Rat der
Europäischen Union

Brüssel, den 31. Januar 2017
(OR. en)

5775/17

COSI 16
CT 5
FRONT 41
DAPIX 34
ENFOPOL 44
VISA 34
FAUXDOC 8
COPEN 22
DROIPEN 10
CYBER 12
JAI 76

ÜBERMITTLUNGSVERMERK

Absender:	Herr Jordi AYET PUIGARNAU, Direktor, im Auftrag des Generalsekretärs der Europäischen Kommission
Eingangsdatum:	26. Januar 2017
Empfänger:	Herr Jeppe TRANHOLM-MIKKELSEN, Generalsekretär des Rates der Europäischen Union
Nr. Komm.dok.:	COM(2017) 41 final
Betr.:	MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN EUROPÄISCHEN RAT UND DEN RAT Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Vierter Fortschrittsbericht

Die Delegationen erhalten in der Anlage das Dokument COM(2017) 41 final.

Anl.: COM(2017) 41 final

EUROPÄISCHE
KOMMISSION

Brüssel, den 25.1.2017
COM(2017) 41 final

MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT, DEN EUROPÄISCHEN RAT UND DEN RAT

Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Vierter Fortschrittsbericht

Auf dem Weg zu einer wirksamen und echten Sicherheitsunion – Vierter Fortschrittsbericht

I. EINLEITUNG

Dies ist der vierte Monatsbericht über die Fortschritte auf dem Weg zu einer wirksamen und echten Sicherheitsunion, der die Entwicklungen im Rahmen zweier großer Säulen beleuchtet: *„Bekämpfung des Terrorismus und der organisierten Kriminalität sowie der Instrumente zu ihrer Unterstützung“* und *„Stärkung unserer Abwehrbereitschaft und Widerstandsfähigkeit gegen diese Bedrohungen“*. Der Bericht behandelt vier Schlüsselbereiche, nämlich Informationssysteme und Interoperabilität, Schutz weicher Ziele, Cyber-Bedrohung und Datenschutz bei strafrechtlichen Ermittlungen.

Der Anschlag auf den Berliner Weihnachtsmarkt im Dezember hat erneut wesentliche Schwächen unserer Informationssysteme aufgezeigt, die insbesondere auf EU-Ebene dringend angegangen werden müssen, um den nationalen Grenzschutz- und Strafverfolgungsbehörden vor Ort dabei zu helfen, ihre anspruchsvollen Aufgaben effektiver wahrnehmen zu können. Die Tatsache, dass die verschiedenen Informationssysteme nicht miteinander vernetzt sind – weshalb sich Attentäter unter Verwendung mehrerer Identitäten auch über Grenzen hinweg unentdeckt bewegen können – und solche Informationen von Mitgliedstaaten nicht routinemäßig in die einschlägigen EU-Datenbanken eingegeben werden, ist eine praktische Anwendungsschwäche, die dringend beseitigt werden muss. Auch im Hinblick auf Strafverfolgungsmaßnahmen an den Grenzen und die Rückführung von Personen, deren Asylanträge abgelehnt wurden, sind noch weitere Anstrengungen erforderlich.[1]

In Bezug auf den Schutz weicher Ziele wird die Kommission rascher daran arbeiten, Sachverständige aus den Mitgliedstaaten zusammenzubringen und bewährte Verfahren auszutauschen sowie standardisierte Leitlinien zu vereinbaren.

Was die Bedrohung der EU im Cyberbereich angeht, über die in den Medien ausführlich berichtet wird, beleuchtet der vorliegende Bericht die verschiedenen Arbeitsbereiche, die sich bereits mit dem Thema befassen. Dabei geht es sowohl um Prävention – durch die Zusammenarbeit mit der Industrie, um das Konzept der „eingebauten Sicherheit“ („Security by Design“) und die Umsetzung der Richtlinie zur Netz- und Informationssicherheit voranzubringen – als auch um die Förderung der Zusammenarbeit zwischen den Mitgliedstaaten und mit internationalen Organisationen und Partnern, um im Ernstfall auf Cyberangriffe reagieren zu können. In den kommenden Monaten werden die Kommission und die Hohe Vertreterin der Union für Außen- und Sicherheitspolitik die Maßnahmen formulieren, die für eine wirksame EU-weite Reaktion auf diese Bedrohungen erforderlich sind. Als Grundlage wird die EU-Strategie für die Cybersicherheit von 2013 dienen.

