

**GENERALDIREKTION INTERNE POLITIKBEREICHE**  
**FACHABTEILUNG FÜR BÜRGERRECHTE UND KONSTITUTIONELLE**  
**ANGELEGENHEITEN**

**BÜRGERLICHE FREIHEITEN, JUSTIZ UND INNERES**

**Interoperabilität der Informationssysteme im**  
**Bereich Justiz und Inneres**

**STUDIE**

Im Auftrag des LIBE-Ausschusses

ZUSAMMENFASSUNG

**Abriss**

In dieser Studie, die von der Fachabteilung für Bürgerrechte und konstitutionelle Angelegenheiten des Europäischen Parlaments auf Ersuchen des Ausschusses für bürgerliche Freiheiten, Justiz und Inneres (LIBE-Ausschuss) des Europäischen Parlaments in Auftrag gegeben wurde, werden hauptsächlich die Vorschläge der Kommission vom Dezember 2017 für eine Verordnung zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen für Justiz und Inneres bewertet. Zunächst werden in der Studie die Beziehungen zwischen den Informationssystemen bei der aktuellen und der vorgeschlagenen Umsetzung analysiert. Anschließend werden zentrale Elemente in den Vorschlägen der Kommission bewertet, darunter auch der verwendete Interoperabilitätsbegriff, die Problembeschreibung, die Ziele und die vorgeschlagenen Lösungen sowie die Umsetzung und die Folgen für die Grundrechte und die Datensicherheit.

## **ÜBER DIE VERÖFFENTLICHUNG**

Diese Studie wurde vom Ausschuss für bürgerliche Freiheiten, Justiz und Inneres des Europäischen Parlaments beantragt und von der Fachabteilung für Bürgerrechte und konstitutionelle Angelegenheiten in Auftrag gegeben, beaufsichtigt und veröffentlicht.

Die Fachabteilungen liefern den internen und externen unabhängigen Sachverstand zur Unterstützung der Ausschüsse des Europäischen Parlaments und anderer parlamentarischer Gremien bei der Ausarbeitung der Gesetzgebung und Ausübung der demokratischen Kontrolle über die externen und internen Politikbereiche der EU.

Um mit der Fachabteilung für Bürgerrechte und konstitutionelle Angelegenheiten Kontakt aufzunehmen oder um ihren Newsletter zu abonnieren, wenden Sie sich bitte an:

[poldep-citizens@ep.europa.eu](mailto:poldep-citizens@ep.europa.eu)

## **Für die Forschung zuständiger Verwaltungsrat**

Dr. Udo Bux

Fachabteilung für Bürgerrechte und konstitutionelle Angelegenheiten

Europäisches Parlament

B-1047 Brüssel

E-Mail: [poldep-citizens@ep.europa.eu](mailto:poldep-citizens@ep.europa.eu)

## **Editionsassistenz**

Monika Laura LAZARUK

## **AUTOREN**

Mirja GUTHEIL, Optimity Advisors

Quentin LIGER, Optimity Advisors

James EAGER, Optimity Advisors

Yemi OVIOSU, Optimity Advisors

Daniel BOGDANOVIC, Optimity Advisors

Mit Unterstützung von Professor Katrin NYMAN-METCALF, Estnische Akademie für e-Governance und Technische Universität Tallinn; Dr. Niovi VAVOULA, Queen Mary, Universität London; Jeremy COLLINS, Optimity Advisors; und Carolin Möller, Optimity Advisors.

## **SPRACHFASSUNGEN**

Original: EN

Redaktionsschluss: April 2018.

© Europäische Union, 2018

Dieses Dokument ist im Internet unter folgender Adresse abrufbar:

<http://www.europarl.europa.eu/supporting-analyses>

## **HAFTUNGSAUSSCHLUSS**

Die hier vertretenen Auffassungen geben die Meinung der Verfasser wieder und entsprechen nicht unbedingt dem offiziellen Standpunkt des Europäischen Parlaments.

Nachdruck und Übersetzung der Veröffentlichung – außer zu kommerziellen Zwecken – mit Quellenangabe gestattet, sofern der Herausgeber vorab unterrichtet und ihm ein Exemplar übermittelt wird.

