190963/EU XXVII. GP
Eingelangt am 28/06/24

Rat der
Europäischen Union

Brüssel, den 21. Juni 2024
(OR. en)

11281/24

COSI 120
ENFOPOL 309
IXIM 169
CATS 62
COPEN 325
CYBER 200

VERMERK

Absender:	Vorsitz
Empfänger:	Delegationen
Nr. Vordok.:	10477/24
Betr.:	Zugang zu Daten für eine wirksame Strafverfolgung – Bericht des Vorsitzes

Der digitale Wandel unserer Gesellschaften birgt ein enormes Potenzial für ein besseres, wohlhabenderes und sichereres Leben. Wenn die Vorteile des digitalen Zeitalters für die Bürgerinnen und Bürger maximiert werden sollen, müssen auch die Möglichkeiten für schwere und organisierte Kriminalität und Terrorismus minimiert werden.

In Europa hat dieser digitale Wandel zu einer neuen Dimension des Raums der Freiheit, der Sicherheit und des Rechts ohne Binnengrenzen geführt; ein neuer Kontext, in dem die Europäische Union die Werte der Achtung der Menschenwürde, der Freiheit, der Demokratie, der Gleichheit, der Rechtsstaatlichkeit und der Achtung der Menschenrechte fördert und schützt. Die Gewährleistung des Rechts der Europäerinnen und Europäer auf Sicherheit und Schutz erfordert eine verbesserte innere Sicherheit in Europa, unter anderem durch die Entwicklung und Nutzung sicherer und auf den Menschen ausgerichteter neuer Technologien und die Umsetzung des Grundsatzes der konzeptionsintegrierten Sicherheit. Die Verhütung, Aufdeckung, Ermittlung und Verfolgung von schwerer und organisierter Kriminalität erfordert die Verfügbarkeit und den Zugang zu elektronischen Beweismitteln, was zu einem entscheidenden Faktor wird.

www.parlament.gv.at

Heutzutage beruht jede erfolgreiche Ermittlung und Verfolgung von Fällen schwerer oder organisierter Kriminalität auf elektronischen Beweismitteln. Paradoxerweise ist festzustellen, dass der digitale Wandel zwar zur Schaffung, Übermittlung und Speicherung eines immer größeren Datenvolumens geführt hat, dass aber die Verfügbarkeit von und der Zugang zu elektronischen Beweismitteln für die Zwecke der Strafverfolgung und der Strafjustiz sich als die größte Herausforderung herausgestellt hat, was den Schutz der Bürgerinnen und Bürger der Union vor der Bedrohung durch Terrorismus sowie schwere und organisierte Kriminalität anbelangt.

Diese Herausforderung ist zwar nicht neu, sie gewinnt aber jeden Tag an Bedeutung. Die Strafverfolgung tappt sprichwörtlich „im Dunkeln". Bereits im Juni 2017 forderte der Europäische Rat, „*die Herausforderungen im Zusammenhang mit Systemen anzugehen, die Terroristen Kommunikationsmöglichkeiten bieten, zu denen die zuständigen Behörden keinen Zugang haben, einschließlich Ende-zu-Ende-Verschlüsselung; gleichzeitig gilt es aber, die Vorteile zu wahren, die diese Systeme für den Schutz der Privatsphäre, den Datenschutz und den Schutz der Kommunikation bieten*" und vertrat die Auffassung, dass „*ein effektiver Zugang zu elektronischen Beweismitteln für die Bekämpfung von schwerer Kriminalität und Terrorismus unabdingbar ist und dass die Verfügbarkeit von Daten vorbehaltlich geeigneter Garantien sichergestellt werden sollte*". Der Gerichtshof betonte in seinem Urteil vom 30. April 2024 in Bezug auf den Zugang zu IP-Adressen im Zusammenhang mit online begangenen Straftaten: „*Würde ein solcher Zugang nicht gestattet, bestünde [...] eine echte Gefahr der systemischen Straflosigkeit [...] von [...] Arten von Straftaten, die online begangen werden oder deren Begehung oder Vorbereitung durch die Merkmale des Internets erleichtert wird*".

Die organisierte Kriminalität, einschließlich des illegalen Drogenhandels, stellt eine große Bedrohung für die europäischen Bürgerinnen und Bürger, Unternehmen und Institutionen sowie für die europäische Wirtschaft und die Sicherheit der Mitgliedstaaten dar. Kriminelle Netze nutzen zunehmend extreme Gewalt, die Unterwanderung der legalen Wirtschaft sowie Korruption, wodurch die Rechtsstaatlichkeit beeinträchtigt und die Grundlagen unserer Demokratien gefährdet werden.

Um das weitere Vorgehen auszuloten, hat der schwedische Vorsitz in Zusammenarbeit mit dem bevorstehenden spanischen und belgischen Vorsitz im Juni 2023 eine Hochrangige Gruppe für den Zugang zu Daten für eine wirksame Strafverfolgung (im Folgenden „Hochrangige Gruppe") ins Leben gerufen, die durch einen Beschluss der Kommission vom 6. Juni 2023 eingesetzt wurde und sich aus von den Mitgliedstaaten benannten Sachverständigen, der Kommission, den einschlägigen Einrichtungen und sonstigen Stellen der EU und dem EU-Koordinator für die Terrorismusbekämpfung zusammensetzt. Den Vorsitz in der Gruppe führen der turnusmäßig wechselnde Ratsvorsitz und die Kommission gemeinsam.

www.parlament.gv.at

Nach einer Analyse der Herausforderungen, denen Strafverfolgungsbehörden in der Union bei ihrer täglichen Arbeit begegnen – in vier Plenarsitzungen, zahlreichen Sitzungen auf Sachverständigenebene und einer öffentlichen Konsultationssitzung – haben die Sachverständigen 42 Empfehlungen formuliert, um aktuelle und zu erwartende Herausforderungen vor dem Hintergrund technologischer Entwicklungen anzugehen und so ein umfassendes EU-Konzept zur Gewährleistung wirksamer strafrechtlicher Ermittlungen und Strafverfolgungsmaßnahmen als wesentliches Element der Rechtsstaatlichkeit zu ermöglichen. Die Empfehlungen sind in drei Cluster untergliedert: Kapazitätsaufbau, Zusammenarbeit mit der Industrie und Normung und Legislativmaßnahmen.

Zudem berieten der Koordinierungsausschuss für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen (CATS) am 23. Mai 2024 und der Ständige Ausschuss für die operative Zusammenarbeit im Bereich der inneren Sicherheit (COSI) am 29. Mai 2024 über die Empfehlungen der Hochrangigen Gruppe, brachten ihre Unterstützung für den Prozess der Hochrangigen Gruppe zum Ausdruck und begrüßten die Arbeit der Sachverständigen.

Die Innenministerinnen und -minister führten am 13. Juni 2024 einen Gedankenaustausch über die Empfehlungen der Hochrangigen Gruppe, begrüßten weitgehend die von den Sachverständigen der Hochrangigen Gruppe geleistete Arbeit und hoben die Notwendigkeit hervor, die Arbeit am Zugang zu Daten für eine wirksame Strafverfolgung zügig voranzubringen. Sie bestätigten die Prioritäten, die der Ständige Ausschuss für die operative Zusammenarbeit im Bereich der inneren Sicherheit ermittelt hatte, insbesondere einen harmonisierten EU-Rechtsrahmen für die Vorratsdatenspeicherung, die Festlegung von Vorschriften für den Zugang zu Daten aus interpersoneller elektronsicher Kommunikation sowie rechtlich und technisch fundierte 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 traten die Ministerinnen und Minister nachdrücklich für die Ausarbeitung eines Fahrplans für die Umsetzung der Empfehlungen mit klaren Fristen, einer Bewertung der Machbarkeit und angemessener Finanzierung ein. Der Ständige Ausschuss für die operative Zusammenarbeit im Bereich der inneren Sicherheit wurde als das geeignete Gremium für die Überwachung der Fortschritte bei der Umsetzung der Empfehlungen erachtet, gegebenenfalls mit Unterstützung durch den Koordinierungsausschuss für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. Die Justizministerinnen und -minister wurden am 14. Juni 2024 über die Empfehlungen der Hochrangigen Gruppe informiert.

www.parlament.gv.at

Der Vorsitz würdigt die von der Hochrangigen Gruppe geleistete Arbeit und ist entschlossen, Folgemaßnahmen bestmöglich zu unterstützen. In diesem Zusammenhang sollte zwar anerkannt werden, dass diese unverbindlichen Empfehlungen von Sachverständigen erarbeitet wurden, doch sollte es möglich sein, einige Maßnahmen unverzüglich umzusetzen, unter anderem die Bestandsaufnahme der bestehenden Rechtsvorschriften und der bestehenden Rechtsprechung, den Kapazitätsaufbau sowie die Normung und die Zusammenarbeit mit der Industrie, wobei vorhandene operative Strukturen wie das EU-Innovationszentrum für die innere Sicherheit und die EU-Agenturen im Einklang mit ihren jeweiligen Mandaten bestmöglich genutzt werden sollten.

Wie von den Innenministerinnen und -ministern am 13. Juni 2024 erörtert, wird es wichtig sein, einen pragmatischen und realistischen Fahrplan zu erarbeiten, um die Koordinierung der vom Ständigen Ausschuss für die operative Zusammenarbeit im Bereich der inneren Sicherheit und vom Koordinierungsausschuss für den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen zu überwachenden Arbeit in den der Strukturen des Rates zu erleichtern. Dies sollte dazu beitragen, die kontinuierliche Einbeziehung des Bereichs Justiz und Inneres in die Entwicklung künftiger Initiativen auf der Grundlage der Empfehlungen der Hochrangigen Gruppe zu gewährleisten. Zusätzlich wird der Kontakt zu anderen Bereichen von entscheidender Bedeutung sein, um diese für die Herausforderungen, mit denen die Strafverfolgungs- und Justizbehörden bei der Bekämpfung von Kriminalität und Terrorismus konfrontiert sind, stärker zu sensibilisieren. Es wird auch wichtig sein, der Öffentlichkeit klar die Zielsetzung und den Mehrwert der geplanten Maßnahmen zu kommunizieren.

Der künftige ungarische Vorsitz und die Kommission haben ihre Absicht bekundet, einen Abschlussbericht der Hochrangigen Gruppe bis Ende 2024 vorzubereiten. Ferner haben die künftigen Vorsitze ihre Absicht bekundet, die Entwicklung dieser Arbeitsbereiche aktiv zu verfolgen.

www.parlament.gv.at

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

Die geäußerten Meinungen sind ausschließlich die Meinungen der Sachverständigen und sollten nicht als repräsentativ für den offiziellen Standpunkt der Europäischen Kommission betrachtet werden.

