Sicherheit im Schengen-Raum: Eine unendliche Datensammelei?

Dipl.-Jur. Jonathan Stoklas ist wissenschaftlicher Mitarbeiter am Institut für Rechtsinformatik (IRI) an der Leibniz Universität Hannover.

Der Beitrag ist ebenfalls veröffentlicht worden in: ZD-Aktuell 2017, 05684.

Die Aufrechterhaltung der öffentlichen Sicherheit, insbesondere der Kampf gegen den internationalen Terrorismus, stellt die EU und ihre Mitgliedstaaten vor schwierige Herausforderungen. Bereits im April 2015 hatte die EU-Kommission eine Europäische Sicherheitsagenda vorgestellt, die verschiedene Ansätze verfolgte, um die innereuropäische Zusammenarbeit der Sicherheitsbehörden zu stärken.

Im Hinblick darauf, dass bei den Einreisekontrollen an den Schengen-Außengrenzen die Verantwortlichkeit für die Sicherheit des gesamten Schengen-Raums in den Händen einzelner Mitgliedstaaten liegt, wurde der Nutzung von Datenbanken, etwa dem Schengener Informationssystem (SIS) oder der INTERPOL-Datenbank für verloren gegangene und gestohlene Reisedokumente (SLTD), dabei besondere Bedeutung zugemessen. Um ihre Bestrebungen zu unterstützen, hat die Kommission außerdem eine Expertengruppe eingesetzt, die die Kommission seit Juni 2016 in Fragen zu Informationssystemen und Interoperabilität berät und sich aus Vertretern zuständiger Behörden der Mitgliedstaaten und assoziierter Staaten sowie verschiedener EU-Institutionen (eu-LISA, Frontex, European Union Agency for Fundamental Rights (FRA), European Asylum Support Office (EASO), Europol und der Counter-Terrorism Coordinator (CTC)) zusammensetzt.

Daneben werden auch in dem von der EU unter dem Horizon 2020 Rahmenprogramm kofinanzierten Forschungsprojekt iBorderCtrl derzeit Software- und Hardware-Komponenten entwickelt, die Grenzkontrollen effektiver gestalten sollen. Das Institut für Rechtsinformatik (IRI) ist hierbei für die datenschutzrechtliche Begleitforschung zuständig. Einige Aspekte der fortdauernden Entwicklung hinsichtlich der Sicherheit des Schengen-Raums sollen im Folgenden vorgestellt werden:

1. Im April 2016: Vorschlag zur Einführung eines EES

Im April 2016 wurde eine Mitteilung über solidere und intelligentere Informationssysteme für das Grenzmanagement veröffentlicht, um Möglichkeiten aufzuzeigen, wie die Sicherheit innerhalb des Schengen-Raums weiter verbessert werden könnte. Neben den drei bereits bestehenden europäischen Systemen – dem SIS, dem Visa-Informationssystem (VIS) und der EURODAC Datenbank für Fingerabdrücke von Asylbewerbern – wurde u. a. die Einführung eines weiteren zentralen Systems vorgeschlagen, ein sog. Einreise-/Ausreisesystem (Entry-Exit System – EES). In diesem System sollen alle Grenzübertritte von Angehörigen aus Drittstaaten registriert werden, die den Schengen-Raum für einen Kurzaufenthalt bis zu 90 Tagen (in einem Zeitraum von 180 Tagen) besuchen. Ein entsprechender Verordnungsentwurf wurde parallel zu der Mitteilung veröffentlicht.

2. Seit April 2016: Umsetzung der Fluggastdaten-RL

Ein weiterer Aspekt, der von der Kommission als wichtig erachtet wird, ist eine zügige Umsetzung der Fluggastdaten(Passenger Name Record – PNR)-Richtlinie (RL 2016/681/EU). Die PNR-RL wird insb. aus datenschutzrechtlicher Sicht als kritisch betrachtet (Wendt/Rasche, ZD-Aktuell 2016, 05205). Ein entsprechendes Gesetz (BT-Drs. 18/11501) wurde inzwischen vom Bundestag am 27.4.2017 angenommen und der Bundesrat hat am 12.5.2017 beschlossen, keinen Antrag nach Art. 77 Abs. 2 GG zu stellen (BR-Drs. 333/17 (Beschluss)). Neben der Richtlinie wird auch das „Gesetz zur Umsetzung der Richtlinie (EU) 2016/681“ als übereilt und unverhältnismäßig kritisiert (Tripp, Digitale Gesellschaft v. 12.5.2017). Relevant dürfte in diesem Zusammenhang auch das anstehende Urteil des

EuGH sein, der die Zulässigkeit der PNR-RL überprüfen soll. Die Schlussanträge von Generalanwalt Paolo Mengozzi lassen jedenfalls erhebliche Zweifel an der Rechtmäßigkeit der PNR-RL zu und haben insofern das Potenzial, auch Auswirkungen auf den nun verabschiedeten Gesetzentwurf in Deutschland zu haben.