## ZUSAMMENFASSUNG

### Interoperabilität der JI-Informationssysteme: Geschichte und Kontext

Diskussionen über die Interoperabilität der Informationssysteme der EU für Justiz und Inneres (JI)<sup>1</sup> kamen im Anschluss an die Terroranschläge am 11. September 2001<sup>2</sup> auf und setzten sich in den gesamten 2000er Jahren fort. Die Terroranschläge auf dem Hoheitsgebiet der EU – die Bombenanschläge von Madrid im Jahr 2004 und die Bombenschläge von London im Jahr 2005 – waren der wichtigste Faktor, der schließlich zur Veröffentlichung der Mitteilung der Kommission über die Verbesserung der Effizienz der europäischen Datenbanken im Bereich Justiz und Inneres und die Steigerung ihrer Interoperabilität sowie der Synergien zwischen ihnen im Jahr 2005 führte.<sup>3</sup> Allerdings sorgte die Kritik bedeutender Interessenträger, wie beispielsweise des Europäischen Datenschutzbeauftragten (ESDB), dafür, dass diese Diskussionen nicht vorangetrieben wurden. Die Kritik bezog sich auf zwei Themen: die **Bestimmung des Begriffs** der Interoperabilität; und die Erwägung der möglichen **Folgen für den Schutz personenbezogener Daten**.<sup>4</sup>

Im folgenden Jahrzehnt wurden mit Blick auf die Interoperabilität nur im begrenzten Umfang Maßnahmen ergriffen, obwohl im Zusammenhang mit der Umgebung für die JI-Informationssysteme der EU bedeutende Entwicklungen zu verzeichnen waren, darunter beispielsweise die Einrichtung des VIS<sup>5</sup>, des SIS II<sup>6</sup> und des ECRIS.<sup>7</sup>

Im Anschluss an weitere Terroranschläge auf dem Boden der EU – und zwar die Anschläge von 2015 in Paris und die Anschläge vom März 2016 in Brüssel – nahmen die Diskussionen über die Interoperabilität neuen Schwung auf. Als Folge davon gelangte die Umsetzung der Interoperabilität der JI-Informationssysteme im Zeitraum von 2015 bis 2017 wieder ganz oben auf die politische Agenda, unter anderem durch die Veröffentlichung folgender Dokumente: mehrerer Schlussfolgerungen des Rates<sup>8</sup>; eines Fahrplans des Rates<sup>9</sup>; und einer gemeinsamen Erklärung der EU-Minister für Justiz und Inneres im Jahr 2016<sup>10</sup>.

Ausgehend von diesem Schwerpunkt und den Forderungen des Rates veröffentlichte die Kommission im Jahr 2016 ihre Mitteilung mit dem Titel „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“.<sup>11</sup> In dieser Mitteilung wurden „vier Aspekte“<sup>12</sup> der Interoperabilität vorgestellt und darin war auch die Gründung einer hochrangigen Expertengruppe für Informationssysteme und Interoperabilität, die die rechtlichen, technischen und operativen Bedingungen dieser vier Aspekte untersuchen sollte, vorgesehen. Im Juni 2017 **gab die Kommission** im Anschluss an den Schlussbericht der hochrangigen

---

<sup>1</sup> Aufgrund seiner gehäuftten Verwendung in den Vorschlägen der Kommission wurde der Begriff „Justiz und Inneres“ (JI) anstelle des Begriffs „Raum der Freiheit, der Sicherheit und des Rechts“ (RFSR) gewählt.

<sup>2</sup> Rat der Europäischen Union, Dokument 13176/01 (24.10.2001).

<sup>3</sup> COM(2005) 597 endgültig vom (24.11.2005).

<sup>4</sup> ESDB (2006) Kommentare zu der Mitteilung der Kommission über die Interoperabilität der europäischen Datenbanken.

<sup>5</sup> Entscheidung 2004/512/EG des Rates.

<sup>6</sup> Verordnung (EG) Nr. 1987/2006 (Zusammenarbeit der Grenzkontrollbehörden); Beschluss des Rates 2007/533/JI (Zusammenarbeit im Bereich der Strafverfolgung); Verordnung (EG) Nr. 1986/2006 (Zusammenarbeit im Bereich der Fahrzeugzulassung).