Einleitung

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.[1] Sie wirkt darauf hin, durch Maßnahmen zur Verhütung und Bekämpfung von schwerer und organisierter Kriminalität, auch durch die Stärkung der grenzüberschreitenden Zusammenarbeit der Strafverfolgungs- und Justizbehörden[2], ein hohes Maß an Sicherheit zu gewährleisten, ohne in irgendeiner Weise in die nationale Sicherheit einzugreifen. Um ein wirksames Vorgehen bei der Bekämpfung von Kriminalität und bei anderen Herausforderungen im Zusammenhang mit der Aufrechterhaltung eines hohen Maßes an Sicherheit zu gewährleisten, müssen die Strafverfolgungsbehörden in der Lage sein, ihre Aufgaben der Verhütung, Aufdeckung und Ermittlung von Straftaten sowie der Gewährleistung der Verfolgung von Straftaten wirksam und rechtmäßig und unter uneingeschränkter Achtung der Grundrechte wahrzunehmen, um im allgemeinen Interesse und insbesondere im Interesse der Opfer für Gerechtigkeit zu sorgen und die öffentliche Sicherheit zu schützen.

1 *Vertrag über die Arbeitsweise der Europäischen Union* (AEUV) Artikel 67 Absatz 1.
2 Ebenda, Absatz 3.

www.parlament.gv.at

Trotz der Erzeugung, Übermittlung und Speicherung immer größerer Datenmengen hat sich der Zugang zu Daten für Strafverfolgungszwecke in den letzten Jahren als eine zentrale Herausforderung für die Ermittlung und Verfolgung von Straftaten und die wirksamen Rechtsdurchsetzung herausgestellt. Die EU hat strenge Vorschriften eingeführt, um den grenzüberschreitenden Zugang zu elektronischen Beweismitteln zu erleichtern („Regelwerk der EU zu elektronischen Beweismitteln“).[3] Das Fehlen einer Verpflichtung zur Vorratsdatenspeicherung wirkt sich jedoch negativ auf die Wirksamkeit des Regelwerks zu elektronischen Beweismitteln aus, da nicht gewährleistet ist, dass alle Informationen verfügbar sind, die Gegenstand europäischer Sicherungs- oder Herausgabeanordnungen sind, unter anderem Verkehrsdaten, ausschließlich zum Zweck der Identifizierung des Nutzers angeforderte Daten und Teilnehmerdaten. Darüber hinaus bezieht sich das Regelwerk der EU zu elektronischen Beweismitteln ausschließlich auf Daten, die sich im Besitz von Diensteanbietern befinden, und befasst sich nicht mit der Herausforderung der Verschlüsselung. Ohne operative Maßnahmen für einen rechtmäßigen Datenzugang besteht daher die Gefahr, dass eine wirksame Strafverfolgung nicht gewährleistet ist. 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. In Fällen, in denen eine solche richterliche Genehmigung aufgrund der Sensibilität der betreffenden Daten erforderlich ist, ist sie in der Regel integraler Bestandteil des geltenden rechtlichen und operativen Rahmens. Der Datenzugang muss unter uneingeschränkter Achtung der Grundrechte sowie der Rechtsprechung des Gerichtshofs der Europäischen Union (EuGH) und der diesbezüglichen Urteile des Europäischen Gerichtshofs für Menschenrechte sowie der geltenden Verfahrensgarantien gewährleistet werden.

---

[3] *Siehe E-evidence – cross-border access to electronic evidence – European Commission (europa.eu) (Elektronische Beweismittel – grenzüberschreitender Zugang zu elektronischen Beweismitteln – Europäische Kommission). Die neuen Vorschriften treten am 17. August 2023 in Kraft und gelten ab dem 17. Februar 2026, was die Richtlinie betrifft, und ab dem 17. August 2026, was die Verordnung betrifft.*

www.parlament.gv.at

Diese Herausforderung steht seit langem auf der politischen Tagesordnung. So haben unter anderem der Europäische Rat, der Rat[4], das Europäische Parlament[5], der EuGH und die EU-Agenturen bei mehreren Gelegenheiten Schlussfolgerungen zu verschiedenen rechtlichen und politischen Aspekten des Zugangs zu elektronischen Kommunikationsdaten, einschließlich Verkehrs- und Standortdaten (Metadaten), und ganz allgemein zu elektronischen Beweismitteln erörtert und formuliert.
Der Europäische Rat forderte bereits in seinen Schlussfolgerungen vom 22./23. Juni 2017[6], „die Herausforderungen im Zusammenhang mit Systemen anzugehen, die Terroristen Kommunikationsmöglichkeiten bieten, zu denen die zuständigen Behörden keinen Zugang haben, einschließlich Ende-zu-Ende-Verschlüsselung; gleichzeitig gilt es aber, die Vorteile zu wahren, die diese Systeme für den Schutz der Privatsphäre, den Datenschutz und den Schutz der Kommunikation bieten“ und hob hervor, dass „ein effektiver Zugang zu elektronischen Beweismitteln für die Bekämpfung von schwerer Kriminalität unabdingbar ist“.

In der EU-Strategie zur Bekämpfung der organisierten Kriminalität 2021-2025 wird betont, wie wichtig der Zugriff auf elektronische Kommunikationsdaten für die Bekämpfung der organisierten Kriminalität ist, und wie wichtig es ist, die Strafverfolgung und die Justiz für das digitale Zeitalter zu rüsten.[7] Der Datenzugang ist auch für alle EMPACT-Prioritäten bei der Bekämpfung der schweren und organisierten Kriminalität für den Zeitraum 2022-2025 von entscheidender Bedeutung;[8] in der EU-Strategie für eine Sicherheitsunion wird erklärt, dass die Kommission Maßnahmen zur Verbesserung der Strafverfolgungskapazitäten bei digitalen Ermittlungen prüfen wird.[9] Im Jahr 2023 legte der schwedische Ratsvorsitz das Dokument „Law Enforcement Operational Needs for Lawful Access to Communications (LEON)“[10] (Operativer Bedarf der Strafverfolgungsbehörden für einen rechtmäßigen Zugang zu Kommunikation (LEON)) vor, das eine umfassende Liste des operativen Bedarfs der Strafverfolgungsbehörden in Bezug auf Kommunikationsnetze und -dienste enthält.[11]

---

4 10007/16, *Schlussfolgerungen des Rates zur Verbesserung der Strafjustiz im Cyberspace.*
5 ABl. 2018/C 346/04, *Entschließung des Europäischen Parlaments vom 3. Oktober 2017 zur Bekämpfung der Cyberkriminalität.*
6 Dok. EUCO 8/17.
7 *Mitteilung der Kommission über eine EU-Strategie zur Bekämpfung der organisierten Kriminalität 2021-2025*, COM(2021)170 final vom 14. April 2021.
8 Dok. 8665/21.
9 *Mitteilung der Kommission zu der EU-Strategie für eine Sicherheitsunion*, COM(2020) 605 final vom 24. Juli 2020.
10 LEON 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.
11 *Mitteilung des Ratsvorsitzes mit dem Titel „Law Enforcement Operational Needs for Lawful Access to Communications (LEON)“ (Operativer Bedarf der Strafverfolgungsbehörden für einen rechtmäßigen Zugang zu Kommunikation (LEON))*, Dok. 6050/23 vom 16. Februar 2023.

www.parlament.gv.at

Um Möglichkeiten für das weitere Vorgehen auszuloten, hat der schwedische Vorsitz in Zusammenarbeit mit dem spanischen und dem belgischen Vorsitz, die auf den schwedischen Vorsitz folgten, im Juni 2023 eine Hochrangige Gruppe für den Zugang zu Daten für eine wirksame Strafverfolgung ins Leben gerufen (im Folgenden „Hochrangige Gruppe"), die sich aus hochrangigen Vertretern der Mitgliedstaaten, der Kommission, der einschlägigen Einrichtungen und sonstigen Stellen der EU und dem EU-Koordinator für die Terrorismusbekämpfung zusammensetzt.[12] Sie wird gemeinsam von der Kommission und dem turnusmäßig wechselnden Vorsitz des Rates der EU geleitet und hat die Herausforderungen analysiert, denen die Strafverfolgungsbehörden in der Union bei ihrer täglichen Arbeit im Zusammenhang mit dem Datenzugang begegnen; sie hat mögliche Lösungen und Empfehlungen zu deren Überwindung ermittelt mit dem Ziel, die Verfügbarkeit wirksamer Strafverfolgungsinstrumente zur Bekämpfung der Kriminalität und zur Verbesserung der öffentlichen Sicherheit im digitalen Zeitalter unter uneingeschränkter Achtung der Grundrechte sicherzustellen.

Im Laufe ihrer Arbeit stellte die Hochrangige Gruppe zahlreiche Belege für den anhaltenden – wenn nicht sogar wachsenden – Mangel an einem wirksamem Datenzugang fest und wies wiederholt auf diesen Mangel hin. Darüber hinaus werden im Rahmen gezielter Konsultationen noch weitere Beweise gesammelt. Digital erzeugte, verarbeitete oder gespeicherte Kommunikationsdaten (sowohl Metadaten als auch Inhaltsdaten) sind ein wichtiger Bestandteil moderner strafrechtlicher Ermittlungen.[13] Im Zuge dessen, dass Kriminelle immer mehr auf Online-Dienste angewiesen sind, haben sich die Datenanfragen an Anbieter von Online-Diensten zwischen 2017 und 2022 verdreifacht.[14]

---

12 *Commission decision setting up a high-level group on access to data for effective law enforcement* (Beschluss der Kommission zur Einsetzung einer Hochrangigen Gruppe für den Zugang zu Daten für eine wirksame Strafverfolgung), C(2023)3647 vom 6. Juni 2023.

13 Folgenabschätzung zu dem Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über Europäische Herausgabeanordnungen und Sicherungsanordnungen für elektronische Beweismittel in Strafsachen und Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zur Festlegung einheitlicher Regeln für die Bestellung von Vertretern zu Zwecken der Beweiserhebung in Strafverfahren, COM(2018) 225 final, COM(2018) 226 final, SWD(2018) 119 final.

14 SIRIUS-Bericht 2023, https://www.eurojust.europa.eu/sites/default/files/assets/sirius-eueesr-2023.pdf, S. 69.

www.parlament.gv.at

Die Hochrangige Gruppe vertritt die Auffassung, dass die Strafverfolgungsbehörden mit zunehmenden operativen Herausforderungen konfrontiert sind, wenn sie einen rechtmäßigen Zugang auf digital erzeugte, verarbeitete oder gespeicherte Daten in einem lesbaren Format anstreben. Bei der jüngsten jährlichen Umfrage des SIRIUS-Projekts zum grenzüberschreitenden Zugang zu elektronischen Beweismitteln nannten 47 % der Befragten den Mangel an Vorratsdatenspeicherung als die größte Herausforderung, mit der sie konfrontiert waren;[15] bereits im Jahr 2018 wurde geschätzt, dass bis 2019 mehr als 22 % der weltweiten Nachrichtenübermittlung Ende-zu-Ende-verschlüsselt und für die Strafverfolgung nicht zugänglich sein würden.[16] Die Hochrangige Gruppe stellte fest, dass das Fehlen eines angemessenen Rechtsrahmens für die rechtmäßige Überwachung nicht herkömmlicher Telekommunikationsdienste auch für Strafverfolgungsmaßnahmen erhebliche Folgen hat: Mehr als 90 % der Nachrichten werden über solche Over-the-Top-Dienste (OTT) abgewickelt.

