne Erwerbszweck, die 30 Strafverfolgungsbehörden aus 20 europäischen Ländern, internationale Gremien und Hochschulen zusammenbringt. Mit Unterstützung durch den ISF entwickelt, fördert und verbreitet die ECTEG Ressourcen, Lösungen und Material für Schulungen. Siehe https://www.ecteg.eu/.

Ebenso wichtig ist es, Ersthelfern grundlegende Kompetenzen im Bereich der digitalen Forensik zu vermitteln. Dazu hat die ECTEG unter anderem das Projekt *eFirst* (Schulung für Ersthelfer der Strafverfolgungsbehörden zu Cyber-Grundlagen) entwickelt. *eFirst* ist ein Online-Schulungsmodul zum Selbststudium für Polizeibeamte im Einsatz (Streife, Tatort, Hausdurchsuchung) oder mit dem Auftrag, die ursprüngliche Anzeige eines Opfers aufzunehmen. Es vermittelt grundlegende Kenntnisse zu Cyberkriminalität und digitaler Forensik. Es kann auch als Grundlage für Präsenzkurse an Polizeiakademien verwendet werden.

Durch die *Zertifizierung von Expertenprofilen* wird sichergestellt, dass jede Person über die notwendigen Kenntnisse und Kompetenzen verfügt. Sie motiviert Fachkräfte, ihre Kompetenzen auszubauen und sich bezüglich der Entwicklungen in ihrem Bereich auf dem Laufenden zu halten; ferner wird damit der berufliche Aufstieg und die persönliche Anerkennung unterstützt. Dies wiederum führt zu hochwertigerer und genauerer Arbeit. Darüber hinaus kann die persönliche Zertifizierung:

- eine klare und transparente Beschreibung der Kompetenzen und Fähigkeiten der Experten für digitale Forensik bieten, die es Praktikern sowie Abteilungsleitern ermöglicht, festzustellen, wen sie brauchen, um die notwendigen Anforderungen für die effiziente Abwicklung einschlägiger Aufgaben zu erfüllen;

- die Entwicklung von Schulungen auf nationaler, regionaler und EU-Ebene erleichtern und deren Organisation lenken; eine vergleichbare polizeiliche Ausbildung in allen EU-Mitgliedstaaten gewährleistet, dass alle Polizeibeamte – unabhängig von ihrem Land – Zugang zu einem einheitlichen Niveau an Kenntnissen und Kompetenzen haben;

- zu transparenteren Gerichtsverfahren beitragen;

- das Vertrauen zwischen Ermittlern und anderen Akteuren stärken und somit die internationale Zusammenarbeit zwischen nationalen Strafverfolgungsbehörden verbessern.

Die CEPOL hat mit der Ausarbeitung eines *sektoralen Qualifikationsrahmens* für Polizeiarbeit begonnen, mit Schwerpunkt auf der grenzüberschreitenden Zusammenarbeit. Dieses Modell kann auf der Grundlage der Arbeit der ECTEG zur Zertifizierung von Experten für digitale Forensik im Rahmen ihres Projekts für globale Zertifizierung im Bereich Cyberkriminalität (*Global Cybercrime Certification Project*[35]) operationalisiert werden.

Sowohl die ECTEG als auch die EACTDA investieren einen Teil ihrer Ressourcen in die Unterstützung der wirksamen *Einbindung einschlägiger Strafverfolgungs-Praktiker in Normungsprozesse*, beispielsweise durch die Erleichterung des Erwerbs der erforderlichen Kompetenzen.

Wichtigste Maßnahme: Die Experten der Hochrangigen Gruppe fordern die Verbesserung fachlicher Kompetenzen und die Zertifizierung von Profilen

Akteure: CEPOL, ECTEG	*Zeitrahmen: laufende Maßnahmen; Zertifizierungssystem für Experten der digitalen Forensik bis 2026*	*Mittelausstattung:*

- Die Experten der Hochrangigen Gruppe fordern die CEPOL auf, weiterhin Schulungen (insbesondere für Ausbilder) **durchzuführen**.
- Die Experten der Hochrangigen Gruppe fordern die ECTEG auf, weiterhin Schulungen zu digitaler Forensik für Experten und Ersthelfer mit besonderem Schwerpunkt auf Entschlüsselung **zu entwickeln, zu aktualisieren und zu erproben**.
- Die Experten der Hochrangigen Gruppe begrüßen die laufenden Bemühungen der Kommission (durch offene Aufforderungen zur Einreichung von Vorschlägen im Rahmen des ISF) zur Unterstützung der ECTEG sowie die **Einführung** von Schulungen auf regionaler Ebene.
- Die Hochrangige Gruppe fordert die ECTEG auf, die Möglichkeit zu sondieren, ein Zertifizierungssystem auf EU-Ebene für Experten der digitalen Forensik einzurichten, und sie fordert die CEPOL auf, im Rahmen des Möglichen zu diesen Bemühungen beizutragen, aufbauend auf ihrer Arbeit zu einem **sektoralen Qualifikationsrahmen** für die Polizeiarbeit und zur **globalen Zertifizierung im Bereich Cyberkriminalität**.
- Die Hochrangige Gruppe fordert die ECTEG auf, weiterhin den Erwerb von **Kompetenzen und Fachkenntnissen bezüglich Normungsprozessen** durch einschlägige Praktiker zu erleichtern.

[35] https://www.ecteg.eu/running/gcc/.

IV. Erleichterung des rechtmäßigen Zugangs

Ohne Normen, die den konzeptionsintegrierten rechtmäßigen Zugang regeln, müssen die Strafverfolgungsbehörden zunehmend auf die Ausnutzung von Schwachstellen zurückgreifen, um Zugang zu Daten auf beschlagnahmten Geräten zu erhalten, die durch Verschlüsselung geschützt sind. Diese Methode kann zwar die Ermittlungen voranbringen, ist aber mit hohen finanziellen Kosten verbunden. Daher müssen Überlegungen über mögliche Alternativen angestellt werden.

Empfehlungen Cluster 4

Zur Einrichtung von Mechanismen für die Zusammenarbeit mit einschlägigen Partnern aus der Industrie und zur Erforschung der Möglichkeit, verbindliche Standards festzulegen und die Rechtsvorschriften im Bereich des rechtmäßigen Zugangs im Einklang mit der Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) und des Europäischen Gerichtshofs für Menschenrechte anzugleichen, empfehlen die Experten Folgendes:

1. *Entwicklung einer Plattform (nach dem Modell von SIRIUS) für den Austausch von Instrumenten, bewährten Verfahren und Wissen darüber, wie der Zugang zu Daten von Produkteignern, Herstellern und Hardwareherstellern gewährt werden kann [Empfehlung 11];*

2. *Kartierung der Stellen der Strafverfolgungsbehörden für den Kontakt mit Herstellern von digitaler Hard- und Software [Empfehlung 11];*

3. *Durchführung einer umfassenden Bestandsaufnahme der geltenden Rechtsvorschriften in den Mitgliedstaaten und Erstellung eines EU-Handbuchs diesbezüglich, um die rechtlichen Verantwortlichkeiten der Hersteller von digitaler Hard- und Software für die Erfüllung von Datenanfragen der Strafverfolgungsbehörden im Einzelnen darzulegen, unter Berücksichtigung spezifischer Szenarien und Anforderungen, die Unternehmen zum Zugriff auf Geräte zwingen [Empfehlung 25];*

4. *Einrichtung einer Forschungsgruppe zur Bewertung der technischen Durchführbarkeit von Verpflichtungen des konzeptionsintegrierten rechtmäßigen Zugangs (einschließlich des Zugangs zu verschlüsselten Daten) für digitale Geräte, bei Erhaltung und ohne Gefährdung der Sicherheit der Geräte und der Geheimhaltung personenbezogener Daten für alle Nutzer sowie ohne die Sicherheit der Kommunikation zu schwächen oder zu untergraben [Empfehlung 26];*

5. *abhängig von der vorstehend genannten Bestandsaufnahme Entwicklung verbindlicher Industriestandards für in der EU auf den Markt gebrachte Geräte im Hinblick auf die Integration des rechtmäßigen Zugangs und Förderung der Angleichung der Rechtsvorschriften in diesem Raum [Empfehlung 25].*

Die derzeitigen Kontakte zwischen den Strafverfolgungsbehörden und der Industrie sind nicht geeignet, konkrete Ergebnisse zu erzielen; eine Verstärkung der Zusammenarbeit mit der Industrie ist erforderlich, um Wege des rechtmäßigen Zugangs zu Geräten und Anwendungen für Strafverfolgungsbehörden zu entwickeln. So sind die Strafverfolgungsbehörden beispielsweise bei Videoüberwachungsaufzeichnungen zunehmend mit verschlüsselten Dateien konfrontiert, die nicht mit automatischer Software analysiert werden können, insbesondere wenn es sich um große Mengen an Videoaufnahmen handelt.

Theoretisch können die Strafverfolgungsbehörden die Gerätehersteller um Unterstützung ersuchen, die ihrerseits den Quellcode ihrer Software bereitstellen können, um den Zugang zu entschlüsselten Inhaltsdaten leichter zu machen, oder technische Dokumentationen der bei strafrechtlichen Ermittlungen angetroffenen Ausrüstung bereitstellen können.

Europol wäre gut aufgestellt, um bewährte Verfahren (wie die Einrichtung von Kontaktstellen für die Strafverfolgungsbehörden) und Wissen darüber, wie Produkteigner, Hersteller und Hardwarehersteller den Zugang erleichtern könnten, zu erheben und allen Strafverfolgungsbehörden über SIRIUS (oder eine gleichwertige Plattform) zur Verfügung zu stellen.

Parallel dazu sollten transparentere Lösungen für die Erleichterung des Zugangs zu entschlüsselten Daten auf beschlagnahmten Geräten erwogen werden, um die Wirksamkeit der Ermittlungen zu erhöhen und gleichzeitig gleiche Wettbewerbsbedingungen zwischen den Akteuren der Industrie zu gewährleisten, wobei die Cybersicherheit gewahrt und die Privatsphäre geschützt werden muss.

Auf der Grundlage einer detaillierten Analyse der Anforderungen der Strafverfolgungsbehörden für den rechtmäßigen Zugang fordern die Experten die Europäische Kommission nachdrücklich auf, einen *Technologiefahrplan*[36] zu erstellen, der Maßnahmen von Experten für Technologie, Cybersicherheit, Privatsphäre, Normung und Sicherheit zusammenbringt und eine angemessene Koordinierung gewährleistet.

Eine zentrale Maßnahme im Rahmen dieses Technologiefahrplans wäre die Bewertung der *technischen Durchführbarkeit von Verpflichtungen des konzeptionsintegrierten rechtmäßigen Zugangs* (einschließlich des Zugangs zu verschlüsselten Daten und verschlüsselten Videoüberwachungsaufzeichnungen) für digitale Dateien und Geräte[37], wobei für robuste Garantien der Cybersicherheit zu sorgen ist und die Sicherheit der Kommunikation nicht geschwächt oder untergraben werden darf. Diese Bewertung würde unter Einbeziehung aller einschlägigen Interessenträger vorgenommen werden.

---

[36] In dem Bericht wird in mehreren Kapiteln wiederholt Bezug auf einen einheitlichen „Technologiefahrplan“ genommen.

[37] Siehe „Moving the Encryption Policy Conversation Forward“ (Die Beratungen zur Verschlüsselungspolitik voranbringen) – Carnegie Endowment for International Peace – https://carnegieendowment.org/research/2019/09/moving-the-encryption-policy-conversation-forward?lang=en.

Insoweit eine solche Bewertung die Verfügbarkeit oder Durchführbarkeit von Verpflichtungen des konzeptionsintegrierten rechtmäßigen Zugangs, die den oben dargelegten Voraussetzungen entsprechen, bestätigt, sollte der Technologiefahrplan auch das Verfahren für eine anhaltende, langfristige *Zusammenarbeit mit den Normungsgremien* bestimmen. Die Einbeziehung der Strafverfolgungsbehörden in diesen Normungsprozess könnte von Europol in Zusammenarbeit mit der EACTDA koordiniert werden.

Auf der Grundlage einer Bestandsaufnahme der bestehenden Rechtsrahmen der Mitgliedstaaten hinsichtlich der Festlegung der Verantwortlichkeiten der Hersteller von digitaler Hard- und Software für die Befolgung von Datenanfragen der Strafverfolgungsbehörden wäre es möglich, die Notwendigkeit von *Rechtsvorschriften oder Leitlinien und Empfehlungen* [zur Förderung der Angleichung der Rechtsvorschriften in diesem Bereich] zu bewerten.

Wichtigste Maßnahme: Die Experten der Hochrangigen Gruppe fordern den Ausbau der Zusammenarbeit mit der Industrie, die Förderung von Bezugnahmen auf einschlägige Standards in künftigen EU-Initiativen und die Angleichung der Rechtsvorschriften im Bereich des rechtmäßigen Zugangs im Einklang mit der Rechtsprechung des EuGH und des Europäischen Gerichtshofs für Menschenrechte

Akteure: Europol, Europäische Kommission	*Zeitrahmen: ab 2025*	*Mittelausstattung: keine Angabe*

- Die Experten der Hochrangigen Gruppe fordern die **Europäische Kommission** auf, einen speziellen **Technologiefahrplan** zu entwickeln, um Optionen für den rechtmäßigen Zugang zu digitalen Geräten zu erforschen.
- Die Experten der Hochrangigen Gruppe fordern **Europol** auf, bewährte Verfahren und Wissen darüber, wie Produkteigner, Hersteller und Hardwarehersteller den Zugang erleichtern könnten, zu erheben und allen Strafverfolgungsbehörden über **SIRIUS** (oder eine gleichwertige Plattform) zur Verfügung zu stellen.

Kapitel II: Vorratsdatenspeicherung

WAS SIND DIE ZUGRUNDE LIEGENDEN PROBLEME?

Während in der Vergangenheit in erster Linie physische Beweismittel erhoben wurden, werden heutzutage große Mengen potenzieller Beweismittel von Kommunikationsanbietern in Form von Metadaten gespeichert. Digitale Daten sind zwar nicht die einzigen Beweismittel, die im Rahmen strafrechtlicher Ermittlungen benötigt werden, sie sind jedoch in fast allen Ermittlungen von entscheidender Bedeutung – insbesondere zur Feststellung der Identität von Verdächtigen oder Personen von Interesse, die möglicherweise über einschlägige Informationen verfügen –, unabhängig davon, ob die zugrunde liegenden Straftaten in der physischen oder in der digitalen Welt begangen wurden. Insbesondere im digitalen Bereich können Verdächte häufig nur anhand von Kommunikationsmetadaten (insbesondere IP-Adressen und Port-Nummern) identifiziert werden.[38]

Damit Strafverfolgungsbehörden Straftaten im digitalen Zeitalter untersuchen können, ist es daher erforderlich, dass digitale Beweismittel in einem lesbaren Format zur Verfügung gestellt und zugänglich gemacht werden, wenn dies erforderlich ist, wobei angemessenen Garantien für Strafverfahren, den Verfahrensrechten sowie dem Schutz der Privatsphäre und dem Datenschutz gebührend Rechnung zu tragen ist. Die Daten können für geschäftliche Zwecke (z. B. Gebührenabrechnung und Rechnungstellung) oder zu Strafverfolgungszwecken gespeichert werden. Die Vorratsdatenspeicherung kann dazu beitragen, die Verfügbarkeit von Daten sicherzustellen, damit die zuständigen Behörden im Rahmen von strafrechtlichen Ermittlungen und Strafverfolgungsmaßnahmen auf diese zugreifen können. Die von den Diensteanbietern auf Vorrat gespeicherten Daten können für eine wirksame Kriminalitätsbekämpfung von entscheidender Bedeutung sein, und die Aufbewahrung dieser Daten ist eine Voraussetzung dafür, dass Strafverfolgungsbehörden anschließend auf diese zugreifen und Ermittlungen durchführen können.[39] Gleichzeitig sieht der in der Datenschutzrichtlinie für elektronische Kommunikation[40] und in der Datenschutz-Grundverordnung[41] (DSGVO) verankerte Grundsatz der Datenminimierung vor, dass Anbieter Verkehrsdaten nur so lange speichern (oder anderweitig verarbeiten dürfen), wie dies für die Zwecke der Kommunikation selbst, für die Gebührenabrechnung oder in bestimmten Situationen für die Vermarktung von elektronischen Kommunikationsdiensten erforderlich ist. Jede andere Speicherung muss einem Rechtsrahmen unterliegen, der den Anforderungen von Artikel 15 der Datenschutzrichtlinie für elektronische Kommunikation entspricht. Diese Regelung spiegelt die Notwendigkeit wider, ein Gleichgewicht zwischen den Grundrechten auf Privatsphäre und auf Datenschutz und den Zwecken der Strafverfolgungsmaßnahmen herzustellen.

---

38 Die Experten erörterten mehrere Beispiele dafür, wie digitale Daten für Ermittlungen von Relevanz sein können, und die Zahl der Datenanfragen. Nach Angaben eines Experten wurden in den letzten fünf Jahren bei allen Ermittlungen im Zusammenhang mit Terrorismus oder organisierter Kriminalität Daten verwendet, die von Diensteanbietern angefordert wurden. Im Jahr 2023 wurden in einem Mitgliedstaat mehr als 1 300 000 Nummern von Betreibern zwecks Identifizierung in Strafverfahren angefordert, von denen nahezu alle im Anschluss vom Justizsystem validiert wurden.

39 Für die Zwecke dieses Dokuments bezeichnet der Begriff „Datenzugang“ den Zugang, der Strafverfolgungsbehörden für die Zwecke strafrechtlicher Ermittlungen und auf Einzelfallbasis gewährt wird und der erforderlichenfalls einer richterlichen Vorabgenehmigung unterliegt.