<sup>7</sup> Rahmenbeschluss 2009/315/JI des Rates; und Beschluss 2009/316/JI des Rates.

<sup>8</sup> Rat der Europäischen Union, Dokument EUCO 28/15 (18.12.2015); Rat der Europäischen Union, Dokument EUCO 34/16 (15.12.2016).

<sup>9</sup> Rat der Europäischen Union, Dokument 9368/1/16 (06.06.2016).

<sup>10</sup> Rat der Europäischen Union, Dokument 158/16 (24.03.2016).

<sup>11</sup> COM(2016) 205 final vom 06.04.2016.

<sup>12</sup> A. a. O., S. 14.

Expertengruppe **ihre Absicht bekannt, einen Rechtsetzungsvorschlag zur Interoperabilität vorzulegen.**<sup>13</sup>

Am 12. Dezember 2017 veröffentlichte die Europäische Kommission ihre Vorschläge für eine Verordnung zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen.<sup>14</sup> Mit den Vorschlägen, die von Form von zwei getrennten und jedoch sehr eng miteinander in Zusammenhang stehenden Rechtsetzungsvorschlägen vorgelegt wurden, sollen vier zentrale Lösungen umgesetzt werden.

Das **Europäische Suchportal (ESP)** würde die gleichzeitige Abfrage mehrerer JI-Informationssysteme unter Verwendung von Identitätsdaten (sowohl biografischer als auch biometrischer Art) (das zentrale SIS, Eurodac, VIS, das künftige EES und das vorgeschlagene ETIAS- sowie das vorgeschlagene ECRIS-TCN-System sowie die einschlägigen Interpol-Systeme und Europol-Daten) ermöglichen (Kapitel II).

Der **gemeinsame Dienst für den Abgleich biometrischer Daten (gemeinsamer BMS)** würde die Abfrage und den Abgleich biometrischer Daten (Fingerabdrücke und Gesichtsbilder) aus mehreren Informationssystemen der EU (SIS, Eurodac, VIS, künftiges EES und vorgeschlagenes System ECRIS-TCN) durch die Erzeugung und Speicherung mathematischer Repräsentationen der biometrischen Daten ermöglichen (Kapitel III).

Der **gemeinsame Speicher für Identitätsdaten (CIR)** wäre die gemeinsame Komponente für die Speicherung biografischer und biometrischer Identitätsdaten von Drittstaatsangehörigen, die in Eurodac, im VIS, in dem künftigen EES, dem vorgeschlagenen ETIAS und dem vorgeschlagenen System ECRIS-TCN gespeichert sind.

Mit dem **Detektor für Mehrfachidentitäten (MID)** würde geprüft, ob die abgefragten Identitätsdaten in mehr als einem der Systeme vorhanden sind, und ein Mechanismus zur Untersuchung und Überprüfung der verbundenen Identitätsdaten (Daten im CIR sowie im SIS) ermöglicht (Kapitel V).

Zudem soll mit den vorgeschlagenen Verordnungen Folgendes umgesetzt werden:

**ein zweistufiges Datenabfrageverfahren für den Datenzugriff von Strafverfolgungsbehörden auf Informationssysteme anderer Behörden** zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung terroristischer und sonstiger schwerer Straftaten (Artikel 22):

- Durch die Trefferkennzeichnungsfunktion im CIR könnten Strafverfolgungsbehörden feststellen, in welchen Informationssystemen Datensätze zu Einzelpersonen vorliegen, ohne dass dabei die zugrundeliegenden Daten sichtbar wären.
- Hierauf könnten die Strafverfolgungsbehörden jeweils im Einklang mit den geltenden Vorschriften und Verfahren nach Maßgabe der Verordnungen für jedes Informationssystem den Zugriff auf jedes System, in dem Daten vorhanden sind, beantragen.

**ein zentraler Speicher für Berichte und Statistiken (CRRS):** Durch diesen Speicher könnten Berichte mit anonymisierten statistischen Daten aus allen

---

<sup>13</sup> COM(2017) 261 final vom 16.5.2017.