Angesichts dieser Erkenntnisse hat die Hochrangige Gruppe vor dem Hintergrund technologischer Entwicklungen strategische, zukunftsorientierte Empfehlungen zur Bewältigung derzeitiger und zukünftiger Herausforderungen formuliert, die ein umfassendes EU-Konzept zur Sicherstellung des Datenzugangs für eine wirksame Strafverfolgung ermöglichen. Diese Empfehlungen wurden von den Sachverständigen der Arbeitsgruppen der Hochrangigen Gruppe formuliert, die von den Mitgliedstaaten und den einschlägigen Einrichtungen und sonstigen Stellen der EU ausgewählt wurden. Zu den Sachverständigen gehörten hauptsächlich Vertreter von Strafverfolgungs- und Justizbehörden, aber auch Fachleute für Cybersicherheit und Datenschutzexperten.

Die Empfehlungen, die nachfolgend in diesem Bericht aufgeführt sind, wurden im Zusammenhang mit den drei Anwendungsfällen formuliert, nach denen die Arbeitsgruppen organisiert waren. Die Empfehlungen wurden den jeweiligen Arbeitsbereichen zugeordnet und von der Hochrangigen Gruppe auf ihrer 4. Plenartagung vom 21. Mai 2024 gebilligt. In einer zweiten Phase werden diese Empfehlungen umgesetzt und einer Bewertung ihrer Durchführbarkeit in rechtlicher, technischer und finanzieller Hinsicht sowie unter Berücksichtigung, dass im Rahmen des EU-Haushalts nur begrenzte Haushaltsmittel und Humanressourcen zur Verfügung stehen, unterzogen, damit im Herbst 2024 ein Abschlussbericht vorgelegt werden kann.

---

15 Ebenda, S. 46.

16 https://www.csis.org/blogs/strategic-technologies-blog/scoping-law-enforcements-encrypted-messaging-problem.

www.parlament.gv.at

Wichtigste Faktoren für die Empfehlungen

Die oben wiedergegebenen Beiträge und ausführliche Beratungen in drei Plenarsitzungen der Hochrangigen Gruppe, neun Sitzungen der Sachverständigengruppe und einer öffentlichen Konsultationssitzung sowie schriftliche Beiträge führten zur Ermittlung der wichtigsten Problemfaktoren, die den oben dargelegten Herausforderungen zugrunde liegen und mit denen die Empfehlungen begründet werden.

In Bezug auf den **Zugang zu Daten, die auf dem Gerät eines Nutzers verbleiben**, nannte die Hochrangige Gruppe folgende Hauptprobleme: mangelnde grenzüberschreitende Zusammenarbeit bei der Strafverfolgung im Hinblick auf die gemeinsame Nutzung digitaler forensischer Instrumente; die unzureichende Zusammenarbeit zwischen den Strafverfolgungsbehörden und den einschlägigen Anbietern, Herstellern und Lieferanten von Hardware und Software, wodurch der Zugang zu den unverschlüsselten Daten erschwert wird; die Schwierigkeit, einen rechtmäßigen Zugang zum Gerät eines Nutzers zu erhalten und, selbst wenn der Zugang möglich ist, die verfügbaren Daten und Metadaten zu extrahieren und zu entschlüsseln, um verständliche Informationen zu erhalten, die für Ermittlungen dienlich sein und als zulässige Beweismittel vor Gericht vorgelegt werden können.

Die Hochrangige Gruppe hält das Tempo der technologischen Entwicklungen in Bezug auf die **Verschlüsselung** von Informationen auf Geräten für so schnell, dass die vorhandenen Entschlüsselungsinstrumente und -techniken im Begriff sind, unwirksam zu werden. Dies gilt insbesondere für Fälle, in denen Verdächtige und organisierte kriminelle Vereinigungen speziell konzipierte Kommunikationsmittel und -netze nutzen. Die Zeit, die für die Entschlüsselung der von Geräten extrahierten Daten benötigt wird, ist ebenfalls ein großes Problem: Die Sachverständigen berichteten, dass es Fälle gibt, in denen dies bis zu zwei Jahre dauern könnte. Der Schwierigkeitsgrad, der bei der Entschlüsselung von speziell für ausschließlich kriminelle Zwecke konzipierte und vermarktete Geräte auftritt, ist noch höher und stellt die digitalen forensischen Dienste in allen Mitgliedstaaten gleichermaßen vor weitere Herausforderungen.

Dennoch ist es wichtig, dass bei technischen Lösungen, die es den Behörden ermöglichen, von ihren Ermittlungsbefugnissen Gebrauch zu machen, alle Vorteile der Verschlüsselung aus Gründen des Datenschutzes, der Privatsphäre, der Cybersicherheit und der nationalen Sicherheit gewahrt bleiben. Dieser Grundsatz der „Sicherheit durch Verschlüsselung und Sicherheit trotz Verschlüsselung“ war ein Kerngedanke der Beratungen der Hochrangigen Gruppe; künftige technische Lösungen oder Instrumente, die entwickelt werden, dürfen nicht dazu führen, dass Verschlüsselungstechnologien für die Kommunikation anderer Nutzer, die nicht einer Maßnahme des rechtmäßigen Zugangs unterliegen, geschwächt oder untergraben werden.

www.parlament.gv.at

Ein zentrales Problem, das von der Hochrangigen Gruppe angesprochen wurde, ist der **Mangel an Mechanismen für die grenzüberschreitende Zusammenarbeit bei der Strafverfolgung** im Hinblick auf die gemeinsame Nutzung digitaler forensischer Instrumente zwischen den Mitgliedstaaten, da diese häufig mit unterschiedlichen Lösungen für ähnliche technische Probleme arbeiten. Europol betreibt zwar ein internes Register für Instrumente, das die nationalen Strafverfolgungsbehörden konsultieren und nutzen können; es ist jedoch davon auszugehen, dass die Mitgliedstaaten Zugang zu weiteren Instrumenten und speziell konzipierter Entschlüsselungssoftware haben. Sie unterlassen es jedoch, diese weiterzugeben, entweder weil es an Vertrauen und Kommunikation zwischen den einschlägigen digitalen forensischen Diensten mangelt oder weil ihnen die Weitergabe gesetzlich nicht gestattet ist, häufig aufgrund von Bedenken hinsichtlich der nationalen Sicherheit.

Die Hochrangige Gruppe war sich darin einig, dass **Netzwerke** wie das Europäische Netz der kriminaltechnischen Institute (ENFSI[17]), die sich mit der Koordinierung und dem Wissensaustausch in Bezug auf digitale forensische Methoden, Instrumente und bewährte Verfahren befassen, für Fachkräfte der digitalen Forensik in der gesamten EU von entscheidender Bedeutung sind. Solche Netze bestehen bereits, doch um die Kommunikation und die Zusammenarbeit zwischen den digitalen forensischen Abteilungen der verschiedenen Mitgliedstaaten zu verbessern, sollten sie weiter unterstützt und erfasst werden, um sowohl mehr Austausch von Wissen als auch eine intensivere gemeinsame Nutzung von Instrumenten zu fördern[18], und zwar mit Unterstützung durch ein zentralisiertes System. Die Hochrangige Gruppe wies ferner darauf hin, dass die Kosten kommerzieller digitaler forensischer Instrumente in den Mitgliedstaaten ein erhebliches Hindernis darstellen und dass auf EU-Ebene weitere Forschungsarbeiten und Instrumente entwickelt und bereits bestehende Mechanismen wie die Europäische Vereinigung zur Entwicklung von Technologien zur Bekämpfung der Cyberkriminalität (European Anti Cybercrime Technology Development Association – EACTDA) und das Instrumentenregister von Europol für ihre Verbreitung genutzt werden sollten.[19] Die Bewertung und Zertifizierung handelsüblicher Instrumente war ein weiterer wiederkehrender Beratungsgegenstand,[20] und die Hochrangige Gruppe war sich weitgehend darin einig, dass die Einführung eines Mechanismus oder Systems, mit dem sichergestellt wird, dass diese Instrumente die Rechenschaftspflicht und die forensischen Normen in der Union einhalten, berechtigt ist. Eine Bewertung und eine Zertifizierung sind erforderlich, um zu gewährleisten, dass die Technologien den Anforderungen an die Vertrauenswürdigkeit (z. B. Anforderungen an die Datenintegrität während des gesamten digitalen forensischen Prozesses) entsprechen, unabhängig davon, ob der Hersteller innerhalb oder außerhalb der EU niedergelassen ist.

---

17 https://enfsi.eu/.
18 Siehe Empfehlung 1.
19 Siehe Empfehlungen 3 und 4.
20 Siehe Empfehlung 5.

www.parlament.gv.at

Zu den von der Hochrangigen Gruppe ermittelten Problemen gehörte auch ein **Rückgang der Kommunikation** zwischen den Strafverfolgungsbehörden und den Anbietern und Lieferanten von Hardware und Software; infolgedessen stoßen die Strafverfolgungsbehörden auf Schwierigkeiten, wenn es darum geht, wie sie mit der Industrie zusammenarbeiten können, um Zugang zu Daten auf beschlagnahmten Geräten zu erhalten. Die Hochrangige Gruppe stellte fest, dass sich mangelnde Kenntnisse auf die Interaktionen der Strafverfolgungsbehörden mit den Herstellern von Hardware und Software auswirken. Der Rückgang der Kommunikation zwischen den Strafverfolgungsbehörden und der Industrie hat auch dazu geführt, dass weniger Protokolle für den rechtmäßigen Zugang zu Daten auf Geräten der Nutzer festgelegt wurden. Die Hochrangige Gruppe wies darauf hin, dass die mangelnde Beteiligung der Strafverfolgungsbehörden an den Normungsgremien die Möglichkeit beeinträchtigt, die Produktprotokolle und die technische Architektur so zu gestalten, dass ihre Bedenken und technischen Anforderungen frühzeitig bei der Entwicklung künftiger technologischer Normen berücksichtigt werden.[21]

Als letztes zentrales Problem befasste sich die Hochrangige Gruppe damit, dass ohne eine freiwillige Zusammenarbeit die Fähigkeit der Strafverfolgungsbehörden zur Durchführung gründlicher Ermittlungen durch **das Fehlen von Verpflichtungen der Industrie** zur Zusammenarbeit bei Ersuchen der Strafverfolgungsbehörden um Daten, die auf dem Gerät eines Nutzers verbleiben, beeinträchtigt wird. Sie gelangte zu der Feststellung, dass es keinen umfassenden Überblick über die bestehenden Verpflichtungen auf Ebene der Mitgliedstaaten gibt.[22]

Was den **Zugang zu Daten, die im System eines Diensteanbieters verbleiben,** betrifft, so dreht sich das erste zentrale Problem, mit dem die Strafverfolgungsbehörden konfrontiert sind, um Diskrepanzen zwischen den einzelnen innerstaatlichen Rechtsrahmen zur Regelung der Vorratsdatenspeicherung innerhalb der Systeme der Anbieter und der Dauer dieser Speicherung.