40 Artikel 6 der Richtlinie 2002/58/EG.

41 Artikel 5 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679.

Derzeit gibt es keine EU-Rechtsvorschriften zur Regelung der Vorratsdatenspeicherung. Der EuGH erklärte die EU-Richtlinie über die Vorratsdatenspeicherung[42] im Jahr 2014 für nichtig, wobei er auf die erheblichen Eingriffe in die Grundrechte auf Privatsphäre und auf Datenschutz verwies, die mit der [allgemeinen und unterschiedslosen] Speicherung von ursprünglich von Diensteanbietern erhobenen Daten zu Strafverfolgungszwecken verbunden sind.[43] Infolgedessen wurden die nationalen Rechtsrahmen geändert, was zu erheblichen Unterschieden innerhalb der EU geführt hat[44]: einige Mitgliedstaaten verfügen zwar nach wie vor über Vorschriften, die Kommunikationsanbieter verpflichten, bestimmte Kategorien von Daten zu Strafverfolgungszwecken zu speichern, andere haben jedoch Änderungen vorgenommen, um das in der Rechtsprechung vorgeschlagene Kriterium der gezielten Vorratsspeicherung von Verkehrsdaten zu erfüllen;[45] andere Mitgliedstaaten verfügen – auch aufgrund späterer Urteile nationaler Gerichte – über keine spezifischen Vorschriften über die Vorratsspeicherung von Daten zu Strafverfolgungszwecken und stützen sich ausschließlich auf Daten, die von Unternehmen für geschäftliche Zwecke gespeichert werden. Die Bedingungen für den Zugang zu diesen Daten hängen vom geltenden nationalen Rechtsrahmen und von der Art der Daten ab (Teilnehmer-, Verkehrs- oder Inhaltsdaten). Aufgrund dieses Mangels an kohärenten und harmonisierten Verpflichtungen zur Vorratsdatenspeicherung in der EU bestehen Unterschiede zwischen den Mitgliedstaaten in Bezug auf die Anforderungen an die Speicherung verschiedener Arten von Metadaten durch Diensteanbieter (und an die Dauer dieser Speicherung).

---

42 Richtlinie 2006/24/EG. Nach der Richtlinie waren die EU-Mitgliedstaaten verpflichtet, Maßnahmen zu ergreifen, um sicherzustellen, dass Anbieter elektronischer Kommunikationsdienste und -netze Verkehrs- und Standortdaten und die damit zusammenhängenden Daten, die zur Identifizierung des Teilnehmers oder registrierten Benutzers erforderlich sind, für einen Zeitraum zwischen sechs Monaten und zwei Jahren auf Vorrat speichern, damit die zuständigen Behörden zum Zweck der Ermittlung, Feststellung und Verfolgung schwerer Straftaten im Sinne der nationalen Rechtsvorschriften darauf zugreifen können.

43 Einen Überblick über die einschlägige Rechtsprechung finden Sie unter: The future of national data retention obligations – How to apply Digital Rights Ireland at national level? – European Law Blog, V. Franssen; Recalibrating Data Retention in the EU – eucrim; Eurojust/EJCN 2024 report. The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU; Cybercrime Judicial Monitor – Ausgabe 6; Cybercrime Judicial Monitor - Ausgabe 9.

44 Die Mitgliedstaaten reagierten unterschiedlich auf die Nichtigerklärung der Richtlinie über die Vorratsdatenspeicherung, und durch die auf nationaler Ebene eingeleiteten Maßnahmen wurden die nationalen Systeme zur Vorratsdatenspeicherung noch vielfältiger. Laut dem Bericht von Eurojust/EJCN über die Vorratsdatenspeicherung von 2024 haben 12 Länder ihre Rechtsvorschriften im Zeitraum 2018-2022 geändert. Die Befragten antworteten, dass diese Änderungen unmittelbar auf die Rechtssachen C-746/18, *Prokuratuur* und die verbundenen Rechtssachen C-511/18, C-512/18 und C-520/18, *La Quadrature du Net u. a*. zurückzuführen seien. In 23 von 27 Mitgliedstaaten gibt es Vorschriften für die Vorratsdatenspeicherung; sieben Mitgliedstaaten haben bereits Vorschriften für die gezielte Vorratsdatenspeicherung eingeführt. Einen Überblick bietet das Kommissionsdokument Study on the retention of electronic communications non-content data for law enforcement purposes, 2020, S. 39.

45 Der Gerichtshof hat das Konzept der gezielten Vorratsspeicherung von Verkehrs- und Standortdaten über mehrere Urteile entwickelt und entschieden, dass die Vorratsdatenspeicherung mit dem Unionsrecht vereinbar sein kann, wenn sie auf bestimmte Ziele und Zwecke ausgerichtet ist. Die praktische Anwendung der vom Gerichtshof für die Festlegung solcher Ziele vorgeschlagenen Kriterien hat jedoch zu Schwierigkeiten und Herausforderungen vor den obersten Gerichten in den Mitgliedstaaten geführt, die dies versucht haben.

In den Mitgliedstaaten, in denen keine Verpflichtung zur Vorratsdatenspeicherung besteht, gestaltet es sich schwierig oder mitunter unmöglich, einen Verdächtigen oder eine Person im Rahmen strafrechtlicher Ermittlungen zu identifizieren, die möglicherweise über einschlägige Informationen verfügt (im Folgenden „Person von Interesse“).[46] Der Mehrwert der neuen Vorschriften über elektronische Beweismittel würde, sobald diese in Kraft sind, ebenfalls erhöht, wenn sie durch Verpflichtungen zur Vorratsspeicherung ergänzt würden, da sonst keine Garantie dafür besteht, dass Informationen, die Gegenstand europäischer Sicherungs- oder Herausgabeanordnungen sind (Verkehrsdaten, ausschließlich zum Zweck der Identifizierung des Nutzers angeforderte Daten und Teilnehmerdaten), zur Verfügung stehen.

Die derzeitigen Umstände betreffen sowohl **Strafverfolgungs-** als auch **Kommunikationsanbieter**, jedoch haben sie insbesondere **Auswirkungen auf Bürgerinnen und Bürger sowie Opfer**, deren Recht auf Zugang zur Justiz nicht gewährleistet werden kann, wenn die Ermittlungen eingeleitet werden, nachdem die Daten bereits gelöscht wurden, oder wenn keine Daten gespeichert wurden.[47]

I. Probleme in der Zuständigkeit der einzelnen Mitgliedstaaten

In Mitgliedstaaten, in denen **keine spezifischen Verpflichtungen** in Bezug auf die Vorratsdatenspeicherung zu Strafverfolgungszwecken bestehen, stützen sich die Ermittlungen neben anderen verfügbaren Beweismitteln auf die Daten, die Unternehmen für ihre geschäftlichen und kommerziellen Zwecke speichern. Kommerzielle Daten unterliegen den internen Vorschriften der Anbieter; so speichern Unternehmen Verkehrsdaten für unterschiedlich lange Zeiträume (z. B. etwa 6 Monate), während Standortdaten, die in der Regel keine geschäftliche Relevanz haben, häufig für einen kürzeren Zeitraum gespeichert werden. Kleine Unternehmen speichern meist überhaupt keine Metadaten zu Teilnehmern oder Kommunikationen oder nur für sehr kurze Zeit. Infolgedessen sind Ermittlungen oft ein Wettlauf gegen die Zeit, da die Ermittler den Bereitsteller der Daten identifizieren und die Anfrage im Einklang mit den geltenden Vorschriften übermitteln müssen, bevor die Daten gelöscht werden, was mitunter innerhalb von Tagen oder Stunden geschieht. In einigen Fällen stellen Unternehmen keine Informationen über die spezifischen Daten bereit, die sie verarbeiten und besitzen, was es den zuständigen Behörden erschwert, gezielte Anfragen zu stellen, wenn sie Daten anfordern. Einige Hostingdienste ermöglichen es Nutzern, Serverkapazitäten unter Verwendung fiktiver Daten zu mieten, was bedeutet, dass selbst wenn Nutzerdaten gespeichert werden, deren Zuverlässigkeit nicht gegeben ist.[48]

---

46 Siehe das Beispiel im Hintergrunddokument Operational challenges faced by law enforcement related to access to data Input to the first plenary meeting of the High-Level Group (HLG) on access to data for effective law enforcement, S. 4.

47 Im Zusammenhang mit den Auswirkungen auf Bürgerinnen und Bürger sowie Opfer siehe *Dwyer* gegen *Commissioner of An Garda Siochána* – [2020] IESC 4 (24.2.2020), insbesondere Rn. 9.

48 https://en.wikipedia.org/wiki/Bulletproof_hosting.

In den meisten Mitgliedstaaten **bestehen Rechtsvorschriften** über die Vorratsdatenspeicherung. Wie oben dargelegt, wurden jedoch einige nationale Rechtsvorschriften infolge der Urteile des EuGH geändert, die auf die Ungültigkeitserklärung der Richtlinie über digitale Rechte zurückzuführen waren. Dies hat zu einer Fragmentierung der Rechtslandschaft geführt, bei der die Mitgliedstaaten unterschiedlich auf die Urteile reagiert haben. Entsprechend eines Vorschlags des EuGH in Bezug auf das mögliche weitere Vorgehen wurden in einigen Mitgliedstaaten Anstrengungen unternommen, um eine gezielte Vorratsdatenspeicherung umzusetzen. Die Experten der Hochrangigen Gruppe betonten jedoch, dass die Umsetzung dieser Kriterien rechtliche und technische Probleme hinsichtlich ihrer Durchführbarkeit aufwerfe[49], und die Anbieter kritisierten die Kosten im Zusammenhang mit der technischen Umsetzung einer gezielten Vorratsdatenspeicherung und – ganz allgemein – mit häufigen Änderungen der Rechtsvorschriften. Ein weiteres schwerwiegendes rechtliches Problem auf nationaler Ebene besteht darin, dass die nationalen Rechtsvorschriften in den meisten Fällen Over-the-Top-Dienste (OTT) nicht abdecken. Der spezifische Fall von OTT-Diensten wird in Abschnitt 1.3 eingehender beleuchtet.

II. Grenzüberschreitende Probleme in der EU

Probleme im Zusammenhang mit der Vorratsdatenspeicherung treten auch bei grenzüberschreitenden Anfragen auf, d. h. wenn eine zuständige Behörde Daten von einem in einem anderen Mitgliedstaat ansässigen Anbieter anfordert. Bei grenzüberschreitenden Anfragen sind die Behörden im Empfängerland möglicherweise nicht in der Lage, eine Anfrage eines anderen Landes zu erledigen (weil keine Daten oder einschlägige Rechtsvorschriften vorliegen).

Da die Verpflichtungen zur Vorratsspeicherung von Metadaten auf EU-Ebene nicht harmonisiert sind, bestehen Herausforderungen für Strafverfolgungsbehörden, die **Daten** von in einem anderen Mitgliedstaat ansässigen Anbietern **anfordern**. Selbst wenn auf nationaler Ebene Regelungen zur Vorratsdatenspeicherung bestehen, gibt es keine Kohärenz zwischen den nationalen Regelungen für die Speicherfristen, die von Mitgliedstaat zu Mitgliedstaat erheblich variieren.[50]

---

[49] Der EuGH bietet zwar einige Leitlinien und Beispiele für die Auslegung der **gezielten Vorratsspeicherung** von Verkehrsdaten, die Rechtsprechung kann jedoch nur Anhaltspunkte liefern und ist nicht präzise genug, um mögliche Einschränkungen bei der Vorratsspeicherung für alle Datenkategorien ausführlich darzulegen. Folglich wurden in den letzten Jahren mehrere Verfahren gegen Vorschriften über die Vorratsdatenspeicherung beim Gerichtshof anhängig gemacht, und die Mitgliedstaaten können nicht für Rechtssicherheit sorgen.

[50] Metadaten werden für einen Zeitraum zwischen 6 und 72 Monaten gespeichert, je nach Art der Daten und Straftat. In dem Bericht von Eurojust/EJCN über die Vorratsdatenspeicherung von 2024 (Eurojust/EJCN data retention report of 2024) wiesen die Befragten darauf hin, dass aufgrund des Mangels an auf Vorrat gespeicherten Daten, der Beschränkungen der Kategorien von Daten, die auf

Ebenso gibt es auf EU-Ebene keinen harmonisierten Ansatz für die **Definition der Daten**, die auf Vorrat zu speichern sind.[51] Diensteanbieter können durch nationale Rechtsvorschriften dazu verpflichtet sein, verschiedene Kategorien von Daten für unterschiedliche Zwecke (Steuern, Audits, Strafverfolgung) auf Vorrat zu speichern. Unterschiede bestehen auch in Bezug auf den Detaillierungsgrad, da einige Rechtsvorschriften detaillierte Listen der auf Vorrat zu speichernden Nichtinhaltsdaten enthalten, während andere weiter gefasste Definitionen von Nichtinhaltsdaten enthalten.[52] Darüber hinaus werden verschiedene Arten von Daten von den Anbietern für unterschiedlich lange Zeiträume auf Vorrat gespeichert, je nach dem von ihnen angebotenen Dienst und ihren geschäftlichen und kommerziellen Bedürfnissen. Dadurch entsteht eine äußerst heterogene Landschaft mit erheblichen Unterschieden nicht nur zwischen den Mitgliedstaaten, sondern auch zwischen den Diensten.

Diese Unterschiede sind auch aufgrund der Unterschiede zwischen den Mitgliedstaaten in Bezug auf den Zugang zu auf Vorrat gespeicherten Daten erheblich: einige Mitgliedstaaten benötigen eine richterliche Genehmigung für den Zugang zu bestimmten Arten von Metadaten, andere hingegen nicht. Diensteanbietern zufolge ist die Rechtsunsicherheit in Bezug auf die für die Offenlegung von Daten geltenden Vorschriften eine der Ursachen für Verzögerungen und die Nichteinhaltung von Strafverfolgungsersuchen.

Vorrat gespeichert werden dürfen, und der kurzen (kürzeren) Aufbewahrungsfristen weniger Daten verfügbar sind. Die fehlende Verfügbarkeit von Daten wirkt sich folglich auch auf die Fähigkeit der Behörden aus, Europäische Ermittlungsanordnungen und Rechtshilfeersuchen zu vollstrecken.

[51] Aus der Studie der Kommission über die Vorratsdatenspeicherung (Seite 48) geht hervor, dass bestimmte Arten von Informationen zwar in allen Mitgliedstaaten stets als Teilnehmer- oder Verkehrsdaten eingestuft werden, jedoch kein Konsens über die Klassifizierung der folgenden Datenpunkte besteht: IP-Adressen, SIM-Nummern, Geräte-Identifizierungsnummern (z. B. IMSI, IMEI) und Portnummern für dynamische IP-Adressen. In einigen Mitgliedstaaten (EE, FR, IE) werden diese Datenpunkte als Teilnehmerdaten eingestuft, während andere (DE, ES, IT, PL, SI) sie als Verkehrsdaten einstufen.

[52] Siehe Anhang III Studie der Kommission über die Vorratsdatenspeicherung für einen Überblick über die in den einzelnen Mitgliedstaaten gespeicherten Daten.

Die zuständigen Behörden müssen die für den Anbieter, der die angeforderten Daten besitzt, geltenden nationalen Vorschriften, aber auch die von den Anbietern selbst festgelegten spezifischen Anforderungen einhalten. Wie im SIRIUS-Jahresbericht 2022[53] angegeben, können Anbieter verlangen, dass spezielle Portale genutzt oder Anfragen unter Verwendung bestimmter Vorlagen oder Sprachen eingereicht werden. Darüber hinaus können sie Informationen über die Art des Falls, einen klaren Verweis auf die nationale Rechtsgrundlage für die Anfrage oder die Festlegung enger Fristen für die angeforderten Daten verlangen. Mit der Umsetzung des Pakets zu elektronischen Beweismitteln bis 2026 werden zwar einige dieser Probleme angegangen werden, die Experten der Hochrangigen Gruppe betonten jedoch, dass zwischen diesen Vorschriften und einem möglichen harmonisierten Rahmen für die Vorratsdatenspeicherung Kohärenz bestehen muss. Das Europäische Institut für Telekommunikationsnormen (European Telecommunications Standards Institute – ETSI) hat zwar Normen für das Format von Anfragen für nummerngebundene interpersonelle Kommunikationsdienste (herkömmliche Telekommunikationsdienste) entwickelt, doch werden diese von den Anbietern nicht in allen Mitgliedstaaten einheitlich angewandt. Die Normen für die Datenübermittlung von OTT-Dienstleistern[54] an Strafverfolgungsbehörden sind noch nicht vollständig ausgearbeitet und umgesetzt. Darüber hinaus können die Diensteanbieter frei entscheiden, in welcher Form sie Nutzerdaten erheben und speichern, was dazu führt, dass die Praktiker Rohdaten in sehr unterschiedlicher Form erhalten; dies führt zu einer erheblichen Belastung für die Strafverfolgungsbehörden, die von gestrafften Verfahren, **Kommunikationssystemen und Formaten** für die Übermittlung von Anfragen und für das Versenden und Empfangen von Antworten auf Anfragen sowie Daten profitieren würden. Darüber hinaus würden standardisierte Kommunikationssysteme und Formate die Kosten für die Bearbeitung von Anfragen für Unternehmen senken.

Sobald die Strafverfolgungsbehörden rechtmäßig Zugang zu Daten erhalten haben, müssen sie in der Lage sein, diese zu nutzen; daher müssen die Daten **lesbar** sein. Die Anbieter bieten jedoch zunehmend Dienste an, die eine Ende-zu-Ende-Verschlüsselung von Verkehrsdaten ermöglichen, und wenn sie diese Daten auf Anfrage den Strafverfolgungs- und Justizbehörden zur Verfügung stellen, dann erfolgt dies häufig in dieser verschlüsselten Form.

---

53 sirius-eu-digital-evidence-situation-report-2022, S. 14.

54 In diesem Bericht bezieht sich der Begriff „Over-the-top-Kommunikationsdienste“ auf Anwendungen und Dienste, die Kommunikations- und Mediendienste (wie Nachrichtenübermittlung sowie Sprach- und Videoanrufe) über das Internet ohne Beteiligung oder Kontrolle herkömmlicher Anbieter von Telekommunikationsdiensten (Telekommunikationsunternehmen) bereitstellen. Gängige Beispiele für OTT-Kommunikationsdienste sind Nachrichtenanwendungen wie WhatsApp, Telegram, Facebook Messenger, Sprach- und Videoanrufdienste wie Skype, Zoom, Google Meet, Viber, und Social-Media-Plattformen wie Instagram und Snapchat (Nachrichtenübermittlung und Teilen von Medien).

Eine weitere empfundene Folge dieses Status quo ist schließlich die Gefahr, dass die **Beweismittel** der Strafverfolgungsbehörden vor Gericht **angefochten werden**.[55] Der EuGH hat klargestellt, dass die Zulässigkeit von durch Vorratsdatenspeicherung erlangten Beweismitteln unter das nationale Recht fällt[56] – vorbehaltlich der Grundsätze der Äquivalenz und der Effektivität[57]; Die Unterschiede zwischen den nationalen Regelungen zur Vorratsdatenspeicherung können sich daher auf die Zulässigkeit von Beweismitteln in grenzüberschreitenden Verfahren auswirken.[58]

---

55 Siehe Kapitel zur Erhebung und Zulässigkeit von Beweismitteln (Collection and admissibility of evidence) im Bericht von Eurojust/EJCN über die Vorratsdatenspeicherung von 2024 (Eurojust/EJCN data retention report of 2024).

56 EuGH, Urteil vom 6. Oktober 2020, *La Quadrature du Net u. a.*, Rechtssache C-511/18 ECLI:EU:C:2020:791, Rd. 222 bis 228, Urteil vom 5. April 2022, *Commissioner of An Garda Síochána u. a.*, Rechtssache C-140/20, ECLI:EU:C:2022:258, Rn. 127.