Der Schutz der Privatsphäre und der personenbezogenen Daten jedes Einzelnen ist ein zentrales Grundrecht und damit ein Eckpfeiler aller Maßnahmen auf dem Weg zu einer

[1] Die Kommission wird in den kommenden Wochen einen überarbeiteten Aktionsplan zum Thema Rückführungen vorlegen, siehe Bericht der Kommission an das Europäische Parlament, den Europäischen Rat und den Rat über die Umsetzung der europäischen Grenz- und Küstenwache, COM(2017) 42 (auf Englisch).

echten Sicherheitsunion. Die im April 2016 verabschiedete Richtlinie für den Datenschutz bei Polizei und Strafjustiz sorgt für hohe gemeinsame Datenschutzstandards und wird dadurch den reibungslosen Austausch einschlägiger Daten zwischen den Strafverfolgungsbehörden der Mitgliedstaaten erleichtern. Im Rahmen ihres sogenannten Datenpakets hat die Kommission zudem eine Überarbeitung der e-Datenschutz-Richtlinie in Angriff genommen, um den Anwendungsbereich der Richtlinie auf alle Anbieter elektronischer Kommunikation auszuweiten und sie mit der Datenschutz-Grundverordnung in Einklang zu bringen. Der Vorschlag soll den Datenschutz bei elektronischer Kommunikation gewährleisten und gleichzeitig Gründe festlegen, die Einschränkungen des Anwendungsbereichs der Verordnung über Privatsphäre und elektronische Kommunikation erlauben, etwa die Wahrung der nationalen Sicherheit oder strafrechtliche Ermittlungen.

II. STÄRKUNG DER INFORMATIONSSYSTEME UND INTEROPERABILITÄT

In Präsident Junckers Rede zur Lage der Union vom September 2016 und in den Schlussfolgerungen des Europäischen Rates vom Dezember 2016 wird herausgestellt, dass die derzeitigen Mängel der Informationssysteme beseitigt und die **Interoperabilität und Vernetzung der bestehenden Informationssysteme** verbessert werden müssen. Die jüngsten Ereignisse haben erneut gezeigt, dass eine Vernetzung der vorhandenen EU-Datenbanken dringend notwendig ist, um nicht zuletzt den Grenzschutz- und Strafverfolgungsbehörden vor Ort die nötigen Instrumente für das Aufdecken von Identitätsbetrug bereitzustellen. Der Attentäter des Terroranschlags von Berlin im Dezember 2016 hat zum Beispiel mindestens 14 verschiedene Identitäten genutzt und konnte sich unerkannt von einem Mitgliedstaat in den anderen bewegen. Um diese Möglichkeit für Terroristen und Straftäter zu beseitigen, müssen die bestehenden und zukünftigen EU-Informationssysteme unbedingt gleichzeitig anhand biometrischer Identifikatoren durchsuchbar sein.

Die Kommission hat diesbezüglich im April 2016 Vorschläge für „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“[2] vorgelegt. Darin wurde auf Mängel bei den Funktionen der bestehenden Systeme, Lücken in der Datenverwaltungsarchitektur der EU, Probleme mit der komplexen Landschaft unterschiedlich geregelter Informationssysteme und eine generelle Fragmentierung hingewiesen, die sich daraus ergibt, dass die vorhandenen Systeme individuell gestaltet und nicht aufeinander abgestimmt wurden. Im Zuge dessen hat die Kommission die **hochrangige Expertengruppe für Informationssysteme und Interoperabilität** mit EU-Agenturen, Mitgliedstaaten und wichtigen Interessenträgern eingerichtet. Der Bericht des Vorsitzenden vom 21. Dezember 2016[3] über die **vorläufigen Ergebnisse** der Gruppe enthält unter anderem die bevorzugte Option, ein einziges Suchportal zu schaffen, damit nationale Strafverfolgungs- und Grenzschutzbehörden die vorhandenen EU-Datenbanken und -Informationssysteme gleichzeitig durchsuchen können. Der Zwischenbericht hebt außerdem die Bedeutung der Datenqualität hervor – denn die Effektivität der Informationssysteme hängt von der

[2] Mitteilung „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“ (COM(2016) 205 final).