---

21 Siehe Empfehlung 12.
22 Siehe Empfehlung 25.

www.parlament.gv.at

Die Sachverständigen hoben insbesondere hervor, dass die **Rechtsvorschriften über die Vorratsdatenspeicherung** in der EU derzeit keinerlei Harmonisierung aufweisen und dass es schwierig ist, die vom EuGH genannten Kriterien zu erfüllen, die allgemeine und unterschiedslose Vorratsspeicherung von Verkehrs- und Standortdaten unter bestimmten Umständen auf die Bekämpfung schwerwiegender Sicherheitsbedrohungen zu beschränken und nur eine gezielte Vorratsspeicherung solcher Daten zur Bekämpfung schwerer Kriminalität zu ermöglichen. Insbesondere erweist sich die Umsetzung des Konzepts der gezielten Vorratsdatenspeicherung für die Mitgliedstaaten als sehr schwierig, was zum Teil auch darauf zurückzuführen ist, dass einige der Kriterien auf Technologien beruhen, die seit dem Erlass der Urteile weiterentwickelt wurden,[23] und dass nach wie vor unklar ist, auf welche Arten von Daten für nicht schwere Straftaten zugegriffen werden kann.

Die Hochrangige Gruppe kam zu dem Schluss, dass ein harmonisierter Ansatz für die Vorratsdatenspeicherung auf EU-Ebene unerlässlich für wirksame Ermittlungen, insbesondere in grenzüberschreitenden Fällen, und für die Zulässigkeit von Beweismitteln vor Gericht ist. Sie erörterte auch, wie das Fehlen von Verpflichtungen zur Vorratsdatenspeicherung die Wirksamkeit der neuen Vorschriften über elektronische Beweismittel beeinträchtigen kann, da Verkehrsdaten, die Gegenstand europäischer Sicherungs- oder Herausgabeanordnungen sind, möglicherweise nicht verfügbar sind.

Die Hochrangige Gruppe teilte die Auffassung, dass jede Lösung für die derzeitigen Herausforderungen technologieneutral sein muss, um künftige technische Entwicklungen abzudecken. Es wurde betont, dass solche Lösungen die Schaffung von Verpflichtungen für alle Diensteanbieter, einschließlich der OTT, beinhalten müssen; diese sollten verpflichtet sein, Anfragen der Strafverfolgungsbehörden zu beantworten und für mehr Transparenz in Bezug auf die Daten, die sie für geschäftliche Zwecke erheben, zu sorgen. Eine solche Regelung könnte durch **Rechtsvorschriften oder nicht zwingendes Recht** erreicht werden, wobei erstere bevorzugt werden.[24]

---

[23] So waren beispielsweise Technologien wie dynamische IP-Adressen und „Carrier Grade Net Address Translation“ (CGNAT) zum Zeitpunkt der Veröffentlichung der Urteile des EuGH, in denen die Vorratsdatenspeicherung auf der Grundlage eines geografischen Bezugs vorgeschlagen wurde, noch nicht vollständig entwickelt (siehe Referenzfälle Digital Rights Ireland, 2014 und Tele2 Sverige AB, 2016).

[24] Siehe Empfehlung 27.

www.parlament.gv.at

Vor dem Hintergrund der Rechtsprechung zur Vorratsdatenspeicherung erörterte die Hochrangige Gruppe die praktische Anwendung der **gezielten Vorratsspeicherung** und betonte die Schwierigkeiten bei der Umsetzung der Anforderungen des Gerichtshofs (d. h. gezielte Vorratsspeicherung auf der Grundlage geografischer Kriterien und Kategorien von Personen). Die Umsetzung der Anforderungen des Gerichtshofs wurde von den Sachverständigen in Bezug auf die Grundrechte (wegen der Diskriminierung von Kategorien von Personen oder der Lage) als problematisch angesehen, einerseits aus operativer Sicht, da die Zielgerichtetheit der Datenerhebung die Fähigkeit, auf wichtige Informationen für Ermittlungen zuzugreifen, drastisch einschränkt, und andererseits aus Sicht der technischen Durchführung für die Betreiber. Angesichts dieser Überlegungen erklärten viele Sachverständige, dass sich eine EU-Regelung nicht nur auf die Speicherung, sondern auch auf den Zugang konzentrieren sollte. Einige Sachverständige vertraten insbesondere die Auffassung, dass für eine Differenzierung der Fristen für den Zugang zu gespeicherten Daten das einzige Kriterium für die Regelung der Vorratsdatenspeicherung die Kategorien von Straftaten sein sollte und dass Lösungen für einen sehr gezielten Zugang auf der Grundlage anderer Kriterien konzipiert werden sollten.[25] Einige andere Sachverständige äußerten jedoch Bedenken, wie diese Maßnahmen mit der Rechtsprechung des EuGH im Einklang stehen würden, da die Rechtsprechung des EuGH sowohl für die Vorratsdatenspeicherung als auch für den Datenzugang gilt.

Zu den festgestellten Problemen zählen auch die Schwierigkeiten der Strafverfolgungsbehörden in Bezug auf die **Arten der** von Diensteanbietern **gespeicherten Metadaten**. Soweit rechtliche Verpflichtungen bestehen, lassen sie den Anbietern von Kommunikationsdiensten zuweilen Flexibilität in Bezug auf die Arten von Metadaten, die gespeichert werden sollten; dies führt zu einer Vielzahl verfügbarer Daten mit unterschiedlichem Grad an Nützlichkeit als Ermittlungshinweise. Die Hochrangige Gruppe vertrat die Auffassung, dass die EU ein Mindestmaß an Vorratsspeicherung verlangen sollte (zumindest der Daten, die zur Identifizierung eines Nutzers erforderlich sind), das den Betreibern auf EU-Ebene auferlegt werden sollte.[26] Die Hochrangige Gruppe kam ferner überein, dass Diensteanbieter, die verschlüsselte Dienste anbieten, verpflichtet sein müssen, die Mittel zu finden, um Daten, die von Strafverfolgungs- und Justizbehörden rechtmäßig angefragt werden, auf verständliche Art und Weise bereitzustellen.[27]

---

25 Siehe Empfehlung 29.
26 Siehe Empfehlung 27 Buchstabe v.
27 Siehe Empfehlung 27 Buchstabe iii.

www.parlament.gv.at

Die Verlagerung von herkömmlichen Kommunikationsanbietern hin zur Nutzung von **OTT** ist ein wichtiger Faktor für die Schwierigkeiten, mit denen die Strafverfolgungsbehörden konfrontiert sind, wenn sie versuchen, auf Daten zuzugreifen, die in den Systemen der Diensteanbieter gespeichert sind. OTT fallen zwar in den Anwendungsbereich des Europäischen Kodex für die elektronische Kommunikation (EKEK), unterliegen aber keinen vergleichbaren Lizenzierungssystemen, die möglicherweise Verpflichtungen nach sich ziehen können. Die Sachverständigen erörterten die dringende Notwendigkeit von Vorschriften, mit denen die OTT verpflichtet werden, Daten auch dann zu speichern, wenn sie in unterschiedlichen Gebieten gerichtlicher Zuständigkeiten ansässig sind. Die Folge des Fehlens solcher Vorschriften ist mangelnde Klarheit und Rechtssicherheit und führt zur Nichteinhaltung der Vorschriften durch die OTT. Darüber hinaus gibt es bestimmte OTT, die zuweilen überhaupt keine Daten speichern.

Die Hochrangige Gruppe war sich darin einig, dass **Transparenz** in Bezug auf die Daten erforderlich ist, die von Kommunikationsanbietern erzeugt, verarbeitet und gespeichert werden; zu diesen Anbietern gehören insbesondere OTT und andere Dienste, die „Kommunikationsdienste“ anbieten (wie Automobilhersteller).[28] Die Hochrangige Gruppe erörterte Instrumente, mit denen die Einhaltung der Vorschriften im Vorfeld einer Tätigkeit auf dem EU-Markt durchgesetzt werden kann.[29] Die Sachverständigen erörterten die Möglichkeit, Rechtsvorschriften über Daten zu erlassen, die sich bereits für Geschäftszwecke im Besitz von Anbietern befinden.[30]

In diesem Zusammenhang waren sich die Sachverständigen darin einig, dass **Mechanismen für die Zusammenarbeit** mit dem Privatsektor eingerichtet werden müssen, um die Transparenz zu erhöhen, und sie schlugen mehrere Möglichkeiten dazu vor, unter anderem durch Vereinbarungen[31] und durch die Stärkung und umfassende Nutzung bestehender Strukturen wie SIRIUS, EJN[32] (Europäisches Justizielles Netz für Strafsachen) und/oder EJCN[33] (Europäisches Justizielles Netz gegen Cyberkriminalität).

---

28 Siehe Empfehlung 17.
29 Siehe Empfehlung 30.
30 Siehe Empfehlung 31.
31 Siehe Empfehlung 14.
32 Das Europäische Justizielle Netz für Strafsachen (EJN) ist ein Netz nationaler Kontaktstellen zur Erleichterung der justiziellen Zusammenarbeit in Strafsachen.
33 Siehe Empfehlung 13.

www.parlament.gv.at

Die Hochrangige Gruppe hielt eine verstärkte Zusammenarbeit für sinnvoll, auch bei der Festlegung standardisierter Formate für die Vorratsdatenspeicherung.[34] Zwar gibt es eine unter der Schirmherrschaft des Europäischen Instituts für Telekommunikationsnormen (ETSI) entwickelte Norm für herkömmliche Telekommunikationsmetadaten, doch wird sie in den Mitgliedstaaten selbst bei Telekommunikationsanbietern nicht allgemein angewandt, und es besteht keine Einigung über ein standardisiertes Format für die Datenübermittlung von OTT an Strafverfolgungsbehörden. Dies erhöht die Komplexität der Datenanalyse, falls überhaupt Daten zur Verfügung gestellt werden können.