57 Ebenda, Rd. 223: „[...] wobei sie [...] nicht ungünstiger sein dürfen als diejenigen, die gleichartige, dem innerstaatlichen Recht unterliegende Sachverhalte regeln (Äquivalenzgrundsatz), und die Ausübung der durch das Unionsrecht verliehenen Rechte nicht praktisch unmöglich machen oder übermäßig erschweren dürfen (Effektivitätsgrundsatz) [...].“

58 In mehreren Gerichtsverfahren wurde die Zulässigkeit von Nichtinhaltsdaten als Beweismittel in Frage gestellt. Eine Zusammenfassung findet sich auf Seite 41 in der Studie der Kommission über die Vorratsdatenspeicherung.

III. Probleme im Zusammenhang mit OTT und anderen Anbietern

Während sich die oben genannten Probleme auf alle Anbieter von elektronischen Kommunikationsdiensten beziehen, stellen OTT-Anbieter Strafverfolgungsbehörden vor zusätzliche Herausforderungen beim rechtmäßigen Zugang zu Daten. Sowohl auf nationaler als auch auf EU-Ebene sehen sich OTT-Anbieter häufig nicht an dieselben Verpflichtungen gebunden wie herkömmliche Kommunikationsanbieter. Während OTT-Anbieter in den Anwendungsbereich des Europäischen Kodex für die elektronische Kommunikation (EKEK) fallen, führen die Tatsache, dass sie häufig außerhalb der EU niedergelassen sind, und das Fehlen von Lizenzierungssystemen (d. h. sie unterliegen womöglich ausschließlich Allgemeingenehmigungen) und Sanktionen zu Unsicherheit hinsichtlich ihrer Verpflichtung zur Vorratsspeicherung von Daten – einschließlich bestimmter Arten von Daten – und zu Herausforderungen bei der Durchsetzung der Einhaltung der Vorschriften. Darüber hinaus speichern herkömmliche Kommunikationsanbieter zwar in den meisten Fällen einige Daten für geschäftliche Zwecke auf Vorrat, anhand derer Nutzer identifiziert werden können (z. B. IP-Adressen mit Port-Nummern und Zeitangaben), dies gilt jedoch nicht für **OTT-Diensteanbieter**, die lediglich die für ihre kommerziellen Zwecke benötigten Nichtinhaltsdaten auf Vorrat speichern, in einigen Fällen nur für einen kurzen Zeitraum.[59] OTT-Anbieter speichern Nichtinhaltsdaten, die mit einer dynamischen IP-Adresse (Port-Nummer und Zeitangaben) verbunden sind, nicht auf Vorrat. Dies kann es erschweren oder sogar unmöglich machen, Metadaten von Kommunikationen abzurufen, die über Systeme wie WhatsApp oder Telegram erfolgen, die zunehmend genutzt werden. Wie bereits erwähnt, unterscheiden sich auch die Arten der auf Vorrat gespeicherten Daten je nach angebotenem Dienst. Die Anbieter geben zwar in einigen Fällen Leitlinien heraus, in denen sie darlegen, welche Arten von Daten sie auf Vorrat speichern[60], OTT-Anbieter legen diese Informationen in anderen Fällen jedoch nicht offen. Zusammen mit dem Mangel an **Transparenzpflichten** in Bezug auf die Arten von Daten, die Anbieter für geschäftliche Zwecke erzeugen, verarbeiten und speichern, führt dies häufig zu Problemen für Strafverfolgungsbehörden bei der Feststellung, ob Daten auf Vorrat gespeichert wurden, wer über welche Daten verfügt und welche Arten von Datensätzen angefordert werden können, und letztlich wenn sie Anfragen an Anbieter richten.

---

[59] Dies gilt insbesondere für kleine Anbieter. Laut der Studie der Kommission über die Vorratsdatenspeicherung (S. 103), werden IP-Adressen im Durchschnitt 30 Tage lang gespeichert.

[60] Siehe z. B. law-enforcement-guidelines-outside-us.pdf (apple.com).

Gleichzeitig trägt die steigende Zahl der bei den Anbietern eingehenden Anfragen[61] in Verbindung mit der Notwendigkeit, umfangreiche Datensätze zu verarbeiten, dazu bei, dass Anfragen verzögert oder abgelehnt werden[62]. Dies ist neben den spezifischen Geschäftsmodellentscheidungen der Anbieter auch auf die **begrenzte Zahl von Mechanismen für die Zusammenarbeit** zwischen Strafverfolgungs- und Justizbehörden einerseits und privaten Unternehmen andererseits zurückzuführen.

Obwohl sie möglicherweise nicht unter die Definition des EKEK für Kommunikationsdienste fallen, erzeugen und verarbeiten einige neue Technologien und andere digitale Akteure (wie Automobilhersteller und KI-Systeme mit Großen Sprachmodellen) Kommunikationsmetadaten, die Informationen über kriminelle Aktivitäten liefern können. Obwohl diese Dienste immer mehr Daten verarbeiten, sind sie derzeit nicht an die Verpflichtungen zur Vorratsdatenspeicherung gebunden.

MÖGLICHE LÖSUNGEN

I. Stärkung der Zusammenarbeit zwischen Kommunikationsanbietern und Praktikern

Da die Erhebung digitaler Beweismittel durch das Fehlen harmonisierter Vorschriften erschwert wird, sind Strafverfolgungsbehörden bei der Durchführung von Ermittlungen häufig auf die **freiwillige Zusammenarbeit** mit Diensteanbietern angewiesen. Diese Lösung hat zwar einige Ermittlungen in besonders beachteten Fällen erleichtert[63], sie ist jedoch mit Rechtsunsicherheit behaftet und nicht immer praktikabel: die freiwillige Zusammenarbeit hängt von der Art und Größe des Diensteanbieters ab, da kleine Anbieter Daten für viel kürzere Zeiträume auf Vorrat speichern als größere Anbieter oder nicht über die Ressourcen verfügen, um auf Anfragen der Strafverfolgungsbehörden zu reagieren.[64]

---

61 Laut dem SIRIUS-Jahresbericht 2023 nimmt die Menge der an Diensteanbieter gerichteten Anfragen jedes Jahr kontinuierlich zu (siehe S. 66 ff.).

62 Der SIRIUS-Jahresbericht 2023 (Fußnote 61) gibt einen Überblick über die Hauptursachen für die Verzögerung/Ablehnung von Anfragen um elektronische Beweismittel (siehe S. 68 ff.).

63 Siehe Beispiele im SIRIUS-Jahresbericht 2023 (Fußnote 61), S. 19.

64 Im SIRIUS-Jahresbericht 2023 (Fußnote 61, S. 79) wird berichtet, dass die große Zahl von Anfragen im Rahmen der freiwilligen Zusammenarbeit für Diensteanbieter eine Herausforderung darstellt, und ihnen wird empfohlen, an internationalen SIRIUS-Veranstaltungen teilzunehmen, damit kleinere Online-Diensteanbieter das Fachwissen des SIRIUS-Projekts im Bereich der Zusammenarbeit mit Behörden nutzen können, um ihr Verständnis in dieser Angelegenheit zu verbessern, ihre Strategien für die Beantwortung der Anfragen der Behörden zu strukturieren und sicherzustellen, dass sie auf künftige rechtliche Entwicklungen vorbereitet sind.

Partnerschaften und die Zusammenarbeit mit der Industrie müssen auf einem **klaren Rechtsrahmen** beruhen, der ein wesentlicher Bestandteil jeder tragfähigen Lösung ist, die es den Strafverfolgungs- und Justizbehörden ermöglicht, Schwierigkeiten beim rechtmäßigen Zugang zu digitalen Beweismitteln zu überwinden. Damit die Praktiker der Strafverfolgungsbehörden und Anbieter ein Verständnis für die Bedürfnisse der anderen Seite entwickeln und gemeinsam praktikable Lösungen finden können, ist es wichtig, dass beide Parteien ihren jeweiligen rechtlichen Verpflichtungen nachkommen und eine dauerhafte und vertrauensvolle Beziehung untereinander aufbauen. Stabile **Mechanismen für die Zusammenarbeit** mit dem Privatsektor sind erforderlich, um die **Transparenz** in Bezug auf die von den Anbietern erzeugten und gespeicherten Daten und die Dauer der Vorratsspeicherung **zu erhöhen**, aber auch um eine **harmonisierte Kategorisierung der** auf Vorrat zu speichernden und abzurufenden **Daten** zu gewährleisten, **standardisierte Formate** für die Anforderung von Daten zu konzipieren und **sichere Kanäle** für den direkten Austausch zwischen zuständigen Behörden und Diensteanbietern einzurichten.

Es können mehrere Optionen zur Stärkung dieser Zusammenarbeit geprüft werden, von denen einige verbindlich sind (zwingendes Recht), während andere Lösungen auf nicht zwingendem Recht beruhen. Einige der in diesem Abschnitt aufgeführten Lösungen müssten im Rahmen der in Abschnitt II genannten Folgenabschätzung bewertet und anschließend in Rechtsvorschriften umgesetzt werden.

Empfehlungen Cluster 5

Um sicherzustellen, dass die zuständigen Behörden in der Lage sind, die richtigen Dateninhaber zu identifizieren und relevante Daten von diesen einzuholen, dass solche Anfragen bei Diensteanbietern in standardisierten Formaten eingehen und dass die grenzüberschreitende Zusammenarbeit nicht durch Rechtskollisionen beeinträchtigt wird, empfehlen die Experten Folgendes:

1. *Aufbau und Verstärkung der Zusammenarbeit zwischen Praktikern der Strafverfolgungsbehörden und Diensteanbietern zur Unterstützung des Informationsaustauschs, des Kapazitätsaufbaus und von Schulungen sowie zur Festlegung der Grundsätze und Modalitäten der Zusammenarbeit [Empfehlung 13], beispielsweise durch die Einrichtung einer Clearingstelle, die es den zuständigen Behörden ermöglicht, einschlägige Diensteanbieter zu ermitteln und rechtmäßige Anfragen gezielter an diese zu richten [Empfehlung 18]. Dies könnte erreicht werden, indem*

    a. *auf bestehenden Strukturen auf EU-Ebene aufgebaut wird, etwa dem SIRIUS-Projekt, dem Europäischen Justiziellen Netz (EJN)/dem Europäischen Justiziellen Netz zur Bekämpfung der Cyberkriminalität (EJCN), dem EU-Internetforum;*

    b. *Vereinbarungen getroffen werden, in die bewährte Verfahren einfließen, die in bestimmten Mitgliedstaaten auf nationaler Ebene etabliert wurden [Empfehlung 14];*

2. *Förderung von Transparenzvorschriften für Anbieter elektronischer Kommunikationsdienste und anderer Kommunikationsdienste in Bezug auf die Daten, die sie im Zuge ihrer Geschäftstätigkeit verarbeiten, erzeugen oder speichern, sowie in Bezug auf die Unterrichtung der Strafverfolgungsbehörden darüber, welche Daten verfügbar sind, wobei den durch die Vertraulichkeit der Ermittlungen gesetzten Grenzen Rechnung getragen wird, im Wege von Kooperationsvereinbarungen mit Diensteanbietern oder erforderlichenfalls durch die Festlegung verbindlicher Verpflichtungen [Empfehlung 17, Empfehlung 16];*

3. *die Entwicklung gestraffter Verfahren und Formate auf der Grundlage vereinbarter Standards für die strukturierte Übermittlung von Anfragen an Anbieter und den Erhalt von Antworten [Empfehlung 15] und die Förderung der Benennung einziger Anlaufstellen (Single Point of Contact – SPoC) innerhalb der Plattformen für die Bearbeitung von Anfragen von und Kontakten mit den zuständigen Behörden [Empfehlung 36];*

4. *Einrichtung von Mechanismen, um sicherzustellen, dass grenzüberschreitende Anfragen in einer Weise an Diensteanbieter gerichtet werden, die effizient ist und potenzielle Konflikte vermeidet, wobei die für elektronische Beweismittel festgelegten Mechanismen als Modell dienen können und die Kohärenz dieser Mechanismen mit den in der Verordnung über elektronische Beweismittel festgelegten Vorschriften sichergestellt wird [Empfehlung 19].*

Derzeit bestehen EU-Strukturen, die es den einschlägigen Akteuren ermöglichen, sich mit Instrumenten und bewährten Verfahren vertraut zu machen. Durch die Zusammenführung von Strafverfolgungsbehörden, Justizbehörden und Diensteanbietern könnte das SIRIUS-Projekt den Austausch von Wissen und Instrumenten im Zusammenhang mit Anfragen von Nutzerdaten, die sich im Besitz von Anbietern befinden, erleichtern[65] und – insbesondere dank des bestehenden Netzes der SIRIUS-SPoC – als Plattform für die direkte Verbindung zwischen anfragenden Behörden und Anbietern dienen[66]. SIRIUS könnte als **zentrales Archiv** für Rechtsinstrumente, Rechtsprechung, Formate usw. dienen, wie dies beim grenzüberschreitenden Austausch elektronischer Beweismittel der Fall ist.[67]

Als bestehendes Kooperationsumfeld für die Mitgliedstaaten, die Internetbranche und andere Partner könnte das **EU-Internetforum**[68] als Raum dienen, in dem auf EU-Ebene zwischen den einschlägigen Akteuren in Bezug auf Tätigkeiten im Zusammenhang mit dem Zugang zu digitalen Daten direkte Kontakte aufgebaut und Vertrauen hergestellt werden könnten. Es könnte zur Erstellung und Aktualisierung eines **offenen Katalogs** der Arten von Daten beitragen, die Anbieter und Datenbearbeiter erheben und verarbeiten und möglicherweise zentral von SIRIUS verwaltet werden. Ein solcher Katalog würde den derzeitigen Mangel an Transparenz abmildern und den Strafverfolgungs- und Justizbehörden mehr Klarheit darüber verschaffen, welche Daten sie anfragen können, und als Clearingstelle fungieren, mit der ermittelt werden kann, an wen eine Anfrage gerichtet werden sollte. Darüber hinaus würde der Katalog für den Fall, dass den Anbietern rechtliche Verpflichtungen auferlegt werden, einen Mehrwert bei der Überwachung und Bewertung der Umsetzung der Transparenzpflichten in Bezug auf die Arten von Daten bieten, die die Anbieter speichern oder anderweitig verarbeiten.

---

65 Das SIRIUS-SPoC-Netz von Experten für rechtmäßige Datenanfragen fördert bewährte Verfahren und ermutigt die Länder, eigene SPoC einzurichten. SPoC sind benannte Personen, Einheiten oder Einrichtungen, die Anfragen von Regierungsbehörden zentralisieren, überprüfen und an Diensteanbieter übermitteln. Derzeit sind 36 Strafverfolgungsbehörden aus 25 Ländern Teil dieses Netzes.

66 Das SIRIUS-Projekt dient als Anlaufstelle für die Beschaffung elektronischer Daten von Diensteanbietern, die in anderen Ländern ansässig sind. SIRIUS bietet eine eingeschränkte Plattform für den Austausch von Wissen und bewährten Verfahren für Strafverfolgungs- und Justizpersonal. Im Rahmen des SIRIUS-Projekts wird ein Archiv mit aktuellen Kontaktdaten von über 1000 Unternehmen geführt, das sich auf kleinere, schwer zu findende oder mitunter unzugängliche Dienstleister konzentriert. Die zuständigen Behörden können daher mehrere Adressen mit einer einzigen Transaktion abrufen, was ihnen dabei hilft, mit großen Mengen komplexer Informationen effizienter umzugehen. SIRIUS project | Europol (europa.eu).

67 SIRIUS ist ein von der EU finanziertes Projekt für die Unterstützung des Zugangs von Strafverfolgungs- und Justizbehörden zu grenzüberschreitenden elektronischen Beweismitteln im Kontext strafrechtlicher Ermittlungen und Verfahren. Das Projekt SIRIUS wird gemeinsam von Europol und Eurojust in enger Partnerschaft mit dem EJN umgesetzt; es dient als zentraler Bezugspunkt in der EU für den Wissensaustausch zum grenzüberschreitenden Zugang zu elektronischen Beweismitteln. SIRIUS project | Europol (europa.eu).

68 Internetforum der Europäischen Union (EUIF) – Europäische Kommission (europa.eu).

Die Nutzung von Synergien mit dem Paket zu elektronischen Beweismitteln würde Kosten und Ressourcen sparen und zur vollständigen Umsetzung der Rechtsvorschriften über elektronische Beweismittel beitragen. So könnte beispielsweise die an Strafverfolgungsbehörden gerichtete Aufforderung, bei Stellen, die als SPoC für (grenzüberschreitende) Anträge auf Offenlegung von Daten fungieren, Kapazitäten zu schaffen oder auszubauen, auf Anträge auf nationaler Ebene ausgeweitet werden oder auf die Verpflichtung, Schulungsprogramme für Ermittler und Ersthelfer anzubieten. Ebenso könnten die derzeit im Zusammenhang mit der Umsetzung des Pakets zu elektronischen Beweismitteln laufenden Bemühungen um die Einrichtung einer **digitalen Plattform**, die den direkten Austausch zwischen zuständigen Behörden und Anbietern ermöglicht, für die Zwecke von Kommunikationsmetadaten, die im Einklang mit nationalen Rechtsvorschriften auf Vorrat gespeichert werden, repliziert werden.

