

GEULEN & KLINGER  
Rechtsanwälte

**Vorab per Telefax: 0611-327618536**  
Verwaltungsgericht Wiesbaden  
PF 57 66

65047 Wiesbaden

Dr. Reiner Geulen  
Prof. Dr. Remo Klinger  
10719 Berlin, Schaperstraße 15  
Telefon +49 / 30 / 88 47 28-0  
Telefax +49 / 30 / 88 47 28-10  
e-mail: klinger@geulen.com  
geulen@geulen.com  
www.geulenklinger.com

19. Juli 2019

In dem Verwaltungsstreitverfahren

De Capitani, Emilio

./.

Bundesrepublik Deutschland

**6 L 807/19.WI**

erwidern wir auf den Schriftsatz der Antragsgegnerin vom 24. Juni 2019 (im Folgenden:  
Antragserwiderung) unter Voranstellung einer Gliederung wie folgt:

## **Gliederung**

|   |           |
|---|-----------|
| <b>A. Vorbemerkung</b> .....  | <b>3</b>  |
| <b>B. Tatbestand</b> .....  | <b>6</b>  |
| <b>C. Zulässigkeit des Anordnungsantrags</b> .....  | <b>8</b>  |
| I. Statthaftigkeit des vorbeugenden Rechtsschutzes .....  | <b>8</b>  |
| II. Keine unzulässige Vorwegnahme der Hauptsache .....  | <b>11</b> |
| III. Unbegründetheit der weiteren Einwände gegen die Zulässigkeit.....  | <b>12</b> |
| IV. Vorsorglich: Unionsrechtliche Anforderungen an den Eilrechtsrechtsschutz liegen vor .....   | <b>15</b> |
| <b>D. Begründetheit des Anordnungsanspruchs</b> .....   | <b>17</b> |
| I. PNR-Richtlinie verletzt Art. 7 und 8 GRCh .....  | <b>18</b> |
| 1. Gewicht der Eingriffe der PNR-Richtlinie vergleichbar mit Vorratsspeicherung von<br>Telekommunikationsverkehrsdaten .....                | <b>18</b> |
| 2. PNR-Richtlinie verletzt Grundrechte des Antragstellers nach den Maßstäben des EuGH aus dem<br>Gutachten zum EU-Kanada-PNR-Abkommen ..... | <b>20</b> |
| a) Anhang I Nr. 8 und Nr. 12 sind zu unbestimmt.....  | <b>21</b> |
| b) Sachlicher und persönlicher Anwendungsbereich sind zu weit .....   | <b>21</b> |
| c) Zeitliche Grenzen der Speicherung sind zu weit .....   | <b>25</b> |
| d) Unzureichende Verfahrensgarantien.....   | <b>26</b> |
| e) Unzureichende Sicherungen bei Übermittlung von PNR-Daten in Drittstaaten .....   | <b>27</b> |
| 3. Im Besonderen: Maschinelle Verdächtigengewinnung („Musterabgleich“) ist grundrechtswidrig.....   | <b>28</b> |
| a) Musterabgleich funktioniert nicht, jedenfalls aber viel zu schlecht .....  | <b>29</b> |
| b) Musterabgleich außerdem potentiell diskriminierend und definitiv intransparent .....   | <b>31</b> |
| c) Fazit .....  | <b>32</b> |
| II. FlugDaG verletzt Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG.....   | <b>32</b> |
| 1. FlugDaG nach Rechtsprechung des BVerfG verfassungswidrig .....   | <b>33</b> |
| a) Maßstab aus Entscheidung zur automatisierten Kennzeichenerfassung verletzt.....  | <b>33</b> |
| b) Maßstäbe der weiteren Entscheidungen des BVerfG ebenfalls verletzt.....  | <b>35</b> |
| 2. Musterabgleich verfassungswidrig .....   | <b>37</b> |
| 3. Möglichkeit der Zweckänderung der PNR-Daten und Verarbeitungsergebnisse ist verfassungswidrig ..   | <b>38</b> |
| 4. Straftatenkatalog ist verfassungswidrig.....   | <b>39</b> |
| <b>E. Anordnungsgrund</b> .....   | <b>40</b> |

## A. Vorbemerkung

Die Antragserwiderung überzeichnet die Wirksamkeit der mit der PNR-Richtlinie eingeführten Maßnahmen und redet die damit verbundenen Grundrechtseingriffe klein. Unter Hinweis auf eher abstrakte terroristische Gefahren werden eine Reihe von Grundrechtseingriffen zu rechtfertigen versucht, die effektiv nicht der Bekämpfung des Terrorismus dienen. Im Ergebnis wird durch die Antragsgegnerin eine algorithmische Wunderwaffe zur Entdeckung unbekannter Verdächtiger vorgestellt, deren Einsatz unabsehbare Folgen hat.

Nach dem Vortrag der Antragsgegnerin bleibt unklar, wie die automatisierte Fluggastdatenverarbeitung, insbesondere der Abgleich mit im Voraus festgelegten Kriterien (Musterabgleich), zur Verhütung, Aufdeckung, Ermittlung und Verfolgung der zahlreichen in Anhang II der PNR-Richtlinie genannten strafbaren Handlungen beitragen soll, die weit über grenzüberschreitenden Terrorismus und Drogenkriminalität hinausgehen. Die PNR-Datenverarbeitung soll auch im Zusammenhang mit diversen nicht-grenzüberschreitenden Delikten genutzt werden können, zu deren Verhütung, Aufdeckung, Ermittlung und Verfolgung ein Abgleich von Fluggastdaten mit Mustern nicht taugt. Dies steht außer Verhältnis zu einer anlasslosen Massenüberwachung.

Zentrales Problem der PNR-Richtlinie ist ihre mangelnde Differenzierung. Sie verfolgt unterschiedliche Ziele. Dafür müsste sie jedoch mit unterschiedlichen Methoden jeweils unterschiedliche Daten überprüfen und unterschiedlich lange vorhalten. Dennoch behandelt sie alle Daten gleich: Alle Daten werden erhoben, alle Daten jahrelang gespeichert, alle zur Verhütung, Aufdeckung, Ermittlung und Verfolgung aller in Anhang II genannten strafbaren Handlungen mit Datenbanken und Mustern abgeglichen.

Besonders problematisch ist jedoch das neue Instrument des Musterabgleichs. Es ist das erste Mal, dass über den anlasslosen Einsatz von Algorithmen zur Identifizierung von gefährlichen Personen entschieden wird. Dieser Rechtsstreit ist damit der Auftakt zu einer in den kommenden Jahren und Jahrzehnten zu erwartenden Reihe von Rechtsstreitigkeiten um automatisierte Entscheidungsprozesse im Sicherheitsbereich. Der nächste Schritt ist mit der Ausweitung der PNR-Datenverarbeitung auf Busse, Schiffe und Züge bereits in Planung. Diese Entwicklung beunruhigt nicht dadurch weniger, dass (vorerst) noch Menschen die Ergebnisse von Maschinen überprüfen. Denn wie auch in anderen Lebensbereichen wird die maschinelle Entscheidungskompetenz in dem Maße die menschliche verdrängen, wie Menschen

Vertrauen in sie fassen. Die aufgeworfenen Fragen sind deshalb von grundsätzlicher Natur.

Der Musterabgleich begründet einen Eingriff völlig neuer Qualität. Er ist mit den Grundrechten der Europäischen Grundrechtecharta und des Grundgesetzes nicht vereinbar, weil er für die Verhütung, Aufdeckung, Ermittlung und Verfolgung der meisten strafbaren Handlungen des Anhangs II der PNR-Richtlinie von vornherein untauglich ist, weil er hinsichtlich der übrigen strafbaren Handlungen aus statistischen Gründen viel zu viele Menschen falsch verdächtigen wird, weil er potentiell diskriminierend wirkt, weil er intransparent ist und vor allem weil er Menschen allein auf Grund ihrer Fluggastdaten zu Verdächtigen erklärt. Die Generierung eines Verdachts auf der Grundlage alltäglicher Daten – wohlgemerkt: gerade unabhängig von einem Treffer aus dem Abgleich mit einer Datenbank –, ist unserem Rechtssystem fremd und führt in eine Gesellschaft, in der jedes Verhalten als verdächtig behandelt wird, in der Menschen zu Verdächtigen werden, ohne je etwas Falsches getan zu haben.

Die Antragsabweisung durchzieht mal offen, mal versteckt die Botschaft, der Eingriff in die Rechte des Antragstellers sei so gering, dass er hinter der großen Gefahr des Terrorismus zurückstehen müsse. Dies schwingt etwa in der Auffassung mit, der Antragsteller müsse zur Begründung seines Rechtsschutzinteresses parallel auch in Belgien Rechtsschutz suchen. Dem hält der Antragsteller entschieden entgegen, dass jede Datenverarbeitung – gerade durch Sicherheitsbehörden – ernst zu nehmen ist; dass er jeden rechtswidrigen Eingriff in die informationelle Selbstbestimmung, mithin auch die Verarbeitung seiner Fluggastdaten nach dem FlugDaG, für sich genommen abwenden können muss; und dass dies erst recht gilt, wenn die Datenverarbeitung im Rahmen einer neuen Form der anlasslosen Massenüberwachung erfolgt.

Weil der Antragsteller nur die Sicherung seiner Rechte – konkret: das Recht, über seine PNR-Daten zu bestimmen – beantragt, ist vor Erlass einer einstweiligen Anordnung auch keine Abwägung der widerstreitenden Interessen bzw. eine Zumutbarkeitsprüfung angezeigt. Es genügt die Gefahr, dass sein Recht durch die Nichtgewährung einstweiligen Rechtsschutzes vereitelt wird. Das aber ist der Fall, weil die Antragsgegnerin seine PNR-Daten unmittelbar vor dem Start der streitgegenständlichen Flüge verarbeiten wird und dies nicht mehr rückgängig gemacht werden kann. Aus demselben Grund liegen auch die Voraussetzungen für einen vorbeugenden Rechtsschutz vor. Denn nach der Rechtsprechung des BVerwG genügt dafür etwa die zu erwartende Betroffenheit durch ein Kennzeichenerfassungssystem. Diese

Rechtsprechung lässt sich ohne Weiteres auf die Fluggastdatenverarbeitung übertragen.

## B. Tatbestand

Die Antragsabweisung vermag keinen kausalen Zusammenhang zwischen den von der PNR-Richtlinie bzw. dem FlugDaG verarbeiteten Fluggastdaten und der erfolgreichen Verhütung, Aufdeckung, Ermittlung und Verfolgung von strafbaren Handlungen nach Anhang II der PNR-Richtlinie bzw. § 4 Abs. 1 FlugDaG zu begründen.

Ein Gesetz, das eine nie dagewesene anlasslose Massenüberwachung mithilfe einer algorithmengesteuerten Gefährdungsprüfung einführt, die nicht nur durch Datenbankabgleiche bereits bekannte Straftäter und sog. Gefährder identifizieren, sondern auch durch Musterabgleiche bislang unbekannte Menschen markieren will, muss diesen Zusammenhang jedoch plausibel darlegen können.

Exemplarisch sei das an den von der Antragsgegnerin selbst vorgetragenen Beispielen erläutert:

Die Antragsgegnerin fokussiert eingangs ihrer Darstellung des Tatbestands die Gefahr des Terrorismus. Einen Zusammenhang zwischen der Fluggastdatenverarbeitung und einer Vermeidung von Terrorstrafataten begründet sie jedoch nicht. Vielmehr stellt sie nach Beschreibung der Fallzahlen im Terrorismusbereich lediglich fest: „Die Sicherheitsbehörden erreichen diesbezüglich immer wieder Hinweise auf mögliche terroristische Einzeltäter oder Teams, die sich auf dem Weg nach Europa befinden, um dort Anschläge durchzuführen. Der Luftweg ist hierbei von erheblicher Relevanz.“ (vgl. Rn. 3 f. der Antragsabweisung)

Dieser Vortrag ist nicht schlüssig, weil viel zu vage. Der Antragsteller bestreitet vorsorglich, dass der Luftweg „von erheblicher Relevanz“ für in die EU bzw. nach Deutschland reisende terroristische Einzeltäter oder Teams ist. Dem Antragsteller scheint vielmehr das Gegenteil plausibel, dass gerade wegen der bereits bislang strengen Einreisemodalitäten bei einer Flugreise dieser Reiseweg nicht gewählt wird. Die Antragsgegnerin möge diese Behauptung deshalb glaubhaft machen. Vorsorglich bestreitet der Antragsteller auch, dass dennoch mit dem Flugzeug einreisende Terroristen mit den Mitteln der PNR-Richtlinie und des FlugDaG rechtzeitig vor Begehung eines Terroranschlags aufgespürt werden können; insbesondere bestreitet er, dass das mit dem Abgleich mit „im Voraus festgelegte[n] Kriterien“ nach Art. 6 Abs. 3 lit. b PNR-Richtlinie bzw. mit „Mustern“ nach § 4 Abs. 2 Satz 1 Nr. 2 FlugDaG gelingen kann.

Die Ausführungen der EU-Kommission im Richtlinienvorschlag vom 2. Februar 2011, auf die sich die Antragsgegnerin beruft (vgl. Rn. 7 ff. der Antragserwiderung), vermögen den Nutzen der PNR-Datenverarbeitung ebenfalls nicht zu belegen. Vielmehr gesteht die EU-Kommission darin ein, dass es auf EU-Ebene keine detaillierten Statistiken darüber gebe, inwieweit PNR-Daten dazu beitragen, schwere Kriminalität oder Terrorismus zu verhüten, aufzudecken, aufzuklären oder strafrechtlich zu verfolgen.

EU-Kommission, Richtlinienvorschlag KOM(2011) 32 endgültig, vom 02.02.2011, S. 6.