<sup>14</sup> Vorschläge für eine Verordnung zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen: COM(2017) 794 final, Brüssel, 12.12.2017; und COM(2017) 793 final, Straßburg, 12.12.2017.

Informationssystemen zu politischen und operativen Zwecken sowie für die Zwecke der Datenqualität erstellt und ausgetauscht werden (Artikel 39).

**universelles Nachrichtenformat (UMF):** Beim UMF würde es sich um eine standardisierte technische Sprache zur Beschreibung und Verknüpfung der Datenelemente handeln, die eine einfachere Integration und Interoperabilität der Informationssysteme der EU und der Mitgliedstaaten ermöglichen würde (Artikel 38).

In den Vorschlägen werden auch **Mechanismen für die automatische Datenqualitätskontrolle** eingeführt (Artikel 37). Diese Mechanismen umfassen die Einführung automatischer Validierungsregeln bei der Dateneingabe und die Schaffung gemeinsamer Datenqualitätsindikatoren und Mindestqualitätsstandards. Wenngleich ihre Entwicklung in Artikel 37 vorgesehen ist und zugehörige Rollen und Verantwortlichkeiten ausführlich dargestellt werden, müssen die wesentlichen Merkmale dieser Mechanismen noch ausgearbeitet werden.

### **Aktuell vorhandene und vorgeschlagene JI-Informationssysteme**

Im Hinblick auf die aktuelle Umsetzung muss unbedingt angemerkt werden, dass **jedes der JI-Informationssysteme für einen bestimmten Zweck eingerichtet – oder vorgeschlagen – wurde** und zwar jeweils innerhalb eines bestimmten institutionellen Kontexts. Auch wenn die verschiedenen Systeme weiterhin grundlegend verschiedenen Zwecken dienen, zeichnen sich klare Trends hinsichtlich der folgenden Aspekte ab:

- i. Die **Ausweitung des Anwendungsbereiches der Systeme im Verlauf der Zeit.** So wurde das Eurodac beispielsweise auf umfassendere Migrationsangelegenheiten und Strafverfolgungszwecke ausgeweitet.
- ii. **Zunehmende Überschneidung bei den sekundären Zwecken der Systeme,** hauptsächlich im Zusammenhang mit dem Zugriff von Strafverfolgungsbehörden. So ist etwa die Ermittlung von Drittstaatsangehörigen, die sich illegal in einem Mitgliedstaat aufhalten, mittlerweile sowohl mithilfe von Eurodac, SIS II, VIS als auch EES möglich.

Die Ergänzung von Funktionen und Zwecken bei den unterschiedlichen Informationssystemen kann zu einer **Verwischung der Grenzen zwischen der Einwanderungskontrolle und der inneren Sicherheit** führen.

Die **Daten, die von jedem System erhoben werden, beziehen sich hauptsächlich, jedoch nicht ausschließlich, auf Drittstaatsangehörige.** Hieraus ergeben sich möglicherweise Folgen für die Interoperabilitätsvorschläge, da mit einigen Lösungen nur Drittstaatsangehörige erreicht werden sollen, aber darin auch Datenbanken mit EU-Staatsangehörigen einbezogen werden. Zudem **gibt es bei den Systemen hinsichtlich der erhobenen biografischen und biometrischen Identitätsdaten erhebliche Überschneidungen.** Darüber hinaus liegen bei anderen Daten als Identitätsdaten, die mit dem VIS und EES sowie mit dem EES und ETIAS erhoben werden, erhebliche Überschneidungen vor. Da für viele Reisende im EES und mindestens einem weiteren dieser Informationssysteme Einträge vorliegen würden, wurde der Interoperabilität zwischen diesen Systemen in den entsprechenden Rechtsetzungsvorschlägen Rechnung getragen.

Als Herausforderungen bei den bestehenden Systemen lässt sich eine **Reihe übergreifender Problemstellungen** feststellen. Am stärksten betont wurden folgende:

Fragmentierung der EU-Datenarchitektur;

effektives Risikomanagement und effektiver Schutz der Rechte betroffener Personen;

schlechte Datenqualität und

heterogene Nutzung in den Mitgliedstaaten.