Die Mitgliedstaaten könnten in Erwägung ziehen, **Vereinbarungen** als Instrumente zur Förderung der Zusammenarbeit und zur Entwicklung eines gemeinsamen Verständnisses zwischen Diensteanbietern, staatlichen Stellen und Strafverfolgungsbehörden einzuführen, um die Anwendung nationaler Rechtsvorschriften zu unterstützen. Positive Beispiele einiger Mitgliedstaaten könnten unter Einbeziehung aller relevanten Akteure (Unternehmen, Agenturen usw.) für ihre Strukturierung herangezogen werden, um sicherzustellen, dass alle relevanten Aspekte der Zusammenarbeit abgedeckt werden (Benennung von einzigen Anlaufstellen für Diensteanbieter und Strafverfolgungsbehörden, technische Erfordernisse, gemeinsame Festlegung der bereitzustellenden Datenkategorien, gemeinsame Verfahren, Ausarbeitung standardisierter Anfragemodelle, Maßnahmen zur Datensicherheit und Datenminimierung usw.).[69] Wie oben dargelegt, wären **standardisierte Protokolle** für die Erhebung von Daten von Anbietern (einschließlich OTT-Dienstleistern) und für Datenanfragen von zuständigen Behörden sowohl für Strafverfolgungsbehörden als auch für Diensteanbieter von Vorteil, die automatisierte Mechanismen für die Bereitstellung von Antworten einrichten könnten, um Kosten zu senken und Zeit zu sparen. Obwohl zwischen **nationalen** und **grenzüberschreitenden** Anfragen (im Rahmen für elektronische Beweismittel) hinsichtlich der Anforderungen Unterschiede bestehen, könnten die Arbeitsabläufe und die Kanäle, über die Daten angefordert werden, dennoch weiterentwickelt werden, da sich die Standardisierung auf das Format der angeforderten/erhaltenen Daten bezieht. Normungsgremien wie ETSI sind am besten in der Lage, solche standardisierten Formate zu entwickeln. Die Strafverfolgungsexperten der Mitgliedstaaten wurden in diese Prozesse bislang jedoch nur beschränkt einbezogen. Aus diesem Grund könnte die bestehende, von Europol und der Kommission geleitete **Europäische Arbeitsgruppe zur Normung im Bereich der inneren Sicherheit** die Beteiligung der Mitgliedstaaten an solchen Foren koordinieren und fördern. Die Arbeiten könnten auf bestehenden, vom ETSI entwickelten Normen aufbauen, die auf andere Datenkategorien ausgeweitet werden könnten.[70]

---

[69] Mit der Vereinbarung Irlands vom 6. April 2024 soll die Anwendung des Gesetzes über die Kommunikation (Vorratsdatenspeicherung) von 2011 (in der geänderten Fassung) unterstützt werden. Das Justizministerium hat einen unabhängigen Vorsitzenden ernannt, ein Mandat festgelegt und Vertreter von Strafverfolgungs- und Diensteanbietern eingeladen.

[70] TS 102 657: Verarbeitung auf Vorrat gespeicherter Daten; Übergabeschnittstelle für die Anfrage und Lieferung von auf Vorrat gespeicherten Daten und Kategorien von auf Vorrat gespeicherten Daten (Teilnehmer, Nutzung, Ausrüstung, Netzelement und Abrechnungsdaten); TS 103 120: Schnittstelle für Informationen über Anordnungen (Definition einer elektronischen Schnittstelle zwischen zwei Systemen für den sicheren Austausch von Informationen im Zusammenhang mit der Einleitung und Verwaltung rechtmäßiger erforderlicher Maßnahmen; sie wird üblicherweise für die rechtmäßige Überwachung genutzt, kann jedoch auch für auf Vorrat gespeicherte Daten verwendet werden; sie kommt üblicherweise zwischen einem Diensteanbieter auf der einen Seite und einer staatlichen Stelle oder einer Strafverfolgungsbehörde, die berechtigt ist, rechtmäßige Maßnahmen zu verlangen, auf der anderen Seite zur Anwendung); TS 103 705: Datenstrukturen für rechtmäßige Offenlegungen (in Entwicklung; nur Datenstrukturen, keine Übergabeschnittstelle, keine vordefinierte Baumstruktur, vom Dienstleister festgelegte Arten und Informationen).

Wichtigste Maßnahme: Die Experten der Hochrangigen Gruppe rufen dazu auf, dass die Zusammenarbeit und die Entwicklung eines gemeinsamen Verständnisses zwischen Dienstleistern, staatlichen Stellen und Strafverfolgungsbehörden gefördert wird.

Akteure: Europäische Kommission, Mitgliedstaaten, Europol (SIRIUS), Eurojust, EU-Internetforum

Zeitrahmen: noch festzulegen

- Die Experten der Hochrangigen Gruppe fordern die **Europäische Kommission**, **Europol** und die **Mitgliedstaaten** auf, zu prüfen, wie die Zusammenarbeit zwischen Strafverfolgungsbehörden und Privatunternehmen gefördert und verbessert werden kann, um einen ständigen Dialog und ein gegenseitiges Verständnis der operativen, technischen und geschäftlichen Bedürfnisse zu fördern. Im Zusammenhang mit der in Abschnitt II genannten Folgenabschätzung fordern die Experten der Hochrangigen Gruppe die Kommission ferner auf, die Entwicklung spezifischer Verpflichtungen in Bezug auf die Transparenz der Datenerhebung und permanente Kooperationsstrukturen in Erwägung zu ziehen.

- Die Experten der Hochrangigen Gruppe ersuchen die **Europäische Kommission**, **Europol** und **Eurojust**, Plattformen für den Austausch zwischen Strafverfolgungsbehörden und der Justiz einerseits und Kommunikationsanbietern andererseits einzurichten oder bestehende Plattformen zu fördern und einen von SIRIUS zu verwaltenden Katalog der Daten zu erstellen, die von Kommunikationsanbietern und Datenbearbeitern im Rahmen ihrer Geschäftstätigkeit generiert und gespeichert werden.

- Die Experten der Hochrangigen Gruppe ersuchen die **Mitgliedstaaten**, die Möglichkeit zu prüfen, Kooperationsabkommen und/oder Vereinbarungen zu schließen, die Dienstleister, staatliche Stellen und Strafverfolgungsbehörden zusammenbringen, um die Anwendung nationaler Rechtsvorschriften durch die gemeinsame Festlegung von Grundsätzen und Standardpraktiken zu unterstützen.

- Die Experten der Hochrangigen Gruppe fordern **Europol** und die **Europäische Kommission** auf, die bestehende Arbeitsgruppe zur Normung im Bereich der inneren Sicherheit zu nutzen, um die Mitgliedstaaten stärker an Normungsforen zu beteiligen und so einen Beitrag zur Schaffung einschlägiger Normen und zur gemeinsamen Ausarbeitung von Protokollen zu leisten, in denen Verfahren für die Zusammenarbeit mit Diensteanbietern festgelegt sind.

- Die Experten der Hochrangigen Gruppe ersuchen die **Europäische Kommission**, **Europol**, **Eurojust/EJN** und die **Mitgliedstaaten**, Synergien mit Instrumenten wie dem Paket zu elektronischen Beweismitteln zu nutzen, um einschlägige Werkzeuge aufzubauen oder zu erwerben, beispielsweise indem in Entwicklung befindliche digitale Plattformen als Portale für die Einreichung von Anfragen nutzbar gemacht werden.

II. Harmonisierung der Mindestvorschriften für die Vorratsspeicherung von Metadaten durch Kommunikationsanbieter und den Zugang der zuständigen Behörden

Die Experten stimmen weitgehend darin überein, dass ein harmonisierter EU-Rahmen zur Regelung der Vorratsspeicherung von Metadaten zu Strafverfolgungszwecken erforderlich ist. Ein solcher Rahmen würde standardisierte Lösungen sowie klare und durchsetzbare Verpflichtungen für Kommunikationsanbieter und Datenbearbeiter in Bezug auf den Zeitpunkt und die Art der Vorratsdatenspeicherung und die Umstände, unter denen Zugang zu diesen Daten gewährt wird, bieten. Dieser Rahmen würde klare Regeln für die Vorratsspeicherung und den Zugang festlegen und somit – unter Berücksichtigung der Anhaltspunkte der anwendbaren Rechtsprechung – klare Garantien für Grundrechte und wesentliche Interessen bieten sowie Klarheit über die Vorschriften für Kommunikationsanbieter für die Vorratsspeicherung und Weitergabe von Daten zu Strafverfolgungszwecken schaffen. Darüber hinaus würde ein solcher Rahmen die vollständige Umsetzung des Pakets zu elektronischen Beweismitteln unterstützen, indem er sicherstellt, dass Daten auf Vorrat gespeichert werden.

Empfehlungen Cluster 6

Um sicherzustellen, dass digitale Beweismittel, die für die Ermittlung und Verfolgung von Straftaten erforderlich sind, zur Verfügung stehen und dass die Vorschriften für die Vorratsdatenspeicherung und die Garantien in Bezug auf die Grundrechte, insbesondere den Schutz der Privatsphäre und den Datenschutz, die Meinungsfreiheit und die Rechte der Beschuldigten, einschließlich des Rechts auf ein ordnungsgemäßes Verfahren, zwischen den Mitgliedstaaten nicht fragmentiert sind, und um Rechtssicherheit sowohl für die zuständigen Behörden als auch für die Anbieter elektronischer und anderer Kommunikationsdienste zu gewährleisten, empfehlen die Experten Folgendes:

1. *Festlegung von Kategorien von Metadaten basierend auf dem Zweck ihrer Nutzung (Identifizierung, Lokalisierung, Feststellung oder Bewertung der Online-Tätigkeit einer Person von Interesse) [Empfehlung 28], um sicherzustellen, dass Anbieter elektronischer Kommunikationsdienste und andere Anbieter von Kommunikationsdiensten zumindest die Daten auf Vorrat speichern, die zur Identifizierung einer Person ausreichen [Empfehlung 27 Ziffer v];*
2. *Festlegung von Mindestspeicherfristen für diese Daten;*
3. *Festlegung von Bedingungen für den Zugang zu auf Vorrat gespeicherten Daten [Empfehlung 27 Ziffer iv], die sich je nach Datenkategorie, Kategorie der Straftat (z. B. Straftaten, die nur im Internet stattfinden) oder der Gefahr für die Opfer unterscheiden [Empfehlung 29];*
4. *Gestaltung von Rechts- und Verwaltungsvorschriften und technischen Bestimmungen, die die uneingeschränkte Achtung der Grundrechte und Grundfreiheiten betroffener Personen gewährleisten und diese Rechte nur einschränken, wenn dies notwendig und verhältnismäßig ist [Empfehlung 27 Ziffer vi];*
5. *Gewährleistung, dass für herkömmliche Kommunikationsanbieter, OTT-Diensteanbieter und andere bestehende oder künftige Anbieter, die Daten erzeugen und verarbeiten, dieselben Vorschriften, Verpflichtungen und Garantien gelten [Empfehlung 27 Ziffern i und ii];*
6. *Gewährleistung, dass für kommerzielle und geschäftliche Zwecke auf Vorrat gespeicherte Nutzerdaten für die Strafverfolgung – unter Beachtung einschlägiger Garantien – wirksam zugänglich sind (Empfehlung 31) und dass die rechtmäßig von Anbietern empfangenen Daten für die zuständigen Behörden lesbar sind [Empfehlung 27 Ziffer iii];*
7. *Gewährleistung, dass die Mitgliedstaaten Sanktionen gegen Anbieter elektronischer Kommunikationsdienste und anderer Kommunikationsdienste, die bei der Vorratsspeicherung und Bereitstellung von Daten nicht kooperieren, durchsetzen können, z. B. durch die Umsetzung von Verwaltungssanktionen oder Beschränkungen ihrer Fähigkeit, auf dem EU-Markt tätig zu sein [Empfehlung 30].*

Wenn es um die **Vorratsspeicherung von Metadaten** geht, sollte zwischen Datenkategorien unterschieden werden, wobei die Daten, die zur Identifizierung einer Person von Interesse erforderlich sind (Teilnehmerdaten[71] und IP-Adressen der Kommunikationsquelle[72]), von Verkehrs-[73] und Standortdaten[74] unterschieden und für jede Kategorie unterschiedliche Speicherfristen und Garantien vorgesehen werden sollten. Auch bei der Phase des Datenzugangs besteht das Ziel darin, ein ausgewogenes Verhältnis zwischen der Schwere der zu untersuchenden Straftat und dem Grad des Eingriffs in die Privatsphäre der zu ergreifenden Maßnahmen zu gewährleisten. Im Einklang mit der jüngsten Rechtsprechung[75] könnten Mindestanforderungen für die allgemeine Vorratsspeicherung von Daten geprüft werden, die ausreichen, um sicherzustellen, dass jeder Nutzer eindeutig identifiziert werden kann. Für Verkehrs- und Standortdaten müssen zusätzliche und strengere Kriterien geprüft werden.

Um einen solchen Rahmen so zukunftssicher und **technologieneutral** wie möglich zu gestalten, sollte die Kategorisierung der auf Vorrat zu speichernden Daten auf der Grundlage eines zukunftsorientierten Ansatzes formuliert werden, einschließlich generischer Datensätze, die beispielsweise auf den Funktionen der Daten beruhen (Daten, die eine eindeutige Identifizierung einer Kommunikationsquelle oder eines Zielorts ermöglichen, Daten, die die Identifizierung des Standorts einer Kommunikationsquelle ermöglichen usw.), in Verbindung mit einer Liste bestehender Datenarten (IP-Adresse, IMEI usw.). Dieser Rahmen würde es ermöglichen, den Grad des Eingriffs jeder Datenkategorie – und damit die erforderlichen Garantien – angemessen zu bewerten.

---

71 Mit einigen Ausnahmen für kleine Anbieter werden Nutzerdaten in der Regel bereits für geschäftliche Zwecke auf Vorrat gespeichert. In diesem Fall und unbeschadet verhältnismäßiger Garantien sollten diese Daten den Strafverfolgungsbehörden zur Verfügung gestellt werden.

72 Die Rechtsprechung erlaubt die allgemeine und unterschiedslose Vorratsspeicherung von Daten, die sich auf die Identität der Nutzer elektronischer Kommunikation beziehen, zum Schutz des öffentlichen Interesses und die allgemeine und undifferenzierte Vorratsspeicherung von IP-Adressen zum Schutz der nationalen Sicherheit, zur Bekämpfung schwerer Kriminalität und zur Verhinderung schwerwiegender Gefahren für die öffentliche Sicherheit (Urteil vom 6. Oktober 2020, *La Quadrature du Net u. a.*, verbundene Rechtssachen C-511/18, C-512/18 und C-520/18, und Urteil vom 30. April 2024, *La Quadrature du Net u. a.*, C-470/21 (Hadopi), ECLI:EU:C:2024:370).

73 „Verkehrsdaten“ bezeichnen Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden (Artikel 2 der Richtlinie 2002/58/EG).

74 „Standortdaten“ bezeichnet Daten, die in einem elektronischen Kommunikationsnetz verarbeitet werden und die den geografischen Standort des Endgeräts eines Nutzers eines öffentlich zugänglichen elektronischen Kommunikationsdienstes angeben (Artikel 2 der Richtlinie 2002/58/EG); Standortdaten des Geräts des Nutzers sollten als andere Standortdaten als Verkehrsdaten im Sinne von Artikel 9 der Richtlinie 2002/58/EG betrachtet werden.

75 Urteil in der Rechtssache Hadopi.

Wie von den Experten und in der jüngsten Rechtsprechung[76] dargelegt, würde die Kombination von Verpflichtungen zur Vorratsdatenspeicherung **mit strengen Anforderungen in Bezug auf den Zugang zu Daten** zusätzliche Garantien für die Grundrechte, insbesondere den Schutz der Privatsphäre und des Datenschutzes, bieten. So erörterten die Experten der Hochrangigen Gruppe die Notwendigkeit, Zugangsregeln zu konzipieren, die sich z. B. je nach Art und Schwere der Straftat, dem Ausmaß der Gefahr für die Opfer durch die Straftat, dem Zweck des Zugriffs und den für den Zugang zu den Daten zuständigen Behörden unterscheiden. Ein solcher Ansatz wurde auch als nützlich erachtet, um spezifische Vorschriften für die Ermittlung und Verfolgung von Straftaten festzulegen, bei denen sich die Ermittlung besonders schwierig gestaltet, z. B. bei Straftaten, die ausschließlich im Internet stattfinden, bei denen digitale Beweismittel die einzigen verfügbaren Beweismittel sind.

Die anfragenden Behörden müssen in der Lage sein, die Daten zu lesen, auf die sie rechtmäßig zugegriffen haben. Daher müssen die Daten von den Anbietern in einem **verständlichen Format** bereitgestellt werden. Häufig bieten die Anbieter Ende-zu-Ende-verschlüsselte Dienste[77] für Verkehrs- und Teilnehmerdaten an und entschlüsseln diese Daten nicht, wenn sie sie an die zuständigen Behörden weitergeben. Die Experten der Hochrangigen Gruppe waren der Ansicht, dass eine Regelung zur Vorratsdatenspeicherung die Verpflichtung für Diensteanbieter umfassen sollte, Daten in unverschlüsselter Form bereitzustellen, wobei eine solide Cybersicherheit und die uneingeschränkte Einhaltung der Rechtsvorschriften zum Datenschutz und zum Schutz der Privatsphäre sichergestellt werden sollten, ohne die Verschlüsselung zu untergraben.

Mindestanforderungen für die Vorratsspeicherung bestimmter Datenkategorien müssten für alle (gegenwärtigen oder künftigen) Wirtschaftsteilnehmer, die elektronische Kommunikationsdienste bereitstellen, gelten (und durchsetzbar sein), damit der Rahmen für die Vorratsdatenspeicherung sowohl jetzt als auch in Zukunft wirksam ist. Um künftigen technologischen Entwicklungen Rechnung zu tragen, sollten Telekommunikationsanbieter, OTT-Anbieter und andere Betreiber, die Daten erheben, die mit einer bestimmten natürlichen oder juristischen Person verbunden sind, die ihren Dienst nutzt, wie z. B. Automobilhersteller oder KI-Systeme mit Großen Sprachmodellen, zu den Einrichtungen gehören, die zur Vorratsdatenspeicherung verpflichtet sind. Diese Verpflichtungen müssen durchsetzbar sein, und Anbieter müssen rechenschaftspflichtig sein; dies könnte mit einer Vielzahl von Lösungen erreicht werden, zu denen Markthindernisse (Betriebslizenzen) und Verwaltungssanktionen gehören könnten.

---

[76] In der aktuellen Rechtssache Hadopi hat der Gerichtshof gefolgert, dass die Privatsphäre gewahrt werden kann, indem die Vorratsdatenspeicherung mit dem Zugang zu Daten kombiniert wird.

[77] Siehe Abschnitt I.

Ein System durchsetzbarer Sanktionen für nicht kooperative Anbieter und jene Anbieter, die illegale Dienste anbieten, ist ein grundlegender Bestandteil eines jeden künftigen EU-Rahmens. Angesichts der Wechselwirkung zwischen diesem spezifischen Aspekt und den möglichen Lösungen, die im Zusammenhang mit der rechtmäßigen Überwachung erörtert wurden, sollen die Sanktionen in der nächsten Sitzung zur rechtmäßigen Überwachung erörtert werden.

Die meisten Anbieter würden den Verpflichtungen zur Vorratsspeicherung und Bereitstellung von Daten zwar in erster Linie durch eine technische Umsetzung nachkommen (um die für geschäftliche Zwecke erhobenen oder verarbeiteten Daten den zuständigen Behörden zugänglich zu machen), jedoch würde dies den Anbietern, die ihre Nutzer derzeit nicht erfassen, weil für sie keine geschäftliche Erfordernis dazu besteht (z. B. OTT-Anbieter), standardmäßig Verfahren zur Registrierung von Nutzern auferlegen. Im Zuge der Beratungen über die Notwendigkeit, die **Transparenz und Rechenschaftspflicht** der Anbieter in Bezug auf die von ihnen erhobenen und gespeicherten Daten und die Speicherzeiträume zu erhöhen, bewerteten die Experten der Hochrangigen Gruppe derartige Verpflichtungen als positiv. Bestehende Verpflichtungen zur Kategorisierung im Rahmen anderer Instrumente (DSGVO) können Einblicke in die von diesen Anbietern verarbeiteten Daten geben.