3. Im November 2016: Vorschlag zur Einführung eines Reiseinformations- und Autorisierungssystems

Ferner hat die EU-Kommission bei der Registrierung von Reisenden aus Drittstaaten eine Informationslücke ausgemacht, die durch ein neu einzuführendes Reiseinformations- und Autorisierungssystem („EU Travel Information and Authorisation System" – ETIAS) geschlossen werden soll. Während Informationen über Angehörige aus Drittstaaten, die der Visapflicht unterliegen, bereits vor Ankunft im VIS vorliegen, ist dies bei Drittstaatlern, die einer Visapflicht nicht unterliegen, nicht der Fall. Bei Flugreisenden werden die Daten zwar in der o. g. Fluggastdatenbank (PNR) gespeichert, dies gilt jedoch nicht für Reisen auf dem Landweg. Hier haben die Sicherheitsbehörden also tatsächlich keinerlei Vorab-Kenntnisse über den Reisenden. Gleichzeitig steige, so die Mitteilung der Kommission, durch die zunehmende Anzahl an Visa-Liberalisierungen und entsprechender Verhandlungen der Bedarf, diesen Entwicklungen zu begegnen. Vergleichbare Systeme seien bereits in den USA, in Kanada und in Australien im Einsatz. Für die Einführung eines ETIAS-Systems wurde im November 2016 ein Verordnungsentwurf vorgelegt.

4. Im Mai 2017: Vorschläge zur Zusammenführung von Daten

Im Mai 2017 wurde durch die Kommission außerdem die Einführung weiterer Maßnahmen, die auf den Abschlussbericht der Expertengruppe zu Fragen der Interoperabilität von Informationssystemen zurückgeht, empfohlen. U. a. wird die Implementierung der folgenden Funktionalitäten angeregt:

a) Die Einführung einer einheitlichen Suchmaske: Durch die Einführung einer einheitlichen Suchmaske soll es ermöglicht werden, verschiedene Datenbanken mit einer Suchanfrage durchsuchen und die Ergebnisse auf einem Bildschirm darstellen zu können. Die Expertengruppe empfiehlt hierzu die Entwicklung eines SSI (Single-Search Interface) für den Zugriff auf die Europäischen Datenbanken SIS, VIS, EURODAC und ECRIS sowie die vorgeschlagenen Systeme EES und ETIAS; darüber hinaus soll das System mit den Datenbanken von Europol und INTERPOL verknüpft werden. Für den Zugriff auf nationale Systeme der Mitgliedstaaten sollen die bereits existierenden, nationalen SSI genutzt werden, wobei von einem nur geringen technischen Anpassungsaufwand ausgegangen wird. Während die Notwendigkeit und die technische Umsetzbarkeit von der Expertengruppe angenommen wurden, heißt es, dass die praktischen Herausforderungen bei der effizienten Nutzung solcher Systeme weiter erforscht werden müssten. Vor diesem Hintergrund verwundert auch das Statement der Expertengruppe, dass eine Umsetzung prinzipiell in voller Einhaltung datenschutzrechtlicher Regeln möglich sei, da letztlich die Verhältnismäßigkeit einer solchen Maßnahme insb. an ihrer Effizienz gemessen werden muss.

b) Abgleich biometrischer Daten: Die Expertengruppe schlägt ferner die Einrichtung eines gemeinsamen Systems zum Abgleich biometrischer Daten vor. Der Expertengruppe zufolge hätte dies zwei wesentliche Vorteile: Einerseits würde ein einheitliches System kostengünstiger im Unterhalt werden, da es die Matching-Funktionalitäten von SIS, VIS, EURODAC, ECRIS, EES, ETIAS und ggf. Europol-Daten ineinander vereinen und somit die Wartung vereinfachen würde. Für diese (zunächst rein technische) Änderung wäre eine Möglichkeit zur Zusammenführung der Daten nicht zwingend erforderlich, sodass dies bereits auf Basis der bestehenden Rechtsgrundlagen möglich wäre. Eine weitere Möglichkeit, die durch eine solche Implementierung allerdings ebenfalls ermöglicht würde und von der Expertengruppe empfohlen wird, ist das sog. „Flagging": Hierbei soll – ebenfalls über ein SSI – die Abfrage aller biometrischer Datenbanken möglich sein. Um dabei möglichst datenschutzfreundlich zu agieren, soll eine „hit/no-hit"-Flag gesetzt werden: Dabei würden bei einer

