Europäischer Grenzschutz 2.0 – Ein Überblick über datenschutzrechtliche Herausforderungen

Dipl.-jur. Jonathan Stoklas ist wissenschaftlicher Mitarbeiter am Institut für Rechtsinformatik der Leibniz Universität Hannover.

Der Beitrag ist ebenfalls veröffentlicht worden in: ZD-Aktuell 2016, 05418.

Der Schutz der europäischen Außengrenzen ist derzeit ein politisch heiß diskutiertes Thema. Gleichzeitig eröffnen die steigenden Rechenkapazitäten und die zunehmende Vernetzung technischer Systeme neue Möglichkeiten, um den Grenzübertritt effektiver zu gestalten. Das von der EU unter dem Horizon 2020-Rahmenprogramm kofinanzierte Forschungsprojekt iCROSS (intelligent portable ContROll SyStem) hat sich die Entwicklung eines portablen Kontrollsystems zum Ziel gesetzt, das das Verfahren beim Grenzübertritt der EU-Außengrenzen an Land für die Grenzschutzbehörden effektiver und für die Reisenden komfortabler gestalten soll.

Dabei sollen sowohl Software- als auch Hardware-Komponenten zum Einsatz kommen. Neben einer Automatisierung von Kontrollabläufen durch den Einsatz portabler Scanner/ID-Reader soll u. a. eine „Traveller Pre-Registration“ zum Einsatz kommen, bei der Reisende ihren Grenzübertritt bereits vor ihrer Ankunft am Grenzübergang anmelden und dadurch die Dauer der tatsächlichen Kontrolle verringern können. Das Institut für Rechtsinformatik der Leibniz Universität Hannover ist als Konsortialpartner in iCROSS involviert und befasst sich mit den datenschutzrechtlichen und ethischen Fragestellungen, die sich aus der Nutzung eines solchen Systems ergeben.

Die Durchführung von Grenzübertrittskontrollen unterliegt grds. dem Schengener Grenzkodex. Gem. Art. 7 Abs. 1 Schengener Grenzkodex ist dabei stets die Menschenwürde zu achten, gem. Absatz 2 sind Diskriminierungen zu unterlassen. Bereits hier lassen sich erste datenschutzrechtliche Implikationen ableiten: Dem Menschen muss demnach eine Privatsphäre verbleiben, deren Durchbrechung nur dann geboten ist, wenn sie zur Erreichung des angestrebten Zwecks geeignet und erforderlich sowie der damit verbundene Eingriff nicht unverhältnismäßig ist (Erbs/Kohlhaas/Ambs, BDSG § 1 Rdnr. 8). Naturgemäß ist für die Grenzkontrolle die mitunter umfangreiche Erhebung personenbezogener Daten zur Feststellung der Identität und Überprüfung der Einreisebedingungen erforderlich, gleichwohl ist gerade mit Blick auf die zunehmende Vernetzung von IT-Systemen und Datenbanken kritisch zu hinterfragen, welche Abfragefunktionalitäten für die Grenzkontrollen tatsächlich erforderlich sind.

Je komplexer die zur Verfügung stehenden Daten sind, desto mehr Potenziale können sich für den Einsatz von Profiling-Techniken ergeben. Während das Profiling von Reisenden als solches bereits in der Vergangenheit kritisiert wurde, dürfte der heutige Stand der Technik eine wesentlich detailliertere Einschätzung des individuellen Risikos, das von einer Person ausgeht, erlauben. Insb. könnten bereits bekannte Merkmale wie Alter, Geschlecht und ethnische Herkunft mit Daten, die aus öffentlichen Quellen entnommen werden können – sog. Open Source Intelligence –, angereichert werden und den Beamten somit einen tiefgreifenden Eingriff in die Privatsphäre erlauben. Doch wie ist es zu bewerten, wenn die Entscheidung, eine Person einer weitergehenden Kontrolle in der „zweiten Kontrolllinie“ (vgl. Art. 2 Nr. 13 Schengener Grenzkodex) zu unterziehen, von einem Algorithmus getroffen wird? Welche Daten dürften für ein solches System verwendet werden? Wie sind die Nutzung von Cloud Computing und die Datenabfrage über mobile Geräte in diesem Kontext zu bewerten? Die Beantwortung dieser Fragen bedarf einer gründlichen Abwägung zwischen der tatsächlichen Notwendigkeit solcher Systeme einerseits und der Eingriffstiefe beim Betroffenen andererseits.

