

Einordnung des deutsch-französischen Eckpunktepapiers „Beitrag zur Erhöhung der inneren Sicherheit in Europa“ vom 23. August 2016:

Eckpunkte für geplantes Ein und Ausreiseregister (Entry-/Exit-System -EES): Daten aller Grenzübertritte an Außengrenzen werden protokolliert, darunter auch Fingerabdrücke und Gesichtsbilder. Die Forderung nach Einbeziehung von EU-Bürger/innen kam von Frankreich („Smart Borders for all“). EES bildet die „Smart-Borders-Infrastruktur“, der weitere (bestehende und neue) Systeme untergeordnet werden. Faktisch entsteht dadurch eine weltweite biometrische Datenbank mit Fingerabdrücken und Gesichtsbildern. Ziel ist die Errichtung eines „EU-weiten integrierten biometrischen Identitätsmanagements für Reisen, Migration und Sicherheit“. Konkrete Vorschläge für diese Gesamt-Plattform soll eine „hochrangige Sachverständigengruppe für IT-Systeme und Interoperabilität“ ausarbeiten, ein erstes Treffen war für Juni geplant. (Drucksache 18/7835, 18/7291, 18/4287)

Einigung über die Einrichtung eines Europäischen Reiseinformations- und Genehmigungssystems (ETIAS): Beträfe Angehörige von Drittstaaten, die für Kurzaufenthalte von der Visumpflicht befreit sind. Vorbild sind Systeme zur Einreisegenehmigung in den USA, Kanada, Australien. Auf einem Internetformular müssten Reisende neben Personendaten auch Informationen zum geplanten Aufenthalt mitteilen, etwa Zweck und Plan der Reise. In der Diskussion ist auch, geplante Verkehrsmittel angeben zu müssen. ETIAS ersetzt ursprünglich im EES geplantes „Registrierungsprogramm“ (RTP). Europäische Kommission will bis Ende 2016 konkreten Vorschlag vorlegen, eine Machbarkeitsstudie ist für Herbst 2016 angekündigt. Wie beim EES fordert Frankreich Einbeziehung von EU-Bürger/innen. (Drucksache 18/8872)

Ausweitung des beschlossenen, aber noch nicht umgesetzten EU-Passagierdatensystems (PNR): Der Einbezug von Charter-Flügen und Flügen innerhalb Europas war stets eine Forderung Frankreichs, wurde aber wegen des Widerstandes des EU-Parlaments nur als Option für die einzelnen Regierungen in die Richtlinie aufgenommen. Werden jetzt alle Mitgliedstaaten zu einheitlichem Vorgehen gedrängt, wird das Parlament nachträglich überrumpelt. (Drucksache 18/2972)

Vollständige Umsetzung der Prüm-Beschlüsse: Abfrage von DNA-Daten und Fingerabdrücken (nicht alle Staaten haben umgesetzt). Außerdem in Planung: Erweiterung des Prüm-Verfahrens auf durchsuchbare Gesichtsbilder, Vorschlag der Europäischen Kommission in 2017.

Nutzung biometrischer Daten in allen relevanten Datenbanken: Bereits existente biometriebasierte Datenbanken (zuerst SIS II, EURODAC, VIS) sollen außer Fingerabdrücken in einigen Jahren auch durchsuchbare Gesichtsbilder speichern. Auch DNA-Daten sind im Gespräch. Die Neuerungen betreffen zuerst Asylsuchende. Vorschlag aus Deutschland findet sich „Roadmap zur Verbesserung des Informationsaustauschs und des Informationsmanagements“ der Europäischen Kommission (Ratsdokument 8437/1/16). Die geplanten Erweiterungen sollen keine Befassung des Europäischen Parlamentes erfordern. (Drucksache 18/8322)

„Eine einzige Suchmaske“ für Datenbanken der EU und Interpol („Single Search Interface“): Weitestgehender Vorschlag dazu kam aus Deutschland, Forderungspapier von de Maizière zu europäischen „Datentöpfen“ vom März 2016. Zentrales „Kernsystem“ soll bestehende Datenbanken für biometrische Daten „verknüpfen“. Beträfe nach gegenwärtigem Stand Überbau von SIS II, VIS, Eurodac, ECRIS, Europol Informationssystem, später auch EES. Im Idealfall zu jeder Person zehn Fingerabdrücke (die sogenannten 10-Finger-Sätze), dafür Einführung eines „Fingerabdruckidentifizierungssystems“ (AFIS) zuerst im SIS II (bis 2017). Technische Infrastruktur wird unter Leitung des Bundeskriminalamtes im Projekt „Universal Message Format“ (UMF 3) beforscht, Interpol, Europol und Frontex sind daran ebenfalls beteiligt. (Drucksache 18/8170, 18/7698), 18/8323)