### **Interoperabilitätsvorschläge: Bestimmung des Begriffs der Interoperabilität**

Das **Konzept der Interoperabilität wird von der großen Mehrheit der Interessenträger positiv betrachtet, sofern eine sachgemäße Umsetzung erfolgt.** Wenn verschiedene Informationssysteme miteinander verbunden werden, um die operative Effizienz für Endnutzer zu verbessern, während gleichzeitig die Zugangsrechte streng reguliert werden und der Schutz personenbezogener Daten uneingeschränkt geachtet wird, kann sich dies als sehr sinnvolle Maßnahme erweisen. Mit der Interoperabilität sollen aber keine neuen Speicherungsarten oder neue Verarbeitungsweisen personenbezogener Daten, die über die Zwecke jedes Systems hinausgehen, oder neue Zugangsrechte geschaffen werden.

In den Rechtsetzungsvorschlägen der Kommission zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen **wird die Begriffsbestimmung für das Konzept der Interoperabilität jedoch nicht ausdrücklich genannt und nicht in ausreichendem Maße dargelegt, wie bereits vom ESDB am deutlichsten hervorgehoben.** Die Ursprünge der Begriffsbestimmung liegen eindeutig im Bereich der elektronischen Behördendienste, aber für die Anwendung ist ein weitaus größeres Maß an Klarheit hinsichtlich der Frage notwendig, wie das Konzept der Interoperabilität – insbesondere die Begriffe der rechtlichen, semantischen, operativen und technischen Interoperabilität – bei der Ausarbeitung und Gestaltung der Lösungen zur Anwendung gekommen ist.

Deshalb besteht **die größte Herausforderung bei den Vorschlägen darin, dass damit in Wirklichkeit kein Rahmen für die Interoperabilität geschaffen wird, sondern dass damit technische Lösungen vorgeschlagen werden, von denen einige mit dem Konzept der Interoperabilität vereinbar sind und einige nicht.** Darüber hinaus beruht das Verständnis von Interoperabilität offenbar auf den angedachten Lösungen und nicht auf Lösungen, die auf der Grundlage eines klaren, transparenten und abgestimmten Verständnisses von Interoperabilität entwickelt wurden. Der Begriff der Interoperabilität bedarf jedoch einer klaren Bestimmung, einschließlich seiner Abgrenzung, da er sich andernfalls als flexibles Konzept erweisen wird, bei dem sich ständig weitere Anforderungsänderungen ergeben.

Zudem kämen den Vorschlägen mehr Klarheit und Transparenz bei den folgenden übergreifenden Problemstellungen sehr zugute:

**Verwendung von präsumtiver Terminologie,** mit der die Notwendigkeit der Vorschläge mit wenigen unterstützenden Nachweisen immer wieder behauptet wird.

**Eingeschränkte Konsultationen,** insbesondere hinsichtlich der Folgen der Vorschläge für den Datenschutz und die Grundrechte.

### **Problembeschreibung und Erfordernisse**

In der Problembeschreibung werden folgende zwei Hauptprobleme im Zusammenhang mit der gegenwärtigen Situation hervorgehoben:

- i. Die Informationen in den bestehenden Datenbanken sind nicht immer vollständig, richtig und zuverlässig.
- ii. Endnutzer haben nicht immer einen schnellen und systematischen Zugriff auf sämtliche Informationen, die sie für die Erledigung ihrer Aufgaben benötigen. In einigen Fällen werden die bestehenden Rechte für den Zugriff auf die verschiedenen Systeme im

Einklang mit den EU-Rechtsinstrumenten nicht in vollem Umfang ausgeübt, da bestimmte technische und praktische Mittel auf einzelstaatlicher Ebene nicht vorhanden sind.<sup>15</sup>

Es ist klar, dass das zweite Problem durch Interoperabilität angegangen werden kann, aber es muss besser geklärt werden, wie die Vollständigkeit, Richtigkeit und Zuverlässigkeit der Daten durch Interoperabilität verbessert werden können. Die vorgeschlagenen Maßnahmen zur Verbesserung der Datenqualität und des Betriebs des CIR, des gemeinsamen BMS und des MID könnten zu Lösungen für die erste Anforderung beitragen, aber damit werden neue Zugriffsrechte, neue Arten der Verarbeitung personenbezogener Daten und neue Zugriffsarten eingeführt.

