

Kleine Anfrage

der Abgeordneten Andrej Hunko, Sevim Dağdelen, Ulla Jelpke, Niema Movassat, Katrin Werner und der Fraktion DIE LINKE.

Umsetzung des deutsch-amerikanischen Abkommens zur Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität

Während es um die transatlantische Datenübermittlung im Rahmen der PNR- und SWIFT-Abkommen zwischen der Europäischen Union und den USA in den letzten Jahren viele Kontroversen gab, haben zahlreiche europäische Länder – ohne dass dies großes Aufsehen erregt hätte – in den letzten Jahren mit den USA sogenannte Preventing and Combating Serious Crime-Abkommen (PCSC) über den bilateralen Austausch personenbezogener Daten unterzeichnet.

Ausdrückliches Vorbild für diese PCSC ist das Abkommen zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika über die Vertiefung der Zusammenarbeit bei der Verhinderung und Bekämpfung schwerwiegender Kriminalität, das am 1. Oktober 2008 in Washington D. C. unterzeichnet wurde. Trotz erheblicher datenschutzrechtlicher Bedenken der Oppositionsparteien, des Bundesrates und des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit wurde das Abkommen am 3. Juli 2009 vom Deutschen Bundestag ratifiziert. Indes kam es in den USA als „executive agreement“ niemals im Kongress zur Abstimmung.

Nach dem Vorbild des Vertrages von Prüm sieht das Abkommen automatisierte Abfragen der nationalen Polizeidatenbanken mit Fingerabdrücken und DNA-Profilen zu Zwecken der Verfolgung – und im Falle der Fingerabdruckdaten auch zur vorausschauenden Verhinderung – „schwerwiegender Kriminalität“ vor. Darüber hinaus können zum Zweck der Verhinderung „terroristischer Straftaten“ ohne vorheriges Ersuchen auch sensible personenbezogene Daten z. B. zum Sexualleben oder der politischen Gesinnung von Betroffenen in sogenannten Spontanübermittlungen an die andere Vertragspartei weitergegeben werden. Daten, die die Vertragsparteien nach diesem Abkommen gewonnen haben, dürfen für den Zweck strafrechtlicher Ermittlungen und zur Verhinderung einer „ernsthaften Bedrohung für die öffentliche Sicherheit“ sowie in Gerichts- und Verwaltungsverfahren, die im Zusammenhang mit strafrechtlichen Ermittlungsverfahren stehen, weiterverarbeitet und gespeichert werden. Mit Einverständnis der datenübermittelnden Vertragspartei können die Daten auch zu jedem anderen Zweck weiterverarbeitet sowie an Drittstaaten, internationale Organisationen und selbst an Privatunternehmen weitergegeben werden.

Artikel 11 des Abkommens betont, dass „Privatpersonen aus dem Abkommen keine Rechte erwachsen“. Das Recht zur Korrektur oder Löschung von übermittelten Daten bleibt allein den datenübermittelnden Behörden vorbehalten. Die

Details der Datenverarbeitung sowie die Möglichkeiten zur Wahrnehmung von Betroffenenrechten überlässt das Abkommen dem jeweiligen nationalen Recht. Allerdings ist das Datenschutzrecht in den USA nur rudimentär entwickelt, und ein Auskunftsrecht existiert für Bürgerinnen und Bürger aus anderen Staaten nicht. Abhilfe schaffen soll das deutsche Gesetz zur Umsetzung des Abkommens (BGBl. 2009 I Nr. 59, S. 2998 bis 2999), das das Bundeskriminalamt (BKA) als nationale Kontaktstelle für den bilateralen Informationsaustausch benennt und Betroffenen das Recht einräumt, dort eine Auskunftserteilung bei der zuständigen US-amerikanischen Kontaktstelle zu beantragen. Allerdings kann das BKA als Stellvertreter der Betroffenen es unterlassen, diese über den Inhalt der von US-Stellen erteilten Auskunft zu unterrichten, wenn dadurch die „ordnungsgemäße Erfüllung“ seiner Aufgaben oder die „öffentliche Sicherheit oder Ordnung“ gefährdet wären oder dem „Wohle des Bundes oder eines Landes Nachteile“ bereitet würden. Der Schutz Betroffener vor behördlicher Willkür ist damit weder jenseits noch diesseits des Atlantiks hinreichend gesichert.

Bereits heute sind die Personenerkennungssysteme der US-amerikanischen Bundespolizei FBI die größten biometrischen Polizeidatenbanken der Welt: Das „Integrated Automated Fingerprint Identification System“ (IAFIS) greift auf Daten von mehr als 90 Millionen Personen zurück, und im „National DNA Index System“ (NDIS) sind DNA-Profile von knapp neun Millionen Menschen gespeichert. Zusätzlich baut das FBI im Rahmen seiner Programme „Next Generation Identification“ (NGI) und „Combined DNA Index System“ (CODIS) massiv die Fähigkeiten zur Speicherung und Weiterverarbeitung biometrischer Merkmale aus. Dabei geht es um die Integration von bislang beim FBI getrennt gehaltenen Datenbeständen für eine verbesserte Identifizierung durch „multi-modal biometrics“, aber auch um deren Interoperabilität mit anderen Bundesbehörden. Insbesondere das Department of Homeland Security (DHS), sein US-VISIT-Programm und das automatisierte Risk Profiling von Reisenden im Rahmen des „Automated Targeting System“ zielen auf die Akkumulation größtmöglicher Datenmengen, um durch deren Analyse die Einreise unerwünschter Personen zu verhindern.