Ausweitung des Pilotprojekts „ADEP“ (Automatischer Daten Austausch Prozess) auf alle Mitgliedstaaten und Europol: Sechs Mitgliedstaaten arbeiten mit Europol am verbesserten Informationsaustausch nach dem „Treffer/ Kein Treffer“-Verfahren. Ziel ist die Vernetzung bestehender Systeme mit dem Europol Informationssystem. Es geht nicht um Verurteilte, sondern um „Gefährder“, „strafrechtlich auffällige Personen“. Frankreich führt das Projekt an, Deutschland bezahlt. Ähnliches Projekt QUEST bei Europol („Querying Europol Systems“). (Drucksache 18/8323)

Ausweitung des Zugangs zu Datenbanken (etwa SIS II, EURODAC) auf weitere Behörden: Betrifft unter anderem Europol und Frontex zum automatisierten Abgleich. Europol will jeden neuen Eintrag in seinem Informationssystem mit dem SIS II abgleichen. „Zugang unter praxistauglichen und effektiven Bedingungen“ heißt: In Echtzeit und ohne Umweg über „Treffer/ Kein Treffer“. Derzeit darf Europol nur im Einzelfall und auch nur indirekt auf das SIS II, das VIS und EURODAC zugreifen. SIS II- und EURODAC-Verordnung werden u.a. deshalb erneuert. Europol darf auch keine eigenen Ausschreibungen in das SIS II eingeben, fordert aber Möglichkeit zur Fahndung nach Artikel 36 des Schengener Grenzkodex.

Mehr finanzielle und personelle Ausstattung von Europol: Nach britischem und niederländischem Vorbild wurde 2014 das Anti-Terror-Zentrum (ECTC) gegründet, Arbeitsbereiche und Analysefähigkeiten sowie Zugang zu EU-Datenbanken stetig erweitert. Mit dem Projekt „Ma3tch“ wird automatisierter Abgleich für Datenbanken wie FIU.NET oder Fluggastdaten bei Europol getestet und eingeführt. Außerdem enthält das Eckpunktepapier den Vorschlag zu neuer Abteilung „Bekämpfung von chemischen, biologischen, radioaktiven und nuklearen Risiken in einer ganzheitlichen Weise“ im ECTC. (Drucksache 18/6239, 18/4437, 18/4193)

„Verstärkung des Kampfs gegen Radikalisierung“: Mit polizeilichen Mitteln. Die vor einem Jahr bei Europol installierte „Meldestelle für Internetinhalte“ soll dazu weiter wachsen. Nach 10.000 Dateien von al-Qaida und dem „Islamischen Staat“ wurden nun erstmals Inhalte im Zusammenhang mit „illegaler Migration“ zur Löschung gemeldet bzw. aus dem Internet entfernt. Die Innenminister fordern zudem die Einrichtung eines „EU-Zentrums zur Bekämpfung von Terrorismus und Radikalisierung im Internet“ zur „Aufdeckung entsprechender Inhalte“. Internetfirmen sollen dazu bewegt werden, Dateien beim Upload mit einem Filter von Microsoft selbst zu überwachen und wenn nötig zu entfernen. Ziel ist die Einrichtung einer öffentlich-privaten Meldeplattform, Europol tauscht dazu ab Mai 2017 Personendaten auch mit Privatfirmen aus. (Drucksache 18/6591)

Aushebelung von verschlüsselter Kommunikation: Es geht laut BMI nicht um Backdoors, aber Möglichkeit für „effektive Ermittlungen“ (Divergenz der französischen und deutschen Version des Papiers). Deutschland und Frankreich hatten bereits vor einigen Monaten gemeinsame Sicherheitsforschungsprojekte für nun benannte „gute Praxis und innovative Ideen“ gegen Verschlüsselung verabredet. „Lösungen“ dürften im vermehrten Einsatz von Trojanern bestehen (Senkung gesetzlicher Hemmschwelle), außerdem könnten Provider wie Telegram oder Facebook gezwungen werden, mitlesende Ermittler/innen in verschlüsselte Chat-Gruppen einzuschleusen. Die Aufforderung an „EU-Mitgliedstaaten und Drittstaaten“ zur Unterzeichnung und Ratifizierung der Budapest Konvention über Cyberkriminalität bedeutet unter anderem den grenzüberschreitenden Einsatz von Trojanern.

Gleichbehandlung von internet-basierten Diensten und Telekommunikationsdiensten: Erweiterung der Vorratsdatenspeicherung auf Anbieter wie Skype, Telegram, Whatsapp oder Facebook. Anbieter müssten Schnittstellen gemäß Telekommunikations-Überwachungsverordnung (TKÜV) bereitstellen. Vorstoß des BMI vom 11. August 2016, Forderung nach Regulierung in der gesamten EU. Europäische Kommission zur Prüfung eines „Regelungsvorschlag“ aufgefordert.