Die „Angaben von Drittländern sowie von Mitgliedstaaten, die diese Daten bereits zu Strafverfolgungszwecken nutzen“, auf die sich die EU-Kommission stützt, bilden keine nachvollziehbare Grundlage für einen so schweren Grundrechtseingriff. Schon zur Vorratsspeicherung von Telekommunikationsdaten hat das Max-Planck-Institut festgestellt, dass die Behauptung, solche Einzelfälle seien typisch, empirisch nicht belastbar sei.

Schutzlücken durch Wegfall der Vorratsdatenspeicherung?, Max-Planck-Institut für ausländisches und internationales Strafrecht, 2011, S. 219, online abrufbar unter <https://www.mpg.de/5000721/vorratsdatenspeicherung.pdf>.

Viele weitere Fragen bleiben offen: Wie genau haben PNR-Daten zur Strafverfolgung beigetragen? Welche Straftaten wurden aufgeklärt? Welche Daten wurden verarbeitet? Wie lange halten sie diese Daten vor? Vor allem aber fehlt es hinsichtlich der Verhütung von Straftaten durch Datenbank- und Musterabgleiche an Einzelfallbeispielen.

Zudem sind die von der EU-Kommission und auch der Antragsgegnerin genannten Beispiele (Rn. 9 der Antragserwiderung) nicht nachvollziehbar. So soll Belgien angegeben haben, 95 % aller (!) Rauschgiftsicherstellungen im Jahr 2009 seien darauf zurückzuführen gewesen, dass PNR-Daten in Echtzeit und proaktiv verwendet worden seien. Das ist nicht plausibel, weil Belgien mit Sicherheit einen höheren Anteil als 5 % des Rauschgifts an Seehäfen, Landesgrenzen und vor allem im Inland selbst sichergestellt haben wird. Selbst wenn sich die 95 % auf die Sicherstellungen an Flughäfen bezögen, ist die Angabe nicht plausibel, weil in der Begründung der EU-Kommission ebenfalls steht, dass Belgien zum Zeitpunkt der Befragung durch die EU-Kommission noch gar kein PNR-System etabliert hatte. Das gleiche gilt für Schweden, dessen Beispiel die Antragsgegnerin ebenfalls übernimmt.

EU-Kommission, Richtlinienvorschlag KOM(2011) 32 endgültig, vom 02.02.2011, S. 4.

Weiter gelten die Ausführungen der Antragsgegnerin zu den Bereichen, in denen sie sich einen besonderen Nutzen der PNR-Daten verspricht, nicht für EU-Flüge. So behauptet die Antragsgegnerin, dass Flüge in die Türkei, die bei Urlaubern beliebt seien, günstige Preise und gute Tarnmöglichkeiten für sog. foreign fighters böten (Rn. 4 der Antragserwiderung). Die Antragsgegnerin nennt keine Beispiele für entsprechende typischerweise von foreign fighters genutzte Flugrouten innerhalb der EU. Im Übrigen sind diese Personen häufig namentlich bekannt (offenbar werden sie auch gezählt, s. Rn. 4 der Antragserwiderung) und ihre Reiserouten sind es offenbar auch, sodass es einer ausgeklügelten Mustererkennung gerade nicht bedürfte. Umgekehrt ist auch kein Fall eines foreign fighters bekannt, der über den Luftweg unerkannt in die EU gereist wäre und hier terroristische Straftaten begangen hätte,

Zudem ist im Bereich organisierter Kriminalität innerhalb der EU der Luftweg nicht von erheblicher Relevanz. Gerade in den von der Antragsgegnerin genannten Bereichen des Rauschgifthandels und -schmuggels (Rn. 5 ff. der Antragserwiderung), die wohl den größten Anteil an der organisierten Kriminalität in Deutschland ausmachen, ist für die Täter der Landweg gegenüber dem Luftweg die leichtere und unauffälligere Art der Fortbewegung. Denn auf diese Weise können vor Flugreisen durchgeführte Personenkontrollen vermieden und innereuropäische Grenzen größtenteils unkontrolliert überschritten werden. Dementsprechend hat auch das Bundeskriminalamt in seinem Bundeslagebericht zur Rauschgiftkriminalität 2017 festgestellt, dass die sichergestellten Rauschgiftlieferungen überwiegend auf dem Landweg nach Deutschland verbracht wurden.

Bundeskriminalamt, Bundeslagebericht Rauschgiftkriminalität 2017, S. 14  
([https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Rauschgiftkriminalitaet/rauschgiftkriminalitaet\\_node.html](https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Rauschgiftkriminalitaet/rauschgiftkriminalitaet_node.html)).

## **C. Zulässigkeit des Anordnungsantrags**

Der Antrag ist zulässig.

### **I. Statthaftigkeit des vorbeugenden Rechtsschutzes**

Das Ersuchen des Antragstellers um vorbeugenden Rechtsschutz ist nach den Maßstäben des BVerwG für ein **qualifiziertes Rechtsschutzbedürfnis** statthaft. Die



Antragsgegnerin gibt diese Maßstäbe zunächst korrekt wieder (Rn. 30 der Antragsabweisung), indem sie die Formel von den „für den Kläger unzumutbaren Nachteilen“ verwendet, die mit einem Absehen vorbeugenden Rechtsschutzes verbunden wären (so die von der Antragsgegnerin und auch bereits dem Antragsteller genannten Fundstellen). Sodann ergänzt sie mit ihren eigenen Worten, die schon kurzfristige Hinnahme der befürchteten Handlung müsse die Rechte des Betroffenen „in besonderer Weise beeinträchtigen“. Das steigert sie in Rn. 35 der Antragsbegründung zum Erfordernis eines „besonders schwere[n] Nachteil[s]“.

Eine derart qualifizierte Rechtsbeeinträchtigung hat nichts mit den Maßstäben des Bundesverwaltungsgerichts zu tun. Es genügt vielmehr, dass durch ein Abwarten irreversible Fakten geschaffen werden und dadurch nicht wiedergutzumachende Nachteile entstehen. Ein besonderes Gewicht der Nachteile wird nicht gefordert.

Statt vieler *Schoch*, in: Schoch/Schneider/Bier, VwGO, Stand: Feb 2019, § 123 Rn. 46 mit zahlreichen Nachweisen und Beispielen aus der Rspr.

Im Zusammenhang mit einem Kennzeichenerfassungssystem genügte es dem BVerwG etwa, dass das System bereits betrieben und auch weiterhin eingesetzt wird. „Zudem“ begründete das Gericht das Rechtsschutzinteresse damit, der dortige Kläger könne der Erfassung seines Kennzeichens nicht ausweichen.

BVerwG, Urt. v. 22. Oktober 2014 – 6 C 7/13 (= NVwZ 2015, 907), Rn. 17 f.

Diese Voraussetzungen sind hier erfüllt. Das deutsche Fluggastdaten-System ist aktiv. Weil der Umfang der Datenerfassung unklar ist, kann der Antragsteller ihr auch nicht ausweichen. Schon die Speicherung der Fluggastdaten des Antragstellers im Fluggastdatensystem der Antragsgegnerin ist aber ein Grundrechtseingriff, der nicht rückgängig gemacht werden kann. Dasselbe gilt für den Abgleich der Fluggastdaten des Antragstellers mit Datenbanken und Mustern, der ad hoc durchgeführt wird, und – sollte es dazu kommen – für die zwischenzeitliche Übermittlung seiner Daten an andere Stellen im In- und Ausland, wo sie wiederum weiterverarbeitet werden könnten. Diese Eingriffe kann der Antragsteller nur durch vorbeugenden Rechtsschutz verhindern. Nachträglicher Rechtsschutz kann hingegen nur noch auf eine Löschung der noch gespeicherten Daten gerichtet sein.

Soweit die Antragsgegnerin meint, dass darüber hinaus beim Antragsteller eine Unsicherheit über das Ob und Wie seiner Beeinträchtigung bestehen müsse (Rn. 32 der Antragsabweisung), ist auch das der Fall: Der Antragsteller wusste bis zur Bestätigung

durch die Antragsgegnerin (Rn. 25 der Antragserwiderung) nicht, ob seine Flüge vom PNR-System erfasst sein würden. Der Antragsteller weiß außerdem nach wie vor nicht, welche Daten genau die Lufthansa zu seinem Flug übermitteln und welche die Antragsgegnerin speichern wird, ob und, falls ja, mit welchen Datenbanken und Mustern die Antragsgegnerin sie abgleichen wird, ob die Antragsgegnerin die Daten an andere Stellen übermitteln wird und wie diese seine Daten ggf. weiterverarbeiten werden.

Die weiteren Argumente der Antragsgegnerin (Rn. 35 ff. der Antragserwiderung) messen sich an ihrem selbst definierten Maßstab eines besonders schweren Nachteils, der – wie dargelegt – weder in der Rechtsprechung noch in der Literatur eine Grundlage hat. Sie überzeugen aber auch selbst an diesem Maßstab gemessen nicht:

Die Antragsgegnerin meint, die Verarbeitung der Fluggastdaten des Antragstellers werde mit hoher Wahrscheinlichkeit folgenlos bleiben. Dem liegt ein Fehlverständnis zugrunde: Die Verarbeitung selbst ist der Grundrechtseingriff, der vermieden werden soll. Auch meint die Antragsgegnerin, dem Antragsteller drohe im Kern nicht mehr als bei jeder Personenkontrolle anlässlich eines Grenzübertritts (Rn. 36 der Antragserwiderung). Im Geltungsbereich des Schengener Grenzkodex – also auch an der Grenze zwischen Belgien und Deutschland – gibt es jedoch keine Personenkontrollen, auch nicht am Flughafen.

Zudem spielt keine Rolle, dass der Antragsteller nicht in derselben Sache parallel um Rechtsschutz in Belgien ersucht (Rn. 37 f. der Antragserwiderung). Das zu fordern verkennt, dass jeder Grundrechtseingriff isoliert zu betrachten ist. Sollte Belgien mit der technischen Umsetzung der PNR-Richtlinie tatsächlich soweit sein, dass es die Fluggastdaten des Antragstellers aus den streitgegenständlichen Flügen ebenfalls verarbeitet – wovon der Antragsteller keine positive Kenntnis hat –, reduziert das nicht sein Interesse, eine Verarbeitung seiner Fluggastdaten in Deutschland zu unterbinden. Die Veränderung seiner Lage im Falle eines Erfolgs des hiesigen Antrags wäre „substantiell“, weil sein Datensatz nicht mehr durch die Antragsgegnerin verarbeitet würde (vgl. zu diesem Punkt näher die Antwort des Antragstellers vom 15. Juli 2019 auf die Fragen des Gerichts).

Das weiter vorgetragene Argument, wegen der Einbettung des Antrags des Antragstellers in eine erweiterte Klagestrategie sei eine Klärung „unter erheblichem Zeitdruck“ nicht erforderlich (Rn. 39 ff. der Antragserwiderung), ist nicht rechtlicher Natur und trägt auch nichts zu dem von der Antragsgegnerin selbst definierten Maßstab des besonders schweren Nachteils bei. Das Bedürfnis nach vorbeugendem Rechtsschutz

rührt allein daher, dass andernfalls die Antragsgegnerin die streitgegenständlichen Fluggastdaten des Antragstellers verarbeiten wird, wodurch naturgemäß Zeitdruck entsteht (wie im Übrigen bei jedem Eilverfahren).

Die abzuwendende Handlung ist auch **hinreichend konkretisiert**. Der Antragsteller kann naturgemäß nicht dazu vortragen, wie wahrscheinlich eine Übermittlung seiner Daten an andere Stellen im In- und Ausland ist (Rn. 45 der Antragsabweisung). Sie ist aber gesetzlich vorgesehen und schon deshalb zu befürchten. Das gilt umso mehr, als nach einer Auskunft der Antragsgegnerin auf eine Kleine Anfrage im Deutschen Bundestag, anbei als

**Anlage K 4** (dort S. 5),

der PNR-Datenbankabgleich bis zum 31. März 2019 zwar 94.098 technische Treffer erzeugte, von denen aber nur 277 Treffer „fachlich positiv überprüft“ wurden. D.h. die Fehlerquote des automatisierten Datenbankabgleichs betrug mehr als 99,7 Prozent. Dies bestätigen die Zahlen der Antragsgegnerin aus ihrem Schreiben vom 15. Juli 2019 (dazu näher unter C.I.3.a)). Bei einer so hohen Fehlerquote ist nie auszuschließen, dass auch völlig unbescholtene Bürger wie der Antragsteller Maßnahmen wie der Übermittlung ihrer Fluggastdaten an andere Stellen im In- und Ausland unterworfen werden.

Nicht nachvollziehbar ist der weitere Einwand der Antragsgegnerin, das vom Antragsteller befürchtete Handeln der Antragsgegnerin sei insoweit nicht hinreichend konkretisiert, als nicht absehbar sei, ob auch Daten nach § 2 Abs. 2 Nr. 7, Nr. 14 und Nr. 16 FlugDaG übermittelt würden. Der Antragsteller begehrt ausweislich seines Antrags, es der Antragsgegnerin einstweilen zu untersagen, jegliche Fluggastdaten zu seiner Person zu den streitgegenständlichen Flügen zu speichern, zu verarbeiten und zu übermitteln. Dass aber die Lufthansa Fluggastdaten an die Antragsgegnerin übermitteln wird, ist (nunmehr) hinreichend absehbar.

## **II. Keine unzulässige Vorwegnahme der Hauptsache**

Die Antragsgegnerin meint, der Antrag des Antragstellers sei auf eine endgültige und vollständige Vorwegnahme der Hauptsache gerichtet, weshalb er unzulässig sei (Rn. 47 ff. der Antragsabweisung).

Dies ist unzutreffend.