[3] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetailDoc&id=28994&no=1

Qualität und dem Format der eingegebenen Daten ab – und enthält Empfehlungen für eine Verbesserung der Datenqualität in EU-Systemen anhand automatischer Qualitätskontrollen.

Die Kommission wird die Option, ein einziges Suchportal zu schaffen, umgehend weiterverfolgen und mit der EU-Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA) an einem Portal arbeiten, das die parallele Suche in allen relevanten bestehenden EU-Systemen ermöglicht. Eine entsprechende Studie sollte im Juni vorliegen und als Grundlage dafür dienen, bis Ende des Jahres einen Prototyp des Portals zu entwickeln und zu testen. Nach Auffassung der Kommission sollte Europol parallel dazu weiter an einer Systemoberfläche arbeiten, die es den Beamten der Mitgliedstaaten vor Ort ermöglicht, beim Durchsuchen ihrer nationalen Systeme gleichzeitig und automatisch auch die Europol-Datenbank abzufragen.

Die Arbeiten an der Interoperabilität der Informationssysteme zielen darauf ab, die derzeitige Fragmentierung in der Architektur der EU-Datenverwaltung im Bereich Grenzschutz und Sicherheit und die dadurch entstehenden Lücken zu beseitigen. Wenn Datenbanken auf einen gemeinsamen Speicher für Identitätsdaten zurückgreifen – wie dies für das vorgeschlagene EU-Einreise-/Ausreisesystem sowie das vorgeschlagene Europäische Reiseinformations- und -genehmigungssystem (ETIAS) vorgesehen ist –, kann für eine Person in verschiedenen Datenbanken nur eine einzige Identität erfasst werden, wodurch die Verwendung mehrerer falscher Identitäten verhindert wird. Wie im Zwischenbericht der hochrangigen Expertengruppe vorgeschlagen, hat die Kommission als ersten Schritt eu-LISA ersucht, die technischen und operativen Aspekte der Umsetzung eines gemeinsamen Systems zum Abgleich biometrischer Daten zu prüfen. Ein solches System würde die datenbankübergreifende Suche anhand biometrischer Daten ermöglichen, wodurch die von einer Person verwendeten falschen Identitäten in anderen Systemen aufgedeckt werden könnten. Darüber hinaus sollte die hochrangige Expertengruppe nunmehr prüfen, ob es notwendig, technisch möglich und verhältnismäßig ist, den für das Einreise-/Ausreisesystem und ETIAS vorgesehenen **gemeinsamen Speicher für Identitätsdaten** auf andere Systeme auszuweiten. Neben den biometrische Daten, die im Abgleichsystem gespeichert sind, würde ein solcher gemeinsamer Speicher für Identitätsdaten auch alphanumerische Identitätsdaten umfassen. Die Gruppe sollte ihre diesbezüglichen Ergebnisse bis Ende April 2017 in ihrem Abschlussbericht vorlegen.

Die jüngsten sicherheitsrelevanten Ereignisse haben deutlich gezeigt, dass die Frage des **verbindlichen Informationsaustauschs** zwischen den Mitgliedstaaten erneut geprüft werden muss. Im Vorschlag der Kommission vom Dezember 2016 zur Stärkung des **Schengener Informationssystems** ist erstmals vorgesehen, die Mitgliedstaaten zur Ausschreibung von Personen mit Bezug zu terroristischen Straftaten zu verpflichten. Nun ist es Sache der gesetzgebenden Organe, für die rasche Verabschiedung der vorgeschlagenen Maßnahmen zu sorgen. Die Kommission ist bereit zu prüfen, ob ein verpflichtender Informationsaustausch auch im Hinblick auf andere EU-Datenbanken eingeführt werden sollte.