„Verschärfung des Host Provider Privilegs bei Mißbrauch für Terrorpropaganda“: Unter Maßgabe einer „Produkthaftung“ sollen „Direktanfragen“ von Ermittlungs- und Strafverfolgungsbehörden und Europol (!) bei Internet Providern möglich werden. Deutschland und Frankreich stimmen wechselseitigen Anfragen zu, die rechtliche Grundlage ist aber unklar. Forderung einer solchen Regelung für die gesamte EU richtet sich an die Europäische Kommission. Die soll Rahmenbedingungen ausarbeiten um „möglichst einheitliche Handhabung dieser Art der Zusammenarbeit“ sicherzustellen (betrifft nicht nur Bestandsdaten). De Maizière arbeitet mit US-Heimatschutzministerium an Verfahren zu „Direktanfragen“ von Strafverfolgungsbehörden bei dortigen Providern („ausschließlich auf freiwilliger Basis“), Vorschlag kam von niederländischer Ratspräsidentschaft. (Drucksache 18/9266)

Noch mehr Zusammenarbeit der Geheimdienste: Schon jetzt vernetzen sich europäische Inlandsgeheimdienste erstmals physisch in einem „Anti-Terror-Zentrum“ in Den Haag. Es gehört zur 2001 gegründeten „Counter Terrorism Group“, (CTG) bzw. übergeordnet zum geheimnisumwitterten „Berner Club“. Ziel ist zunächst der Austausch und die Verarbeitung von Informationen zum Phänomenbereich „Islamistischer Terrorismus“ mit einer Datenbank und interaktivem „Echtzeit-Informationssystem“. Die EU hat keine Kompetenz zur Koordination der Geheimdienste, als Parallelstruktur wird dies von CTG und „operativer Plattform“ übernommen. EU-Anti-Terrorbeauftragter nimmt an wichtigen Konferenzen teil, CTG soll fortan zu JI-Rat eingeladen werden. Europol und CTG wollen „strukturelle Zusammenarbeit“ intensivieren. Parlamentarische Kontrolle der CTG scheitert an „Third-Party-Rule“.

Ausrüstung der Außengrenzen „mit der geeigneten und neusten technischen Ausrüstung“: Verpflichtender Abgleich aller Einreisenden mit internationalen Datensystemen, darunter auch mit Interpols Datenbank für gestohlene oder verlorene Ausweisdokumente (SLTD). Einführung von „systematischen Kontrollen“ an Schengen-Grenzen auf Forderung Deutschlands. (Drucksache 18/8324, 18/4033, 18/3236, 18/2429)

„Rechtliches Instrumentarium, mit dem Grenzkontrollen wiedereingeführt werden können“: Deutschland und Frankreich sorgten nach dem Arabischem Frühling schon 2012 für Änderung des Artikel 26 SGK zur Wiedereinführung von Grenzkontrollen für bis zu zwei Jahre. Mehrere Mitgliedstaaten berufen sich derzeit darauf. Um auch danach weiterhin kontrollieren zu können, wird der Terminus „lageangepasste Kontrollen unterhalb der Schwelle von flächendeckenden Grenzkontrollen“ und neue Begründung „terroristische Bedrohung“ eingeführt.

„Neuer Partnerschaftsrahmen mit Drittstaaten“: Engere Kooperation mit den Türstehern der Festung Europa („neue EU-Polizeipartnerschaften“). Polizeiliche Ausbildungs- und Ausstattungshilfe für Tunesien kommt derzeit vor allem aus Deutschland, nun wird Ägypten Schlüsselpartner. Frontex verhandelt Arbeitsabkommen mit Tunesien, Marokko, Libyen und Ägypten, schloss außerdem 18 Arbeitsvereinbarungen mit Nicht-EU-Staaten zum „Kapazitätsaufbau“. (Drucksache 18/9262, 18/7839, 18/7724)

Stärkung des „Ständigen Ausschuss des Rates für die innere Sicherheit“ (COSI) für „bessere operationelle Koordinierung im Bereich Sicherheit“: Eigentlich übergeordnetes Gremium um operative Maßnahmen der Mitgliedstaaten und EU-Agenturen Europol, Frontex, Eurojust, OLAF, CEPOL zu koordinieren. Derzeit wichtige politische Funktion durch „Empfehlungen“ für die Beseitigung von Defiziten. Früher auf „schwere organisierte Kriminalität“ beschränkt, jetzt zunehmende Ausweitung auf „Terrorismus“. Für Deutschland nehmen regelmäßig das Bundesinnenministerium, der Leiter der Unterabteilung ÖS I „Polizeiangelegenheiten“ sowie Bundesländer teil. Kritiker/innen sehen im COSI ein „Mini-Innenministerium“. Zur Debatte steht, Untergruppen oder „Expertengruppen“ einzurichten.