Längst geht es dabei nicht mehr nur um Terrorismusverdächtige, sondern auch um gänzlich andere Personenkategorien. Angesichts dessen lässt es sich kaum ausschließen, dass durch deutsche Behörden übermittelte Daten aus den vom BKA geführten Personenerkennungsdateien dauerhaft in den USA in diesem Zusammenhang verarbeitet, gespeichert und zweckentfremdet werden, während sich deren Kontrolle und ggf. Korrektur oder Löschung den Möglichkeiten der Betroffenen entzieht.

Wir fragen die Bundesregierung:

1. Wie viele EU-Staaten haben mittlerweile bilaterale PCSC-Abkommen nach dem Vorbild des deutsch-amerikanischen Abkommens mit den USA unterzeichnet?
2. Existieren für den Bereich der Übermittlung von Daten zur Verhinderung terroristischer Straftaten neben dem deutsch-amerikanischen Abkommen vom 1. Oktober 2008 weitere bilaterale Abkommen, z. B. entsprechend der US-amerikanischen Homeland Security Presidential Directive 6?
Wenn ja, welche, und mit welchem Inhalt?
3. Wie sind zwischen der Bundesrepublik Deutschland und den USA die Einzelheiten der technischen Ausgestaltung für den automatisierten Abruf von daktyloskopischen Daten geregelt (bitte die in Artikel 6 Absatz 2 des Abkommens vorgesehene Durchführungsvereinbarung(en) beifügen)?

4. Sind die Einzelheiten der technischen Ausgestaltung für den automatisierten Abruf von DNA-Profilen inzwischen durch eine oder mehrere Durchführungsvereinbarungen geregelt, so dass Artikel 7 bis 9 des Abkommens in Kraft getreten ist (wenn ja, bitte die Durchführungsvereinbarung(en) beifügen)?
5. Welche Behörden und Abteilungen (bitte Organisationseinheiten konkret benennen) sind auf US-amerikanischer Seite als nationale Kontaktstellen für den Datenaustausch nach Artikel 6 (daktyloskopische Daten), Artikel 9 (DNA-Profile) und Artikel 10 Absatz 7 (Daten zur Verhinderung terroristischer Straftaten) des Abkommens benannt?
6. Wie viele „Spontanübermittlungen“ zur angeblichen Verhinderung terroristischer Straftaten hat es seit Unterzeichnung des Abkommens gegeben, und welche Stellen haben sie veranlasst bzw. empfangen?
7. Seit wann ist der automatisierte Abruf von daktyloskopischen Daten bzw. DNA-Profilen im Wirkbetrieb?
8. Falls der automatisierte Datenabruf noch nicht im Wirkbetrieb ist, wie ist der aktuelle Stand der Umsetzung, und wann ist die Aufnahme des Wirkbetriebes zu erwarten?
9. Wie viele Anfragen für einen automatisierten Datenabruf hat es seit Beginn des Wirkbetriebs zwischen den Vertragspartnern gegeben (bitte nach abfragender Kontaktstelle und Datenkategorie aufschlüsseln)?
10. Wie viele Übereinstimmungen von daktyloskopischen Daten oder DNA-Profilen nach Artikel 4 bzw. 7 des Abkommens hat es seitdem gegeben (bitte nach abfragender Kontaktstelle und Datenkategorien aufschlüsseln)?
11. In wie vielen Fällen einer Übereinstimmung wurden im Rahmen der Rechtshilfe weitere personenbezogene und sonstige Daten übermittelt (bitte nach abfragender Kontaktstelle und Datenkategorie aufschlüsseln)?
12. Wie viel Zeit vergeht in der Regel zwischen der Feststellung einer Übereinstimmung von automatisiert abgerufenen Daten und der Übermittlung weiterer personenbezogener und sonstiger Daten im Rahmen der Rechtshilfe?
13. In wie vielen und welchen Fällen hat das BKA entsprechend Artikel 13 Absatz 1 des Abkommens seine Zustimmung zur Weiterverarbeitung der übermittelten Daten zu anderen als den im Abkommen vorgesehenen Zwecken gegeben, und mit welcher Begründung?
14. Auf welcher Ebene wird innerhalb des BKA die Zustimmung zur Weiterverarbeitung der übermittelten Daten zu anderen Zwecken entschieden, und wie wird eine solche Zustimmung dokumentiert?

Berlin, den 23. August 2011

Dr. Gregor Gysi und Fraktion