Denn im Falle eines Erfolgs des Eilantrags wäre die Hauptsache nicht endgültig vorweggenommen. Selbstverständlich könnte sich eine spätere Datenübertagung der Lufthansa an die Antragsgegnerin auf § 2 Abs. 5 FlugDaG stützen (gegen Rn. 50 der Antragserwiderung). Aus demselben Grund könnte die Lufthansa – ggf. auf Aufforderung der Kammer – zum Vorhalten des Fluggastdatensatzes des Antragstellers angehalten werden. Zur Löschung wäre sie jedenfalls nach Art. 5 Abs. 1 lit. 2 DS-GVO gerade nicht verpflichtet, weil der Datensatz bis zum rechtskräftigen Abschluss des Verfahrens noch für eine Datenverarbeitung erforderlich werden könnte. Die Lufthansa könnte den streitigen Fluggastdatensatz also noch nach einer etwaigen rechtskräftigen Abweisung der Hauptsache übermitteln und die Antragsgegnerin könnte die Daten anschließend verarbeiten.

Selbst wenn und soweit eine einstweilige Anordnung die Hauptsache endgültig vorwegnahme, wäre dies ausnahmsweise zulässig. Nach den Maßstäben des Bundesverwaltungsgerichts ist das dann der Fall, wenn eine Entscheidung in der Hauptsache nicht mehr rechtzeitig erwirkt werden kann und das Begehren nach summarischer Prüfung Erfolg haben muss.

BVerwG, Beschl. v. 13. August 1999 – 2 VR 1.99 (= NJW 2000, 160, 162).

Beides ist hier zu bejahen: Eine Entscheidung in der Hauptsache könnte den Grundrechtseingriff nicht mehr verhindern (vgl. o. Abschn. I.) und das Begehren hat nach summarischer Prüfung Erfolg (dazu nochmals unten Teil D.).

### **III. Unbegründetheit der weiteren Einwände gegen die Zulässigkeit**

Auch die übrigen Einwände der Antragsgegnerin gegen die Zulässigkeit des Antrags greifen nicht durch.

Das **Normverwerfungsmonopol des Bundesverfassungsgerichts** steht dem nicht entgegen, selbst nach den von der Antragsgegnerin rezipierten Maßstäben der Rechtsprechung.

Danach kommt einstweiliger Rechtsschutz in Anträgen, die sich auf den Verstoß einer Norm gegen höherrangiges Recht stützen, dann in Betracht, wenn es im Interesse eines effektiven Rechtsschutzes geboten erscheint und die Hauptsache nicht vorweggenommen wird (Rn. 55 der Antragserwiderung; vgl. insbes. BVerfGE 86, 382, LS 1). Wie bereits dargelegt (vgl. o. Abschn. I. und II.), ist vorläufiger Rechtsschutz

geboten, weil sonst eine irreparable Rechtsverletzung droht, und es wird die Hauptsache nicht bzw. nicht unzulässig vorweggenommen.

Ungeachtet dessen ist einstweiliger Rechtsschutz auch dann zu gewähren, wenn die Vorlage an das BVerfG gem. Art. 100 Abs. 1 GG einen wirksamen Rechtsschutz vereiteln würde.

OVG Hamburg, Beschl. v. 23. Juni 1999 – 5 Bs 118/99 (= NJW 1999, 2754, 2759); *Schoch*, in: ders./Schneider/Bier, VwGO, Stand: Feb. 2019, § 123 Rn. 129 m.w.N.

Das ist hier der Fall. Es ist nicht zu erwarten, dass das BVerfG über einen konkreten Normenkontrollantrag vor dem Tag des ersten streitgegenständlichen Flugs entscheiden würde.

Weil die Antragsgegnerin diese Frage systematisch an dieser Stelle verortet hat, ist darauf hinzuweisen, dass das FlugDaG auch **an der GRCh zu messen** ist. Es trifft nicht zu, dass die Voraussetzungen des Art. 51 Abs. 1 Satz 1 GRCh nicht vorliegen (gegen Rn. 58 ff. der Antragserwiderung). Nach Art. 51 Abs. 1 Satz 1 GRCh gilt die GRCh für die Mitgliedstaaten ausschließlich bei der Durchführung des Rechts der Union. Dass die Antragsgegnerin bei der Anwendung des FlugDaG auf EU-Flüge (wie die streitgegenständlichen Flüge) Unionsrecht durchführt, ergibt sich zwanglos bereits aus Art. 2 Abs. 2 i.V.m. Abs. 1 PNR-Richtlinie. Danach sind im Falle einer Entscheidung des Mitgliedstaats, „diese Richtlinie auf Flüge innerhalb der Europäischen Union (EU-Flüge) anzuwenden“ (Abs. 1), „alle Bestimmungen dieser Richtlinie für EU-Flüge so, als handele es sich um Drittstaatsflüge (...)“ (Abs. 2).

Eindeutiger hätte der europäische Gesetzgeber nicht formulieren können, dass jedes nationale Gesetz – und jede dieses Gesetz ausführende Handlung – Grund und Anleitung in der PNR-Richtlinie findet, also i.S.d. Art. 51 Abs. 1 Satz 1 GRCh Recht der Union durchführt. Folglich ist die Antragsgegnerin auch insoweit unmittelbar an die Grundrechte der GRCh gebunden und das FlugDaG hieran zu messen.

Nur ergänzend sei darauf hingewiesen, dass die Antragsgegnerin sich im Rat der Europäischen Union mit allen anderen Mitgliedstaaten darin einig erklärte, von der Möglichkeit des Art. 2 PNR-Richtlinie Gebrauch zu machen, und dadurch auf europäischer Ebene das Ob der Erstreckung des FlugDaG auf EU-Flüge vorwegnahm. S. dazu die Erklärung vom 18. April 2016, beigelegt als

#### **Anlage K 5.**

Schließlich stehen auch die **unionsrechtlichen Anforderungen an den Eilrechtsrechtsschutz** nationaler Gerichte (Rn. 66 ff. der Antragsrüge) der Zulässigkeit nicht entgegen. Denn sie gelten im vorliegenden Fall nicht. Die von der Antragsgegnerin zitierten Grundsätze entwickelte der EuGH im Zusammenhang mit der Aussetzung des Vollzugs von Verwaltungsakten, die unmittelbar auf einer EU-Verordnung beruhen.

Vgl. *Schoch*, in: ders./Schneider/Bier, VwGO, Stand: Feb. 2019, § 80 Rn. 392 ff.

Deutsche Gerichte wenden die Grundsätze mittlerweile auch auf nationale Gesetze an, soweit sie europäische Richtlinien eins zu eins umsetzen.

Vgl. etwa VGH München, Beschl. v. 3. September 2004 – 19 CE 04.1973  
(= BeckRS 2005, 20264).

Keine Anwendung finden sie jedoch, wenn die angegriffene Handlung auf einer nationalen Rechtsvorschrift basiert, deren Europarechtswidrigkeit geltend gemacht wird. Das EU-Recht regelt nicht, wie in einem solchen Fall zu verfahren ist. Folglich bestimmen sich die Anforderungen an die Gewährung vorläufigen Rechtsschutzes nach nationalem Recht.

EuGH, Urt. v. 13. März 2007, C-432/05, Unibet [London] Ltd. (= EuZW 2007, 247), Rn. 80 ff.; *Schoch*, in: ders./Schneider/Bier, VwGO, Stand: Feb. 2019, § 80 Rn. 396.

Die Übermittlung der Fluggastdaten zu den streitgegenständlichen Flügen beruht auf dem FlugDaG. Die Flüge erfolgen innerhalb der EU (Belgien-Deutschland-Belgien). Das FlugDaG erfasst auch EU-Flüge und bewegt sich damit außerhalb des zwingenden Teils der PNR-Richtlinie, die nur eine Fluggastdatenverarbeitung für Nicht-EU-Flüge vorschreibt. Sofern also die Kammer die Verarbeitung der Fluggastdaten des Antragstellers einstweilen untersagt, stellt das die Geltung des Europarechts nicht in Frage.

Daran ändert auch nichts, dass Art. 2 Abs. 2 PNR-Richtlinie für den Fall der Erstreckung des nationalen PNR-Systems auf EU-Flüge die Geltung der PNR-Richtlinie auch für solche Fälle anordnet. Denn dies führt nur dazu, dass sich das nationale Recht umfassend am Unionsrecht messen lassen muss; nicht aber dazu, dass nunmehr die Verarbeitung von Fluggastdaten von EU-Flügen europarechtlich geboten wäre und die einstweilige Untersagung der Verarbeitung den Anwendungsvorrang des europäischen Rechts unterlaufen würde.

Der Antragsteller schlägt mit Blick auf das Vorstehende – worüber er sich endgültige Klarheit erst aus Anlass der Antragsabweisung verschaffen hat – statt der in der Antragschrift formulierten (dort S. 34 f.) die folgende Vorlagefrage vor:

*Sind Artikel 7 und 8 der Charta dahingehend auszulegen, dass sie einer nationalen Regelung wie der im Ausgangsverfahren streitigen entgegenstehen, wonach Luftfahrtunternehmen die in Anhang I der Richtlinie 2016/681 des Europäischen Parlaments und des Rates vom 27. April 2016 über die Verwendung von Fluggastdatensätzen (PNR-Daten) zur Verhütung, Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten und schwerer Kriminalität genannten PNR-Daten für alle Flüge des Linien-, Charter- und Taxiverkehrs zu übermitteln haben, die nicht militärischen Zwecken dienen und die von dem normerlassenden Mitgliedstaat der Europäischen Union aus starten und in einem anderen Mitgliedstaat der Europäischen Union landen oder die von einem anderen Mitgliedstaat der Europäischen Union starten und in dem normerlassenden Mitgliedstaat der Europäischen Union landen, wenn der normerlassende Mitgliedstaat die PNR-Daten kurz vor dem Start der Flüge mit Datenbanken und mit im Voraus festgelegten Kriterien abgleicht und anschließend fünf Jahre lang speichert?*

#### **IV. Vorsorglich: Unionsrechtliche Anforderungen an den Eilrechtsrechtsschutz liegen vor**

Für den Fall, dass sich die Kammer gleichwohl an die unionsrechtlichen Anforderungen an den Eilrechtsschutz gebunden fühlt, liegen diese jedenfalls vor.

Wie bereits dargelegt, bestehen erhebliche Zweifel an der Gültigkeit der PNR-Richtlinie (vgl. S. 19 ff. der Antragsbegründung sowie unten D.I). Darüber hinaus ist die Entscheidung auch nach den Maßstäben des EuGH dringlich in dem Sinne, dass der Antragsteller ohne sie einen schweren und nicht wiedergutzumachenden Schaden erleiden würde.

Der Begriff der Dringlichkeit ist unionsrechtlich zu bestimmen. Dabei gelten für nationale Gerichte bei der Gewährung des vorläufigen Rechtsschutzes dieselben Anforderungen wie bei der Gewährung einstweiligen Rechtsschutzes durch den EuGH.

EuGH, Urt. v. 21. Februar 1991 C-143/88 und C-92/89, Zuckerfabrik Süderdithmarschen AG, EU:C:1991:65, Rn. 27; EuGH, Urteil v. 9. November 1995, C-465/93, EU:C:1995:369, Atlanta, Rn. 40.

Die Begriffe des schweren und des nicht wiedergutzumachenden Schadens in der Rechtsprechung des Europäischen Gerichts (EuG) sind nicht unabhängig voneinander, sondern einheitlich unter dem Begriff der Dringlichkeit zu betrachten. Dabei ist die Dringlichkeit wiederum am Maßstab des Rechts auf effektiven Rechtsschutz (Art. 47 Abs. 1 GRCh) zu beurteilen.

EuG, Beschluss des Präsidenten v. 29. November 2012, Alstom, T-164/12 R,  
EU:T:2012:637, Rn. 46.

Gewichtiges Indiz für den erforderlichen Schaden ist, dass es dem Antragsteller verwehrt wäre, einen Ausgleich im Wege einer Schadensersatzklage gemäß Art. 340 AEUV zu erlangen; rein vermögensrechtliche Streitigkeiten sollen ausscheiden. So hat das EuG entschieden, dass Aussagen, die die Ehre und das Ansehen des Antragstellers ernsthaft in Frage stellen, einen schweren Schaden begründen können. Wesentliche Begründung für die Dringlichkeit ist danach, dass der Schaden wegen seiner Natur bereits nicht Gegenstand einer tatsächlichen Wiederherstellung sein könne.

EuG, Beschluss v. 12. Dezember 1995, Bernard Connolly, T-203/95 R,  
EU:T:1995:208, Rn. 42 f.

Auch hier ist die Verarbeitung der Fluggastdaten des Antragstellers durch die Antragsgegnerin ein unverhältnismäßiger Grundrechtseingriff, der nicht rückgängig gemacht werden kann (vgl. oben I. sowie Antragschrift S. 19 ff.). Bereits die Speicherung führt dazu, dass die Daten des Antragstellers dem unkontrollierten Zugriff staatlicher Stellen ausgesetzt sind; erst recht greift der Abgleich der Fluggastdaten des Antragstellers mit Datenbanken und Mustern tief in seine Grundrechte ein. Das gilt insbesondere, weil er zu beidem keinen Anlass gegeben hat. Der Schaden für seine Grundrechte wäre nicht wiedergutzumachen, sein Recht auf effektiven Rechtsschutz liefe ohne Erlass der einstweiligen Anordnung folglich leer.

Schließlich wären die Auswirkungen einer einstweiligen Anordnung zu Gunsten des Antragstellers auf das Vollzugsinteresse der Union außerordentlich gering. Es würden lediglich die Fluggastdaten des ganz sicher völlig ungefährlichen Antragstellers nicht verarbeitet. Diese Fluggastdaten gehören zudem zu einem EU-Flug, der gar nicht unter den zwingenden Teil der PNR-Richtlinie fällt. Die Entscheidung der Kammer hätte folglich keine „Aussetzung des Richtlinienvollzugs“ mit „gravierende[n] Auswirkungen auf das Funktionieren des Systems in den anderen Mitgliedstaaten“ (Rn. 68 der Antragsabweisung) zur Folge. Zu derlei Entscheidungen ist ein nationales Gericht



überhaupt nicht befugt; es übersteigt auch das Rechtsschutzinteresse des Antragstellers in diesem Verfahren.