Wichtigste Maßnahme: Die Experten der hochrangigen Gruppe fordern einen neuen EU-Rahmen für die Vorratsdatenspeicherung und den Zugang zu Daten

Akteure: Europäische Kommission, Rat, Europäisches Parlament

Zeitrahmen: 2025-2026

- Die Experten der Hochrangigen Gruppe fordern die **Europäische Kommission** nachdrücklich auf, das Verfahren für eine Folgenabschätzung einzuleiten, um die verschiedenen Optionen für den Ausbau der Kapazitäten der zuständigen Behörden zur wirksamen Ermittlung und Verfolgung von Straftaten durch den Zugriff auf historische Metadaten, die von Kommunikationsanbietern erzeugt und gespeichert werden, zu bewerten. Die Folgenabschätzung sollte auch die Subsidiaritätsanforderungen, die Auswirkungen auf die Grundrechte und den Binnenmarkt sowie das Verhältnis zu anderen bestehenden Rechtsinstrumenten umfassen. Sie sollte als Grundlage für einen Gesetzgebungsvorschlag dienen, der im Wege des ordentlichen Gesetzgebungsverfahrens angenommen werden soll.

Kapitel III: Rechtmäßige Überwachung

WAS SIND DIE ZUGRUNDE LIEGENDEN PROBLEME?

„Rechtmäßige Überwachung des Kommunikationsverkehrs“ bezieht sich auf einen Dritten – eine Behörde oder eine andere gesetzlich oder auf der Grundlage eines Gesetzes ermächtigte Stelle –, der verdeckten Zugang zu Daten aus einer verdächtigen Kommunikation erhält. Während die rechtmäßige Überwachung in der Vergangenheit vor allem für Telefonanrufe relevant war, hat der zunehmende Wechsel von herkömmlichen Sprachanrufen zu Nachrichtenübermittlungsdiensten und anderen Formen der elektronischen Kommunikation neue Herausforderungen mit sich gebracht.

Diesem Wechsel wird im EKEK Rechnung getragen, mit dem der Teil des Rechtsrahmens, der für die herkömmliche Telekommunikation gilt, auf Unternehmen ausgeweitet wird, die internetgestützte Dienste über eine Telekommunikationsinfrastruktur anbieten, die sie nicht besitzen oder verwalten, einschließlich nummernunabhängiger interpersoneller Kommunikationsdienste (Number-Independent Interpersonal Communications Services, NI-ICS). In der Praxis bedeutet dies, dass NI-ICS-Anbieter potenziell demselben Rechtsrahmen unterliegen können, der für herkömmliche Telekommunikationsbetreiber gilt, auch im Hinblick auf die rechtmäßige Überwachung. Die Mitgliedstaaten können verlangen, dass Betreiber die rechtmäßige Überwachung der elektronischen Kommunikation durch die zuständigen nationalen Behörden im Einklang mit der Verordnung (EU) 2016/679 und der Richtlinie 2002/58/EG, die die Bestimmungen über die Vertraulichkeit der Kommunikation und die Ausnahmen davon enthalten, gestatten. Im Rahmen der Allgemeingenehmigung nach dem EKEK können die Mitgliedstaaten diese Anforderung bekräftigen.

Der rechtmäßige Zugang muss nicht auf Netzebene erfolgen – wie es bei herkömmlichen Telefonanrufen und Textnachrichten (SMS) üblich war –, sondern kann auch auf dem Gerät des Nutzers (vor der Übermittlung der Informationen) oder auf der Ebene des Bestimmungsorts (z. B. wenn Nachrichten in der Cloud gespeichert werden) erfolgen. Im Zusammenhang mit diesem Bericht deckt die rechtmäßige Überwachung diese drei Anwendungsfälle ab und betrifft Daten, auf die in Echtzeit oder mit geringer Verzögerung zugegriffen wird.

Es ist wichtig, Überwachungstechnologien, **die von einem Kommunikationsbetreiber umgesetzt werden**, von Technologien zu unterschieden, die von Strafverfolgungsbehörden autonom eingesetzt werden können. Nur die erstgenannten Technologien [im Folgenden „**betreiberbasierte Überwachung**“], bei denen der Kommunikationsbetreiber technische Systeme installieren muss, um die überwachten Daten erheben und an die anfragenden Behörden übermitteln zu können, sind in der Definition des Begriffs der rechtmäßigen Überwachung in den ETSI-Normen enthalten. Die letztgenannten Technologien [im Folgenden „**taktische Überwachung**“] beziehen sich auf Werkzeuge, für die keine dauerhafte physische Installation in einem Netz erforderlich ist, wie IMSI-Catcher[78] oder Software zur Überwachung von Daten auf Smartphones. Mit diesen Anwendungsfällen, die nicht unter dieselbe rechtliche Regelung fallen, gehen Eingriffe unterschiedlichen Schweregrads und Herausforderungen verschiedener Art einher.

Auch wenn die rechtmäßige Überwachung der herkömmlichen Telekommunikation in vielen Ermittlungen nach wie vor ein wesentliches Instrument ist[79], hat die Wirksamkeit dieser Maßnahme drastisch abgenommen, da die Telekommunikationsdienste nun größtenteils von anderen Akteuren erbracht werden: verschiedenen Quellen zufolge werden derzeit rund 97 % aller mobilen Nachrichten über Nachrichtenanwendungen wie WhatsApp, Facebook Messenger und WeChat gesendet, während herkömmliche SMS- und MMS-Nachrichten nur etwa 3 % der Nachrichten ausmachen. Darüber hinaus wurden 2023 mehr als 90 % der OTT-Kommunikation über Ende-zu-Ende-verschlüsselte Dienste abgewickelt.[80]

Die Experten sind sich über folgende Trends einig: zuerst begannen Kriminelle, von herkömmlichen Kommunikationsbetreibern zu etablierten OTT-Diensten überzugehen; anschließend begannen die wichtigsten kriminellen Akteure schrittweise mit der Nutzung spezieller krimineller Netze (wie Encrochat und Sky ECC); seit 2020 haben viele von ihnen – nach der Zerschlagung großer verschlüsselter krimineller Kommunikationsnetze – beschlossen, zu gewöhnlichen Ende-zu-Ende-verschlüsselten OTT zurückzukehren.

---

78 IMSI-Catcher sind Überwachungsgeräte, die Mobilfunkmasten zur Überwachung von Mobiltelefonsignalen nachbilden und Nummern der internationalen Mobilteilnehmerkennung (IMSI) sowie Kommunikationsdaten erfassen.

79 Die Zahl der Anträge auf rechtmäßige Überwachung in Europa hat in den letzten Jahren erheblich und stetig zugenommen. In Ländern wie Deutschland, Frankreich und dem Vereinigten Königreich hat die Anzahl solcher Anträge besonders stark zugenommen, wobei allein in Deutschland ein deutlicher Anstieg zu verzeichnen ist. So meldete die Deutsche Telekom im Jahr 2023 mehr als 31 000 Anträge auf Überwachung, gegenüber rund 26 000 im Jahr 2022 (https://www.telekom.com/en/company/data-privacy-and-security/news/germany-363566).

80 Quellen: Comparitech und Statista.

In diesem Zusammenhang stehen Kommunikationsanbieter bei der Beantwortung von Anträge auf rechtmäßige Überwachung vor dermaßen großen Herausforderungen, dass sie die grundlegenden Anforderungen an die rechtmäßige Überwachung im Sinne des Budapester Übereinkommens über Computerkriminalität[81] kaum erfüllen können. Folglich beschränkt sich der operative Wert der herkömmlichen rechtmäßigen Überwachung oft auf taktische Erkenntnisse, wie etwa die Feststellung, ob ein Gerät ein- oder ausgeschaltet ist, wo sich eine Mobilfunkantenne befindet oder wer mit wem verbunden ist; eine rechtmäßige Überwachung von Inhaltsdaten, die über OTT-Diensteanbieter übermittelt werden, ist jedoch in den meisten Fällen nicht möglich.

Infolgedessen sind Strafverfolgungsbehörden häufig nicht in der Lage, auf den Inhalt gezielter Kommunikation[82] zuzugreifen und zu lesen oder gar nachzuvollziehen, wer einen bestimmten Internetdienst in Echtzeit nutzt, und relevante Informationen zu filtern. Dieser erhebliche Verlust des Zugangs zu Daten auf dem Übermittlungsweg wirkt sich in mehrfacher Hinsicht auf Ermittlungen aus:

- die Verhütung von Straftaten, die Erfassung krimineller Organisationen und die Zuordnung von online oder offline begangenen kriminellen Aktivitäten sind mit großen Schwierigkeiten verbunden;

- die Strafverfolgungsbehörden setzen vermehrt auf sogenannte Spezialtechniken[83], die oft stärker in die Privatsphäre eingreifen und weitaus gefährlicher für Beamte sind, z. B. wenn die Justizbehörde die Installation von Kameras oder Mikrofonen in der Nähe der Zielperson vorschreibt;

- die Strafverfolgungsbehörden nutzen verstärkt weniger zielgerichtete Ermittlungstechniken: ohne Zugang zu Kommunikationsinhalten oder genauen Geolokalisierungsdaten müssen Ermittler häufig **alle** Personen untersuchen, die mit einer Person in Verbindung stehen, die einer Straftat verdächtigt wird.

Vor diesem Hintergrund wiesen die Experten der Hochrangigen Gruppe auf vier Hauptkategorien von Herausforderungen hin.

---

81 https://rm.coe.int/1680081561 [Artikel 20 und 21].

82 Ein Experte wies darauf hin, dass Inhaltsdaten in 99 % der Fälle nicht über herkömmliche rechtmäßige Überwachung verfügbar seien.

83 Die sogenannten Spezialtechniken umfassen eine Reihe taktischer Mittel, um über Kameras, Mikrofone, Fernzugriff auf Geräte, GPS-Tracker usw. Informationen über das Ziel zu erhalten.

I. Rechtmäßige Überwachung des Kommunikationsverkehrs über nicht herkömmliche Kommunikationsanbieter

Die meisten Mitgliedstaaten haben in irgendeiner Form Vorschriften für die rechtmäßige Überwachung eingeführt, mit denen die Anbieter von Kommunikationsdiensten verpflichtet werden, Überwachungskapazitäten einzusetzen.[84] Während die Bedingungen für den Erlass von Anordnungen zur rechtmäßigen Überwachung von Land zu Land sehr unterschiedlich sind, gelten für Betreiber häufig ähnliche Verpflichtungen[85]: sie müssen in der Lage sein, die gesamte einschlägige Kommunikation einer bestimmten Zielperson auf dem nationalen Boden lückenlos zu überwachen, und sie müssen die Infrastruktur bereitstellen, die für die Erhebung und Übermittlung der überwachten Daten an die Strafverfolgungsbehörden erforderlich ist.

In den Fällen, in denen die Betreiber von Telekommunikationsnetzen (Kommunikationsanbieter, die Eigentümer des Netzes sind und Zugang zu dessen Infrastruktur haben) auch die Kommunikationsdienste (Telefonanrufe, SMS usw.) erbringen, sind diese meist in der Lage, den Verpflichtungen zur rechtmäßigen Überwachung nachzukommen.[86] In den meisten Fällen bauen sie auf ETSI-Normen auf und stützen sich auf spezialisierte Technologieanbieter, um ihre eigenen Zwänge wie Kosteneffizienz, minimale Auswirkungen auf die Netzinfrastruktur, Interoperabilität, Zuverlässigkeit und Sicherheit zu bewältigen.

Bei OTT-Diensten ist die Situation komplexer: die rechtmäßige Überwachung kann entweder von Telekommunikationsnetzbetreibern oder von dem OTT-Anbieter, der den Dienst erbringt, durchgeführt werden.

Erfolgt die Überwachung der Kommunikation über OTT-Dienste auf der Ebene des Telekommunikationsnetzes, so ist ihre Wirksamkeit oft begrenzt. Erstens ist der Telekommunikationsnetzbetreiber möglicherweise nicht in der Lage, die Kommunikation der Zielperson zu identifizieren (z. B. bei der Verbindung über ein öffentliches WLAN). Darüber hinaus verwenden OTT-Dienste oft proprietäre Protokolle, die über Systeme zur rechtmäßigen Überwachung entschlüsselt werden müssen, wodurch sich der Prozess teurer, zeitaufwändiger und komplexer gestaltet. Schließlich gestaltet sich der Zugang zu Inhaltsdaten äußerst problematisch und wird der Zugang zu Metadaten zunehmend verhindert, wenn OTT-Anbieter auf Ende-zu-Ende-Verschlüsselung zurückgreifen, da die überwiegende Mehrheit der Länder der Ansicht ist, dass die Telekommunikationsnetzbetreiber im Einklang mit dem Budapester Übereinkommen nicht mehr verpflichtet sind, Informationen unverschlüsselt bereitzustellen, wenn die Verschlüsselung von einem Dritten umgesetzt wird.

---

84 Siehe „Lawful interception – A market access barriers in the European Union“, Vadim Doronin in Computer Law & Security Review 51 (2023) 105867.

85 Bei den Verpflichtungen im Zusammenhang mit Inhaltsdaten oder Nichtinhaltsdaten bestehen allerdings Unterschiede.

86 Merkmale wie Home Routing, Slicing oder erweiterte Kommunikationsdienste können es Betreibern von Telekommunikationsnetzen allerdings erschweren, ihren Verpflichtungen nachzukommen (siehe Abschnitt über technologische Herausforderungen).

Die Datenschutzrichtlinie für elektronische Kommunikation greift in Form eines Verweises in Artikel 5 Absatz 1 auf die Definition des EKEK für „elektronische Kommunikationsdienste“ zurück, die seit 2018 NI-ICS umfasst. Dies wiederum bedeutet, dass sich die Mitgliedstaaten bei der rechtmäßigen Überwachung direkt auf OTT-Anbieter verlassen können, da das Konzept der elektronischen Kommunikationsdienste mittlerweile weiter gefasst ist als zum Zeitpunkt der Annahme der Datenschutzrichtlinie für elektronische Kommunikation.[87] Bislang haben die Mitgliedstaaten von dieser Möglichkeit in unterschiedlichem Maße Gebrauch gemacht, wobei einige ähnliche Verpflichtungen für alle Arten von Anbietern elektronischer Kommunikation, einschließlich OTT-Anbietern, eingeführt haben, während andere OTT-Anbieter ausschließen.[88] **Ungeachtet bestehender Verpflichtungen haben die herkömmlichen OTT-Dienste in der Praxis keine technischen Mechanismen entwickelt, um auf Anträge auf rechtmäßige Überwachung der Behörden der EU-Mitgliedstaaten zu reagieren**, vor allem aus rechtlichen Gründen.[89]

Im Gegensatz dazu hat das Vereinigte Königreich im Rahmen des Investigatory Powers Act einen Rahmen für die rechtmäßige Überwachung der OTT-Kommunikation geschaffen, der dank der Annahme des Abkommens zwischen dem Vereinigten Königreich und den USA über den Zugang zu Daten auch für OTT-Dienste mit Sitz in den USA gilt. Den zuständigen Behörden des Vereinigten Königreichs zufolge macht dies bei der Kriminalprävention und strafrechtlichen Ermittlungen einen bedeutenden Unterschied.

Schließlich stellten die Experten der nationalen Behörden klar, dass die taktische Überwachung, die darauf beruht, Schwachstellen auszunutzen, weder eine wirksame noch eine wünschenswerte Alternative zu durchsetzbaren Vorschriften zur rechtmäßigen Überwachung für OTT-Anbieter darstellt und auf bestimmte Fälle beschränkt werden sollte, wobei starke Garantien bestehen sollten, die in den nationalen Rechtsvorschriften festgelegt sind, um die Verhältnismäßigkeit zu gewährleisten.

---

87 Die Beratungen über den genauen Anwendungsbereich sind allerdings noch nicht abgeschlossen und die Auslegungen unterscheiden sich von Mitgliedstaat zu Mitgliedstaat.

88 Siehe „Lawful interception – A market access barriers in the European Union“, Vadim Doronin in Computer Law & Security Review 51 (2023) 105867.

89 Dies wird nicht durch Statistiken untermauert, da die nationalen Behörden Anträge auf rechtmäßige Überwachung äußerst selten an OTT richten – ihnen ist bewusst, dass dies wahrscheinlich nicht zu Ergebnissen führen wird.

II. Grenzüberschreitende Anträge

Grenzüberschreitende Anträge auf rechtmäßige Überwachung, die an Anbieter von OTT-Diensten und – in geringerem Maße – an Anbieter herkömmlicher Kommunikationsdienste gerichtet werden, stellen Strafverfolgungsbehörden in mehrerlei Hinsicht vor Herausforderungen.

Was die Anbieter herkömmlicher Kommunikationsdienste betrifft, so sind die Behörden in erster Linie mit organisatorischen Herausforderungen konfrontiert. Erstens sind Instrumente der internationalen Zusammenarbeit, insbesondere Rechtshilfemechanismen, für dringende Überwachungsmaßnahmen, die innerhalb von Stunden – nicht Tagen oder Wochen – genehmigt und umgesetzt werden müssen, womöglich nicht praktikabel.[90] Dies ist darauf zurückzuführen, dass viele Schritte unternommen werden müssen, um sicherzustellen, dass die Rechtsvorschriften der beiden Mitgliedstaaten eingehalten werden, die einen Antrag ausstellen bzw. erhalten. Insgesamt wird davon ausgegangen, dass das Rechtshilfeverfahren bei der rechtmäßigen Überwachung ineffizient und aufwändig ist. Die herkömmlichen Rechtshilfeverfahren wurden in der EU durch die im Jahr 2017 in Kraft getretene Europäische Ermittlungsanordnung (EEA) ersetzt[91], mit der strenge Fristen für die Beweiserhebung festgelegt[92], die Gründe für die Ablehnung solcher Ersuchen beschränkt und ein einheitliches Standardformblatt eingeführt wurden, mit dem die Behörden bei der Beweiserhebung Hilfe anfordern können. Wird bei der Durchführung der Überwachung von dem Mitgliedstaat, in dem sich die Zielperson der Überwachung aufhält, keine technische Hilfe benötigt, so wird dieser Mitgliedstaat außerdem mit einem Standardformblatt über die Überwachung unterrichtet und erhält die Möglichkeit, innerhalb von 96 Stunden Einwände dagegen zu erheben. In der wegweisenden Rechtssache C-670/22 hat der EuGH den Begriff der „Überwachung des Telekommunikationsverkehrs“ weit ausgelegt und festgestellt, dass die Infiltration von Endgeräten zur Abschöpfung von Verkehrs-, Standort- und Kommunikationsdaten eines internetbasierten Kommunikationsdienstes eine „Überwachung des Telekommunikationsverkehrs“ darstellt. Die Experten sind jedoch der Auffassung, dass die durch die EEA bewirkten erheblichen Verbesserungen nicht ausreichen, um einen raschen und harmonisierten grenzüberschreitenden Zugang zu Daten bei der Übertragung zu ermöglichen.