III. SCHUTZ WEICHER ZIELE VOR TERRORANSCHLÄGEN

Der Anschlag in Berlin war der jüngste Terrorakt in der EU, der sich gegen ein sogenanntes weiches Ziel richtete; dabei handelt es sich typischerweise um zivile Ziele,

an denen sich größere Menschenmengen sammeln (z. B. öffentliche Plätze, Krankenhäuser, Schulen, Sportplätze, kulturelle Zentren, Cafés und Restaurants, Einkaufszentren und Verkehrsknotenpunkte). Diese Ziele sind aufgrund ihrer Beschaffenheit anfällig und schwierig zu schützen; zudem ist im Fall eines Anschlags von hohen Opferzahlen auszugehen. Aus diesen Gründen werden solche Ziele von Terroristen bevorzugt. Die Gefahr weiterer Anschläge auf weiche Ziele, etwa Verkehrsmittel, ist den verfügbaren Bewertungen zufolge nach wie vor hoch; dies wird auch im Europol-Bericht über die Änderung der Vorgehensweise von Da'esh[4] bestätigt.

In der Europäischen Sicherheitsagenda von 2015 und der Mitteilung zur Sicherheitsunion von 2016 wird hervorgehoben, dass zum Schutz weicher Ziele intensiver an der Erhöhung der Sicherheit und der Verwendung innovativer Aufdeckungsinstrumente und -technologien gearbeitet werden muss. Die Kommission unterstützt und fördert den Austausch bewährter Verfahren zwischen den Mitgliedstaaten bei der Entwicklung besserer Instrumente, um Anschlägen auf weiche Ziele vorzubeugen und darauf zu reagieren. Zu diesem Zweck wurden operative Handbücher und Leitfäden erstellt. Derzeit erarbeitet die Kommission in enger Zusammenarbeit mit den Mitgliedstaaten ein umfassendes Handbuch über Sicherheitsverfahren sowie Vorlagen für verschiedene weiche Ziele (z. B. Einkaufszentren, Krankenhäuser, Sport- und Kulturveranstaltungen). Den Mitgliedstaaten sollen Anfang 2017 Leitlinien für den Schutz weicher Ziele auf der Grundlage bewährten Verfahren der Mitgliedstaaten an die Hand gegeben werden.

Darüber hinaus wird die Kommission im Februar den ersten Workshop mit nationalen Behörden zum Thema Schutz weicher Ziele abhalten, um Informationen auszutauschen und bewährte Verfahren zu den komplexen Fragen des Schutzes weicher Ziele und der öffentlichen Ordnung und Sicherheit zu erarbeiten. Außerdem fördert die Kommission im Rahmen des Fonds für die innere Sicherheit ein Pilotprojekt Belgiens, der Niederlande und Luxemburgs zur Schaffung eines regionalen Kompetenzzentrums für Sondermaßnahmen in der Strafverfolgung, das Fortbildungen für Polizeikräfte, die im Fall eines Angriffs meist die Ersthelfer sind, anbieten wird.

Die Reaktion auf Anschläge auf weiche Ziele ist eine Schlüsselkomponente der Arbeit der Kommission im Bereich Katastrophenschutz. Im Dezember kündigte die Kommission Maßnahmen an, die sie mit den Mitgliedstaaten zu ergreifen gedenkt, um die EU-Bürger zu schützen und die Krisenanfälligkeit unmittelbar nach einem Terroranschlag zu verringern. Diese Maßnahmen werden eine bessere Koordinierung aller Akteure ermöglichen, die an der Bewältigung der Folgen von Anschlägen beteiligt sind. Zudem hat sich die Kommission verpflichtet, die Bemühungen der Mitgliedstaaten zu unterstützen, indem sie gemeinsame Schulungen und Übungen fördert und über bestehende Anlaufstellen und Sachverständigengruppen einen kontinuierlichen Dialog sicherstellt. Darüber hinaus wird die Kommission die Entwicklung von Fachmodulen für die Reaktion auf terroristische Anschläge im Rahmen des Katastrophenschutzverfahrens der Union sowie Initiativen für den Erfahrungsaustausch und die Sensibilisierung der Öffentlichkeit unterstützen.

Gemeinsam mit den Mitgliedstaaten wird die Kommission außerdem prüfen, welche Art der EU-Unterstützung mobilisiert werden könnte, um Widerstandsfähigkeit aufzubauen

[4] Europol, *Changes in modus operandi of Islamic State (IS) revisited*, November 2016 – Europol-Veröffentlichungen, https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited

und die Sicherheit im Umfeld potenzieller weicher Ziele zu verbessern. Die Mitgliedstaaten könnten im Einklang mit den Vorgaben der EU und der EIB-Gruppe außerdem Mittel der Europäischen Investitionsbank (EIB) (einschließlich des Europäischen Fonds für strategische Investitionen) beantragen. Solche Projekte würden den regulären Beschlussfassungsverfahren gemäß den Vorschriften unterliegen.