Hat die Kammer also erhebliche Zweifel an der Gültigkeit der PNR-Richtlinie, sollte sie die in der Antragschrift (dort S. 34 f.) vorgeschlagenen Fragen mit Erlass der einstweiligen Anordnung dem EuGH vorlegen.

EuGH, Urt. v. 21. Februar 1991 C-143/88 und C-92/89, Zuckerfabrik Süderdithmarschen AG, EU:C:1991:65, Rn. 24; EuGH, Urteil v. 9. November 1995, C-465/93, EU:C:1995:369, Atlanta, Rn. 51.

Das ist zulässig, weil die Kammer nach Erlass einer einstweiligen Anordnung diese gem. § 80 Abs. 7 analog VwGO abändern kann,

vgl. *Kuhla*, in: Posser/Wolff, BeckOK VwGO, Stand: 1.7.2018, § 123 Rn. 182 mit zahlreichen Nachweisen aus der Rspr.

wodurch sie generell auch im Eilverfahren vorlageberechtigt ist,

EuGH, Urt. v. 21. April 1988, Rs. 338/85, EU:C:1988:194, Rn. 12 ff.; s. dazu auch *Marsch*, in: Schoch/Schneider/Bier, VwGO, Art. 267 AEUV Rn. 46;

hier ist sie aber – wenn sie die Frage nach der Gültigkeit der PNR-Richtlinie wie der Antragsteller bewertet – wie bereits ausgeführt (Antragschrift S. 34) sogar vorlageverpflichtet.

So ausdrücklich auch für das Eilverfahren EuGH, Urt. v. 21. Februar 1991 C-143/88 und C-92/89, Zuckerfabrik Süderdithmarschen AG, EU:C:1991:65, Rn. 24.

## **D. Begründetheit des Anordnungsanspruchs**

Der Anordnungsanspruch des Antragstellers ist auch begründet.

Die Verarbeitung der Fluggastdaten des Antragstellers zu den streitgegenständlichen Flügen ist rechtswidrig, weil das FlugDaG gegen Art. 7 und 8 GRCh sowie gegen Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verstößt. Ersteres ergibt sich schon daraus, dass die PNR-Richtlinie, deren – überobligatorischer – Umsetzung das FlugDaG dient, gegen Art. 7 und 8 PNR-Richtlinie verstößt (dazu unter I.), Letzteres ergibt sich aus einer

Verletzung der Maßstäbe des BVerfG zur Zulässigkeit anlassloser Massenüberwachung (dazu unter II.).

## **I. PNR-Richtlinie verletzt Art. 7 und 8 GRCh**

Entgegen der Ansicht der Antragsgegnerin (Rn. 71 ff. der Antragserwiderung) kommt es auf die Grundrechtskonformität der PNR-Richtlinie insoweit an, als nach Art. 2 Abs. 2 i.V.m. Abs. 1 PNR-Richtlinie diese und damit die Grundrechte der GRCh auch auf EU-Flüge Anwendung finden (vgl. oben C.III). Wenn und soweit die PNR-Richtlinie gegen die GRCh verstößt, gilt das auch für das FlugDaG.

### **1. Gewicht der Eingriffe der PNR-Richtlinie vergleichbar mit Vorratsspeicherung von Telekommunikationsverkehrsdaten**

Die Antragsgegnerin ist der Auffassung, dass die Vorratsspeicherung von Telekommunikationsverkehrsdaten schwerer wiege als die von der PNR-Richtlinie bewirkte Datenverarbeitung (Rn. 80 ff. der Antragserwiderung).

Das ist unrichtig.

Der Eingriff wiegt mindestens ebenso schwer.

Die Vergleichbarkeit ergibt sich bereits daraus, dass in beiden Fällen massenweise personenbezogene Daten von Menschen verarbeitet und auf Vorrat gespeichert werden, die sich nichts haben zuschulden kommen lassen oder auch nur Indizien geliefert haben für einen gegen sie gerichteten Verdacht. Die Einwände der Antragsgegnerin ändern daran nichts:

Der betroffene Personenkreis ist nicht erheblich kleiner (Rn. 80 der Antragserwiderung), denn selbst ohne EU-Flüge sind von Flügen mit Abflugs- oder Zielflughafen in Deutschland rund 65 Mio. Fluggäste betroffen; mit EU-Flügen steigt die Zahl auf rund 170 Mio. Fluggäste (dazu bereits Antragschrift S. 11). Selbst wenn man davon Personen abzieht, die mehrfach fliegen, bleiben Dutzende Millionen Menschen betroffen.

Dass durch die PNR-Richtlinie keine zusätzlichen Daten erhoben werden müssen (Rn. 81 der Antragserwiderung), ist aus Perspektive der Fluggäste unerheblich, weil jedenfalls alle vorhandenen Fluggastdaten übermittelt werden. Außerdem steht zu befürchten, dass die Fluglinien aus eigenem Interesse an den Daten unter Vorschub der

PNR-Richtlinie bzw. der nationalen Umsetzungsgesetze künftig mehr Daten als bislang bei den Fluggästen erheben werden.

Auch stehen PNR-Daten in ihrer Bedeutung für die Betroffenen nicht hinter Telekommunikationsverkehrsdaten zurück (Rn. 82 f. der Antragserwiderung). Denn sie lassen umfassende Rückschlüsse auf das Privat- und das – ebenfalls geschützte – Geschäftsleben der Betroffenen zu, nämlich wer wann wohin gereist ist, in wessen Begleitung, welches Zahlungsmittel sie genutzt, welche Kontaktdaten sie angegeben haben oder ob sie mit leichtem oder schwerem Gepäck gereist sind. Über das Freitextfeld können auch diverse weitere Daten anfallen, von denen nicht einmal klar ist, welchen Inhalt sie haben (dazu bereits Antragschrift S. 26).

Weiter kann die Antragsgegnerin die Bedenken gegenüber der Sicherheit der Daten nicht zerstreuen (Rn. 84 der Antragserwiderung): Jede neue Datenbank begründet ein neues Sicherheitsrisiko. Keine Datenbank ist sicher. Das gilt umso mehr für Datensätze mit so sensiblen Informationen wie Kreditkartendaten.

Sofern die Antragsgegnerin anführt, dass bei Flügen seit jeher strengere Sicherheitsvorkehrungen und Kontrollen gelten (Rn. 85 der Antragserwiderung), ist dies völlig unerheblich. Im Gegenteil: Wenn schon so streng kontrolliert wird, rechtfertigt es keine weiteren Kontrollen.

Auch die Heimlichkeit der Fluggastdatenverarbeitung ist ein Argument für die Vergleichbarkeit mit der Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten.

Die von der Antragsgegnerin identifizierten Unterschiede in den vom EuGH gewählten Begriffen (Rn. 88 der Antragserwiderung) waren vom EuGH sicher nicht bewusst gewählt, zumal sie keinen gefestigten Kategorien für die Gewichtung von Eingriffen entsprechen. In dieser Hinsicht ist auch zu berücksichtigen, dass der persönliche Anwendungsbereich des EU-Kanada-Abkommens sehr viel kleiner ist als der der PNR-Richtlinie.

Ungeachtet dessen wiegt die Vorratsspeicherung von Fluggastdaten nach der PNR-Richtlinie in anderen Beziehungen sogar schwerer als die Vorratsspeicherung von Telekommunikationsverkehrsdaten, was die Übertragung der Maßstäbe der EuGH-Entscheidungen zur Vorratsspeicherung von Telekommunikationsverkehrsdaten auf Fluggastdaten erst recht begründet:

(1) Die PNR-Daten werden weitaus länger vorgehalten (nämlich fünf Jahre statt sechs Monate (!)), wogegen auch die Pseudonymisierung keinen effektiven Schutz bietet, weil sie eben umkehrbar ist.

(2) Die Daten werden nicht von Unternehmen bevorratet, sondern vom Staat selbst. Das verschafft ihm eine unmittelbare Zugriffsmöglichkeit, während der Zugriff auf die Telekommunikationsverkehrsdaten durch den Staat immer eines Anlasses bedurfte.

(3) Schließlich werden Fluggastdaten beim BKA zentral vorgehalten, was gegenüber einer dezentralen Bevorratung ein erhöhtes Risiko für die Sicherheit der Daten begründet.

Damit sind die Maßstäbe des EuGH für die Vorratsspeicherung von Telekommunikationsverkehrsdaten übertragbar auf die Vorratsspeicherung von Fluggastdaten.

So auch der Rechtsausschuss des Deutschen Bundesrates in seiner Empfehlung zum Entwurf eines Gesetzes über die Verarbeitung von Fluggastdaten zur Umsetzung der Richtlinie (EU) 2016/681 (Fluggastdatengesetz – FlugDaG) vom 20.03.2017, BR-Drs. 161/1/17, S. 2; sowie das Gutachten des Juristischen Dienstes des Europäischen Parlaments vom 22. Dezember 2014 („LIBE – Questions relating to the judgment of the Court of Justice of 8 April 2014 in Joined Cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger and others – Directive 2006/24/EC on data retention – Consequences of the judgment“), abrufbar unter: <http://www.statewatch.org/news/2015/apr/ep-ls-opinion-digital-rights-judgment.pdf>, Rn. 63.

Das sieht offenkundig auch der EuGH so, der sich in seinem Gutachten zum EU-Kanada-PNR-Abkommen wiederholt auf die Entscheidungen zur Vorratsspeicherung von Telekommunikationsverkehrsdaten bezieht.

Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 124 ff., insbes. auch Rn. 192 ff.

## **2. PNR-Richtlinie verletzt Grundrechte des Antragstellers nach den Maßstäben des EuGH aus dem Gutachten zum EU-Kanada-PNR-Abkommen**

Die einzelnen Einwände der Antragsgegnerin gegen die Anwendung der Maßstäbe des Gutachtens des EuGH zum EU-Kanada-PNR-Abkommen auf die PNR-Richtlinie überzeugen nicht.

### **a) Anhang I Nr. 8 und Nr. 12 sind zu unbestimmt**

Entgegen der Auffassung der Antragsgegnerin (Rn. 107 ff. der Antragsabwehr) sind die Datenkategorien gem. Anhang I Nr. 8 und Nr. 12 der PNR-Richtlinie zu unbestimmt.

Hinsichtlich des Vielfliegereintrags hielt der EuGH die entsprechende Rubrik des EU-Kanada-PNR-Abkommens nicht nur wegen des „usw.“ für zu unbestimmt, sondern auch deshalb, weil

„aus dem Wortlaut dieser Rubrik nicht ersichtlich [ist], ob mit ihr Informationen allein über die Teilnahme der Fluggäste an Bonusprogrammen gemeint sind oder sämtliche Informationen über die Flüge und Buchungen, die im Rahmen solcher Programme durchgeführt werden“.

Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 157.

Das ist bei der Datenkategorie gem. Anhang I Nr. 8 noch weniger gewährleistet, weil dort nur von einem „Vielfliegereintrag“ die Rede ist, was offenlässt, ob davon nur die Teilnahme an einem Vielfliegerprogramm oder sämtliche Einträge im Rahmen dieses Programms gemeint sind.

Hinsichtlich der Datenkategorie Anhang I Nr. 12 („Allgemeine Hinweise“) zeigt bereits die Darstellung der Antragsgegnerin (Rn. 110 ff. der Antragsabwehr) wie unbestimmt diese Kategorie ist. Die Ausführungen zu „SSR“ sind unverständlich: „SSR“ werden in der PNR-Richtlinie nicht in Bezug genommen.

### **b) Sachlicher und persönlicher Anwendungsbereich sind zu weit**

Der sachliche und persönliche Anwendungsbereich sind – entgegen der Darstellung der Antragsgegnerin (Rn. 116 ff. der Antragsabwehr) – auch nach den Maßstäben des EuGH-Gutachtens zu weit.

Der Antragsteller hatte als milderer Mittel zunächst eine Beschränkung der PNR-Datenverarbeitung auf bestimmte, besonders bedeutsame Flugstrecken vorgeschlagen. Dagegen zitiert die Antragsgegnerin einen Auszug aus dem EuGH-Gutachten. Dieses fußt jedoch auf einer ganz anderen Prämisse: Kanada hatte Flugunternehmen dazu verpflichtet, PNR-Daten vor der Landung bereitzustellen.

Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 14.

Das EU-Kanada-PNR-Abkommen möchte einen Rahmen bereitstellen, der dieser Pflicht entspricht. Anders als bei der PNR-Richtlinie bestand also kein Spielraum, den sachlichen Anwendungsbereich zu begrenzen.

Ungeachtet dessen hat sich der EuGH in der von der Antragsgegnerin zitierten Passage (Rn. 186-189 des Gutachtens) lediglich mit dem persönlichen, nicht mit dem sachlichen Anwendungsbereich auseinandergesetzt.

Wenn die Antragsgegnerin zu begründen versucht (Rn. 118 ff. der Antragserwiderung), warum die PNR-Datenverarbeitung alle Flugstrecken und Passagiere erfassen muss, tritt ein Kernproblem der PNR-Richtlinie zutage: Sie differenziert nicht hinreichend. Die Beispiele der Antragsgegnerin verdeutlichen, dass die PNR-Richtlinie unterschiedliche Zwecke verfolgt, für die sie jeweils unterschiedliche Daten auf unterschiedliche Art überprüfen und unterschiedlich lange vorhalten müsste; dennoch behandelt sie alle Daten gleich. Zu unterscheiden sind folgende Zwecke:

1. Die Verhütung von terroristischen Straftaten,
2. die Verhütung von anderen schweren Straftaten, die in ihrem Gewicht terroristischen Straftaten entsprechen (z.B. Anhang II Nr. 2 Menschenhandel, Nr. 5 Waffenhandel, Nr. 12 Tötung),
3. die Verhütung von anderen „schweren“ Straftaten, die weniger schwer wiegen als terroristische Straftaten (z.B. Anhang II Nr. 7 Betrugsdelikte, Nr. 8 Geldwäsche, Nr. 11 illegale Einreise, Nr. 16 Kulturgüterhandel, Nr. 17 Produktpiraterie),
4. die Aufdeckung, Ermittlung und Verfolgung von terroristischen Straftaten,
5. die Aufdeckung, Ermittlung und Verfolgung von anderen schweren Straftaten, die in ihrem Gewicht terroristischen Straftaten entsprechen,
6. die Aufdeckung, Ermittlung und Verfolgung von anderen „schweren“ Straftaten, die weniger schwer wiegen als terroristische Straftaten,
7. die Aufstellung und Analyse von Kriterien für den algorithmischen Abgleich.