Ein elementarer Bestandteil von Grenzübertrittskontrollen ist die Feststellung der Identität des Reisenden, vgl. Art. 8 Abs. 2 Schengener Grenzkodex. Um die Identität einer Person zu bestätigen, wird auf biometrische Verfahren zurückgegriffen. Hier wird – sowohl nationalstaatlich, vgl. etwa § 81 b StPO – als auch auf europäischer Ebene stets auf Fingerabdrücke der Betroffenen zurückgegriffen. Die Erhebung und der Abgleich von Fingerabdrücken i. R. v. Grenzkontrollen findet sich u. a. in folgenden Verordnungen der EU wieder:

- Das „Schengen Information System" (SIS), in dem biometrische Daten von ausgeschriebenen Personen hinterlegt werden, vgl. Art. 20 Abs. 2 lit. e und f der VO (EG) Nr. 1987/2006. Ausgeschrieben werden etwa Personen, die eine Gefahr für die öffentliche Sicherheit oder Ordnung eines Mitgliedstaats begründen, die Rechtsgrundlagen finden sich im nationalen Recht wieder, vgl. §§ 95 ff. Schengener Durchführungsübereinkommen.
- Das „Visa-Informationssystem" (VIS), in dem zentral die von Drittausländern beantragten Visa gespeichert werden. Bei der Antragstellung ist die Erhebung biometrischer Daten in Form von Fingerabdrücken und einem Bild vorgesehen, vgl. Art. 9 Nr. 5 und 6 der VO (EG) Nr. 767/2008.
- Die Speicherung von Fingerabdrücken von Drittausländern und Asylbewerbern ist auch in der EURODAC-Datenbank vorgesehen, vgl. VO (EG) Nr. 2725/2000.
- In Ausweisdokumenten, die von Mitgliedstaaten der Europäischen Union ausgestellt wurden, ergibt sich die Aufnahme von Lichtbildern und Fingerabdrücken in das Ausweisdokument aus der VO (EG) Nr. 2252/2004.

Die Nutzung von Fingerabdrücken hat sich insofern als allgemeiner Standard zur Identitätsfeststellung etabliert. Gleichwohl ist die Erfassung von Fingerabdrücken aus Sicht der Grenzschutzbehörden nicht immer zufriedenstellend: So wird die Qualität der genommenen Fingerabdrücke von verschiedenen Faktoren beeinflusst (kalte Hände, Schweiß, etc.). Eine vollständige Erfassung aller zehn Finger benötigt mitunter mehrere Versuche, die für zehn Finger notwendige Zeit liegt somit mitunter bei über einer Minute (vgl. Smart Borders Pilot Project der EU, Report on the technical conclusions of the Pilot). Grenzschutzbehörden sind jedoch bemüht, die Wartezeit an Grenzübergängen möglichst gering zu halten.

Berücksichtigt werden muss ferner das Risiko von Manipulationen der Fingerkuppen, die zu einer Unauswertbarkeit führen und die erkennungsdienstliche Behandlung somit unterbinden können (vgl. etwa VG Regensburg, U. v. 8.1.2015 – RN 7 K 14.30430). Doch auch umgekehrt können sich Risiken ergeben: So ist es nach Medienberichten möglich, Fingerabdruck-Scanner und IRIS-Scanner zu überlisten. Wenngleich die Nutzung von Replika unter den Augen eines Grenzschutzbeamten in der Praxis schwierig sein dürfte, konstituiert die Erhebung von reproduzierbaren biometrischen Merkmalen dennoch ein Risiko für die Nutzung gefälschter Ausweisdokumente und Identitätsdiebstahl.

Vor diesem Hintergrund soll das im Rahmen des iCROSS-Projekts zu entwickelnde portable Kontrollsystem um die „Handvenenerkennung" ergänzt werden: Bei diesem biometrischen Verfahren wird das Venenmuster der Handfläche erfasst und in einen einzigartigen Schlüssel umgerechnet. Der Scanvorgang funktioniert berührungslos und ist schneller als das Erfassen von Fingerabdrücken. Ein solcher Systemwechsel wird in der Praxis jedoch nicht ohne weiteres möglich sein: So hält der EU-Gesetzgeber in seinem im April 2016 vorgestellten Vorschlag zur Schaffung eines „Entry-Exit-Systems" (EES), das das Ein- und Ausreisedatum von Drittausländern erfassen und dadurch die Stempel in Ausweisdokumenten ersetzen soll, an der Nutzung von Fingerabdrücken und Lichtbildern zur Identifikation einer Person fest. Immerhin wird jedoch – im Vergleich zur Proposal-Regulation aus dem Jahr 2013 – die Anzahl der zu erfassenden Fingerabdrücke von zehn auf vier reduziert, was die Dauer des Scanvorgangs gemäß der zuvor zitierten technischen Studie deutlich verringert.