Darüber hinaus berichteten die Behörden der Mitgliedstaaten, dass die bestehende technische Architektur häufig dem Zweck nicht gerecht wird, rechtmäßige Überwachungen in einem Mitgliedstaat durchzuführen und die Daten echtzeitnah an einen anderen Mitgliedstaat zu übermitteln. Sind entsprechende Organisationsprotokolle vorhanden, so ist in einigen Fällen das zu übertragende Datenvolumen mit der über gesicherte Kommunikationskanäle verfügbaren Bandbreite schlicht unvereinbar.

---

[90] Die Experten nannten Fälle, in denen sich die Angelegenheit erledigt hatte bevor die rechtmäßige Überwachung wirksam durchgeführt werden konnte oder in denen der Rückstand bei der Rechtshilfe mehr als acht Monate betrug.

[91] Mit Ausnahme von DK und IE, in denen die EEA keine Anwendung findet.

[92] 30 Tage für die Anerkennung einer EEA und 90 zusätzliche Tage für ihre Vollstreckung.

Die Überwachung von OTT-Kommunikation wirft im Vergleich zur Überwachung von Telefongesprächen komplexe Fragen der Zuständigkeit auf, wenn Anbieter ihre Dienste in einem genau abgegrenzten Gebiet anbieten. Herkömmliche Telekommunikationsdienste sind an eine bestimmte physische Netzinfrastruktur gebunden, wodurch sichergestellt wird, dass der Diensteanbieter über Einrichtungen und eine Niederlassung in dem Land verfügt, in dem die Überwachung erfolgt. Diese lokale Struktur verringert das Risiko von Rechtskollisionen innerhalb der EU und erleichtert die Einhaltung der Vorschriften.

Im Falle von OTT-Diensten können sich die ersuchende Behörde, die Zielperson der Überwachung, die physische Umsetzung und der Ort der Niederlassung des Unternehmens hingegen auf mehrere unterschiedliche Hoheitsgebiete erstrecken. Das Zusammenspiel zwischen den Rechtsrahmen dieser Rechtsordnungen könnte zu Rechtskollisionen führen.[93]

Für die Experten der Polizei- und Justizbehörden steht außer Frage, dass es nicht praktikabel ist, Anträge auf rechtmäßige Überwachung über internationale Instrumente abzuwickeln. Umgehen Strafverfolgungsbehörden das Rechtshilfeverfahren und richten sie Anordnungen stattdessen nach ihrem innerstaatlichen Recht direkt an Diensteanbieter, so können OTT-Anbieter wie Microsoft, META oder Google mit widersprüchlichen rechtlichen Anforderungen konfrontiert sein. So gäbe es im ersuchenden Mitgliedstaat in vielen Fällen Vorschriften über den rechtmäßigen Zugang, die im Widerspruch zum irischen Recht[94] stehen, das für mehrere große OTT-Anbieter gilt, da sie ihren Sitz in Irland haben; diese Anbieter können jedoch auch dem innerstaatlichen Recht der Mitgliedstaaten unterliegen, in denen sie ihre Dienstleistungen erbringen.

Diese Herausforderungen können durch gemeinsame Maßnahmen und ein gewisses Maß an Harmonisierung der Vorschriften für die rechtmäßige Überwachung auf EU-Ebene wirksam angegangen werden, um grenzüberschreitende Anträge auf rechtmäßige Überwachung zu erleichtern und zu beschleunigen. Dies wäre eine Voraussetzung für die Bewältigung anderer organisatorischer und technischer Herausforderungen, für die Lösungen gefunden werden können, wenn die Vorschriften eindeutig festgelegt und praktikabel sind.

---

93 Siehe „LE interception concerns under the EECC“, Microsoft, Januar 2020.

94 Nach irischem Recht ist es OTT-Anbietern untersagt, Live-Überwachungen durchzuführen.

III. Technologie

Ungeachtet rechtlicher Erwägungen wirkt sich die Entwicklung der Kommunikationstechnologien auf die technische Fähigkeit der Strafverfolgungsbehörden aus, Kommunikationen über die unmittelbar von den Anbietern von Kommunikationsdiensten oder OTT-Diensten erbrachten Dienste zu überwachen.

Bei herkömmlichen Kommunikationsanbietern werden die Kapazitäten zur rechtmäßigen Überwachung in der Regel von Technologieanbietern auf der Grundlage von ETSI-Normen entwickelt und in 3GPP[95] integriert. Infolgedessen können gut ausgestattete Polizeidienste herkömmliche Kommunikation – Sprach- und SMS-Nachrichten – zufriedenstellend überwachen und internetgestützte Kommunikation potenziell über Dienste überwachen, die über ihre Netze bereitgestellt werden.

Die zunehmende Komplexität der 5G-Kommunikationsinfrastrukturen und -protokolle, wie Virtualisierung, Network-Slicing, Edge-Computing und datenschutzfreundliche Funktionen, stellt herkömmliche Betreiber jedoch vor neue technologische Herausforderungen.[96] Die Experten der Hochrangigen Gruppe wiesen insbesondere auf die Herausforderungen im Zusammenhang mit dem Home-Routing[97] und den erweiterten Kommunikationsdiensten (Rich Communication Services – RCS)[98] hin.

Aus einer zukunftsorientierten Perspektive und auf der Grundlage der Erfahrungen mit 5G rechnen die Experten der Hochrangigen Gruppe damit, dass die künftige Einführung von 6G (voraussichtlich für die Zeit nach 2030) – in deren Rahmen der Schutz der Privatsphäre[99] verbessert und die Ende-zu-Ende-Verschlüsselung möglicherweise als Standard etabliert wird – mit Herausforderungen verbunden sein wird, die zusammengenommen die Überwachung erschweren könnten. Gleichzeitig bringen neue Kommunikationstechnologien wie das Internet der Dinge, die Satellitenkommunikation und die Entwicklung der Quanteninformatik[100] eine weitere Reihe von Herausforderungen mit sich, die es zu antizipieren gilt.

---

95 Partnerschaftsprojekt der dritten Generation, das die Grundlage für die Entwicklung von Kommunikationstechnologien wie 5G, Internet der Dinge und Mobilfunk-Breitbanddienste bildet.

96 Siehe „Law enforcement and judicial aspects related to 5G“, EU-Koordinator für die Terrorismusbekämpfung, 2019. https://data.consilium.europa.eu/doc/document/ST-8983-2019-INIT/en/pdf.

97 Europol - Position paper on Home routing.pdf (europa.eu).

98 Das RCS-Protokoll ermöglichet den Austausch von Gruppenchats, Video-, Audio- und hochauflösenden Bildern; es wird häufig anstelle von SMS verwendet. Je nach Umsetzung kann sich die rechtmäßige Überwachung von RCS-Nachrichten als unmöglich erweisen, was erhebliche Auswirkungen auf die Strafverfolgung hat (im Jahr 2023 gab es mehr als 1 Milliarde aktive RCS-Nutzer).

99 Siehe 6G-Fahrplan: https://5g-ppp.eu/wp-content/uploads/2021/06/WhitePaper-6G-Europe.pdf.

100 The Second Quantum Revolution: the impact of quantum computing and quantum technologies on law enforcement | Europol (europa.eu).

Schließlich wiesen die Experten der Hochrangigen Gruppe darauf hin, dass eine der größten technischen Herausforderungen für Strafverfolgungsbehörden in der Ende-zu-Ende-Verschlüsselung besteht, insbesondere bei der OTT-Kommunikation – mehr als 80 % der Kommunikation wird über Ende-zu-Ende-verschlüsselte Dienste (Live-Kommunikation und Backup-Speicherung) abgewickelt, wodurch die Ermittler am Zugang zu Kommunikationsinhalten gehindert werden. Gleichzeitig stimmen die Experten darin überein, dass die Ende-zu-Ende-Verschlüsselung als solide Sicherheitsmaßnahme betrachtet wird, die die Bürgerinnen und Bürger wirksam vor verschiedenen Formen der Kriminalität schützt. Indem sichergestellt wird, dass nur die kommunizierenden Nutzer auf den Inhalt ihrer Nachrichten zugreifen können, schützt die Ende-zu-Ende-Verschlüsselung wirksam vor unrechtmäßigem Abhören, Datendiebstahl, staatlich geförderter Spionage und anderen Formen des unbefugten Zugriffs durch Hacker, Cyberkriminelle oder sogar die Diensteanbieter selbst.

Die Herausforderungen zu quantifizieren, mit denen Strafverfolgungsbehörden bei der Überwachung der Kommunikation von Kriminellen und Terroristen mittels Ende-zu-End-Verschlüsselung konfrontiert sind, gestaltet sich schwierig. Dies ist darauf zurückzuführen, dass sich Strafverfolgungsbehörden häufig dagegen entscheiden, Zeit und Ressourcen zu investieren, um gerichtliche Anordnungen für die elektronische Überwachung auf Plattformen zu erwirken, die bekanntermaßen die Ende-zu-Ende-Verschlüsselung standardmäßig verwenden[101]; daher ist die effektive Anzahl der wirksamen Anträge auf rechtmäßige Überwachung von Inhaltsdaten, die aufgrund der Ende-zu-Ende-Verschlüsselung nicht durchgeführt werden können, sehr gering und nicht aussagekräftig. Den Strafverfolgungsbehörden zufolge ist dieser Mangel an Überwachungskapazitäten aus dem Blickfeld geraten und stellt eine erhebliche Schwachstelle dar, derer Kriminelle und Terroristen voll und ganz bewusst sind und die aktiv ausgenutzt wird, wie die Fälle EncroChat[102] und Sky ECC gezeigt haben, die zu Tausenden von Festnahmen in ganz Europa geführt haben, darunter viele hochkarätige Straftäter. Diese Bedenken wurden u. a. in mehreren Erklärungen der europäischen Polizeichefs[103] und der G7[104] aufgegriffen. Um die Auswirkungen des Verlusts des Zugangs zu Inhaltsdaten zu veranschaulichen, verwiesen die Experten auf mehrere der Öffentlichkeit bekannte Beispiele, die unter anderem Fälle von Terrorismus[105], Drogenhandel[106] und Vergewaltigung[107] betrafen, bei denen die Fähigkeit der Strafverfolgungsbehörden, schwere und organisierte Kriminalität zu verhindern und zu bekämpfen, durch Verschlüsselung erheblich beeinträchtigt wurde.

Die Vertreter der Strafverfolgungsbehörden würden einen Ansatz bevorzugen, der Unternehmen dazu verpflichtet, den Strafverfolgungsbehörden unter strengen Bedingungen unverschlüsselte Daten zugänglich zu machen. Es sei jedoch darauf hingewiesen, dass Cybersicherheitsexperten Bedenken geäußert haben, dass solche Lösungen die Cybersicherheit untergraben würden. Einige Strafverfolgungsexperten wiesen darauf hin, dass die Verschlüsselung in einigen Fällen in einer Weise umgesetzt wurde, die sowohl mit der Cybersicherheit als auch mit der Notwendigkeit vereinbar ist, einige Dienste beizubehalten, wie Betriebssystemaktualisierungen, das Scannen von Inhalten (z. B. E-Mails oder Web-Sitzungen) für Cybersicherheitszwecke oder wichtige Wiederherstellungsmechanismen, wenn sich der Nutzer zur Verwendung dieser Funktion entscheidet.

---

101 Manpearl, 2017.

102 Für weitere Informationen zu EncroChat und Sky ECC siehe Europol und Eurojust, „Third Report of the Observatory Function on Encryption“, Juni 2021.

103 https://www.europol.europa.eu/cms/sites/default/files/documents/EDOC-%231384205-v1-Joint_Declaration_of_the_European_Police_Chiefs.PDF.

104 https://www.gov.uk/government/publications/g7-interior-and-security-ministers-meeting-september-2021/g7-london-interior-commitments-accessible-version.

105 Im März 2017 verübte Khalid Masood, ein 52-jähriger Mann, in der Londoner Innenstadt einen islamistischen Terroranschlag, bei dem sechs Menschen ums Leben kamen und 29 verletzt wurden. Berichte über den Vorfall deuteten zwar darauf hin, dass Masood allein geplant und gehandelt habe, jedoch wurde festgestellt, dass er Minuten vor dem Anschlag ein PDF-Dokument mit dem Titel „Jihad“ an eine große Zahl seiner Kontakte auf WhatsApp und iMessage geschickt hatte, die beide standardmäßig von Ende-zu-Ende verschlüsselt waren und noch immer sind. Quellen: Max Hill, „The Westminster Bridge Terrorist Attack“ (London: The Stationery Office, 2018); BBC News, „WhatsApp Must Not Be a ‚Place for Terrorists to Hide‘“, 26. März 2017.

106 Die Experten erwähnten bedeutende Fälle von Drogenhandel, bei denen Fortschritte erst erzielt werden konnten, nachdem ein Zugang zu der verschlüsselten Kommunikation über Encrochat und Sky ECC erlangt wurde.

107 In einem besonders beachteten Vergewaltigungsfall im Vereinigten Königreich wurden polizeiliche Ermittlungen dadurch behindert, dass Verdächtige WhatsApp zur Kommunikation nutzten und die Ende-zu-Ende-Verschlüsselung den Zugang zu wichtigen Beweismitteln erschwerte. Die Ermittlungen wurden dadurch beeinträchtigt, dass die Strafverfolgungsbehörden WhatsApp-Nachrichten nicht ohne Einwilligung des Nutzers entschlüsseln konnten.

Auf dieser Grundlage waren sich die Strafverfolgungsexperten darin einig, dass die Herausforderungen, die sich aus der Verschlüsselung ergeben, einen vielschichtigen Ansatz erfordern, bei dem das Recht auf Privatsphäre, die Sicherheit und die Notwendigkeit, dass die Strafverfolgungsbehörden auf Daten zugreifen können, um Kriminalität zu bekämpfen und das Leben, die körperliche Unversehrtheit und das Eigentum der Menschen zu schützen, miteinander in Einklang gebracht werden. Es ist zwar unwahrscheinlich, dass mit einer einzigen Lösung alle relevanten Bedenken ausgeräumt werden, jedoch könnte eine Kombination von Ansätzen dazu beitragen, das Problem abzumildern.

IV. Kommunikationsanbieter krimineller Art

Kriminelle nutzen gängige Ende-zu-Ende-verschlüsselte Plattformen, um ihre Kommunikation zu verschleiern; sie können jedoch auch beschließen, sichere Kommunikationskanäle zu nutzen, die speziell für kriminelle Aktivitäten konzipiert sind (im Folgenden „kriminelle Kommunikationskanäle“– Criminal Communication Channels, CCC)[108]. EncroChat und Sky ECC sind bekannte CCC, die Telefone mit einem integrierten Ende-zu-Ende-verschlüsselten Nachrichtenübermittlungsdienst verkauften, der auf die Verschleierung krimineller Aktivitäten zugeschnitten und im Dark Web beworben wurde. Beide Plattformen wurden 2020 und 2021 durch gemeinsame internationale Strafverfolgungsmaßnahmen zerschlagen, wobei ihre umfassende Beteiligung an der organisierten Kriminalität offenbart wurde. Mehrere ähnliche Plattformen, wie Phantom Secure[109] und Exclu[110], wurden ebenfalls zerschlagen, während viele kleinere Plattformen noch in Betrieb sind und sichere Knotenpunkte für den kriminellen Informationsaustausch bieten. In dieser fragmentierten Landschaft ist es von entscheidender Bedeutung, dass Strafverfolgungsbehörden in der Lage sind, CCC zu identifizieren, ihre Tätigkeit zu überwachen und zu blockieren, sie zu zerschlagen und Straftäter vor Gericht zu bringen.

[108] https://www.eurojust.europa.eu/sites/default/files/Documents/pdf/joint_ep_ej_third_report_of_the_observatory_function_on_encryption_en.pdf.

[109] https://www.fbi.gov/news/stories/phantom-secure-takedown-031618.

[110] New strike against encrypted criminal communications with dismantling of Exclu tool | Eurojust | European Union Agency for Criminal Justice Cooperation (europa.eu).

Die betreiberbasierte Überwachung ist für diese Art von unseriösen Kommunikationsanbietern zwar keine Option, jedoch benötigen die Strafverfolgungsbehörden einschlägige Kapazitäten zur taktischen Überwachung – Instrumente und Fachwissen –, um ihre Nutzer trotz Verschlüsselung gezielt überwachen zu können. Die Strafverfolgungsexperten machten insbesondere auf die erheblichen Herausforderungen, Risiken und Einschränkungen im Zusammenhang mit der Entwicklung und dem Einsatz solcher Techniken aufmerksam, die nicht skalierbar sind und den wichtigsten Fällen vorbehalten sein sollten. Je nach ihren Kapazitäten und dem Rechtsrahmen wenden die nationalen Behörden unterschiedliche Ansätze an, einschließlich intern entwickelter, von Dritten erworbener oder als Dienstleistung betriebener Instrumente; unabhängig davon, welche Option sie nutzen, stimmen die Experten darin überein, dass Schutzmaßnahmen und Garantien für den Einsatz solcher Instrumente erforderlich sind. Darin könnten Überlegungen über eine verbesserte Aufsicht, Bewertung und Zertifizierung der Instrumente sowie ein solider Rahmen für das Schwachstellenmanagement einfließen, wobei die Verfahrensautonomie der Mitgliedstaaten in Strafsachen und ihre ausschließliche Zuständigkeit in Bezug auf die nationale Sicherheit uneingeschränkt zu achten sind.

Die Ermittlungsbehörden stehen auch vor rechtlichen Herausforderungen, wie z. B. Schwierigkeiten bei der Kriminalisierung von Kommunikations- und Hostingdiensten, die hauptsächlich kriminelle Dienste anbieten (da der gesamte Datenverkehr verschlüsselt ist), was ein notwendiger erster Schritt ist, bevor gerichtliche oder Verwaltungsmaßnahmen ergriffen werden. Darüber hinaus müssen die Mitgliedstaaten in der Lage sein, Sanktionen gegen CCC zu verhängen, um den Zugang zu solchen Diensten in der EU zu beschränken oder zu sperren und so ihr kriminelles Geschäftsmodell zu durchkreuzen. Dies wird notwendig sein, wenn für OTT-Dienste Verpflichtungen zur rechtmäßigen Überwachung gelten, damit verhindert wird, dass Kriminelle zu unseriösen Kommunikationsanbietern zurückkehren.