Als Mittel sieht die PNR-Richtlinie vor:

1. Den Abgleich mit Datenbanken vor Einreise (Art. 6 Abs. 2 lit. a PNR-Richtlinie),
2. den Abgleich mit im Voraus festgelegten Kriterien vor Einreise (Abs. 3 lit. b),
3. die Beantwortung von Anfragen anderer Sicherheitsbehörden (Abs. 2 lit. b).

Für das Beispiel einer Ausschreibung zur Fahndung (Rn. 121 der Antragserwiderung) ist womöglich der Abgleich der PNR-Daten sämtlicher Flüge und Passagiere mit der entsprechenden Datenbank erforderlich. Für einen solchen Abgleich bedarf es aber nicht

der Gesamtheit der in Anhang I der PNR-Richtlinie aufgeführten Daten. Es würden z.B. die bereits nach § 31a Abs. 3 BPolG übermittelten Fluggastdaten oder jedenfalls ein auf diese Angaben reduzierter Datensatz genügen. Auch könnten die Daten sogleich nach einem (ergebnislosen) Abgleich wieder gelöscht werden. Zudem wäre die anlasslose Massenspeicherung von Fluggastdaten zu Fahndungszwecken sicher nicht hinsichtlich von Straftaten angemessen, die weniger schwer wiegen als terroristische Straftaten.

Das verdeutlichen auch die Zahlen der Antragsgegnerin aus ihrem Schriftsatz vom 15. Juli 2019. Mit Stand 30. Juni 2019 sind danach 17.672.744 Passagierdatensätze verarbeitet worden. Das führte zu 274 erfolgreich umgesetzten Fahndungsmaßnahmen, was einer Quote von 0,000155 % entspricht. Darunter wiederum waren nur 35 Festnahmen, wobei aus der Aufstellung der Antragsgegnerin leider nicht deutlich wird, ob hierunter auch Verdächtige terroristischer oder zumindest anderer ebenso schwerer Straftaten waren. Selbst wenn die PNR-Daten künftig mit noch mehr Datenbanken abgeglichen werden, wird sich der geringe Ertrag nicht substantiell erhöhen. Jedenfalls ist das nicht dargelegt.

Für den Abgleich mit im Voraus festgelegten Kriterien (Rn. 121 der Antragsabweisung) mag die Antragsgegnerin den gesamten PNR-Datensatz für erforderlich halten (dazu näher unter 3.). Für den ganz überwiegenden Teil der in Anhang II der PNR-Richtlinie genannten strafbaren Handlungen ist diese Form des Abgleichs aber bereits ungeeignet. Durch den Abgleich von Fluggastdaten mit im Voraus festgelegten Kriterien lässt sich z.B. keine Vergewaltigung (Anhang II Nr. 21) durch einen bislang Unbekannten aufdecken, aufklären oder verfolgen – und erst recht nicht verhindern. Denn es gibt kein typisches Flugverhalten von Vergewaltigern. Oder von Betrügern (Anhang II Nr. 7). Oder von Dokumentenfälschern (Anhang II Nr. 18).

Für die Aufklärung solcher Fälle mag wiederum eine retrograde Recherche (Rn. 122 der Antragsabweisung) helfen. Das wird aber nur die absolute Ausnahme sein (es müsste immerhin die Aufklärung etwa einer grenzüberschreitenden Computerstraftat [Anhang II Nr. 9] tatsächlich von PNR-Daten abhängen); vor allem aber wäre es völlig unangemessen, etwa zur Förderung der Aufklärung von Betrugs- und Geldwäschdelikten (Anhang II Nr. 7 und 8), illegaler Einreise (Nr. 11), illegalem Kulturgüterhandel (Nr. 16) oder Produktpiraterie (Nr. 17), die PNR-Daten sämtlicher Personen zu sämtlichen Flügen in die EU oder aus ihr heraus über Jahre hinweg zu speichern. Der bloße Umstand, dass ein Datum irgendwann irgendwie einmal bei der Aufklärung irgendeiner Straftat helfen kann, rechtfertigt nicht bereits seine Speicherung. Wäre dem so, wäre jede Form der Massenüberwachung gerechtfertigt, weil es immer

sein könnte, dass das Gespeicherte vielleicht einmal bei der Aufklärung einer Straftat helfen wird. Das widerspricht dem Verhältnismäßigkeitsgrundsatz und ignoriert das Interesse der Betroffenen, nicht total erfasst zu werden. Im Übrigen würden für eine retrograde Recherche etliche PNR-Daten (Gepäck, Sitzplatznummer, allgemeine Hinweise etc.) nicht benötigt; und es würde eine Speicherung bei den Fluggesellschaften ausreichen, was immerhin die Datensicherheit nicht im selben Maße wie eine zentrale Speicherung bei der Fluggastdatenzentralstelle (hier: dem BKA) kompromittieren würde.

Was damit gesagt sein soll: Mit der großen Keule „Terrorismus“ in der Hand schafft die PNR-Richtlinie bzw. schaffen die nationalen Umsetzungsgesetze in den Mitgliedstaaten gigantische Datenbanken, in denen sich – einmal geschaffen – die verschiedensten Sicherheitsbehörden nach Belieben auch im Zusammenhang mit vielen anderen Deliktsformen und zu unterschiedlichen Zwecken bedienen können, ohne ein ausgewogenes Verhältnis zwischen dem tatsächlichen Mehrwert dieser Datenbank, den jeweils auf sie angewandten Methoden und den jeweils damit verbundenen Grundrechtseingriffen zu beachten. Erforderlich und allein angemessen wären unterschiedliche Datenbanken mit unterschiedlichen Datensätzen, unterschiedlicher Speicherdauer sowie unterschiedlichen Einsatzzwecken und Analysemethoden. Andernfalls ist der Weg zu einer Totalüberwachung jedes mobilen Menschen, die auch Busse, Züge und Schiffe einbezieht, sehr kurz, die Politik arbeitet gerade daran.

Die Süddeutsche Zeitung vom 17. Juli 2019, S. 4 kommentiert daher wie folgt:

„Ein unsichtbares Netz legt sich über Europa. Es hat enge Maschen, in denen Informationen über Menschen hängen bleiben, die in Flugzeuge steigen: Wer wohin fliegt, wie er bezahlt, wo er sitzt, ob er einen Flug nicht angetreten hat. Die Informationen landen in Datenspeichern der Polizei, wo sie mit Algorithmen durchleuchtet werden sollen. Diese sollen vorhersagen, welcher Passagier in Zukunft zum Verbrecher wird. Jetzt sollen die Maschen noch enger werden.“

Ob die Erfassung der Fluggäste etwas bringt, ist noch nicht einmal bewiesen, da diskutieren die EU-Mitglieder schon, ob nicht auch ein "Passenger Name Record" (PNR) von Reisenden in Fernbussen, Zügen und Schiffen erfasst werden soll. Die Bundesregierung sollte den Plan der Hardliner unter den Staaten ablehnen.

Buchen, ohne seinen Namen anzugeben, ohne Zugbindung, das geht in Deutschland. Neue Regeln im Namen des Anti-Terror-Kampfes würden den Ticketkauf verkomplizieren. In genau jenem Moment, in dem viele Menschen dem Flugzeug abschwören und auf Bus und Bahn umsteigen. Es geht aber um mehr als um längere Schlangen an Ticketautomaten. Die Ausweitung von PNR wäre ein Verrat an einer der besten Ideen Europas: Reisen ohne Angst vor Überwachung. Denn wie frei ist eine Reise noch, wenn der Staat jede Buchung registriert und analysiert?“



### **c) Zeitliche Grenzen der Speicherung sind zu weit**

Die Argumente der Antragsgegnerin, die extrem lange Speicherdauer der PNR-Daten sei gerechtfertigt (Rn. 137 ff. der Antragserwiderung), überzeugen nicht.

Entgegen der Antragsgegnerin wäre eine Löschung der PNR-Daten nach Ausreise aus dem Zielland jedenfalls in der weit überwiegenden Anzahl der Fälle möglich: Die meisten Menschen, die in ein bestimmtes Land fliegen, verlassen es auf demselben Weg. So könnten die Daten von Menschen, die mit dem Flugzeug in einen Mitgliedstaat der Europäischen Union reisen, nach Ausreise mit dem Flugzeug aus demselben Mitgliedstaat wieder gelöscht werden. Die Daten von Staatsangehörigen eines Mitgliedstaats der Europäischen Union, die ins Ausland fliegen, könnten (spätestens) nach seiner Rückkehr gelöscht werden. Ein Abgleich innerhalb der PNR-Datenbank (sowie die Ermittlung von Staatsangehörigkeit und Wohnsitz) sollte ohne Weiteres möglich sein (vgl. die entsprechenden PNR-Daten nach Anhang I Nr. 5 und 18). Das Problem von über Land oder über Wasser weiterreisenden Menschen könnte durch eine Obergrenze der Speicherung gelöst werden (z.B. 90 Tage, was der Dauer eines Schengen-Tourismus-Visums entspricht).

Für eine solche Lösung wäre keine „Wiedereinführung systematischer Kontrollen an sämtlichen EU-Binnengrenzen“ erforderlich (so aber Rn. 137 der Antragserwiderung); wenn eine solche aber für eine grundrechtskonforme Ausgestaltung des PNR-Systems erforderlich wäre, würde dies nur unterstreichen, dass sein Betrieb insgesamt unverhältnismäßig ist.

Es ist nicht Sache des Antragstellers, Vorschläge dafür zu machen, wie eine übermäßige Speicherdauer vermieden werden kann. Selbst wenn es keine solche Möglichkeit gäbe (quod non), würde dies nicht die Zulässigkeit einer jahrelangen Speicherdauer begründen, vielmehr müssten diese Daten schlicht sofort nach (ergebnislosem) Abgleich wieder gelöscht werden.

Dass durch ein grundrechtskonformes PNR-System die retrograde Recherche erschwert würde (Rn. 139 f. der Antragserwiderung), ist sicher richtig, jedenfalls für die verschwindend wenigen Fälle (gemessen an der Gesamtzahl der erhobenen Datensätze), in denen es auf die PNR-Daten ankäme. Wie bereits dargelegt (oben b)) rechtfertigt das aber nicht für sich die jahrelange Speicherung der PNR-Daten aller Fluggäste, weil sonst praktisch jede Form der massenhaften Datenspeicherung stets gerechtfertigt wäre.

#### **d) Unzureichende Verfahrensgarantien**

Die Ausführungen der Antragsgegnerin überzeugen auch hinsichtlich des in der PNR-Richtlinie unzureichend geregelten Verfahrens nicht (Rn. 142 ff. der Antragserwiderung).

Zunächst wird darauf hingewiesen, dass der Antragsteller nicht gerügt hat, „dass die PNR-Richtlinie keine Vorgaben enthalte, wonach die Speicherung und Verwendung der PNR-Daten einer unabhängigen (Vorab-) Kontrolle unterliegen“ (gegen Rn. 142 der Antragserwiderung). Der Antragsteller hat vielmehr den Maßstab des EuGH aus seinem Gutachten 1/15 zum EU-Kanada-PNR-Abkommen wiedergegeben, wonach die Verwendung der gespeicherten PNR-Daten nach Einreise in das Zielland (dort: Kanada) nur zulässig ist, wenn sie grundsätzlich einer vorherigen Kontrolle durch ein Gericht oder eine unabhängige Verwaltungsstelle unterworfen wird (Antragsschrift S. 32). Er hat sodann festgestellt, dass diese Vorgaben nicht eingehalten sind. Denn für die retrograde Recherche (Art. 6 Abs. 2 lit. b PNR-Richtlinie), die regelmäßig nach Einreise des Betroffenen erfolgt, ist eine Entscheidung durch ein Gericht oder eine unabhängige Verwaltungsstelle nicht erforderlich. Ebenfalls in der Antragsschrift wurde bereits ausgeführt, warum daran die Verfahrensvoraussetzungen für die (grundsätzliche) Prüfung der Aufhebung der Depersonalisierung durch eine Justizbehörde nichts ändern. Es bleibt dabei, dass zwischen Einreise und Depersonalisierung retrograde Recherchen ohne unabhängige Kontrolle zugelassen sind – und dass eben dies vom EuGH in seinem Gutachten 1/15 für unzulässig befunden wurde.

Der vorliegende Kontext unterscheidet sich nicht „erheblich“ vom EU-Kanada-PNR-Abkommen (Rn. 145 der Antragserwiderung). Der EuGH stützte seine Anforderung an das Verfahren nicht darauf, dass im EU-Kanada-PNR-Abkommen auch sensible Daten betroffen waren (gegen Rn. 145 der Antragserwiderung). Es ging ihm allein darum, durch unabhängige Kontrollen zu gewährleisten, dass die Verwendung der PNR-Daten nach Einreise nur zugelassen wird, wenn sie auf neue Umstände gestützt werden kann, die eine solche Verwendung rechtfertigen.

Gutachten des EuGH 1/15 v. 26. Juli 2017, EU:C:2017:592, Rn. 196 ff., insbes.  
Rn. 200 ff.