In der Problembeschreibung werden zudem zwei wesentliche Problemfaktoren hervorgehoben. **Die Unterschiede zwischen den Faktoren werden nicht klar erläutert, und die Faktoren lassen darauf schließen, dass fehlende Interoperabilität der Nährboden für die oben genannten Probleme ist.** In Wirklichkeit sind es die Einzelpersonen, die mit der Eingabe der Daten beauftragt sind, die für die Vollständigkeit, Richtigkeit und Zuverlässigkeit der Daten in jedem System verantwortlich sind.

Ferner wurden die verschiedenen Informationssysteme, ausgehend von den spezifischen Zwecken jedes Systems und im Einklang mit dem Datenschutzgrundsatz der Zweckbindung, absichtlich getrennt entwickelt<sup>16</sup>; und bei den Erfordernissen, die in den Vorschlägen zum Ausdruck gebracht werden, fehlen häufig unterstützende Nachweise.

## Ziele

In den **Vorschlägen werden verschiedene Gruppen von Zielen aufgeführt, deren Verbindungen nicht klar erläutert werden.** In der Begründung werden allgemeine, im Vertrag verankerte Ziele und spezifische Ziele vorgebracht, und in Artikel 2 des Rechtsetzungstextes werden weitere Ziele präsentiert.

Weiterhin werden in den allgemeinen Zielen, die in der Begründung erläutert werden, Ziele im Zusammenhang mit der Einwanderung und der inneren Sicherheit zusammengeführt. Dies kann, wie bereits vom EDSB betont, zu einer **Verschmelzung der Migrationssteuerung mit der Steuerung der inneren Sicherheit sowie einem Verwischen der Grenzen zwischen den beiden Politikfeldern** mit einer praktisch austauschbaren Verwendung der Begriffe im Zusammenhang mit den JI-Informationssystemen führen. Ferner sollte klar angegeben werden, dass die sicherheitsbezogenen Ziele bei den meisten Informationssystemen, auf die sich die Vorschläge beziehen (nicht SIS II oder ECRIS-TCN), auch sekundäre Ziele darstellen.

In der Begründung der Vorschläge werden auch vier spezifische Ziele festgelegt. Mit diesen **Zielen werden bedeutsame neue Zwecke für die bestehende Umgebung der JI-Informationssysteme eingeführt.** Die Aufdeckung von Mehrfachidentitäten und die Vereinfachung von Identitätsprüfungen bei Drittstaatsangehörigen im Hoheitsgebiet eines Mitgliedsstaats sind zwei bedeutsame neue Ziele für die bestehenden und die geplanten JI-Informationssysteme. Darüber hinaus weisen diese beiden neuen Ziele jeweils ein ausgeprägtes Sicherheitselement und eine eingeschränkte Relevanz für die Ziele der bestehenden und geplanten JI-Informationssysteme auf.

---

<sup>15</sup> Folgenabschätzung Begleitunterlage zum Vorschlag für eine Verordnung zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen, S. 9.

<sup>16</sup> Datenschutz-Grundverordnung (DSGVO), Artikel 5 Absatz 1.

In Artikel 2 der Vorschläge werden die Ziele des Rechtsetzungstextes vorgestellt. In Absatz 1 werden einfach die allgemeinen Ziele der bestehenden und geplanten Informationssysteme genannt und damit **verschiedenartige Systeme und ihre Ziele gleichgesetzt**.

### **Zwecke und Gestaltung der Lösungen**

Das **Europäische Suchportal (ESP)** könnte eine **äußerst erfolgreiche Innovation sein, die wahrscheinlich zu einer verbesserten operativen Effizienz führen wird**. Zudem ist keine bedeutsame Datenaggregation möglich, und es werden keine zusätzlichen Informationssysteme entwickelt. Daher wird das ESP zur Verwirklichung des ersten spezifischen Ziels (d. h. Vereinfachung eines schnellen, nahtlosen, systematischen und kontrollierten Zugriffs durch Behörden) beitragen und könnte ohne Folgen für den Datenschutz eingeführt werden. Allerdings könnte sich der Schutz personenbezogener Daten bei der Ausarbeitung der delegierten Rechtsakte im Zusammenhang mit den Nutzerprofilen und der Pflege bestehender Zugriffsrechte als Herausforderung erweisen. Diese sollten mit erheblicher Zuarbeit aus dem Bereich des Datenschutzes ausgearbeitet werden.