Die **Normierung** sollte fortgesetzt werden, um eine harmonisierte Kategorisierung der Daten, die gespeichert und abgerufen werden sollen, zu gewährleisten, aber auch um sichere Kanäle für den Austausch zwischen zuständigen Behörden und Diensteanbietern einzurichten. Die Hochrangige Gruppe erörterte diesbezüglich mehrere Möglichkeiten, wobei sie sich insbesondere auf die Stärkung einer koordinierten Beteiligung von Strafverfolgungsvertretern in den einschlägigen Normungsgremien konzentrierte.[35]

Die meisten Mitgliedstaaten verfügen über spezielle nationale Rechtsrahmen für den **Echtzeitzugang zu Kommunikationsdaten**, die nach wie vor ein wesentliches Instrument für die Bekämpfung der Kriminalität, einschließlich der Online-Kriminalität und der organisierten Kriminalität sowie des Terrorismus, sind.

In Bezug auf nicht herkömmliche Dienstanbieter können sich die Strafverfolgungsbehörden jedoch nicht auf einen durchsetzbaren und harmonisierten Rahmen stützen. Zwar haben einige Mitgliedstaaten Regelungen erlassen, die die OTT dazu verpflichten, auf rechtmäßige Anträge auf einen solchen Zugang zu reagieren, doch ist die **Umsetzung** zwischen den Anbietern von Kommunikationsdiensten und den OTT in Bezug auf den Echtzeitzugang zu Daten **uneinheitlich**; in der Regel erfüllen die OTT solche Verpflichtungen aus rechtlichen und technischen Gründen nicht.

---

34 Siehe Empfehlungen 15 und 16.

35 Siehe Empfehlung 20.

www.parlament.gv.at

Die Sachverständigen waren sich darin einig, dass eines der Hauptziele im Hinblick auf durchsetzbare Verpflichtungen zur rechtmäßigen Überwachung darin bestehen würde, **gleiche Wettbewerbsbedingungen für Anbieter von Kommunikationsdiensten[36] und andere Arten von Anbietern elektronischer Kommunikation zu schaffen**; die rechtmäßige Überwachung muss gesetzlich vorgesehen und von Gerichten oder unabhängigen Verwaltungsbehörden im Einklang mit technischen Normen und unter uneingeschränkter Einhaltung des Datenschutzes und der Privatsphäre sowie von Cybersicherheits- und Interoperabilitätsmaßnahmen genehmigt werden. Die Sachverständigen verwiesen wiederholt darauf, dass die rechtmäßige Überwachung elektronischer Kommunikationsdienste die bevorzugte Maßnahme für den Zugriff auf Daten in Echtzeit sein sollte. Solche Vorschriften für die rechtmäßige Überwachung sollten auf Grundsätzen beruhen, die derzeit für herkömmliche Kommunikationsanbieter gelten, z. B. in Bezug auf die Aufsicht und die Zusammenarbeit mit Kommunikationsbetreibern, aber auch in Bezug auf die Fähigkeit, auf unverschlüsselte Daten zuzugreifen, wenn dies von den Justizbehörden für notwendig und verhältnismäßig erachtet wird.[37]

Unterschiede zwischen den einzelnen innerstaatlichen Rechtsrahmen der EU-Mitgliedstaaten für die Überwachung von Metadaten oder Inhaltsdaten stellen die Strafverfolgung in Fällen mit grenzüberschreitenden Elementen vor Herausforderungen. So kann es beispielsweise für Strafverfolgungsbehörden schwierig sein, die Echtzeit-Kommunikation zwischen zwei Bürgern in ihrem Land zu überwachen, die einen Kommunikationsdienst nutzen, der in einem anderen EU-Mitgliedstaat mit unterschiedlichen Verfahrensvorschriften für die Live-Überwachung betrieben wird. Die Sachverständigen erörterten die Möglichkeit, diese Probleme auf EU-Ebene zu lösen, und führten verschiedene Maßnahmen aus, die zu diesem Zweck umgesetzt werden könnten, z. B. legislative Maßnahmen.[38] Die Rechtsunsicherheit, die sich aus den unterschiedlichen Anforderungen der nationalen Rechtsrahmen in Bezug auf die Überwachung ergibt, war ein zentrales Diskussionsthema der Sachverständigen, die über die Notwendigkeit berieten, sich mit Fragen wie der territorialen Anwendung bestimmter Verpflichtungen zu befassen, die zu Rechtskollisionen und Verzögerungen oder administrativen Hindernissen für Ermittlungen führt.[39]

Neben den Problemen, die sich aus dem Mangel an harmonisierten Rechtsvorschriften in den Mitgliedstaaten ergeben, erörterten die Sachverständigen auch die Tatsache, dass **die fehlende Kenntnis des genauen Standorts der Nutzer und der Daten häufig die Bestimmung des territorialen Zusammenhangs einer Straftat erschwert.**

---

36 Herkömmliche Telekommunikationsanbieter im Sinne der ETSI-Definition, d. h. Infrastruktureigentümer.

37 Siehe Empfehlung 37.

38 Siehe Empfehlung 38.

39 Siehe Empfehlung 39.

www.parlament.gv.at

Die Sachverständigen einigten sich zwar darauf, die Europäische Ermittlungsanordnung (EEA) als Instrument für die Beantragung einer Überwachung durch einen anderen Mitgliedstaat und für den Austausch von Beweismitteln, die durch Überwachung erhoben wurden, weiter zu nutzen, erörterten aber auch deren Grenzen, z. B in Bezug darauf, dass sie über die Mitgliedstaaten hinweg nur teilweise anwendbar ist.[40]

Bei den Beratungen wurde das Konzept der territorialen Zuständigkeit für Daten angesprochen. Die Sachverständigen vertraten die Auffassung, dass es in Fällen mit nationalem Zusammenhang (z. B. eine Straftat wird in einem Mitgliedstaat durch einen im selben Mitgliedstaat befindlichen Täter verübt) möglich sein sollte, dass eine staatliche Behörde Überwachungsmaßnahmen ergreift – im Rahmen des nationalen Verfahrensrechts, nach dem Anforderungen und Garantien festgelegt sind –, ohne auf ein Instrument der grenzüberschreitenden Zusammenarbeit zurückzugreifen. Für den Fall, dass es erforderlich sein sollte, Rechtskollisionen mit anderen Gebieten gerichtlicher Zuständigkeiten zu überwinden, erörterten die Sachverständigen mögliche Initiativen, die die EU ergreifen könnte, wobei diese sich an der Verordnung über elektronische Beweismittel orientieren und auch in bilateralen Abkommen mit Ländern wie den Vereinigten Staaten bestehen könnten, unterstützt durch weitere Analysen sowie eine Folgenabschätzung, bei der auch die Grundrechte und die Souveränität des Staates berücksichtigt werden.

Die Sachverständigen teilten die Auffassung, dass ein gewisses Maß an Harmonisierung auf EU-Ebene durch nicht zwingendes Recht (z. B. eine Empfehlung der Kommission) angestrebt werden könnte, und schlugen vor, dass auf der Grundlage des LEON-Dokuments gemeinsame operative Erfordernisse einer rechtmäßigen Überwachung entwickelt werden könnten.[41]

Aus technischer Sicht erörterten die Sachverständigen die **Notwendigkeit, Mechanismen und Infrastrukturen einzurichten, die mit der Echtzeitübertragung potenziell großer Mengen von Daten verschiedener Art bei der Überwachung vereinbar sind**.[42] In diesem Zusammenhang erörterten die Sachverständigen ausführlich die Vorteile der Normierung und mögliche Ansätze in diesem Bereich. Sie forderten eine stärkere Vertretung der nationalen Regierungen/Verwaltungen bei der Entwicklung von 5G/6G-Normen und der Kommunikation im Allgemeinen und betonten, dass sie in den wichtigsten Foren wie 3GPP, ETSI, ISO und ITU vertreten sein müssen. Die Unterstützung durch die Kommission, Europol oder andere Einrichtungen oder Stellen der EU wurde ebenfalls für notwendig erachtet.[43]

---

40 Siehe Empfehlung 40.
41 Siehe Empfehlung 21.
42 Siehe Empfehlung 9.
43 Siehe Empfehlung 20.

www.parlament.gv.at

Parallel dazu erörterten die Sachverständigen eingehend die Fälle im Zusammenhang mit nicht kooperativen Anbietern, um ihnen je nach Grad der Fahrlässigkeit gegebenenfalls verwaltungs- und/oder strafrechtliche Sanktionen auferlegen zu können.[44] Die Sachverständigen waren sich darin einig, dass dieser Unterschied bei jedem künftigen EU-Instrument in diesem Zusammenhang berücksichtigt werden sollte.[45] Es sollte auch dem EU-Besitzstand, insbesondere dem Gesetz über digitale Dienste, Rechnung tragen.

Die Sachverständigen erörterten auch Fälle von nicht kooperativen Anbietern; dabei teilten sie die Auffassung, dass **die Strafverfolgungsbehörden** ungeachtet der bestehenden Rechtsinstrumente in **bestimmten Fällen** (z. B. bei in erster Linie kriminellen Diensten wie EncroChat) **weiterhin auf die Nutzung von Schwachstellen** (d. h. eingreifende Maßnahmen) **zurückgreifen müssen**. Zwar bestand Einigkeit darüber, dass diese Fälle Ausnahme bleiben sollten und solche Lösungen alles andere als ideal sind, es jedoch wichtig ist, bei der Harmonisierung dieser Aspekte zusammenzuarbeiten, insbesondere im Hinblick auf die Einführung von Garantien[46] und – nach Möglichkeit – harmonisierten Regeln für die gegenseitige Zulässigkeit von Beweismitteln zwischen den Mitgliedstaaten, soweit dies erforderlich ist, um die gegenseitige Anerkennung gerichtlicher Urteile und Entscheidungen sowie die polizeiliche und justizielle Zusammenarbeit in Strafsachen zu erleichtern.[47] Die Sachverständigen hoben hervor, wie das Vorgehen der Behörden gegen Kriminelle, die Messaging-Systeme wie EncroChat oder Sky ECC nutzen, vor Gericht angefochten wird, und wiesen auf die Rechtsunsicherheit hin, die sich aus den unterschiedlichen Anforderungen in den nationalen Rechtsvorschriften in Bezug auf die Verwendung eines Überwachungsergebnisses in einem Mitgliedstaat als Beweismittel in einem anderen Mitgliedstaat ergibt.

Ein weiteres Thema, das als Problem erkannt und ausführlich erörtert wurde, betrifft den **Zugang zu Daten in lesbarem Format**.