Was spezifische weiche Ziele im Bereich öffentlicher Verkehrsflächen anbelangt, etwa die allgemein zugänglichen Bereiche von Flughäfen oder Bahnhöfen, wurde im Rahmen des einschlägigen Workshops der Kommission, der im November 2016 unter Beteiligung eines breiten Spektrums von Interessenträgern stattfand, betont, dass das Gleichgewicht zwischen den Sicherheitsanforderungen, den Bedürfnissen der Reisenden und den Verkehrsleistungen zu wahren ist. In den Schlussfolgerungen wird hervorgehoben, welche Bedeutung die Schaffung einer Sicherheitskultur hat, die nicht nur das Personal, sondern auch die Reisenden miteinbezieht, wie wichtig lokale Risikobewertungen als Grundlage für die Festlegung geeigneter Gegenmaßnahmen sind und dass die Kommunikation zwischen allen Beteiligten verbessert werden muss.

IV. CYBER-BEDROHUNGEN BEGEGNEN

Cyberkriminalität und Cyberangriffe stellen zentrale Herausforderungen für die Union dar. Gegenmaßnahmen auf EU-Ebene können dazu beitragen, unsere kollektive Widerstandsfähigkeit zu stärken. Jeden Tag beeinträchtigen Sicherheitsvorfälle im Cyberraum ernsthaft das Leben der Bürger und verursachen der europäischen Wirtschaft und den Unternehmen erheblichen Schaden. Cyberangriffe sind ein wesentlicher Bestandteil hybrider Bedrohungen, die verheerende Auswirkungen entfalten können, wenn sie zeitlich genau auf physische Bedrohungen (etwa im Zusammenhang mit Terrorismus) abgestimmt sind. Sie können außerdem ein Land weiter destabilisieren oder dessen politische Institutionen und die grundlegenden demokratischen Prozesse schwächen. Da wir zunehmend auf Online-Technologien zurückgreifen, werden unsere kritischen Infrastrukturen (von Krankenhäusern bis zu Kernkraftwerken) immer anfälliger.

Die Cybersicherheitsstrategie der EU von 2013 steht im Kern der politischen Antwort auf sicherheitsbezogene Herausforderungen im Cyberraum. Die wichtigste Maßnahme, die Richtlinie über Netz- und Informationssicherheit („NIS-Richtlinie“)[5], wurde vergangenen Juli angenommen. Die Richtlinie bildet das Fundament für mehr Zusammenarbeit auf EU-Ebene und eine verbesserte Widerstandsfähigkeit gegenüber Cyberangriffen, indem die Zusammenarbeit und der Austausch von Informationen zwischen den Mitgliedstaaten unterstützt und die operative Zusammenarbeit bei spezifischen Cyber-Zwischenfällen sowie der Austausch von Informationen über Risiken gefördert werden. Zur Gewährleistung einer einheitlichen Umsetzung in verschiedenen Sektoren und über Grenzen hinweg wird die Kommission im Februar die erste Sitzung der NIS-Kooperationsgruppe mit den Mitgliedstaaten abhalten.

[5] Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union.

Im April 2016 haben die Kommission und die Hohe Vertreterin einen gemeinsamen Rahmen für die Abwehr hybrider Bedrohungen angenommen[6], in dem 22 operative Maßnahmen zur Sensibilisierung, zur Stärkung der Widerstandsfähigkeit, zur besseren Reaktion auf Krisen und zur Intensivierung der Zusammenarbeit zwischen der EU und der NATO vorgeschlagen werden. Wie vom Rat gefordert, werden die Kommission und die Hohe Vertreterin bis Juli 2017 einen Bericht über die erzielten Fortschritte vorlegen.