Schließlich muss weiter geklärt werden, inwieweit die Eigentümer von Interpol-Daten über Abfragen mit einer Relevanz für ihre Daten benachrichtigt werden. Es ist beispielsweise unklar, ob der Eigentümer von Interpol-Daten über erfolgte Abfragen benachrichtigt wird.

Der **gemeinsame Dienst für den Abgleich biometrischer Daten (gemeinsamer BMS)** wird wahrscheinlich zur Verwirklichung der Ziele, für die er bestimmt ist, durch die Speicherung und Verwendung mathematischer Repräsentationen biometrischer Daten für das ESP, den CIR und den MID beitragen. Jedoch handelt es sich beim gemeinsamen BMS um eine neue Datenbank, die daher nicht mit einer angemessenen Definition des Begriffs der Interoperabilität übereinstimmt. Darüber hinaus muss weiter geklärt werden, ob es sich bei mathematischen Repräsentationen (d. h. biometrische Templates), die im gemeinsamen BMS gespeichert werden, um personenbezogene Daten handelt.

Ungeachtet des Umstands, ob es sich bei mathematischen Repräsentationen um personenbezogene Daten handelt oder nicht, ist jedoch klar, dass der gemeinsame BMS bei der Aufdeckung von Mehrfachidentitäten in den verschiedenen Informationssystemen einen Mehrwert bieten kann. Allerdings wird nicht anerkannt, und hierin spiegelt sich die eingeschränkte Untersuchung der Optionen in der Folgenabschätzung wider, dass der gemeinsame BMS auch ohne die anderen Interoperabilitätskomponenten einen Nutzen bieten würde. **Mit dem gemeinsamen BMS wäre es immerhin möglich, in allen Systemen außer dem ETIAS Mehrfachidentitäten aufzudecken, wenn die Aufdeckung von Mehrfachidentitäten auf dem Vergleich und der Abfrage biometrischer Daten beruht**. Betrachtet man die Folgen der Einführung des CIR und des MID, handelt es sich hierbei um eine mögliche alternative Umsetzungsoption.

Der **gemeinsame Speicher für Identitätsdaten (CIR)** wird wahrscheinlich zur Erreichung seines Zwecks und seiner zugehörigen Ziele beitragen. Er wird insbesondere die Identifizierung von Drittstaatsangehörigen im EU-Hoheitsgebiet enorm erleichtern, die Arbeitsweise des MID bei der Aufdeckung und Bestätigung von Mehrfachidentitäten in den verschiedenen Systemen unterstützen und den einheitlichen Prozess für den Zugriff von Strafverfolgungsbehörden auf Datenbanken anderer Behörden vereinfachen. Jedoch stellt die Einrichtung des CIR den invasivsten Aspekt der Interoperabilität – gemäß Begriffsbestimmung der Kommission – dar und wirft in vielerlei Hinsicht datenschutzrechtliche Bedenken auf:

Zunächst **geht aus dem Text über seine Architektur nicht klar hervor, ob es sich dabei um eine getrennte Datenbank handelt wird**. Ferner wird in den Vorschlägen ausdrücklich festgestellt, dass



es sich beim CIR nicht um eine neue Datenbank handelt, sondern um einen „Speicher“, wobei Begriffe wie „gespeichert“ und „speichern“ verwendet werden.<sup>17</sup> Diese Auffassung wird ebenfalls im Rechtsetzungstext gestützt, in dem der CIR in gleicher Weise wie die gegenwärtigen und geplanten Informationssysteme erörtert wird (siehe beispielsweise Artikel 9, 11 und 14). Vor dem Hintergrund der obigen Ausführungen **handelt es sich beim CIR offenbar nicht um eine Interoperabilitätslösung, und falls dies so ist, sollte dieser Umstand dementsprechend erklärt und behandelt werden.**