Es ist auch nicht ersichtlich, warum der EuGH von diesem Erfordernis Abstand nehmen sollte, wenn es um eine Massenübertragung von Daten in einen EU-Mitgliedstaat geht (gegen Rn. 146 der Antragserwiderung). Denn das möglicherweise höhere Datenschutzniveau in der EU hat nichts mit der Frage zu tun, ob gewährleistet ist, dass Fluggastdaten, die primär zur Überprüfung bei der Einreise erhoben und verarbeitet

werden, nach Einreise nur noch in begründeten Fällen weiter verwendet werden. Soweit die Antragsgegnerin in diesem Zusammenhang „mit Blick auf das Ziel der Terrorismusbekämpfung“ auf die Schlussanträge des Generalanwalts Mengozzi im Verfahren um das EU-Kanada-PNR-Abkommen verweist (Rn. 148 der Antragserwiderung), ist festzustellen, dass der EuGH eben diesen Schlussanträgen seine eigenen Ausführungen in der zitierten Passage des Gutachtens entgegengesetzt hat. Auch greift der Verweis auf das Ziel der Terrorismusbekämpfung abermals zu kurz, weil sich die PNR-Richtlinie gerade auch auf andere, weit weniger schwerwiegende Deliktsbereiche bezieht (vgl. Anhang II PNR-Richtlinie).

Daran ändert nichts, dass Art. 6 Abs. 7 PNR-Richtlinie dem Datenschutzbeauftragten einen Zugang zu sämtlichen von der Fluggastdatenzentralstelle verarbeiteten Daten gewährt (gegen Rn. 149 der Antragserwiderung). Denn dies ist kein adäquater Ersatz für eine Einzelfallprüfung, die berücksichtigt, ob Gründe für einen retrograden Zugriff auf bestimmte Fluggastdaten vorliegen.

Auch hinsichtlich der Benachrichtigungspflicht überzeugen die Ausführungen der Antragsgegnerin nicht (Rn. 150 f. der Antragserwiderung). Dass „entsprechende Benachrichtigungen über die (...) durch die Bedarfsträger vorgenommene (sic!) Folgemaßnahmen (...) durch die verantwortliche Stelle“ erfolgen, mag im jeweiligen nationalen Recht so vorgeschrieben sein; in der Richtlinie ist es das nicht.

#### **e) Unzureichende Sicherungen bei Übermittlung von PNR-Daten in Drittstaaten**

Schließlich überzeugt auch die Argumentation der Antragsgegnerin im Zusammenhang mit der Übermittlung von PNR-Daten an Drittstaaten nicht (Rn. 153 ff. der Antragserwiderung).

Sie meint, der EuGH habe in seinem Gutachten 1/15 nur einen Angemessenheitsbeschluss hinsichtlich des Drittstaates, in den Kanada Daten übermitteln wollte, genügen lassen können, weil Kanada die weiteren Instrumente der Art. 37 und 38 der Richtlinie (EU) 2016/680 nicht zur Verfügung standen.

Dies verkennt, dass Kanada das Instrument des Angemessenheitsbeschlusses nach Art. 36 der Richtlinie (EU) 2016/680 nicht zur Verfügung stand. Der EuGH hielt es für erforderlich, dass die EU-Kommission einen solchen Angemessenheitsbeschluss hinsichtlich des Drittlandes fasst, bevor Kanada an das Drittland Daten übermittelt. Er hätte es ebenso gut für ausreichend halten können, dass der Mitgliedstaat des

Abflugortes vor Übermittlung durch Kanada vom Drittland geeignete Garantien erhält (jetzt Art. 37 der Richtlinie (EU) 2016/680). Das hat er indes nicht getan. Er wollte nur einen Angemessenheitsbeschluss ausreichen lassen.

### **3. Im Besonderen: Maschinelle Verdächtigengewinnung („Musterabgleich“) ist grundrechtswidrig**

Die wesentlichste Neuerung der PNR-Richtlinie – und offenbar Grund für die Verarbeitung einer Vielzahl von abwegigen Datenpunkten (Gepäck, Sitzplatz usw.) – ist der Abgleich von massenhaft erhobenen Daten mit im Voraus festgelegten Kriterien (im Folgenden wie im FlugDaG: „Musterabgleich“). Es ist richtig, dass sich der EuGH in seinem Gutachten zum EU-Kanada-PNR-Abkommen nicht im Einzelnen mit dem Musterabgleich auseinandergesetzt hat. Gelegenheit bekäme er dazu nun aus Anlass von Musterabgleichen durch Behörden der Mitgliedstaaten. Eine Befassung ist auch dringend nötig. Denn der automatisierte Musterabgleich ist nicht einfach eine weitere anerkannte Maßnahme der Gefahrenabwehr, sondern seiner Art und Eingriffsweise nach völlig neu. Er ist mit den Grundrechten der GRCh – und des Grundgesetzes – schlicht unvereinbar.

Der Musterabgleich soll Personen ermitteln, die bislang nicht im Verdacht standen, an terroristischen Straftaten oder schwerer Kriminalität beteiligt zu sein (Erwägungsgrund 7 PNR-Richtlinie). Mit den Worten der EU-Kommission, sollen „bisher ‚unbekannte‘ Verdächtige identifiziert“ werden (Richtlinienvorschlag KOM(2011) 32 endgültig, vom 02.02.2011, S. 4). Es geht also um vorbeugendes Profiling.

Schon dieses Ziel ist hoch fragwürdig. Denn es impliziert, dass die Person, die mittels Musterabgleich identifiziert wird, (zu Recht) verdächtig ist. Der einzige verdachterregende Umstand ist jedoch der Musterabgleich selbst. Es geht also tatsächlich nicht darum, „bisher ‚unbekannte‘ Verdächtige“ zu identifizieren, sondern der Musterabgleich allein begründet einen Verdacht gegen die Betroffenen. Das ist ein großer Unterschied. Denn während in dem Fall eines gewöhnlichen Datenbankabgleichs bereits Verdachtsmomente gegen den Betroffenen bestehen, die seine Aufnahme in die Datenbank begründeten – jedenfalls sei das unterstellt –, ist beim Musterabgleich das einzig Verdächtige die von einem Algorithmus als verdächtig identifizierte Zusammenschau der Fluggastdaten des Betroffenen. Die Begründetheit dieses Verdachts hängt also entscheidend davon ab, ob der Algorithmus tatsächlich dazu in der Lage ist, eine Person zu identifizieren, die eine Straftat begangen hat oder begehen wird. Wohlgemerkt: Aus dem Nichts. Es geht nicht um die Markierung einer Person, die mit

einer als verdächtig registrierten Kreditkarte bezahlt hat oder den gleichen Namen wie ein registrierter Terrorverdächtiger oder foreign fighter trägt. Derlei Fälle könnte man mit (ggf. noch zu schaffenden) Datenbanken aufspüren. Sondern es geht um die Markierung einer Person, deren Fluggastdaten aus anderen Gründen verdächtig sind.

Das wäre vielleicht hinzunehmen, wenn der Algorithmus so gut wäre, dass er regelmäßig (und nicht nur im Ausnahmefall) zu Recht Alarm schlägt. Dieser Traum technikgläubiger Sicherheitspolitiker ist aber nichts weiter als das: ein Traum. Im Übrigen ist der Einsatz von Algorithmen zur Verdächtigengewinnung auch aus weiteren Gründen grundrechtswidrig.

Im Einzelnen:

#### **a) Musterabgleich funktioniert nicht, jedenfalls aber viel zu schlecht**

Wer sich vornimmt, in Abermillionen Datensätzen von nahezu vollständig unverdächtigen Personen durch das Erkennen von Mustern (künftige) Terroristen oder Schwermisstraftäter zu identifizieren, unterliegt dem Prävalenzfehler (engl: Base Rate Fallacy). D.h. er sucht in einer sehr großen Grundmenge eine sehr kleine Treffermenge, ohne die Fehlerquote der Trefferermittlung zu berücksichtigen.

Ein Beispiel: Kommen auf 100 Millionen Flugpassagiere im Jahr 100 Terroristen, die nur durch Musterabgleich identifiziert werden können (was sicher zu hoch gegriffen ist), und hätte das System eine Trefferquote von 90 % (was sicher zu hoch gegriffen ist) und eine Falschalarm-Rate von nur 0,1 % (was vermutlich zu niedrig ist), dann würden zwar 90 Terroristen korrekt erkannt (richtig-positiv), zugleich aber 100.000 Passagiere (0,1 % Falschalarm-Rate multipliziert mit 100 Millionen Flugpassagieren) zu Unrecht verdächtig (falsch-positiv). Anders formuliert: 99,9 % der als Terroristen markierten Personen sind keine Terroristen. Die Sicherheitsbehörden müssten dann aus 100.090 Personen die 90 Richtigen identifizieren, was einer Chance von etwa 1:1100 entspricht. Es ist also mit dem Musterabgleich – so schön er theoretisch klingt – nichts gewonnen. Im Gegenteil: Es drohen massenhafte Falschverdächtigungen.

Vgl. zur Frage der Leistungsfähigkeit von Musterabgleichen auch ausführlich  
*Korff/Georges*, Passenger Name Records, data maining & data protection,  
Bericht an den Europarat, S. 24 ff., 94 ff., online abrufbar unter  
<https://rm.coe.int/16806a601b>.

Es ist aber auch bereits äußerst fraglich, ob auf Fluggastdaten gestützte Algorithmen jemals auf eine nennenswerte Trefferquote kämen (im obigen Beispiel: 90 %). Die Behörden könnten sich zur Entwicklung der Muster auf maschinelles Lernen stützen, jedenfalls untersagt die PNR-Richtlinie dies nicht. D.h. es würden Softwareprogramme versuchen, auf Grundlage historischer Kenntnisse der Fluggastdaten von Terroristen aus allen nunmehr verarbeiteten Fluggastdaten diejenigen von (künftigen) Terroristen zu identifizieren. Das Problem liegt darin, dass die Basis an Daten, mit denen der Algorithmus trainiert werden kann, sehr gering ist. Es gab in der Vergangenheit in Europa nicht viele Terroristen, die per Flugzeug nach Europa einreisten. Der Algorithmus wird somit nicht zuverlässig sein können.

Wenn maschinelles Lernen die Muster nicht ermittelt, müssen Menschen sie definieren. Dadurch ist aber nichts gewonnen, weil auch sie nur auf eine geringe Anzahl an Präzedenzfällen zurückgreifen können, und außerdem zu erwarten ist, dass Terroristen und andere Kriminelle ihre (Flug-)Verhaltensmuster ständig ändern.

Die Fehlerträchtigkeit solcher Ansätze unterstreicht auch die bisherige Fehlerquote beim technisch weitaus weniger komplexen Datenbankabgleich. Aus einer Antwort der Bundesregierung auf eine Kleine Anfrage ergibt sich, dass PNR-Daten bis zum 31. März 2019 nur automatisiert mit dem Fahndungsdatenbestand in INPOL-Z und im Schengener Informationssystem abgeglichen und dabei seit dem Start des Fluggastdatenabgleichs 94.098 Treffer erzielt wurden, die zur manuellen Überprüfung ausgeleitet wurden. Daraus ergaben sich lediglich 277 Treffer. Das entspricht einer Fehlerquote von sage und schreibe 99,7 %.

BT-Drs. 19/9536, S. 5.

Das bestätigen die Zahlen der Antragsgegnerin aus ihrem Schriftsatz vom 15. Juli 2019. Nach ihren aktualisierten Zahlen kommen auf 187.002 technische Treffer nur 643 fachliche Treffer, was ebenfalls einer Fehlerquote von knapp 99,7 % entspricht. Aus dem Schreiben wird aber auch deutlich, dass selbst diese Fehlerquote noch zu niedrig ist. Die Antragsgegnerin führt nämlich weiter aus, dass von 467 an die Bundespolizei und/oder den Zoll ausgeleiteten fachlichen Treffern in 193 Fällen Fahndungsmaßnahmen leer liefen. Unter diesen Fällen war eine leider nicht näher bezifferte Zahl an Passagieren, die „nicht identisch mit der zur Fahndung ausgeschriebenen Person“ waren (Schriftsatz vom 15. Juli 2019, S. 7). Diese echten falschen Verdächtigungen sind folglich ebenfalls herauszurechnen. Sie unterstreichen außerdem die negativen Nebenwirkungen von an sich sehr einfach strukturierten

Datenbankabgleichen – und lassen erahnen, mit wie vielen Falschverdächtigungen bei Musterabgleichen zu rechnen ist.

Wohl auch wegen der hohen Fehlerquote enthält der Richtlinienvorschlag der EU-Kommission über anekdotische, nicht näher beschriebene PNR-Analyse-Erfolgsfälle hinaus keine Nachweise, dass und wie ein Musterabgleich überhaupt funktionieren kann. Auch die Antragsgegnerin nennt die immer gleichen Beispiele – der Drogenkurier, der foreign fighter –, ohne indes konkret zu werden. Vollends problematisch ist, dass die PNR-Richtlinie Musterabgleiche auch zu strafbaren Handlungen gestattet, die in einem noch geringeren Sachzusammenhang zu Flugreisen stehen als terroristische oder Drogenstraftaten. So wird kein Musterabgleich je die Aufdeckung, Ermittlung, Verfolgung oder gar Verhütung einer Betrugsstraftat (Anhang II Nr. 7) leisten können.

#### **b) Musterabgleich außerdem potentiell diskriminierend und definitiv intransparent**

Der Musterabgleich ist auch aus anderen Gründen grundrechtswidrig. Die PNR-Richtlinie untersagt zwar die Nutzung „sensibler Daten“ (Erwägungsgrund 37 sowie Art. 6 Abs. 4 Satz 4 PNR-Richtlinie) und formuliert in Art. 6 Abs. 4 Satz 1 PNR-Richtlinie die Maßgabe, der Musterabgleich erfolge in „nichtdiskriminierender“ Weise. Das genügt aber nicht, um eine Diskriminierung durch Algorithmen zuverlässig auszuschließen. In algorithmische Prozesse können sich ungewollt und unerkannt Vorurteile einschleichen. Denn Algorithmen werden von Menschen programmiert, selbstlernende Algorithmen werden von Menschen mit Trainingsdaten versorgt. In beiden Fällen ist nicht ohne Weiteres gewährleistet, dass die Analyseergebnisse des Algorithmus nicht durch in Gesellschaft und Menschen verankerte Vorurteile kompromittiert sind.