Zusätzlich zu den Problemen beim Zugang zu Daten auf dem Gerät erhöht die Verschlüsselung die Komplexität des Zugriffs auf Echtzeit-Inhaltsdaten, und zwar sowohl für OTT bei der Einführung eines Ende-zu-Ende-Verschlüsselungsmechanismus als auch für herkömmliche Telekommunikationsbetreiber, wenn sie beispielsweise „Home Routing“ für 5G implementieren.

---

44 Siehe Empfehlung 33.
45 Siehe Empfehlung 34.
46 Siehe Empfehlung 10.
47 Siehe Empfehlung 42.

www.parlament.gv.at

Die Sachverständen erörterten ausführlich den **Zugang zu Inhaltsdaten trotz Verschlüsselung** und waren sich darin einig, dass die Strafverfolgungsbehörden Zugang zu unverschlüsselten Daten haben müssen. Sie betonten, dass technologische Lösungen umgesetzt werden können, wenn sie vorhanden sind, oder dass sie entwickelt werden sollten, um die Privatsphäre und den Datenschutz zu wahren, die Cybersicherheit zu gewährleisten und gleichzeitig gezielte rechtmäßige Zugangsmaßnahmen, auch in Bezug auf Inhaltsdaten, zu ermöglichen. Die Sachverständigen erörterten die Notwendigkeit einer Normung, um den operativen Anforderungen der Strafverfolgungsbehörden Rechnung zu tragen, insbesondere in neuen Telekommunikationsnormen wie 6G. Für die derzeitigen und künftigen Kommunikationstechnologien sollten Normen entwickelt werden, die einen rechtmäßigen Zugang ermöglichen, ohne die Privatsphäre, den Datenschutz und Cybersicherheitsmechanismen[48] zu schwächen. Dieser Ansatz, der die Bewertung und Zertifizierung von Systemen zur rechtmäßigen Überwachung umfassen soll, um zu gewährleisten, dass die Anforderungen in den Bereichen der Cybersicherheit, der Privatsphäre und des rechtmäßigen Zugangs tatsächlich erfüllt werden, eröffnet längerfristig und für künftige Technologien wie 6G eine Perspektive.

Die Sachverständigen äußerten den Wunsch, in Abstimmung mit Cybersicherheitsexperten **zunächst die technischen Aspekte** zu untersuchen. Sie stellten klar, dass die Herausforderungen der Verschlüsselung (und im weiteren Sinne der Echtzeitüberwachung) schon **ab der Gestaltung der Kommunikationstechnologie** angegangen werden müssen, insbesondere durch **die Entwicklung von Projekten, bei denen Experten für Technologie, Cybersicherheit, Privatsphäre, Normung und Sicherheit einbezogen sind.** Sie betonten, dass die Strafverfolgungsbehörden zur Erfüllung ihrer Aufgaben in der digitalen Welt einen vorab festgelegten rechtmäßigen Zugang zu lesbaren Daten im Einklang mit internationalen Instrumenten wie dem Budapester Übereinkommen und unter Wahrung der Cybersicherheitsanforderungen haben müssen. Zu diesem Zweck forderte die Hochrangige Gruppe die EU auf, einen Fahrplan aufzustellen und die Arbeit durch einen ständigen Strukturprozess zu koordinieren, der möglicherweise beim EU-Innovationszentrum für innere Sicherheit angesiedelt werden könnte.[49]

[48] Siehe Empfehlung 23.
[49] Siehe Empfehlung 22.

www.parlament.gv.at

In Bezug darauf gab es weitere besorgniserregende Elemente: die Nutzung erweiterter Kommunikationsdienste (Rich Communication Services – RCS) für den durchgehend verschlüsselten SMS-Austausch und die verstärkte 5G-Kommunikation für ankommende Roamingkunden (Inbound-Roamer) und Initiativen wie Apple Private Relay. Technologien wie diese schneiden herkömmliche Anbieter von Telekommunikationsdiensten von den wichtigsten Informationen ab, die ansonsten unverschlüsselt verfügbar wären, und wirken sich somit auf die Fähigkeit der Strafverfolgungsbehörden aus, auf Echtzeitdaten bei der Übertragung wirksam und rechtmäßig zuzugreifen. Die Sachverständigen erörterten diese Herausforderungen und betonten die Notwendigkeit, die legale Überwachungsfähigkeit der herkömmlichen Telekommunikationsbetreiber trotz 5G und 6G aufrechtzuerhalten, und sie forderten, die Zusammenarbeit mit Diensteanbietern auf EU-Ebene zu erleichtern.[50]

[50] Siehe Empfehlung 24.

www.parlament.gv.at

Empfehlungen der Hochrangigen Gruppe

In Bezug auf Maßnahmen zum Kapazitätsaufbau empfiehlt die Hochrangige Gruppe Folgendes:

1. Kartierung und Verknüpfung der **bestehenden Netze für digitale Forensik** bei gleichzeitiger Steigerung der Zugänglichkeit, Vermeidung von Überschneidungen und Förderung der Führungsrolle. In Bezug auf Letzteres sollte ein Sekretariat für die Netze eingerichtet werden, um die Verbreitung von Wissen unter den Sachverständigen zu vereinfachen; das Sekretariat sollte Mechanismen sondieren, mit denen sichergestellt wird, dass empfindliche Instrumente unter uneingeschränkter Achtung nationaler Vorschriften gemeinsam genutzt werden können.

2. Sondierung von **Mechanismen zur Bündelung von Wissen**, um sicherzustellen, dass Instrumente der digitalen Forensik in einem vertrauensvollen Umfeld zwischen den Mitgliedstaaten ausgetauscht werden können, unter Berücksichtigung der nationalen Vorschriften. Dazu könnte gehören, einen europäischen Ansatz für die Verwaltung und Offenlegung von Schwachstellen durch die Strafverfolgungsbehörden zu erforschen, und zwar auf der Grundlage bestehender bewährter Verfahren.

3. Entwicklung eines Mechanismus auf EU-Ebene für die **gemeinsame Beschaffung von Lizenzen für Instrumente der digitalen Forensik**, zur gemeinsamen Nutzung durch die Mitgliedstaaten.

4. Erhöhung der **Mittel für Forschung und Entwicklung in Bezug auf Instrumente für die Datenerfassung, Zugang zu unverschlüsselten Daten, einschließlich Entschlüsselungsfähigkeiten, und KI-gestützte Kapazitäten für Datenanalyse** mit klaren Zielvorgaben, und Förderung des Instrumentenarchivs von Europol als zentrale Plattform für die Verbreitung dieser Instrumente.

5. 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 Ermittlungs- und Strafverfolgungsverfahren (wie z. B. zusätzlicher unnötiger Aufwand).

6. Einrichtung eines speziellen Verfahrens für den **Austausch von Kapazitäten**, bei denen potenziell die Nutzung von Schwachstellen naheliegt, das die Bündelung von Wissen und Ressourcen ermöglichen würde, unter Wahrung der Vertraulichkeit und Sensibilität der Informationen.

www.parlament.gv.at

7. Vergrößerung der Anzahl von **Schulungsmöglichkeiten** für Sachverständige und Schaffung eines **Zertifizierungssystems auf EU-Ebene für Sachverständige der digitalen Forensik** (einschließlich für Entschlüsselung), um die Qualität und Einheitlichkeit der fachlichen Schulungen zu garantieren.

8. Investitionen zur Schließung der Lücke bei den technischen Kompetenzen im Bereich der Normung und zur Sensibilisierung – beides unterstützt durch den Abschluss von **Vereinbarungen mit Hochschulen** und anderen einschlägigen Institutionen.

9. Aufbau von **Mechanismen (Interoperabilität und Cybersicherheit) und Infrastrukturen (Bandbreite und Skalierbarkeit), die mit dem Echtzeittransfer von umfangreichen Datensätzen kompatibel sind**, wie jene, die erhoben werden, wenn die Behörden in einem Mitgliedstaat einen Antrag auf rechtmäßigen Zugang im Namen eines anderen Mitgliedstaats ausführen. Dies erfordert weitere Arbeit an der Normung von Datenstrukturen, an Vertrauensmechanismen und an der Datenfilterung, um zu vermeiden, dass für die Ermittlung(en) nicht relevante Daten übermittelt werden, und um den Datenschutzgrundsätzen der Zweckbindung, der Verhältnismäßigkeit und der Datenminimierung zu genügen, zusammen mit den Arbeiten auf EU-Ebene zur Gestaltung und Dimensionierung von Übermittlungsmethoden und der damit verbundenen Kosten.

10. Bessere Koordinierung der Arbeit – mit Unterstützung durch EU-Mittel – an einer **Methode zur Entwicklung, Handhabung und Nutzung von Maßnahmen des gezielten rechtmäßigen Zugangs** für Fälle, in denen der Zugang zu Daten durch die Zusammenarbeit mit Anbietern elektronischer Kommunikationsdienste nicht möglich ist. Angesichts der Sensibilität dieses Ansatzes sollte er einer richterlichen Genehmigung unterliegen und mit einem robusten Rahmen für die Zulässigkeit von Beweismitteln verbunden sein. Diese Fälle sollten Ausnahmen bleiben – d. h. die Strafverfolgungsbehörden sollten nur als letztes Mittel auf diese Instrumente zurückgreifen – und sie sollten einer obligatorischen Bewertung der Verhältnismäßigkeit unterliegen.

www.parlament.gv.at

In Bezug auf die Zusammenarbeit mit der Industrie und auf Normung empfiehlt die Hochrangige Gruppe Folgendes:

11. Schaffung einer **Plattform (nach dem Modell von SIRIUS[51])** für den Austausch von Instrumenten, bewährten Verfahren und Wissen darüber, wie der Zugang zu Daten von Produkteignern und Herstellern gewährt werden kann. Weiter aufbauend auf SIRIUS sollte das Mandat auf Hardware-Hersteller ausgeweitet werden, und es sollten Stellen der Strafverfolgungsbehörden für den Kontakt mit Herstellern von digitaler Hard- und Software geschaffen und kartiert werden.

12. 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.

13. Weitere Finanzierung, Ausweitung und **dauerhafte Einrichtung von EU-Strukturen** und Foren, einschließlich SIRIUS, EJN und/oder EJCN, zu folgenden Zwecken: a) Herstellung von Kontakten zwischen Praktikern und Diensteanbietern zur Unterstützung von Informationsaustausch, Kapazitätsaufbau und Schulung, b) Förderung eines dauerhaften Dialogs, unter anderem durch ein Forum oder eine unabhängige Behörde, bei dem Praktiker (Strafverfolgungsbehörden, Justiz und Diensteanbieter) zusammenkommen, um die Grundsätze und Modalitäten der Zusammenarbeit festzulegen. Dazu könnte die Schaffung und Unterstützung eines **zentralen Archivs von Instrumenten und Informationen** gehören, das den Austausch von Informationen über Rechtsprechung, Änderungen von Rechtsvorschriften und sonstigen Informationen ermöglicht, die für die Mitgliedstaaten und die Diensteanbieter relevant wären.