Ferner **wird der CIR** bei Identitätsprüfungen von Drittstaatsangehörigen auf dem Hoheitsgebiet eines Mitgliedstaats durch Strafverfolgungsbeamte **als Datenbank fungieren**. Daher entspricht sein Betrieb der Schaffung einer neuen Datenbank mit folgenden Merkmalen: Schaffung neuer Zugriffsrechte auf personenbezogene Daten in den Informationssystemen; Gleichsetzung aller Arten von Drittstaatsangehörigen; wesentliche Zweckänderung für erhobene personenbezogene Daten in allen Systemen. Ferner steht diese Zweckänderung im Zusammenhang mit den sekundären Zwecken der Systeme, was weitere Fragen bezüglich ihrer Verhältnismäßigkeit aufwirft. Schließlich werden die gegenwärtig bestehenden Herausforderungen und Probleme, die diesen neuen Zweck scheinbar erforderlich werden lassen, nicht gründlich genug erläutert oder nachgewiesen.

Die bestehenden Mechanismen für den Zugriff von Strafverfolgungsbehörden auf das VIS sind in die Kritik geraten. Sowohl in der Rechtssache *Digital Rights Ireland* als auch in der Rechtssache *Watson* wurde in den Urteilen erklärt, dass unabhängige Behörden oder Justizbehörden für die Überprüfung der Bedingungen für den Zugriff auf das VIS zuständig sein sollten, und nicht zentrale Zugangsstellen oder Prüfbehörden, die in der selben Organisation, die Zugriff auf das VIS erhalten soll, angesiedelt sein können. Vor diesem Hintergrund wird deutlich, dass diese Bedingungen durch den zweistufigen Ansatz, der in den Interoperabilitätsvorschlägen aufgeführt wird, weiter gelockert werden, wodurch sich folgende Herausforderungen ergeben:

Für die Strafverfolgungsbehörden wäre es möglich, ohne Genehmigung eine Erkenntnis zu erlangen, da das Fehlen eines Datensatzes in den Informationssystemen (d. h. keine Kennzeichnung bei einer Identität) eine Erkenntnis wäre;

durch die Erkenntnisse, die durch die Trefferkennzeichnungsfunktion geliefert werden – d. h. in welcher Datenbank eine Einzelperson geführt wird – werden die gegenwärtigen Zugriffsbedingungen aufgehoben, erhalten Strafverfolgungsbehörden Zugriff auf neue Informationen und werden sämtliche Drittstaatsangehörige aus den verschiedenen Systemen gleichgesetzt.

Daher **werden mit dem CIR die bedeutsamsten Veränderungen gegenüber der gegenwärtigen Umsetzung eingeführt**, und in diesem Zusammenhang stellt der CIR die bedeutsamste Bedrohung für den Schutz personenbezogener Daten und das Recht auf Privatsphäre dar.

Der **Detektor für Mehrfachidentitäten (MID)** wird wahrscheinlich den Zwecken dienen, für die er bestimmt ist, und zur Verwirklichung der festgelegten Ziele beitragen. Allerdings handelt es sich dabei nicht um eine Interoperabilitätslösung, die mit einer angemessenen Definition des Begriffs der Interoperabilität in Einklang steht. Dies liegt daran, dass damit neue Daten in Form von Verknüpfungen und Identitätsbestätigungsdateien geschaffen werden; und damit werden auch neue Zugriffsrechte für Einzelpersonen geschaffen, bei denen eine gelbe Verknüpfung vorliegt.

---

<sup>17</sup> Vorschlag für eine Verordnung zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen, 2017/0352 (COD) und 2017/0351 (COD), S. 7, Absatz 3.

Weiterhin wird der Zweck des MID zur Bekämpfung von Identitätsbetrug nicht durch die Rechtsgrundlage für Eurodac gestützt. Bei der Aufnahme von Eurodac-Daten wäre eine weitere Änderung des Zwecks des Informationssystems notwendig.

Die zusätzlichen Elemente, die in den Vorschlägen vorgetragen werden, stellen ebenfalls keine Interoperabilitätslösungen dar. Allerdings handelt es sich bei der durchgängigen Umsetzung des UMF und der Entwicklung eines CRRS um berechtigte Vorhaben, die ohne weitere Folgen einen Mehrwert bieten.