Die Kommission unterstützt außerdem technologische Innovationen, indem u. a. EU-Forschungsmittel genutzt werden, um neue Lösungen zu fördern und neue Technologien zu entwickeln, die dazu beitragen können, die Widerstandsfähigkeit gegenüber Cyberangriffen zu erhöhen (z. B. „Security by Design"-Projekte). Vergangenen Sommer wurde mit der Industrie eine öffentlich-private Partnerschaft für Cybersicherheit mit einem Volumen von 1,8 Mrd. EUR gegründet.[7]

Im Verkehrssektor wird die Digitalisierung zu einem wichtigen Impulsgeber für die dringend erforderliche Umgestaltung des heutigen Verkehrssystems. Das schnelle Voranschreiten der Digitalisierung bringt viele Vorteile mit sich, macht den Verkehrssektor jedoch auch anfälliger für Risiken im Bereich der Cybersicherheit. Es wurden zahlreiche Maßnahmen eingeleitet, um die Bedrohung auf verschiedenen Ebenen zu verringern, insbesondere im Luftverkehr, aber auch im See-, Binnenschifffahrts-, Straßen- und Schienenverkehr.[8] Die Herausforderung besteht nunmehr darin, die Tätigkeiten der verschiedenen Interessenträger, die auf die Stärkung unterschiedlicher Aspekte der Widerstandsfähigkeit gegenüber Cyberangriffen abzielen, weiter zu präzisieren, zu harmonisieren und zu ergänzen.

Angesichts der sich rasch wandelnden Art der Bedrohung werden die Kommission und die Hohe Vertreterin der EU in den kommenden Monaten – aufbauend auf der Cybersicherheitsstrategie der EU von 2013 – allgemein festlegen, welche Maßnahmen erforderlich sind, um EU-weit wirksam auf diese Bedrohungen zu reagieren.

V. SCHUTZ PERSONENBEZOGENER DATEN UND UNTERSTÜTZUNG EFFIZIENTER STRAFRECHTLICHER ERMITTLUNGEN

Die Richtlinie für den Datenschutz bei Polizei und Strafjustiz[9] stellt ein wichtiges Element der Bekämpfung von Terrorismus und Schwerkriminalität dar. Auf der

---

6 JOIN (2018)18.

7 Diese Partnerschaft war in der Mitteilung über die Stärkung der Abwehrfähigkeit im Bereich der Cybersicherheit aus dem Jahr 2016 (COM(2016) 410 final) angekündigt worden.

8 Beispiele hierfür sind internationale Leitlinien, wie diejenigen, die von der Internationalen Seeschifffahrts-Organisation entwickelt oder die durch eine vor kurzem verabschiedete ICAO-Entschließung angenommen wurden (gemeinsame Initiative der EU und der USA); die Berichterstattung über Zwischenfälle, für die derzeit von der Europäischen Agentur für Flugsicherheit ein stärker reaktiver Modus entwickelt wird, und die „konzeptuelle Cybersicherheit", die auf neue in der Entwicklung befindliche Systeme, etwa den europäischen Generalplan für das Flugverkehrsmanagement des gemeinsamen Unternehmens SESAR, Anwendung findet.

9 Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses

Grundlage eines in der Richtlinie festgelegten gemeinsamen Datenschutzstandards werden die Strafverfolgungsbehörden der Mitgliedstaaten nun problemlos einschlägige Daten austauschen können, während die Daten von Opfern, Zeugen und Verdächtigen bei strafrechtlichen Ermittlungen angemessen geschützt bleiben.

Um sowohl für Einzelpersonen als auch für Unternehmen ein hohes Maß an Vertraulichkeit bei der Kommunikation sowie – im Einklang mit der Strategie für einen digitalen Binnenmarkt vom April 2015 – gleiche Wettbewerbsbedingungen für alle Marktakteure zu gewährleisten, hat die Kommission am 11. Januar die vorgeschlagene **Verordnung über Privatsphäre und elektronische Kommunikation** (die die Richtlinie 2002/58/EG ersetzt) angenommen.[10] Wie in der derzeit geltenden Richtlinie wird auch in der überarbeiteten Verordnung über Privatsphäre und elektronische Kommunikation die Datenschutz-Grundverordnung[11] spezifiziert und ein Rahmen für den Schutz der Privatsphäre und der personenbezogenen Daten im elektronischen Kommunikationssektor festgelegt.