---

51 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 Europäischen Justiziellen Netz umgesetzt; es dient als zentraler Bezugspunkt in der EU für den Wissensaustausch zum grenzüberschreitenden Zugang zu elektronischen Beweismitteln. Das Projekt SIRIUS hilft den Ermittlern bei der Bewältigung sowohl der Komplexität als auch des Umfangs der Informationen in einem sich rasch wandelnden Online-Umfeld. Das Projekt bietet Produkte wie standardisierte Leitlinien zu Verfahren der Zusammenarbeit zwischen zuständigen Behörden und spezifischen Diensteanbietern. Daneben bietet SIRIUS unter anderem Ermittlungsinstrumente und Kontaktangaben für Diensteanbieter, und es bietet Möglichkeiten für den Erfahrungsaustausch mit Fachkollegen, sowohl online als auch persönlich.

www.parlament.gv.at

14. Annahme von **Vereinbarungen** durch die Mitgliedstaaten als wirksamer Mechanismus zur Förderung der Zusammenarbeit und Entwicklung eines gemeinsamen Verständnisses zwischen Diensteanbietern, staatlichen Stellen und Strafverfolgungsbehörden im Hinblick auf die Unterstützung der Anwendung nationaler Rechtsvorschriften, unter Verwendung von in bestimmten Mitgliedstaaten etablierten bewährten Verfahren.

15. Entwicklung von Datenformaten nach den **vom Europäischen Institut für Telekommunikationsnormen (ETSI)** oder anderen Normungsgremien **entwickelten Normen**, um die Interoperabilität zu fördern und die Nutzung durch alle Mitgliedstaaten zu erleichtern.

16. Schrittweise Ersetzung der von den einzelnen Diensteanbietern (und folglich den Behörden der jeweiligen Mitgliedstaaten) verwendeten spezifischen Formate durch einen horizontalen Ansatz, auf der Grundlage der vom ETSI oder anderen Normungsgremien für das Format der Anträge und Antworten entwickelten Normen. *[Die Kohärenz dieser Empfehlung mit den durch die Verordnung über elektronische Beweismittel festgelegten Vorschriften sollte weiter geprüft werden.]*

17. **Förderung von Transparenzvorschriften für Anbieter elektronischer Kommunikationsdienste** in Bezug auf die Daten, die sie im Zuge ihrer Geschäftstätigkeit verarbeiten, erzeugen oder speichern (wobei dies nicht notwendigerweise dieselben sind), sowie in Bezug auf die Unterrichtung der Strafverfolgungsbehörden darüber, welche Daten verfügbar sind, unter Berücksichtigung der durch die Vertraulichkeit der Ermittlungen gesetzten Grenzen. Sachverständige schlagen vor, dieses Ziel durch Kooperationsvereinbarungen mit Diensteanbietern oder – sofern erforderlich – durch die Festlegung verbindlicher Verpflichtungen zu erreichen. Mehr Transparenz ist auch bei der Umsetzung der Verpflichtungen der rechtmäßigen Überwachung für justizielle Zwecke erforderlich, sowohl seitens der Anbieter elektronischer Kommunikationsdienste als auch seitens der Behörden. Diese Vorschriften sollten mit dem Konzept des Untersuchungsgeheimnisses vereinbar sein. So ist es beispielsweise bei allen Untersuchungen von größter Bedeutung, dass Verdächtige während der gesamten Dauer der Untersuchung nicht benachrichtigt werden.

18. Schaffung einer **Clearingstelle**, um einschlägige Diensteanbieter zu ermitteln und rechtmäßige Anträge an sie zu richten (z. B. für Nummernübertragbarkeit für Telekommunikationsanbieter, die bereits in einigen EU-Mitgliedstaaten besteht).

www.parlament.gv.at

19. Einrichtung von Mechanismen, um sicherzustellen, dass grenzüberschreitende Anträge 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. *[Die Kohärenz dieser Empfehlung mit den durch die Verordnung über elektronische Beweismittel festgelegten Vorschriften sollte weiter geprüft werden.]*

20. Begleitung künftiger Initiativen durch einschlägige **Normungsmaßnahmen**. Zu diesem Zweck wird vorgeschlagen, dass die Kommission einen **Fahrplan** mit einer langfristigen Perspektive vorlegt, in dem klare Ziele festgelegt werden, eine angemessene Finanzierung zur Unterstützung einer stärkeren Teilnahme von Sachverständigen der Mitgliedstaaten vorgesehen wird und ein Mechanismus zur Koordinierung, etwa durch Europol und andere EU-Agenturen, vorgeschlagen wird. Es sollte sichergestellt werden, dass der Geltungsbereich der Normungstätigkeiten breit gefasst ist und das Internet der Dinge umfasst, einschließlich beispielsweise vernetzter Fahrzeuge, sowie alle Formen der Konnektivität, einschließlich beispielsweise Satellitenkommunikation. Tätigkeiten im Zusammenhang mit der digitalen Forensik, dem rechtmäßigen Zugang und der rechtmäßigen Überwachung sollten abgedeckt werden.

21. Anregung für künftige legislative, praktische und technische Initiativen durch eine **gemeinsame Definition der Anforderungen**, wie etwa in **LEON (Law enforcement Operational Needs for Lawful Access to Communication** – operative Anforderungen der Strafverfolgung für den rechtmäßigen Zugang zu Kommunikation[52]) dargelegt. Die Einrichtung einer Ad-hoc-Sachverständigengruppe, möglicherweise koordiniert durch Europol, würde dafür sorgen, dass LEON aktualisiert wird, wenn dies erforderlich ist, möglicherweise unter Koordinierung der bei Europol angesiedelten Gruppe zu Normung für Sicherheit, die fortgeführt werden sollte. Jede Initiative sollte technologieneutral sein. Verschiedene Optionen für die Bezugnahme auf LEON in künftigen EU-Initiativen sind möglich: 1. EU-Gesetzgebungsvorschlag, der auf LEON Bezug nimmt, 2. Empfehlung, 3. Inspirationsquelle.

---

52 LEON 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 für einen rechtmäßigen Zugang zu Kommunikationsinhalten, inhaltsbezogenen Daten und Teilnehmerinformationen zu ermitteln und zu beschreiben.

www.parlament.gv.at

22. Entwicklung eines Technologie-Fahrplans, der Sachverständige für Technologie, Cybersicherheit, Privatsphäre, Normung und Sicherheit zusammenbringt und für eine angemessene Koordinierung sorgt, z. B. durch eine permanente Struktur, um den **konzeptionsintegrierten rechtmäßigen Zugang** im Einklang mit dem von den Strafverfolgungsbehörden geäußerten Bedarf in allen relevanten Technologien umzusetzen, wobei gleichzeitig eine starke Sicherheit und Cybersicherheit gewährleistet und die rechtlichen Verpflichtungen für den rechtmäßigen Zugang uneingeschränkt geachtet werden sollten. Gemäß der Hochrangigen Gruppe sollten die Strafverfolgungsbehörden zur Definition der Anforderungen beitragen, aber es sollte nicht ihre Rolle sein, den Unternehmen spezifische Lösungen vorzuschreiben, damit sie rechtmäßigen Zugang zu Daten für die Zwecke strafrechtlicher Ermittlungen gewähren können, ohne die Sicherheit zu gefährden.

23. Gewährleistung, dass mögliche neue Verpflichtungen, ein neues Rechtsinstrument und/oder Normen **weder direkt noch indirekt zu Verpflichtungen für die Anbieter führen, die Sicherheit der Kommunikation zu schwächen**, indem die Übermittlungsverschlüsselung generell untergraben oder geschwächt wird. Daher müssten mögliche neue Vorschriften über den Zugang zu entschlüsselten Daten einer vorsichtigen Bewertung auf der Grundlage von dem aktuellen Stand der Technik entsprechenden Lösungen unterzogen werden (bei denen wiederum die Herausforderungen der Verschlüsselung berücksichtigt werden sollten). Bei der Gewährleistung der Möglichkeit des gesetzlich vorgeschriebenen konzeptionsintegrierten rechtmäßigen Zugangs sollten die Hersteller oder Diensteanbieter so vorgehen, dass keine negativen Auswirkungen für die Sicherheitslage ihrer Hardware- oder Software-Architektur entstehen.

24. Verbesserung der **Koordinierung und Unterstützung durch die EU** zur Bewältigung von Situationen, in denen technische Lösungen für eine rechtmäßige Überwachung bestehen, aber von den Anbietern elektronischer Kommunikationsdienste nicht umgesetzt werden. In solchen Fällen, beispielsweise wenn Home-Routing-Vereinbarungen oder die spezifische Umsetzung von Rich Communication Services (RCS) keine Fähigkeiten der rechtmäßigen Überwachung zulassen, würden klare Leitlinien und ein auf EU-Ebene angesiedelter Dialog die Zusammenarbeit mit den Anbietern elektronischer Kommunikationsdienste verbessern.

www.parlament.gv.at

In Bezug auf Legislativmaßnahmen empfiehlt die Hochrangige Gruppe Folgendes:

25. Durchführung einer **umfassenden Bestandsaufnahme** der geltenden Rechtsvorschriften in den Mitgliedstaaten, um die rechtlichen Verantwortlichkeiten der Hersteller von digitaler Hard- und Software für die Erfüllung von Datenanfragen der Strafverfolgungsbehörden im Einzelnen darzulegen. Dabei würden auch spezifische Szenarien und Anforderungen berücksichtigt, die Unternehmen zum Zugriff auf Geräte zwingen, unter Einhaltung der Rechtsprechung des EuGH und des Europäischen Gerichtshofs für Menschenrechte. Ziel sollte es sein, auf dieser Grundlage ein **Handbuch auf EU-Ebene** zu erarbeiten und – abhängig von der vorstehend genannten Bestandsaufnahme – die Angleichung der Rechtsvorschriften in diesem Raum zu fördern, und verbindliche Industriestandards für in der EU auf den Markt gebrachte Geräte im Hinblick auf die Integration des rechtmäßigen Zugangs zu entwickeln.

26. 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.