Schließlich werden verschiedene Aspekte von Rechtssachen, z. B. bei den Verfahren gegen EncroChat und Sky ECC, gerichtlich angefochten. Die Anforderungen dafür, die in einem anderen Mitgliedstaat überwachten Daten als Beweismittel zu verwenden, sind in der EU sehr unterschiedlich, wodurch Rechtsunsicherheit entsteht, wenn ähnliche Maßnahmen von einem Mitgliedstaat durchgeführt werden, sich jedoch auf viele Mitgliedstaaten auswirken könnten.

MÖGLICHE LÖSUNGEN

I. Anträge auf rechtmäßige Überwachung für alle Arten von Anbietern elektronischer Kommunikationsdienste durchsetzbar machen

In der EU sind die Kapazitäten für die rechtmäßige Überwachung auf herkömmliche Kommunikationsanbieter beschränkt, während die meisten Kommunikationen derzeit über nicht herkömmliche Kommunikationsanbieter erfolgen.[111] Unabhängig davon, ob ein Kommunikationsdienst vom Eigentümer der Infrastruktur erbracht wird oder nicht, sollten die Strafverfolgungsbehörden in der Lage sein, eine rechtmäßige Überwachung einer Person von Interesse durchzuführen. Alternative Lösungen wie die rechtmäßige Überwachung von NI-ICS und anderen Kommunikationsdiensten ausschließlich auf Ebene des Telekommunikationsnetzes, die Nutzung internationaler Kooperationsinstrumente zur rechtmäßigen Überwachung von NI-ICS-Anbietern oder ein umfassender Rückgriff auf taktische Überwachung sind nicht praktikabel.[112]

Daher muss nach Auffassung der Experten der Hochrangigen Gruppe vorrangig dafür gesorgt werden, dass die Verpflichtungen zur rechtmäßigen Überwachung verfügbarer Daten für herkömmliche und nicht herkömmliche Kommunikationsanbieter in gleicher Weise gelten und gleichermaßen durchsetzbar sind. Die Harmonisierung dieser Verpflichtungen sollte dazu dienen, die Herausforderungen im Zusammenhang mit der Erledigung grenzüberschreitender Anträge zu bewältigen.

Um dieses Ziel zu verfolgen und allmählich auf die Angleichung und Harmonisierung der Vorschriften für die rechtmäßige Überwachung in der EU hinzuarbeiten, schlagen die Experten der Hochrangigen Gruppe einen schrittweisen Ansatz vor: erstens sollten Strukturierungsgrundsätze auf EU-Ebene vereinbart werden (Schritt 1); die Umsetzung dieser Grundsätze sollte in der Folge von der Kommission unterstützt werden (Schritt 2); und schließlich können die Grundsätze auf der Grundlage einer weiteren Bewertung in einem Rechtsinstrument kodifiziert werden (Schritt 3).

---

111 Im Jahr 2022 wurden im Vereinigten Königreich 36 Milliarden SMS und MMS versandt, während sich die Zahl der Online-Nachrichten auf 1,3 Billionen belief (WhatsAppening in the world of online communications? – Ofcom).

112 Siehe Abschnitt zu den Herausforderungen.

Schritt 1: Einigung auf eine gemeinsame Ausgangsbasis

Zu aller Erst muss ein gemeinsames Verständnis dafür entwickelt werden, welche Kategorien elektronischer Kommunikationsdienste nationalen Verpflichtungen in Bezug auf die rechtmäßige Überwachung gemäß den Vorschriften der Datenschutzrichtlinie für elektronische Kommunikation und der DSGVO unterliegen können.

Zweitens muss eine Einigung über übergeordnete operative Anforderungen erzielt werden, in der klar festgelegt ist, was von den nationalen Behörden in Bezug auf die rechtmäßige Überwachung erwartet wird und welche Garantien damit verbunden sein sollten. LEON[113] wurde als gute Grundlage für die Festlegung der Strafverfolgungsanforderungen ermittelt. Dieses Dokument sollte mit Anforderungen z. B. in Bezug auf Verhältnismäßigkeit, Aufsicht und Transparenz einhergehen, wobei möglicherweise zwischen den für Inhaltsdaten und Nichtinhaltsdaten geltenden Vorschriften zu unterscheiden ist und die Cybersicherheit, der Datenschutz und die Privatsphäre uneingeschränkt zu achten sind und die Verschlüsselung nicht untergraben werden darf. Durch die mögliche Einsetzung einer Ad-hoc-Expertengruppe, einschließlich Experten in den Bereichen Cybersicherheit, Privatsphäre und Strafverfolgung, könnte sichergestellt werden, dass die Anforderungen erforderlichenfalls aktualisiert werden, möglicherweise aufbauend auf der Arbeit der Europol-Arbeitsgruppe zur Normung im Bereich der inneren Sicherheit, die fortgesetzt werden sollte.

Drittens muss das Konzept der örtlichen Zuständigkeit im Hinblick auf dessen Anwendbarkeit auf OTT-Dienste unter Berücksichtigung der unterschiedlichen Auslegungen zwischen den nationalen Behörden und vor allem zwischen den nationalen Behörden und den OTT-Anbietern geklärt werden. So sollten beispielsweise die Vorschriften für Fälle, in denen der Standort der Zielperson ungewiss ist, präzisiert werden. Außerdem bedarf es Leitlinien dazu, wer die Rechtmäßigkeit eines Antrags bewerten kann, z. B. in Bezug auf die Rolle der Diensteanbieter in diesem Zusammenhang. Nicht zuletzt hat die überwiegende Mehrheit der Gerichtsurteile die Rechtmäßigkeit von Verfahrenshandlungen gegen EncroChat und Sky ECC bestätigt, doch sind noch mehrere Gerichtsverfahren anhängig[114], die erhebliche Auswirkungen auf die Verurteilung von hochkarätigen Straftätern haben könnten. Daher müssen die Zulässigkeit von Beweismitteln, die durch taktische Überwachungsmaßnahmen zwischen den Mitgliedstaaten erlangt wurden, die gegenseitige Anerkennung von Urteilen und gerichtlichen Entscheidungen sowie die polizeiliche und justizielle Zusammenarbeit in Strafsachen möglicherweise erleichtert werden.

---

113 LEON (Law Enforcement Operational Needs for Lawful Access to Communications – Operativer Bedarf der Strafverfolgungsbehörden für einen rechtmäßigen Zugang zu Kommunikation) ist das Ergebnis der Arbeit schwedischer Strafverfolgungsbehörden in enger Zusammenarbeit mit Strafverfolgungsvertretern in den EU-Mitgliedstaaten, Nordamerika und Australien. Ziel ist es, den Bedarf der Strafverfolgungsbehörden in Bezug auf einen rechtmäßigen Zugang zu Kommunikationsinhalten, inhaltsbezogenen Daten und Teilnehmerinformationen zu ermitteln und zu beschreiben. Siehe Mitteilung des Ratsvorsitzes mit dem Titel *„Law Enforcement Operational Needs for Lawful Access to Communications (LEON)*“, Dokument 6050/23 vom 16. Februar 2023.

114 Siehe Rechtssachen T- 1180/23, T- 148/24, T- 167/24, T- 484/24 und T- 560/24.

Empfehlungen Cluster 7

Um auf EU-Ebene gemeinsame Grundsätze für die rechtmäßige Überwachung verfügbarer Daten zu vereinbaren, die für alle Arten von Anbietern elektronischer Kommunikationsdienste gelten, empfehlen die Experten Folgendes:

1. *Präzisierung der Definition und des Umfangs der rechtmäßigen Überwachung im Einklang mit bestehenden EU-Rechtsakten und anderen einschlägigen europäischen und internationalen Instrumenten wie dem Budapester Übereinkommen über Cyberkriminalität [Empfehlung 38];*

2. *Festlegung gemeinsamer operativer Anforderungen in Anlehnung an das LEON-Dokument [Empfehlung 21];*

3. *Ermittlung erforderlicher Garantien [Empfehlung 17, Empfehlung 41];*

4. *Berücksichtigung der Cybersicherheitsperspektive, sodass keine Maßnahme die Anbieter dazu verpflichtet, ihre IKT-Systeme in einer Weise anzupassen, die sich negativ auf die Cybersicherheit ihrer Nutzer auswirken würde [Empfehlung 41];*

5. *Präzisierung des Konzepts der örtlichen Zuständigkeit für Daten zur Behebung potenzieller Rechtskollisionen [Empfehlung 39] und Förderung der Annahme von Mindestvorschriften auf EU-Ebene, die die Zulässigkeit von Beweismitteln ermöglichen, die gegebenenfalls durch taktische Überwachungsmaßnahmen zwischen den Mitgliedstaaten erlangt wurden, sofern dies erforderlich ist, um die gegenseitige Anerkennung von Urteile und gerichtlichen Entscheidungen und die polizeiliche und justizielle Zusammenarbeit in Strafsachen zu erleichtern [Empfehlung 42].*

Es ist zu prüfen, wie gemeinsame Grundsätze, wie in Cluster 7 von Empfehlungen erwähnt, am besten zusammengestellt und vereinbart und das relevanteste Instrument für die gemeinsame Nutzung dieser Grundsätze ermittelt werden können. Rückblickend trug die Entschließung des Rates über die rechtmäßige Überwachung vom 17. Januar 1995[115] entscheidend dazu bei, die Harmonisierung der Lösungen für die rechtmäßige Überwachung zu erleichtern, da sie für die vom ETSI entwickelten Normen für die rechtmäßige Überwachung als Referenz diente. Ein ähnlicher Ansatz, möglicherweise durch eine Empfehlung der Kommission oder des Rates, könnte ebenfalls von Vorteil sein.

[115] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A31996G1104.

Wichtigste Maßnahme: Die Experten der Hochrangigen Gruppe fordern die EU auf, im Jahr 2025 eine Empfehlung zum Echtzeitzugang zu Daten zu vorzulegen.

Zeitrahmen: 2025 *Mittelausstattung: noch festzulegen*

- Die Experten der Hochrangigen Gruppe fordern die Europäische Kommission auf, eine Empfehlung vorzulegen, in der der Begriff der rechtmäßigen Überwachung[116] von Anbietern elektronischer Kommunikationsdienste und die verschiedenen Anforderungen präzisiert werden, die für die rechtmäßige Überwachung verfügbarer Nichtinhalts- und Inhaltsdaten gelten können, wobei die Cybersicherheit, der Datenschutz und die Privatsphäre uneingeschränkt zu achten sind – ohne die Verschlüsselung zu untergraben – und auf gemeinsamen operativen Anforderungen gemäß dem LEON-Dokument aufgebaut wird.

Schritt 2: EU-Unterstützung zur Gewährleistung gleicher Wettbewerbsbedingungen und zur Verbesserung der grenzüberschreitenden Zusammenarbeit

Die in Schritt 1 dargelegten gemeinsamen Grundsätze würden die Grundlage für die technische, rechtliche und organisatorische Harmonisierung auf EU-Ebene bilden. Ihre Umsetzung in klare Zielvorgaben bedarf der Koordinierung und finanziellen Unterstützung durch die Kommission. Dazu würde die Schaffung eines speziellen Verfahrens gehören, für das auf bestehenden Arbeitsgruppen aufgebaut wird und erforderlichenfalls neue Arbeitsgruppen eingerichtet werden und bei dem die Koordinierung mit den einschlägigen Interessenträgern, einschließlich OTT-Anbietern und Vertretern der Industrie, sichergestellt, den einschlägigen Gremien, insbesondere dem Rat und dem Europäischen Parlament, Bericht erstattet und Transparenz gegenüber der Öffentlichkeit gewährleistet wird. Dies könnte auch die Finanzierung gezielter Studien direkt oder über einschlägige Partnerschaften einschließen, z. B. mit einschlägigen Agenturen oder Partnern aus der Wissenschaft.

[116] Beschränkt auf die betreiberbasierte Überwachung gemäß der obigen Definition.

Darüber hinaus betonten die Experten der Hochrangigen Gruppe, dass die Effizienz von Anträgen auf grenzüberschreitende rechtmäßige Überwachung nach dem derzeitigen Rahmens dringend verbessert werden muss und gleichzeitig die oben dargelegten Arbeiten durchgeführt werden müssen. Dieses Ziel würde Folgendes umfassen:

- Bewertung der derzeitigen Grenzen der EEA[117] und Arbeiten zur Verbesserung der operativen Effizienz;
- Bewältigung der technischen und organisatorischen Beschränkungen im Zusammenhang mit dem grenzüberschreitenden Austausch von Beweismitteln, die durch rechtmäßige Überwachung erhoben wurden, was wiederum weitere Arbeiten in folgenden Bereichen erfordern würde:
    - Erfassung des Problems (welche Grenzen bestehen, welche Mitgliedstaaten haben es usw.),
    - Normung von Datenstrukturen, Vertrauensmechanismen und Datenfilterung, um die Übermittlung nicht relevanter Daten zu vermeiden und die Datenschutzgrundsätze der Zweckbindung, Verhältnismäßigkeit und Datenminimierung zu wahren;
    - Gestaltung grenzüberschreitender Übertragungswege und deren Kapazitäten,
    - Ermittlung entsprechender Finanzierungssysteme;
- Erleichterung grenzüberschreitender Anträge auf rechtmäßige Überwachung durch Benennung und Schulung von SPoC in Abstimmung mit der umfassenderen Arbeit an SPoC und dem Zugang zu digitalen Beweismitteln, wobei dem SIRIUS-Projekt eine bedeutende Rolle zukommt;
- gegebenenfalls Förderung bilateraler Abkommen zwischen den Mitgliedstaaten und den USA als Voraussetzung für die Erleichterung der von den nationalen Behörden direkt an die gängigsten Anbieter von OTT-Diensten gerichteten Anträge, da der Anwendungsbereich des Abkommens zwischen der EU und den USA über den grenzüberschreitenden Zugriff auf elektronische Beweismittel, über das derzeit verhandelt wird, nach den Verhandlungsrichtlinien die rechtmäßige Überwachung nicht abdeckt, was bedeutet, dass spezifische Abkommen erforderlich sind, um gegen Rechtskollisionen vorzugehen.

---

[117] In der Richtlinie 2014/41/EU des Europäischen Parlaments und des Rates vom 3. April 2014 über die Europäische Ermittlungsanordnung in Strafsachen (EEA) wird auf „Telekommunikationsverkehr“ Bezug genommen; während die meisten Mitgliedstaaten – im Einklang mit dem aktualisierten EKEK – einer weiter gefassten Auslegung folgen; es könnte in Erwägung gezogen und weiter geprüft werden, ob die EEA in dieser Hinsicht geändert werden muss.

Schließlich forderten die Experten, dass Maßnahmen geprüft werden, mit denen die Abschreckungsmaßnahmen der nationalen Behörden gegen nicht kooperative Anbieter elektronischer Kommunikationsdienste verbessert werden könnten. Die Experten forderten insbesondere, dass die Durchführbarkeit und Verhältnismäßigkeit möglicher technischer Lösungen bewertet wird.

Empfehlungen Cluster 8

Um sicherzustellen, dass ein breites Spektrum von Anbietern elektronischer Kommunikationsdienste, einschließlich OTT-Anbietern, auf Anträge auf rechtmäßige Überwachung gemäß den nationalen Rechtsvorschriften reagieren kann, empfehlen die Experten Folgendes:

1. *Unterstützung der Umsetzung der in Empfehlung 1.1 festgelegten Grundsätze durch Koordinierung und Finanzierung;*
2. *Sondierung, wie die EEA effiziente grenzüberschreitende Anträge auf rechtmäßige Überwachung besser unterstützen könnte, z. B. durch Verbesserung der Rechtssicherheit, Verkürzung der Fristen für die Reaktion auf Anordnungen und Förderung einer einheitlichen Nutzung der EEA [Empfehlung 40];*
3. *Aufbau von Mechanismen (Interoperabilität und Cybersicherheit) und Infrastrukturen (Bandbreite und Skalierbarkeit, die mit dem Echtzeittransfer von umfangreichen Datensätzen kompatibel sind [Empfehlung 9];*
4. *Förderung der Benennung von SPoC in der EU für die Bearbeitung von Anträgen von und Kontakten mit Behörden mit dem Ziel, die Durchsetzung der Verpflichtungen zur rechtmäßigen Überwachung zu erleichtern, und Einrichtung von Mechanismen für eine effiziente gezielte Bearbeitung grenzüberschreitender Anträge [Empfehlungen 19 und 36];*
5. *Förderung der Entwicklung bilateraler Abkommen über den Echtzeitzugang zu Daten mit Drittländern, insbesondere mit den Vereinigten Staaten [Empfehlung 38.4].*

Eine Reihe von Maßnahmen könnte die wirksame Umsetzung einer EU-Empfehlung zur rechtmäßigen Überwachung unterstützen.

Wichtigste Maßnahme: Die Experten der Hochrangigen Gruppe fordern die Kommission auf, die Umsetzung einer EU-Empfehlung zur rechtmäßigen Überwachung mit einer angemessenen Koordinierung und Finanzierung zu begleiten.

- Die Experten der Hochrangigen Gruppe fordern die Kommission auf, einen klaren Plan zur Unterstützung der Umsetzung einer EU-Empfehlung zur rechtmäßigen Überwachung vorzuschlagen, auch im Hinblick auf die Finanzplanung.

Schritt 3: Prüfung der Möglichkeit eines Rechtsinstruments zur rechtmäßigen Überwachung

Die Koordinierung allein kann sich als unzureichend erweisen, um das erforderliche Maß an Harmonisierung zu erreichen, auch wenn sie durch Maßnahmen zur Steigerung der Effizienz der bestehenden Rechtsinstrumente ergänzt wird. Es könnte ein neues Regelwerk erforderlich sein, um die Durchsetzbarkeit von Anträgen und Rechtssicherheit zu gewährleisten, Rechtskollisionen zu beseitigen und den Verwaltungsaufwand im Zusammenhang mit Konformitäts- und Legalitätsprüfungen zu verringern. Darüber hinaus stellen die Unterschiede zwischen den Vorschriften über die rechtmäßige Überwachung in der EU aufwändige Anforderungen an beaufsichtigte Unternehmen wie OTT-Anbieter dar, was möglicherweise zu Marktzugangshindernissen für Kommunikationsanbieter führt.[118] In diesem Zusammenhang würden harmonisierte EU-Vorschriften über die rechtmäßige Überwachung verfügbarer Daten zum Aufbau der künftigen digitalen Infrastruktur Europas beitragen und ein Modell begünstigen, bei dem die Telekommunikationsinfrastruktur potenziell den gesamten Kontinent abdecken könnte.[119]

Der Übergang zur Internetkommunikation ist ein starker Anreiz für die Festlegung harmonisierter Zugangsregeln auf EU-Ebene; allerdings sollten die Akzeptanz, die Durchführbarkeit und die Auswirkungen eines Rechtsinstruments auf die Branche, die Cybersicherheit und die Sicherheit sorgfältig geprüft werden, wobei den derzeitigen Unterschieden zwischen den Rechtssystemen der Mitgliedstaaten in Bezug auf die rechtmäßige Überwachung Rechnung zu tragen ist. Den Experten der Hochrangigen Gruppe zufolge sollte ein mögliches Instrument i) die in Empfehlung 1.1 dargelegten Grundsätze einhalten, ii) der Perspektive der Grundrechte und der Souveränität der Staaten in Strafsachen und der nationalen Sicherheit in vollem Umfang Rechnung tragen und iii) sich an den Arbeiten zum Paket zu elektronischen Beweismitteln orientieren.