Anfrage keine spezifischen Daten übertragen werden, sondern lediglich der Hinweis erfolgen, ob Daten in einem anderen System vorhanden sind. Um eine solche „Flag“ einem Datensatz hinzuzufügen, wäre allerdings eine Anpassung der jeweiligen Rechtsgrundlagen für die betroffenen Systeme erforderlich. Der Zweck einer solchen Funktionalität wäre insb. die verbesserte Identifizierung von Personen, die mehrere Identitäten benutzen.

c) Gemeinsames Identitätsregister: Das zuvor genannte System zum Abgleich biometrischer Daten soll nach der Expertengruppe zudem um ein gemeinsames Identitätsregister ergänzt werden. Dieses soll alphanumerische Daten wie den Namen, das Geburtsdatum und das Geschlecht erfassen und ebenfalls dazu dienen, die Nutzung mehrerer Identitäten und Identitätsdiebstahl zu erschweren. Zudem könnte ein solches Register helfen, die Qualität vorhandener Daten zu verbessern. Insb. würde, so die Expertengruppe, die Fragmentierung der Daten in verschiedene Datenbanken – teils als Duplikat – reduziert. Das Identitätsregister wäre mit denselben Datenbanken verknüpft wie das SSI. Das Register selbst solle auch gar keine eigenen Daten beinhalten, sondern diese auf der zuvor genannten „hit/no-hit“-Basis nur aus den bekannten Datenbanken zusammenführen. Dadurch sollen weder die Zugangsrechte noch die Hoheit über die Daten beeinträchtigt werden.

5. Fazit

Die Zusammenführung von Daten und die Schaffung neuer Möglichkeiten zur Analyse von Daten sind Risiko und Chance zugleich: Wird die Qualität von Daten insgesamt erhöht, ergeben sich gerade für die vielen unbescholtenen Reisenden weniger Risiken, als potenziell gefährlich stigmatisiert zu werden. Gleichzeitig ist es jedoch umso wichtiger, Betroffenen wirksame Rechtsmittel an die Hand zu geben, um gegen fehlerhafte Daten und darauf basierende Entscheidungen vorgehen zu können. Gleichzeitig müssen die mit der Zusammenführung von Daten einhergehenden Risiken minimiert werden: Der Zugriff auf Daten sollte auf das notwendige Minimum reduziert werden, die Datenabfrage einer strengen Zweckbindung unterliegen. Weitere Herausforderungen ergeben sich mit Blick auf die geplante Interoperabilität außerdem darin, Daten nur den Behörden zugänglich zu machen, die tatsächlich Zugriff benötigen. Hier wird auch das vorgeschlagene „hit/no-hit“-System an seine Grenzen stoßen: So kann bereits das Vorhandensein einer „Flag“ Auskunft über personenbezogene Merkmale geben, etwa ob die Person über ein Visum verfügt oder eine Meldung im SIS vorliegt. Zudem hat das bloße Wissen, dass Daten existieren, für die Entscheidungsfindung der Behörden keinerlei Mehrwert und wird sich tendenziell eher negativ auf die Datenqualität auswirken. Vor diesem Hintergrund ist genau zu überlegen, in welchen Bereichen der Einsatz von SSI überhaupt sinnvoll umsetzbar ist. Und auch mit Blick auf die Tendenz des Gesetzgebers, einmal vorhandene Daten später auch für weitere Zwecke nutzbar zu machen – wie etwa bei dem am 2.6.2017 vom Bundesrat bestätigten Gesetzentwurf „zur Förderung der Funktion zum elektronischen Identitätsnachweis“, der den Sicherheitsbehörden Zugriff auf im Melderegister gespeicherte Identitätsdaten mit Verfahren zum automatischen Abruf erlaubt – scheint es ratsam, mit der Ermöglichung zusätzlicher Datensammelei zurückhaltend zu sein.