Dazu hat der Antragsteller bereits das offensichtliche Beispiel einer Fokussierung auf Flüge aus der Türkei gebildet (Antragsschrift S. 30). Die Antragsgegnerin weist es zwar einerseits zurück (Rn. 132 der Antragserwiderung), verstärkt andererseits aber seine Relevanz durch eigenen Vortrag, indem sie für ihr wiederholt aufgegriffenes Beispiel der foreign fighters darauf hinweist, es würden „insbesondere Flüge in die Türkei“ genutzt (Rn. 4 der Antragserwiderung). Jenseits dieser offensichtlichen Beispiele für eine mittelbare Diskriminierung können sich Vorurteile aber auch in ganz anderen, nicht vorhersehbaren Formen ihren Weg bahnen.

Vgl. etwa „Programmierter Rassismus“, ZEIT Online vom 19. Juni 2018, online abrufbar unter <https://www.zeit.de/digital/internet/2018-05/algorithmen-rassismus-diskriminierung-daten-vorurteile-alltagsrassismus> mit zahlreichen Beispielen aus dem Sicherheitsbereich.

Die PNR-Richtlinie müsste mindestens – um grundrechtskonform zu sein – dieses Problem adressieren und Mechanismen vorsehen, die eine mittelbare Diskriminierung durch Algorithmen verhindern.

Ein weiteres Problem algorithmischer „Verdächtigengewinnung“ durch den Musterabgleich ist die mangelnde Transparenz. Während ein Betroffener bei einem Treffer nach einem Datenbankabgleich ggf. noch darlegen kann, warum er nicht die gesuchte Person ist oder warum er zu Unrecht in der Datenbank steht, ist Vergleichbares bei einem durch einen Musterabgleich generierten Treffer nicht gewährleistet. Im schlimmsten Fall verstehen nicht einmal die Nutzer des Algorithmus, warum eine Person einen Treffer generiert. Selbst wenn ihnen aber das Muster bekannt ist, nach dem der Betroffene ausgewählt wurde, könnte dem Betroffenen – etwa aus Geheimhaltungsgründen – eine Offenlegung des Musters verweigert werden. Selbst wenn ihm das Muster offengelegt würde, hätte er keine Mittel, sich zu wehren: Er müsste darlegen, warum das Muster tatsächlich ungeeignet ist, einen Verdacht gegen ihn zu begründen. Weil die PNR-Richtlinie dieses Problem nicht adressiert, fehlt eine wesentliche Voraussetzung für einen effektiven Rechtsschutz gegen aus dem Musterabgleich resultierende Folgemaßnahmen.

### **c) Fazit**

Selbst wenn der Musterabgleich alle genannten Probleme in den Griff bekommen könnte (quod non), müsste die PNR-Richtlinie Verfahren zur Sicherstellung der Wirksamkeit und der Diskriminierungsfreiheit sowie Regeln für einen effektiven Rechtsschutz gegen positive Treffer von Musterabgleichen bzw. daraus resultierende Maßnahmen enthalten. (Auch) weil sie dies nicht enthält, ist die PNR-Richtlinie grundrechtswidrig.

## **II. FlugDaG verletzt Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG**

Die Antragsgegnerin kann auch nicht die Feststellung zerstreuen, dass das FlugDaG den Antragsteller in seinem Grundrecht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG verletzt.



## **1. FlugDaG nach Rechtsprechung des BVerfG verfassungswidrig**

### **a) Maßstab aus Entscheidung zur automatisierten Kennzeichenerfassung verletzt**

Die Antragsgegnerin gewinnt den Maßstab für ihre anschließende Prüfung zu Recht zum Teil aus einer Entscheidung des BVerfG zur automatisierten Kennzeichenerfassung (Rn. 160 ff. der Antragserwiderung). Die automatisierte Kennzeichenerfassung ist mit der Fluggastdatenverarbeitung vergleichbar, weil beide der Gefahrenabwehr dienen, personenbezogene Daten automatisiert mit Datenbanken abgleichen, fast vollständig die Daten von Personen verarbeiten, die keinen Anlass zu ihrer Überwachung gegeben haben, und (im Falle der automatisierten Kennzeichenerfassung zumindest auch) beim Übertritt innereuropäischer Grenzen durchgeführt werden. Die Fluggastdatenverarbeitung geht freilich insoweit noch über die automatisierte Kennzeichenerfassung hinaus, als die Fluggastdaten fünf Jahre lang gespeichert bleiben, u.a. für retrograde Recherchen; und dass auch ein Musterabgleich erfolgt, mit den bereits beschriebenen (vgl. oben I.3) Folgen. Selbst unter Außerachtlassung dieser erschwerenden Umstände ist die massenhafte Verarbeitung von Fluggastdaten nach dem FlugDaG nach den Maßstäben des BVerfG zur automatisierten Kennzeichenerfassung verfassungswidrig:

Die Antragsgegnerin gibt den Maßstab des BVerfG aus der Entscheidung zur automatisierten Kennzeichenerfassung verkürzt wieder. So lässt sie unerwähnt, dass derlei Kontrollen (1) jeweils durch einen hinreichend konkreten, objektiv bestimmten Grund veranlasst sind und (2) dem Schutz von Rechtsgütern von zumindest erheblichem Gewicht dienen. Die Ausgestaltung muss (3) im Blick auf das Grundrecht auf informationelle Selbstbestimmung zumutbar sein. Des Weiteren sind (4) Transparenz, individueller Rechtsschutz und aufsichtliche Kontrolle zu gewährleisten sowie Regelungen zur Datennutzung und Löschung zu treffen.

BVerfG, Beschl. v. 18. Dezember 2018 – 1 BvR 142/1 –, Rn. 90 ff.

Zum ersten Punkt führt das BVerfG aus:

„Allein das allgemeine Interesse, zur Fahndung ausgeschriebene Personen oder Sachen zu identifizieren und aufzugreifen, reicht zur Rechtfertigung solcher Kontrollen noch nicht. Zwar ist ein auch für sich bestehendes legitimes staatliches Interesse anzuerkennen, solche Personen oder Sachen aufzufinden. Dies rechtfertigt jedoch nicht schon für sich die Durchführung beliebiger Kontrollen gegenüber jedermann. Auch wenn die Fahndungsausschreibung auf eigenen

Rechtsgrundlagen beruht, besagt das nicht, dass zur Fahndung jede Maßnahme eingesetzt werden darf. Vielmehr bedürfen diese jeweils eines eigenen Anlasses. Die Durchführung von Kontrollen zu beliebiger Zeit und an beliebigem Ort ins Blaue hinein ist mit dem Rechtsstaatsprinzip grundsätzlich unvereinbar.“

BVerfG, a.a.O., Rn. 92.

Das BVerfG erkennt zwar an, dass anlasslose Kontrollen nicht generell ausgeschlossen sind. Dazu müssten die Kontrollen aber an ein gefährliches oder risikobehaftetes Tun anknüpfen, etwa im Falle stichprobenhaft durchgeführter Straßenverkehrskontrollen zur Überprüfung der Fahrtüchtigkeit der Fahrzeugführer.

BVerfG, a.a.O., Rn. 94.

Eben hierum geht es aber beim FlugDaG nicht. Damit sollen keine Gefahren bekämpft werden, die vom Fliegen selbst ausgehen (gegen Rn. 176 der Antragserwiderung). Diesem Zweck dienen vielmehr umfangreiche Gepäckbeschränkungen und -kontrollen sowie Leibesvisitationen vor dem Betreten des Sicherheitsbereichs eines Flughafens. Das hat in der Vergangenheit offenkundig auch erfolgreich verhindert, dass in Europa Flugzeuge als Waffen eingesetzt wurden. Selbst wenn das FlugDaG aber auch die Abwehr von Gefahren durch das Fliegen abwenden wollen sollte und könnte, würde dies nur die Datenverarbeitung zugunsten der Bewältigung eben dieser Gefahren rechtfertigen – also die Abwehr von Terrorangriffen mit entführten Flugzeugen. Der Katalog strafbarer Handlungen, die verhütet, aufgedeckt, ermittelt und verfolgt werden sollen, geht darüber aber weit hinaus (vgl. § 4 Abs. 1 FlugDaG).

Dass der permanente und alle Flüge nach und aus Deutschland erfassende Abgleich von Fluggastdaten mit Datenbanken und Mustern nicht anlasslos sein soll (Rn. 178 der Antragserwiderung), ist schlicht nicht nachvollziehbar (vgl. dazu bereits Antragsschrift S. 44 f.).

Dass das BVerfG die automatisierte Kennzeichenkontrolle grundsätzlich als Ersatz für den Wegfall von Grenzkontrollen anerkennt,

BVerfG, a.a.O., Rn. 144,

hilft der Antragsgegnerin nicht weiter. Es fehlt nämlich an dem vom BVerfG ebenfalls geforderten „konsequenten Grenzbezug“, den eine automatisierte Kennzeichenerfassung in diesem Fall haben muss. Dazu ist insbesondere erforderlich, dass die geschützten Rechtsgüter eine klar grenzbezogene Ausrichtung haben müssen,

indem sie der Bekämpfung grenzüberschreitender Kriminalität und damit der Bekämpfung von Gefahren dienen, die durch die (innereuropäische) Grenzöffnung eine besondere Dringlichkeit erfahren.

BVerfG, a.a.O., Rn. 147 f.

Eine solche Begrenzung kennt das FlugDaG nicht (vgl. § 4 Abs. 1 FlugDaG). Gleiches gilt auch für die vom BVerfG für automatisierte Kennzeichenerfassungen geforderte sofortige Löschung der erfassten Daten nach Abgleich (außer im Falle eines Treffers).

Vgl. BVerfG, a.a.O., Rn. 160.

Alles Vorstehende lässt die bereits erwähnten erschwerenden Merkmale der automatisierten Fluggastdatenspeicherung nach dem FlugDaG außer Betracht. Dies gilt sowohl für die lange Speicherdauer samt retrograder Recherche als auch für den Musterabgleich (zu letzterem sogleich unter 2.).

#### **b) Maßstäbe der weiteren Entscheidungen des BVerfG ebenfalls verletzt**

An der Verletzung der in der Antragschrift genannten Maßstäbe des BVerfG durch das FlugDaG wecken die weiteren Ausführungen der Antragsgegnerin keine Zweifel (Rn. 163 ff. der Antragserwiderung). Sie kann nicht konkret darlegen, auf welche Weise alle in § 2 Abs. 2 FlugDaG vorgesehenen Fluggastdaten zu EU-Flügen unter Anwendung aller in § 4 FlugDaG genannten Methoden (automatisierter Abgleich mit Datenbanken und Mustern, retrograde Recherche) zur Verhütung und Verfolgung sämtlicher in § 4 Abs. 1 FlugDaG genannten Straftaten geeignet und erforderlich sein sollen.

Die Erstreckung des FlugDaG auf EU-Flüge ist unverhältnismäßig. Sofern tatsächlich Terroristen zur Umgehung der Grenzkontrollen eines Mitgliedstaats einen Gabelflug über einen anderen Mitgliedstaat nutzen (so Rn. 164 der Antragserwiderung), können solche Konstellationen bereits durch Erfassung des gesamten Reiseverlaufs (§ 2 Abs. 2 Nr. 11 FlugDaG bzw. Anhang I Nr. 7 PNR-Richtlinie) im Rahmen des zwingend umzusetzenden Teils der PNR-Richtlinie erkannt werden. Selbst wenn gleichwohl ein Abgleich mit Datenbanken von Terrorverdächtigen auch bei EU-Flügen unbedingt erforderlich wäre, könnte sich das FlugDaG hierauf beschränken. Es könnten Abgleiche mit Datenbanken von Terrorverdächtigen, ggf. auch mit Datenbanken von Verdächtigen grenzüberschreitender Drogenkriminalität, stattfinden. Eben das zeigen auch die beiden

von der Antragsgegnerin aufgeführten Beispiele für erfolgreiche Datenbankabgleiche (Rn. 165 der Antragserwiderung).

In der Folge scheitert der Versuch der Antragsgegnerin, die automatisierte Fluggastdatenverarbeitung von der Rasterfahndung abzugrenzen (Rn. 168 ff. der Antragserwiderung). Dazu definiert die Antragsgegnerin die Rasterfahndung wie folgt:

„Sie ist eine besonders eingriffsintensive, verdeckte Maßnahme zu präventiven und repressiven Zwecken und stellt eine besondere Ermittlungsmethode unter Nutzung der elektronischen Datenverarbeitung dar, bei der sich die Strafverfolgungsbehörden (bzw. polizeiliche Gefahrenabwehrbehörden) von anderen öffentlichen oder privaten Stellen personenbezogene Daten übermitteln lässt, um einen Abgleich, die sogenannte Rasterung, mit anderen Daten vorzunehmen. Es handelt sich dabei um einen automatisierten Vergleich von personenbezogenen Daten, die in Dateien anderer Stellen ursprünglich zu jeweils anderen Zwecken erhoben und gespeichert sind. (...) Durch die Verknüpfung mit anderen Informationen können persönlichkeitsbezogene Einblicke im Sinne eines Persönlichkeitsprofils ermöglicht werden.“

Rn. 168 der Antragserwiderung unter Bezug auf BVerfG, Beschl. v. 17. Februar 2009 – 2 BvR 1372/07 –, Rn. 23 f.