Die Experten der Hochrangigen Gruppe waren sich darin einig, dass jede Initiative zur Förderung oder Auferlegung von Vorschriften über die rechtmäßige Überwachung für alle Arten von elektronischen Kommunikationsdiensten mit einem klaren und durchsetzbaren Rahmen für Maßnahmen gegen Kommunikationsanbieter einhergehen sollte, die illegal tätig sind und/oder jegliche Form der Zusammenarbeit mit Strafverfolgungsbehörden ablehnen. Ohne einen solchen Rahmen würden die Vorschriften untergraben, und eine Vielzahl krimineller Akteure würde für ihre Kommunikation auf Anbieter wechseln, die die Vorschriften nicht einhalten. Bei jeder künftigen EU-Initiative in diesem Zusammenhang sollte der Unterschied zwischen OTT-Anbietern, die ihren rechtlichen Verpflichtungen nicht nachkommen, und Anbietern elektronischer Kommunikationsdienste, die ihre Dienste bewusst auf kriminelle Aktivitäten zuschneiden, berücksichtigt werden. Darüber hinaus sollte bei jeder Initiative auch der EU-Besitzstand berücksichtigt werden, insbesondere das Gesetz über digitale Dienste.

---

118 Siehe „Lawful interception – A market access barriers in the European Union“, Vadim Doronin in Computer Law & Security Review 51 (2023) 105867.

119 White Paper – How to master Europe’s digital infrastructure needs? | Shaping Europe’s digital future (europa.eu).

Eine solche Initiative könnte gerichtliche oder Verwaltungsmaßnahmen umfassen. Die Experten der Hochrangigen Gruppe forderten eingehende Überlegungen zu dieser Angelegenheit, mit denen sowohl Grundrechts- als auch Cybersicherheitsfragen und die damit verbundenen komplexen technologischen Herausforderungen angegangen würden.

Empfehlungen Cluster 9

Auf der Grundlage weiterer Analysen und einer Folgenabschätzung empfehlen die Experten die ***Ausarbeitung eines EU-Instruments zur rechtmäßigen Überwachung (bestehend aus nicht zwingenden Rechtsinstrumenten oder verbindlichen Rechtsinstrumenten) zu Strafverfolgungszwecken****, mit dem durchsetzbare Verpflichtungen für Anbieter von elektronischen Kommunikationsdiensten in der EU eingeführt würden. Die Experten empfehlen, dass dieses potenzielle Instrument [Empfehlung 38]*

1. *den in Cluster 7 von Empfehlungen vereinbarten Grundsätzen folgt;*
2. *technologieneutral ist [Empfehlung 21];*
3. *die Harmonisierung der strafrechtlichen Maßnahmen, einschließlich Freiheitsstrafen, auf EU-Ebene gegen nicht kooperative Anbieter elektronischer Kommunikationsdienste zur Durchsetzung der Zusammenarbeit fördert [Empfehlung 34];*
4. *der Perspektive der Grundrechte und der Souveränität der Staaten in Strafsachen und der nationalen Sicherheit in vollem Umfang Rechnung trägt [Empfehlung 38];*
5. *sich an der Arbeit orientiert, die im Zusammenhang mit der Annahme der Vorschriften über elektronische Beweismittel geleistet wurde [Empfehlung 38 Ziffer iv];*
6. *Verpflichtungen für Diensteanbieter festlegt, bestimmte Funktionen in ihren Diensten an- oder abzuschalten, um Informationen zu erhalten, nachdem eine Anordnung ergangen ist (z. B. Speicherung der Geolokalisierung eines spezifischen Nutzers, nachdem dieser Gegenstand eines rechtmäßigen Antrags ist) [Empfehlung 32];*
7. *Mechanismen aufnimmt, mit denen sichergestellt wird, dass die Mitgliedstaaten Sanktionen gegen nicht kooperative Anbieter elektronischer Kommunikationsdienste durchsetzen können (entweder verwaltungs- oder strafrechtliche Maßnahmen, je nachdem, ob ein Anbieter lediglich nicht kooperativ ist oder einen Dienst krimineller Art anbietet), im Einklang mit und möglicherweise aufbauend auf den Vorschriften des Gesetzes über digitale Dienste, und dass solche Sanktionen abschreckend gegen diese Einrichtungen wirken [Empfehlung 33].*

Die Durchsetzung der in einer EU-Empfehlung zur rechtmäßigen Überwachung festgelegten Grundsätze wäre ein wichtiger Schritt hin zu stärker harmonisierten und durchsetzbaren Vorschriften für die rechtmäßige Überwachung. Allerdings kann ein Rechtsinstrument erforderlich sein, um die Rechtssicherheit zu verbessern, sicherzustellen, dass die erforderlichen Garantien für alle einschlägigen elektronischen Kommunikationsdienste bei der Durchführung der rechtmäßigen Überwachung bestehen, und um sicherzustellen, dass Anbieter elektronischer Kommunikationsdienste, die nicht gewillt sind, die von den Mitgliedstaaten festgelegten Vorschriften durchzusetzen, dazu gezwungen werden.

Wichtigste Maßnahme: Die Experten der Hochrangigen Gruppe ersuchen die Kommission, die Weiterentwicklung des Rechtsrahmens für die rechtmäßige Überwachung zu Strafverfolgungszwecken zu bewerten.

- Die Experten der Hochrangigen Gruppe ersuchen die Europäische Kommission, vor einer möglichen Folgenabschätzung die Möglichkeit eines EU-Rechtsinstruments zur rechtmäßigen Überwachung zu prüfen, das auf den Arbeiten zur Vorbereitung der EU-Verordnung und -Richtlinie über elektronische Beweismittel aufbaut und in erster Linie auf die Ermittlung potenzieller technologieneutraler Lösungen abzielt.

II. Bewältigung technologischer Herausforderungen

Viele Herausforderungen, mit denen die Strafverfolgungsbehörden beim Zugang zu Daten konfrontiert sind, sind darauf zurückzuführen, wie schwierig es für sie ist, technologische Entwicklungen zu antizipieren und sich an diese anzupassen. Dies liegt daran, dass die Strafverfolgungsbehörden im Gegensatz zu Akteuren in anderen Bereichen wie Verteidigung oder Raumfahrt nicht über die dafür erforderlichen Ressourcen oder engen Beziehungen zur Industrie verfügen und dies in der Regel auch nicht notwendig war. In vielen Fällen versuchen die Akteure der inneren Sicherheit, technologische Lücken reaktiv zu schließen, oder – was häufiger der Fall ist – ihren Bedarf mit herkömmlichen Technologien zu decken, die verfügbar und erschwinglich sind. Um den Übergang von einem reaktiven zu einem proaktiveren Ansatz zu fördern, müssen technologische Herausforderungen auf strukturierte, zukunftsorientierte und multidisziplinäre Weise mit zwei Hauptprioritäten angegangen werden: aus der Sicht der nationalen Behörden muss unbedingt sichergestellt werden, dass die Strafverfolgungsbehörden Zugang zu den einschlägigen Kapazitäten für den Erwerb und die Verarbeitung verfügbarer Daten auf dem Übermittlungsweg haben; für Betreiber und Technologieanbieter ist es von entscheidender Bedeutung, dass sie in der Lage sind, ihren Verpflichtungen in Bezug auf den Zugang zu Daten, die Privatsphäre und die Cybersicherheit nachzukommen, und dass ihre Interessen gewahrt werden.

Die Experten schlagen daher vor, technologische Herausforderungen durch eine umfassende und zukunftsorientierte Politik zu antizipieren, die auf einem **Technologiefahrplan für den rechtmäßigen Zugang** beruht, in dem Ziele und Maßnahmen mit entsprechenden Finanzmitteln festgelegt werden, um diese Ziele zu erreichen.

Beim Kapazitätsaufbau sind die Herausforderungen zwar unterschiedlich, doch ist der von den Experten vorgeschlagene Ansatz häufig ähnlich für die digitale Forensik, die Vorratsdatenspeicherung und die rechtmäßige Überwachung[120] und baut auf denselben Empfehlungen auf, wobei eine starke Forderung nach einer zielorientierten Planung zur Steuerung von Finanzierungsmöglichkeiten besteht und die Akteure aus der Industrie und wichtige Interessenträger wie das EU-Innovationszentrum für innere Sicherheit enger einbezogen werden.

Die Strafverfolgungsexperten beharrten jedoch auf zwei Elementen, die spezifisch für die rechtmäßige Überwachung sind.

- Die verstärkte Nutzung von Metadaten – z. B. Standortdaten, Anrufaufzeichnungen und E-Mail-Header – kann zusätzliche Ermittlungshinweise liefern. **Da immer mehr Geräte mit dem Internet verbunden werden, nimmt die Menge der erzeugten Daten zu, wodurch sich mehr Möglichkeiten bieten, Verhaltensmuster zu erkennen.** Die Experten forderten mehr Forschung, Innovation und Akzeptanz in Bezug auf eine **erweiterte Nutzung von Metadaten**, z. B. durch KI, um den mangelnden Zugang zu Inhaltsdaten abzumildern. Gleichzeitig wiesen sie auf die Risiken für die Privatsphäre hin, die mit der umfassenden und massenhaften KI-Verarbeitung personenbezogener Metadaten verbunden sind, die mit einer gezielten Nutzung von Inhaltsdaten in Einklang gebracht werden müssen. Die Strafverfolgungsexperten haben unmissverständlich darauf hingewiesen, dass es nicht möglich ist, den Beweiswert von Kommunikationsinhalten zum Nachweis einer Absicht allein durch Metadaten vollständig zu ersetzen.
- Wenn Kriminelle spezielle Ende-zu-Ende-verschlüsselte Kommunikationsplattformen nutzen, müssen die Strafverfolgungsbehörden taktische Lösungen nutzen, die auf der Ausnutzung von **Schwachstellen** beruhen, um Zugang zur Kommunikation von Verdächtigen zu erhalten. Einige Strafverfolgungsbehörden sind bereits auf der Grundlage eines Rechtsrahmens tätig, der die Überwachung an Kommunikationsendpunkten ermöglicht, und verfügen über die dafür erforderliche Technologie, und es gibt noch Spielraum für weitere Fortschritte in dieser Hinsicht. Diese könnten erzielt werden, indem die Entwicklung von in der EU konzipierten Instrumenten unterstützt und es den Strafverfolgungsbehörden ermöglicht wird, diese Instrumente innerhalb des bestehenden Rechtsrahmens zu erwerben und zu nutzen.

  Strafverfolgungsexperten wiesen jedoch darauf hin, dass diese Methode nicht als primäres Mittel der Beweiserhebung ausgeweitet werden sollte, da die taktische Überwachung weder skalierbar ist noch sich problemlos gestaltet. So könnten beispielsweise aufgrund des Standorts des Zielunternehmens Fragen der Zuständigkeit auftreten. Darüber hinaus steht die Nutzung von Schwachstellen, die nicht offengelegt werden können, unweigerlich im Widerspruch zu den zentralen Cybersicherheitsgrundsätzen.

[120] Im Einzelnen im Kapitel über die digitale Forensik.

In Bezug auf den konzeptionsintegrierten rechtmäßigen Zugang schlugen die Strafverfolgungsexperten einen vorsichtigen Ansatz vor, da die Akteure der Industrie nicht aufgefordert werden sollten, Systeme zu integrieren, die die Verschlüsselung auf allgemeine oder systemische Weise für alle Nutzer eines Dienstes schwächen könnten; der rechtmäßige Zugang sollte weiterhin gezielt für einzelne Kommunikationen erfolgen. Die Experten waren sich über die Relevanz des übergeordneten Ziels einig, betonten jedoch, dass Fortschritte schrittweise erzielt werden müssen und alle relevanten Kategorien von Interessenträgern, einschließlich Experten für Technologie, Cybersicherheit und Privatsphäre, einbezogen werden müssen, wobei die potenziellen Risiken und die Sensibilität der öffentlichen Debatte zu berücksichtigen sind. Insbesondere empfahlen sie nachdrücklich, einen evidenzbasierten Ansatz zu verfolgen und sorgfältig zu prüfen, ob technische Lösungen zur Verfügung stehen, die die Cybersicherheit der Kommunikation nicht schwächen oder sich negativ auf die Cybersicherheit der Betreiber auswirken.

Empfehlungen Cluster 10

Um den technologischen Herausforderungen der rechtmäßigen Überwachung zu begegnen, empfehlen die Experten die Entwicklung eines ***Technologiefahrplans für den rechtmäßigen Zugang***[121]*, der insbesondere Folgendes vorsieht:*

1. *Zusammenführung von Experten für Technologie, Cybersicherheit, Privatsphäre, Normung und Sicherheit und Gewährleistung einer angemessenen Koordinierung, möglicherweise durch eine ständige Struktur [Empfehlung 22];*
2. *Förderung der Erforschung, Entwicklung und Einführung von Instrumenten für die Datenerfassung und den Zugang zu Daten, einschließlich Entschlüsselungsfähigkeiten, sowie KI-gestützter Kapazitäten für die Datenanalyse [Empfehlung 4]*[122]*;*
3. *Förderung eines koordinierten Ansatzes für die Normung, der gegebenenfalls den Erfordernissen des rechtmäßigen Zugangs zu Daten Rechnung trägt und [Empfehlungen 15, 16 und 20]*
    a. *die Einbeziehung von Praktikern aus allen einschlägigen Gemeinschaften in die einschlägigen Normungsgruppen fördert,*
    b. *künftige Initiativen durch angemessene Normungsmaßnahmen begleitet (zur Förderung eines technologieneutralen Ansatzes),*
    c. *Kommunikationstechnologien im Allgemeinen, das Internet der Dinge (einschließlich z. B. vernetzter Fahrzeuge) und alle Formen der Konnektivität (einschließlich z. B. Satellitenkommunikation) abdeckt;*
4. *Verbesserung der EU-Koordinierung mit der Industrie, um Situationen anzugehen, in denen es zwar technische Lösungen gibt, diese aber nicht umgesetzt werden; in solchen Fällen*[123] *sind klare Leitlinien und ein auf EU-Ebene angesiedelter Dialog erforderlich [Empfehlung 24];*
5. *Umsetzung des konzeptionsintegrierten rechtmäßigen Zugangs in allen relevanten Technologien im Einklang mit dem von den Strafverfolgungsbehörden geäußerten Bedarf, wobei gleichzeitig eine starke Sicherheit und Cybersicherheit gewährleistet und die rechtlichen Verpflichtungen für den rechtmäßigen Zugang eingehalten werden [Empfehlung 22];*
6. *umfassende Bewältigung der Herausforderungen der Verschlüsselung, indem*
    a. *gewährleistet wird, dass etwaige neue Verpflichtungen und/oder Normen weder direkt noch indirekt dazu führen, dass die Anbieter die Sicherheit der Kommunikation durch eine generelle Untergrabung oder Schwächung der Ende-zu-Ende-Verschlüsselung verringern [Empfehlung 23];*
    b. *gewährleistet wird, dass sich der konzeptionsintegrierte rechtmäßige Zugang nicht negativ auf die Sicherheitslage der betreffenden Hardware- oder Software-Architekturen auswirkt [Empfehlung 23];*
    c. *in koordinierter Weise und mit Unterstützung durch EU-Mittel an einer Methode zur Entwicklung, Handhabung und Nutzung von Maßnahmen des gezielten rechtmäßigen Zugangs für Fälle gearbeitet wird, in denen der Zugang zu Daten durch die Zusammenarbeit mit Anbietern elektronischer Kommunikationsdienste nicht möglich ist [Empfehlung 10].*

---

121 Der Technologiefahrplan sollte die drei Arbeitsbereiche abdecken: digitale Forensik, Vorratsdatenspeicherung und rechtmäßige Überwachung.

122 Diese Empfehlung gilt auch für den Zugang zu Daten auf einem Gerät (siehe Abschnitt über digitale Forensik), die Anwendungsfälle unterscheiden sich jedoch geringfügig.

123 Wenn beispielsweise Home-Routing-Vereinbarungen oder eine bestimmte Art der Umsetzung von RCS eine rechtmäßige Überwachung nicht zulassen.

Zwar existieren einige von den Experten der Hochrangigen Gruppe vorgeschlagene Initiativen bereits zum Teil, doch besteht ein dringender Bedarf an einer besseren Strukturierung der mittel- und langfristigen Technologiepolitik in Bezug auf den rechtmäßigen Zugang im Technologiefahrplan mit konkreten Zielen und einem zugehörigen Überwachungsinstrument. Dieser Ansatz sollte nicht nur den Zugang zu Daten auf dem Übermittlungsweg, sondern auch die digitale Forensik und die Vorratsdatenspeicherung umfassen.

Der Technologiefahrplan sollte zukunftsorientiert und durchsetzbar, auf vorrangige Themen ausgerichtet und in der Digitalstrategie der EU verankert sein. Er sollte alle relevanten Kategorien von Interessenträgern, insbesondere die Organe, Einrichtungen und sonstigen Stellen der EU, nationale Behörden, Wissenschaftler aus allen relevanten Bereichen, die Industrie und NRO, in enger Partnerschaft einbeziehen und über eine klare Governance verfügen.

Wichtigste Maßnahme: Die Experten der Hochrangigen Gruppe fordern die Kommission nachdrücklich auf, einen Technologiefahrplan für den Zugang zu Daten vorzulegen und umzusetzen.

- Die Experten der Hochrangigen Gruppe fordern die Europäische Kommission auf, einen Technologiefahrplan auszuarbeiten und umzusetzen, der auf die Herausforderungen im Zusammenhang mit der Verschlüsselung ausgerichtet ist und alle relevanten Aspekte berücksichtigt, einschließlich Technologie, Markt, Cybersicherheit, Grundrechte, Normung, Strafverfolgung und Forschung. Dieser Technologiefahrplan sollte 2025 vorliegen und auf dem gesamten einschlägigen Fachwissen der Mitgliedstaaten und der Organe und Einrichtungen der EU aufbauen, auch in den Bereichen Cybersicherheit, Datenschutz und Privatsphäre.