Nach der überarbeiteten Verordnung werden alle Daten der elektronischen Kommunikation, auch im Rahmen ergänzender Kommunikationsdienste, als vertraulich/privat betrachtet, ungeachtet dessen, ob die Daten über traditionelle Telekommunikationsdienste oder über andere sogenannte Over-the-Top (OTT)-Dienste übertragen werden, die funktional gleichwertig sind (z. B. Skype und Whatsapp) und für viele Nutzer an die Stelle herkömmlicher Telekommunikationsanbieter getreten sind.[12] Zu den Verpflichtungen, die den Diensteanbietern auferlegt werden, gehört – neben der Achtung der Nutzereinstellungen der Kunden in Bezug auf ihre Privatsphäre sowie die Speicherung und Verarbeitung ihrer Daten – auch die Verpflichtung für außerhalb der EU ansässige Diensteanbieter, einen Vertreter in einem Mitgliedstaat zu benennen. Dadurch wird den Mitgliedstaaten auch ermöglicht, die Zusammenarbeit von Strafverfolgungs- und Justizbehörden mit Diensteanbietern im Hinblick auf den Zugang zu elektronischen Beweismitteln zu erleichtern (siehe unten).

Wie auch im Rahmen der derzeit geltenden Vorschriften über die Privatsphäre in der elektronischen Kommunikation wird der Zugang der Strafverfolgungs- und Justizbehörden zu einschlägigen elektronischen Informationen, die zur Untersuchung von Straftaten erforderlich sind, einer Ausnahme unterliegen, die in Artikel 11 der vorgeschlagenen Verordnung festgelegt ist.[13] Diese Bestimmung ermöglicht es, die

---

2008/977/JI des Rates. Die Richtlinie ist seit dem 5. Mai 2016 in Kraft und von den Mitgliedstaaten bis zum 6. Mai 2018 umzusetzen. Die Kommission hat eine Sachverständigengruppe mit den Mitgliedstaaten eingerichtet, um einen Meinungsaustausch über die Umsetzung der Richtlinie anzuregen.

10 Verordnung über Privatsphäre und elektronische Kommunikation, COM(2017) 10.

11 Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und zur Ersetzung von Richtlinie 95/46/EC (Datenschutz-Grundverordnung), Geltungsbeginn: 25. Mai 2018.

12 Dies ergibt sich aus dem Ansatz gemäß dem Vorschlag für eine Richtlinie über den europäischen Kodex für die elektronische Kommunikation, der von der Kommission am 14. September 2016 vorgelegt wurde (Telekommunikations-Paket), COM(2016) 590 final.

13 Siehe Artikel 11 Absatz 1; die Klausel zur Vorratsdatenspeicherung wurde unverändert aus Artikel 15 der Datenschutzrichtlinie für elektronische Kommunikation übernommen und den Anforderungen der Datenschutz-Grundverordnung angeglichen. Eine solche Beschränkung muss den Wesensgehalt der Grundrechte achten sowie erforderlich, geeignet und verhältnismäßig sein.

Vertraulichkeit der Kommunikation durch EU- oder einzelstaatliche Rechtsvorschriften zu beschränken, sofern dies erforderlich und verhältnismäßig ist, um die nationale Sicherheit, die Landesverteidigung, die öffentliche Sicherheit oder die Verhütung, Ermittlung, Aufdeckung und Verfolgung von Straftaten oder den Strafvollzug zu gewährleisten. Nachdem der Europäische Gerichtshof (EuGH) die Richtlinie über die Vorratsspeicherung von Daten im Jahr 2014 für ungültig erklärt hat[14], ist diese Bestimmung insbesondere für die nationalen Vorschriften zur **Vorratsdatenspeicherung** relevant, d. h. wenn Anbieter von Telekommunikationsdiensten verpflichtet werden, Kommunikationsdaten für einen bestimmten Zeitraum vorzuhalten, um den Strafverfolgungsbehörden Zugang zu diesen Daten zu ermöglichen. Seit dem Urteil gibt es kein EU-Instrument mehr für die Vorratsdatenspeicherung; einige Mitgliedstaaten haben jedoch ihre eigenen nationalen Gesetze zur Vorratsdatenspeicherung angenommen. Die einschlägigen schwedischen und britischen Gesetze wurden vor dem EuGH angefochten, der am 21. Dezember sein Urteil in der Sache *Tele2*[15] erließ. Der EuGH erklärte darin nationale Regelungen, die für die Zwecke der Bekämpfung von Straftaten eine allgemeine und unterschiedslose Vorratsspeicherung sämtlicher Verkehrs- und Standortdaten aller Teilnehmer und Nutzer in Bezug auf alle elektronischen Kommunikationsmittel vorsehen, für nicht mit EU-Recht vereinbar. Die Auswirkungen des Urteils werden analysiert und die Kommission wird Leitlinien dazu ausarbeiten, wie nationale Gesetze zur Vorratsdatenspeicherung im Einklang mit dem Urteil ausgestaltet werden können.