Unter diese Definition lässt sich der Abgleich von Fluggastdaten mit Mustern ebenso subsumieren: Er dient präventiven und repressiven Zwecken, nutzt die elektronische Datenverarbeitung, das BKA als Gefahrenabwehrbehörde lässt sich Fluggastdaten von Privatunternehmen übermitteln, die diese Daten ursprünglich zu andern Zwecken erhoben und gespeichert haben (für die Abwicklung des Vertrags über eine Flugleistung), und gleicht sie automatisiert mit anderen Daten, nämlich Datenbanken und Mustern, ab. Durch den Musterabgleich können und sollen auch Persönlichkeitsprofile entstehen, nämlich von „bislang ‚unbekannte[n]‘ Verdächtigen“. Anders als die Antragsgegnerin behauptet (Rn. 169 der Antragserwiderung) ist Anknüpfung für das Muster gerade nicht „kriminelles Verhalten“ des Betroffenen – das ist ja gerade unbekannt –, sondern es sind eben nur die Fluggastdaten selbst, die jemanden verdächtig machen.

Nicht nachvollziehbar ist auch der Versuch, die Rasterfahndung von der Fluggastdatenverarbeitung dadurch abzugrenzen, dass die Befugnis zur Fluggastdatenverarbeitung in Form des FlugDaG im Bundesgesetzblatt veröffentlicht wurde (Rn. 170 f. der Antragserwiderung). Den wenigsten Fluggästen wird das bekannt sein. Ein Fluggast wird nicht wissen, was etwa im Rahmen eines Musterabgleichs mit seinen Daten geschieht, weil die Muster nicht bekannt sind. Im Übrigen bleibt die

Flugastdatenverarbeitung im Einzelfall schon deshalb heimlich, weil sie vom Betroffenen nicht wahrgenommen wird.

Damit gelten die in der Antragsschrift (dort S. 42 ff.) fruchtbar gemachten Maßstäbe aus den Entscheidungen des BVerfG zur Rasterfahndung entsprechend. Man muss die bestehende Rechtsprechung nur übertragen. Ohne dass es darauf ankäme, gilt das aus den bereits genannten Gründen (vgl. oben I.1) auch für die Entscheidungen zur Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten (gegen Rn. 172 der Antragserwiderung).

## **2. Musterabgleich verfassungswidrig**

Der anlasslose Abgleich mit Mustern (§ 4 Abs. 2 Satz 1 Nr. 2, Abs. 3 FlugDaG) ist noch einmal gesondert hervorzuheben.

Denn er ist auf einer fundamentalen Ebene mit dem System des Grundrechtsschutzes des Grundgesetzes nicht vereinbar.

Oben (vgl. I.3.) wurde bereits aufgezeigt, unter welchen Mängeln die hochgesteckten Ziele der Aufspürung „bislang ‚unbekannte[r]‘ Verdächtiger“ leiden. Vorbehaltlich struktureller Vorsorgemaßnahmen, die im FlugDaG nicht getroffen sind, wird der Musterabgleich zur Verhütung und Verfolgung der allermeisten in § 4 Abs. 1 FlugDaG genannten Straftaten von vornherein untauglich sein; er wird hinsichtlich der potentiell tauglichen Straftaten zu weit mehr falschen Verdächtigungen führen als zu korrekten Treffern; er wird wahrscheinlich diskriminierend wirken; und er wird effektiven Rechtsschutz gegen Folgemaßnahmen, die sich auf den Musterabgleich stützen, sehr schwierig, wenn nicht unmöglich machen. Schon dies ist mit dem Grundgesetz nicht zu vereinbaren.

Der Abgleich mit Mustern – so harmlos er semantisch daherkommt – rüttelt aber auch an den Grundfesten des Menschenbildes, das dem Grundgesetz zugrunde liegt. Denn er soll die Gefährlichkeit von Menschen anhand von alltäglichen Daten beurteilen können, die keinen Bezug zu einer konkreten Straftat haben. Eine solche Form der Vermessung des Menschen ist Teil einer gefährlichen Entwicklung, die Menschen immer früher zu kategorisieren versucht. Es verletzt die Betroffenen in ihrem Anspruch aus Art. 1 Abs. 1 Satz 1 GG, vom Staat nicht als bloßes Objekt, als potentielle Gefahrenquelle behandelt zu werden.

Die Pflicht zur individuellen Überprüfung der vom Musterabgleich ausgeworfenen Ergebnisse (vgl. § 4 Abs. 2 Satz 2 FlugDaG) beugt dem nicht hinreichend vor. Denn das setzt voraus, dass der Prüfer des Ergebnisses die Kompetenz und Autorität besitzt, sich über das Ergebnis hinwegzusetzen. Das wiederum begegnet verschiedenen Problemen. So könnten die Muster vom Prüfer nicht verstanden werden, weil sie maschinell gewonnen oder aus anderen Gründen für ihn nicht transparent sind; der Prüfer könnte dem Urteil der Maschine ein höheres Vertrauen schenken als seinem eigenen,

vgl. zum Problem der *algorithmic appreciation* etwa Logg/Minson/Moore, Algorithm Appreciation: People Prefer Algorithmic To Human Judgment, Harvard Business School 2018, online abrufbar unter:  
[http://www.hbs.edu/faculty/Publication%20Files/17-086\\_610956b6-7d91-4337-90cc-5bb5245316a8.pdf](http://www.hbs.edu/faculty/Publication%20Files/17-086_610956b6-7d91-4337-90cc-5bb5245316a8.pdf);

oder sein Vorgesetzter könnte dem Urteil der Maschine ein höheres Vertrauen schenken als dem des Prüfers. Alle Probleme könnten sich im Laufe der Zeit zudem verstärken, jedenfalls wenn der Musterabgleich (gefühlte) Treffer generiert.

### **3. Möglichkeit der Zweckänderung der PNR-Daten und Verarbeitungsergebnisse ist verfassungswidrig**

Die Antragsgegnerin (Rn. 179 ff. der Antragsserwiderung) irrt darin, die in § 6 Abs. 4 FlugDaG vorgesehene Möglichkeit der Zweckänderung als verfassungsgemäß anzusehen. Sie meint, eine weitere Konkretisierung der Formulierung einer „bestimmten anderen Straftat“ sei nicht erforderlich, da die jeweilige Behörde i.S.d. § 6 Abs. 1 FlugDaG bei jeder Zweckänderung die Einhaltung der Grundsätze des Bundesverfassungsgerichts zur hypothetischen Datenneuerhebung nach dem für sie geltenden Polizeigesetz zu prüfen habe (vgl. Rn. 181 der Antragserwiderung).

Die Antragsgegnerin verkennt, dass das zu einer Zweckänderung ermächtigende Gesetz selbst den verfassungsrechtlichen Anforderungen genügen und somit auch die vom Bundesverfassungsgericht entwickelten Grundsätze zur Zweckänderung beachten muss.

Vgl. BVerfGE 100, 313 <389 f.>; 109, 279 <376 f.>, 130, 1 <33 f.>; 133, 277 <372 f.>; 141, 220 <327 f.>.

Die gesetzliche Ermächtigung zur Zweckänderung ist vorliegend § 6 Abs. 4 FlugDaG. Die Vorschrift verweist nicht auf andere Gesetze und ist daher abschließend und eigenständig. Aus diesem Grund kommt es nicht darauf an, ob das für die jeweilige in

§ 6 Abs. 1 FlugDaG genannte Behörde geltende Gesetz den Anforderungen des Bundesverfassungsgerichts genügt.

#### **4. Straftatenkatalog ist verfassungswidrig**

Die Ausführungen der Antragsgegnerin zur Verfassungsmäßigkeit des in § 4 Abs. 1 Nr. 6 FlugDaG enthaltenen Verweises auf strafbare Handlungen nach Anhang II der PNR-Richtlinie (Rn. 183 ff. der Antragserwiderung) tragen nicht.

Der Antragsgegnerin ist insoweit zuzustimmen, dass Verweisungen auf Normen des Unionsrechts grundsätzlich zulässig sind. Wie auch die Antragsgegnerin zugesteht, müssen solche Verweisungen auf das Unionsrecht genauso behandelt werden wie Verweisungen auf das nationale Recht (vgl. Rn. 185 der Antragserwiderung). Sie müssen somit den verfassungsmäßigen Anforderungen, insbesondere dem allgemeinen, auch außerhalb von Art. 103 Abs. 2 GG geltenden Bestimmtheitsgebot genügen. Danach sind Anlass, Zweck und Umfang des jeweiligen Eingriffs sowie die entsprechenden Eingriffsschwellen durch den Gesetzgeber bereichsspezifisch, präzise und normenklar zu regeln.

BVerfGE 100, 313 <359 f.>; 110, 33 <53>; 113, 29 <51>; 113, 348 <375>; 115, 320 <365>; 118, 168 <186 f.>; 125, 260 <328>.

Auf Grundlage eines Verweises auf strafbare Handlungen, die keine unmittelbare Entsprechung im deutschen Strafrecht finden, kann der Normadressat jedoch nicht ohne Weiteres erkennen, bei Verwirklichung welcher Straftatbestände, also aus welchem Anlass, ein Datenabgleich stattfinden kann. Vorliegend ist es für einen Sicherheitsbeamten nur schwer ermittelbar, welche im deutschen Strafrecht geregelte Straftat etwa der in Nr. 17 Anhang II der PNR-Richtlinie aufgeführten „Betrügerischen Nachahmung und Produktpiraterie“ entspricht.

Zudem ermöglicht das Erfordernis, dass eine strafbare Handlung mit einer Freiheitsstrafe im Höchstmaß von mindestens drei Jahren bedroht ist, nicht die Feststellung, dass die Straftat auch im Einzelfall schwer wiegt.

Vgl. zu diesem Erfordernis BVerfGE 125, 260 < 329>.

Aus der Formulierung „Einzelfall“ folgt, dass die rein abstrakte, objektive Einordnung einer Straftat als „schwer“ nicht ausreicht. Dementsprechend unterscheidet das Bundesverfassungsgericht in seinem Urteil zur Vorratsdatenspeicherung zwischen der

abstrakten Qualifizierung einer Straftat als schwer und einer auch im Einzelfall schwer wiegenden Straftat. Dazu heißt es im Urteil, dass die abstrakte Qualifizierung einer Straftat als schwer insbesondere anhand des geltenden Strafrahmens Ausdruck findet.

BVerfGE 125, 260 < 329>.

Die Schwere der Tat im Einzelfall kann nach Auffassung des Bundesverfassungsgericht anhand einzelner Indizien wie etwa der Schutzwürdigkeit der verletzten Rechtsgüter, dem Grad der Bedrohung der Allgemeinheit, der Art der Begehung der Straftat, der Anzahl der Geschädigten und/oder dem Ausmaß des Schadens ermittelt werden. Um zu einer Berücksichtigung dieser Indizien anzuhalten, genügt bereits eine Formulierung wie in § 100a Abs. 1 Nr. 2 StPO StPO, dass „die Tat auch im Einzelfall schwer wiegt“.

BVerfGE 129, 208 < 244>; vgl. auch BVerfGE 121, 1 <26>.

Das Kriterium einer Mindesthöchststrafe von drei Jahren ist dahingegen rein abstrakt.

## **E. Anordnungsgrund**

Der Antragsteller kann auch einen Anordnungsgrund glaubhaft machen.

Für das Vorliegen eines Anordnungsgrundes kommt es auf die Frage, ob dem Antragsteller durch Zeitablauf wesentliche Nachteile i.S.d. § 123 Abs. 1 Satz 2 VwGO entstehen können, nicht an (so aber Rn. 193 ff. der Antragserwiderung). Denn das (vorbeugende) Begehren des Antragstellers ist auf den Erlass einer Sicherungsanordnung i.S.d. § 123 Abs. 1 Satz 1 VwGO gerichtet. Eine Sicherungsanordnung dient der Sicherung des status quo, der durch bereits zugeordnete oder ausgeübte Rechte gekennzeichnet ist und insbesondere durch tatsächliches Verwaltungshandeln beeinträchtigt wird.

Vgl. *Schoch*, in: ders./Schneider/Bier, Stand: Feb. 2019, § 123. Rn. 53.

Das Bestimmungsrecht über seine PNR-Daten ist ein solches dem Antragsteller zugeordnetes Recht, dessen Beeinträchtigung durch die Datenübermittlung er unter Aufrechterhaltung des status quo zu verhindern sucht.

Anders als im Falle einer Regelungsanordnung besteht ein Anordnungsgrund für den Erlass einer Sicherungsanordnung gemäß § 123 Abs. 1 Satz 1 VwGO bereits, wenn zu besorgen ist, dass durch die Veränderung des bestehenden Zustands die Verwirklichung



eines Rechts des Antragstellers vereitelt oder wesentlich erschwert wird. Dies ist vorliegend der Fall. Eine Interessenabwägung findet – anders als bei der Regelungsanordnung – gerade nicht statt.

Vgl. *Schoch*, in: ders./Schneider/Bier, Stand: Feb. 2019, § 123. Rn. 79a mit zahlreichen weiteren Nachweisen.

Selbst wenn eine solche vorzunehmen wäre, hat die Antragsgegnerin keinen einzigen Aspekt vorgetragen, der für eine Verarbeitung der Fluggastdaten gerade des Antragstellers zum dafür vorgesehenen statt zu einem späteren Zeitpunkt spricht. Vielmehr beschränkt sie sich darauf, auf „die Bedeutung des mit der Richtlinie verfolgten Ziels – der Gewährleistung öffentlicher Sicherheit“ hinzuweisen (Rn. 196 der Antragserwiderung). Im Falle einer einstweiligen Anordnung zu Gunsten des Antragstellers wird also ein Eingriff in sein Recht auf informationelle Selbstbestimmung (einstweilen) abgewendet, während der Antragsgegnerin daraus keine Nachteile drohen.

Zwei beglaubigte Abschriften anbei.

Prof. Dr. Remo Klinger  
(Rechtsanwalt)

### **Anlagenverzeichnis**

Anlage 4: BT-Drs. 19/9536

Anlage 5: Gemeinsame Erklärung des Rates vom 18. April 2016