27. Einführung einer **harmonisierten EU-Regelung für Vorratsdatenspeicherung** mit folgenden Merkmalen:

    i. sie ist technologieneutral und zukunftssicher;

    ii. sie deckt derzeitige und künftige „Datenbearbeiter“ ab (d. h. OTT-Dienste und Diensteanbieter jeder Art, die Zugang zu elektronischen Geräten gewähren könnten);

    iii. sie gewährleistet den Zugang zu lesbaren Daten (der Diensteanbieter sollte die Möglichkeit haben, Metadaten und Teilnehmerdaten zu entschlüsseln, falls diese zu irgendeinem Zeitpunkt der Erbringung des Dienstes verschlüsselt werden);

    iv. der Schwerpunkt liegt nicht nur auf der Vorratsdatenspeicherung, sondern auch auf dem Zugang zu Daten, aufbauend auf den Vorschriften für elektronische Beweismittel;

    v. mit ihr wird – als Mindestmaßnahme – eine Verpflichtung für Unternehmen festgelegt, ausreichend Daten auf Vorrat zu speichern, um sicherzustellen, dass jeder Nutzer eindeutig identifiziert werden kann (z. B. IP-Adresse und Port-Nummer);

    vi. sie entspricht uneingeschränkt den Vorschriften über Datenschutz und Schutz der Privatsphäre.

www.parlament.gv.at

28. **Kategorisierung** von Daten nach ihrem Zweck (Identifizierung, Lokalisierung, Bestimmung und Bewertung der Online-Aktivitäten einer Person, gegen die ermittelt wird), wobei noch einige Arbeiten erforderlich sind, um die Zwecke in klare technische Anforderungen umzusetzen.

29. **Gewährleistung, dass der Zugang zu Daten gezielt und differenziert** nach Datenkategorien oder spezifischen Kategorien von Straftaten (z. B. Straftaten, die nur im Internet stattfinden) oder auf der Grundlage der Gefahr für die Opfer erfolgt.

30. **Einbeziehung von Vorschriften über Rechenschaftspflicht und Durchsetzbarkeit** für Diensteanbieter, um Verpflichtungen zur Vorratsspeicherung und Bereitstellung von Daten durchzusetzen, z. B. durch Verwaltungsstrafen oder Beschränkungen der Tätigkeit auf dem EU-Markt.

31. **Gewährleistung, dass für kommerzielle und geschäftliche Zwecke auf Vorrat gespeicherte Nutzerdaten** für Strafverfolgungsbehörden im Rahmen der einschlägigen Garantien wirksam zugänglich sind.

32. Erwägung der Festlegung von **Verpflichtungen für Diensteanbieter**, bestimmte Funktionen in ihren Diensten an- oder abzuschalten, um bestimmte Informationen zu erhalten, nachdem eine Anordnung ergangen ist (z. B. Speicherung der Geolokalisierung eines spezifischen Nutzers, nachdem dieser Gegenstand eines rechtmäßigen Antrags ist).

33. Entwicklung eines Mechanismus, um sicherzustellen, dass die Mitgliedstaaten **Sanktionen gegen nicht kooperative Anbieter elektronischer Kommunikationsdienste durchsetzen**[53] können und dass diese Maßnahmen gegenüber diesen Einrichtungen abschreckend wirken. Sowohl verwaltungs- als auch strafrechtliche Maßnahmen sollten verfügbar sein und angewandt werden, je nachdem ob ein Anbieter lediglich nicht kooperativ ist oder ob er vorsätzlich Hosting für kriminelle Aktivitäten bietet.

34. Harmonisierung der strafrechtlichen Maßnahmen – einschließlich Freiheitsstrafen – auf EU-Ebene zur Durchsetzung der Zusammenarbeit. Gleiches sollte für **nicht kooperative Hosting-Anbieter** (zusätzlich zu nicht kooperativen Anbietern elektronischer Kommunikationsdienste) gelten, um sicherzustellen, dass diese Unternehmen den an sie ergehenden richterlichen Anordnungen angemessen nachkommen, wenn sie Kommunikationsdienste krimineller Art hosten. *[Die Kohärenz dieser Empfehlung mit den durch die Verordnung über digitale Dienste festgelegten Vorschriften sollte weiter geprüft werden.]*

---

53 In diesem Kontext wird ein **nicht kooperativer Anbieter elektronischer Kommunikationsdienste** definiert als jeder Betreiber, der rechtlichen Anordnungen und technischen Anträgen der Strafverfolgungsbehörden nicht nachkommt und keinen objektiven Grund dafür hat.

www.parlament.gv.at

35. Bei potenziellen Initiativen sollte unterschieden werden zwischen **kriminellen Anbietern elektronischer Kommunikationsdienste** (d. h. Plattformen, die eigens dafür konzipiert sind, Dienste nur oder hauptsächlich für kriminelle Akteure anzubieten, wie EncroChat), und **nicht kooperativen Anbietern elektronischer Kommunikationsdienste**, die legal niedergelassen sind und rechtmäßige Tätigkeiten ausüben, aber ihren nationalen Verpflichtungen zur rechtmäßigen Überwachung nicht in vollem Umfang nachkommen.

36. Einführung einer **durchsetzbaren Verpflichtung für Plattformen** (oder alternativ weiche Maßnahmen durch Zusammenarbeit mit der Branche) zur Benennung einer **einzigen Anlaufstelle**[54] (Single Point of Contact – **SPOC**) in der EU für die Bearbeitung von Anträgen von und Kontakten mit EU-Behörden, insbesondere für Diensteanbieter, für die ein Notfallkontakt erforderlich ist. Ein ähnlicher Mechanismus (oder idealerweise dieselbe SPOC, mit erweiterten Befugnissen) sollte auch bestehen, um die **Durchsetzung der Verpflichtungen zur rechtmäßigen Überwachung** zu erleichtern.

37. Anwendung der gleichen Vorschriften auf Anbieter elektronischer Kommunikationsdienste (gemäß Definition im Europäischen Kodex für die elektronische Kommunikation – EKEK[55]) wie auf herkömmliche Diensteanbieter.

38. Weitere **Harmonisierung der nationalen Rechtsrahmen für den Zugang zu Daten auf dem Übermittlungsweg**[56] durch mehrere Schritte:

    i. Sicherstellung, dass die in nationalen Rechtsvorschriften festgelegten Verpflichtungen zur rechtmäßigen Überwachung **für ein breiteres Spektrum von Kommunikationsanbietern durchsetzbar** sind, einschließlich einschlägiger Kategorien von Internetdiensteanbietern (nach dem Modell des Pakets über elektronische Beweismittel).

    ii. Anstreben der Harmonisierung auf Ebene der EU-Mitgliedstaaten auf der Grundlage **vereinbarter gemeinsamer Grundsätze** (insbesondere jener, die Teil des LEON-Dokuments sind) durch nicht zwingendes Recht (z. B. eine Empfehlung der Kommission).

---

54 Im Rahmen der SIRIUS-Initiative wurde 2020 das Netz der SIRIUS-SPoC mit einer speziellen Plattform auf der Europol-Expertenplattform eingerichtet. Es besteht derzeit aus 39 Strafverfolgungsbehörden aus 22 EU-Ländern und 2 Drittländern.

55 Artikel 2 Nummer 4 der Richtlinie (EU) 2018/1972.

56 Der Begriff „Daten auf dem Übermittlungsweg“ kann Fälle abdecken, in denen die Erfassung der Daten nicht erfolgt, während sie auf dem Übermittlungsweg sind, sondern wenn die Kommunikationsdaten gesendet werden sollen oder empfangen worden sind (mitunter als „Live-Daten“ bezeichnet).

www.parlament.gv.at

iii. Überlegungen über eine **Definition der rechtmäßigen Überwachung** im breiteren Kontext von Internet-Kommunikationsdiensten, auch mit Unterscheidung zwischen der rechtmäßigen Überwachung von Nichtinhaltsdaten und Inhaltsdaten.

iv. Auf der Grundlage einer weiteren Analyse und einer Folgenabschätzung, einschließlich aus der Sicht der Grundrechte und unter Berücksichtigung der Souveränität der Staaten in Strafsachen, möglicherweise Vorlage einer EU-Initiative über rechtmäßige Überwachung (bestehend aus nicht zwingendem Recht oder Rechtsinstrumenten) nach dem Modell der im Rahmen elektronischer Beweismittel durchgeführten Arbeiten und aufbauend auf internationalen und bilateralen Abkommen (z. B. mit den Vereinigten Staaten). Mit dieser Initiative müsste sichergestellt werden, dass die Grundsätze des „konzeptionsintegrierten rechtmäßigen Zugangs“ von den einschlägigen Interessenträgern (z. B. Anbieter elektronischer Kommunikationsdienste) ordnungsgemäß umgesetzt werden, damit die festgelegten Anforderungen eingehalten werden, insbesondere die Ermöglichung des Zugangs zu entschlüsselten Daten, wenn dies für erforderlich und verhältnismäßig erachtet wird.

39. Anpassung des **Konzepts der örtlichen Zuständigkeit für Daten** zur Behebung potenzieller Gesetzeskollisionen mit anderen Zuständigkeiten. In Fällen mit nationalem Zusammenhang (z. B. eine Straftat wird in einem Mitgliedstaat durch einen im selben Mitgliedstaat befindlichen Täter verübt) sollte es möglich sein, im Rahmen des nationalen Verfahrensrechts mit Anforderungen und Garantien eine Überwachungsmaßnahme einzurichten, ohne auf ein Instrument der grenzüberschreitenden Zusammenarbeit zurückzugreifen.

40. Sondierung, wie die **Europäische Ermittlungsanordnung (EEA)** effiziente Anträge auf grenzüberschreitende rechtmäßige Überwachung besser unterstützen könnte, durch Verbesserung der Rechtssicherheit, Verkürzung der Fristen für die Reaktion auf Anordnungen und Förderung einer einheitlichen Nutzung der EEA und des Budapester Übereinkommens über Computerkriminalität des Europarats in ganz Europa, um bestehende Lücken beim Zugang zu Daten zu schließen.

www.parlament.gv.at

41. Überlegungen über **erforderliche Garantien** für den Fall, dass die rechtmäßige Überwachung auf Anbieter nicht herkömmlicher Kommunikationsdienste Anwendung findet. Einige Sachverständige schlagen vor, dass diese Ermittlungsmaßnahme nur Kommunikationen betreffen sollte, die nach dem Eingang eines rechtmäßigen Antrags der Behörden erfolgen. Außerdem sollten die Maßnahmen die Anbieter nicht verpflichten, ihre IKT-Systeme so anzupassen, dass sie sich negativ auf die Cybersicherheit ihrer Nutzer auswirken.

42. Annahme von Mindestvorschriften auf EU-Ebene, die die gegenseitige Zulässigkeit zwischen den Mitgliedstaaten von **Beweismitteln**, die aus Maßnahmen der rechtmäßigen Überwachung gegen nicht kooperative Anbieter stammen, ermöglichen und die die Zulässigkeit auch im Fall des Rückgriffs auf einschneidende Maßnahmen vorsehen, sofern dies erforderlich ist, um die gegenseitige Anerkennung von Urteilen, gerichtlichen Entscheidungen sowie die polizeiliche und justizielle Zusammenarbeit in Strafsachen zu erleichtern.

www.parlament.gv.at