Straftaten hinterlassen digitale Spuren, die in Gerichtsverfahren als Beweismittel eingebracht werden können; für Strafverfolgungsbehörden und Staatsanwälte stellt elektronische Kommunikation zwischen Verdächtigen häufig den einzigen greifbaren Anhaltspunkt dar. Zugriff auf **elektronische Beweismittel** zu erlangen – insbesondere, wenn diese im Ausland oder in einer Cloud gespeichert sind – kann jedoch sowohl technisch als auch juristisch komplex und verfahrenstechnisch oft umständlich sein, was Ermittler daran hindert, rasch tätig zu werden. Um diesen Herausforderungen zu begegnen, prüft die Kommission derzeit Lösungen, die Ermittlern erlauben, grenzüberschreitend elektronische Beweismittel zu erlangen; dazu gehören auch Möglichkeiten, die Rechtshilfe effizienter zu gestalten, die direkte Zusammenarbeit mit Anbietern von Internetdiensten zu erleichtern und Kriterien vorzuschlagen, um unter uneingeschränkter Einhaltung der geltenden Datenschutzvorschriften die Zuständigkeit für Ermittlungsmaßnahmen im Cyberspace festzulegen und durchzusetzen.[16] Die Kommission berichtete dem Rat „Justiz und Inneres“ am 9. Dezember 2016 über die erzielten Fortschritte[17].

Eine umfassende (noch nicht abgeschlossene) Konsultation von Sachverständigen hat es der Kommission ermöglicht, die verschiedenen, oftmals vielschichtigen Probleme im

---

14 Urteil des EuGH in den verbundenen Rechtssachen C-293/12 und C-594/12 *Digital Rights Ireland* vom 8. April 2014.

15 Urteil des EuGH in den verbundenen Rechtssachen C-203/15 und C-698/15 *Tele2* vom 21. Dezember 2016.

16 Im Einklang mit der Europäischen Sicherheitsagenda (COM(2015) 185 final) und der Mitteilung „Umsetzung der Europäischen Sicherheitsagenda im Hinblick auf die Bekämpfung des Terrorismus und die Weichenstellung für eine echte und wirksame Sicherheitsunion“ der Kommission (COM(2016) 230 final).

17 Der Rat forderte die Kommission in seinen Schlussfolgerungen zur Verbesserung der Strafjustiz im Cyberspace vom 9. Juni 2016 auf, konkrete Maßnahmen zu ergreifen, ein gemeinsames Konzept der EU zu entwickeln und bis Juni 2017 Ergebnisse vorzulegen.

Zusammenhang mit dem Zugang zu elektronischen Beweismitteln zu identifizieren, einen besseren Einblick in die derzeit in den Mitgliedstaaten geltenden Regelungen und Praktiken zu erhalten und mögliche politische Optionen zu ermitteln. Der Fortschrittsbericht enthält einen Überblick über die bislang im Rahmen der Informationssammlung und der Konsultation der Sachverständigen entstandenen Ideen, die von der Kommission in Zusammenarbeit mit den Interessenträgern nun in den kommenden Monaten weiter geprüft werden. Wie im Arbeitsprogramm der Kommission angekündigt, wird die Kommission 2017 eine Initiative vorlegen.

VI. SCHLUSSFOLGERUNG

Der nächste Bericht ist am 1. März vorzulegen und wird Gelegenheit bieten, die Fortschritte in diesen und anderen wichtigen Arbeitsbereichen zu prüfen.