Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)336 D

Freie Universität Berlin

Univ.-Prof. Dr. Klaus Hoffmann-Holland
Geschäftsführender Direktor der
Wissenschaftlichen Einrichtung Strafrecht (WE 02)

Fachbereich Rechtswissenschaft
WE 2 – Strafrecht
Lehrstuhl für Kriminologie und Strafrecht

Stellungnahme
im Rahmen der öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages

zum Entwurf eines Gesetzes über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (BT-Drucksache 17/5096)

I. Ausgangslage und europarechtlicher Hintergrund*

Anlass für den Gesetzentwurf ist die Umsetzung des Rahmenbeschlusses 2006/960/JI des Rates der Europäischen Union zur Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen Strafverfolgungsbehörden der Mitgliedstaaten der Europäische Union (RbDatA) vom 18.12.2006 (Abl. L 386, S. 89)[1] in die deutsche Rechtsordnung. Stichtag der Umsetzung war der 19. Dezember 2008. Ausweislich eines Arbeitspapiers der Europäischen Kommission[2] sind in zwei Dritteln der Mitgliedstaaten bereits entsprechende Umsetzungsgesetze erlassen worden. Großbritannien und Irland haben erklärt, dass ihre nationalen Rechtsvorschriften bereits den Anforderungen des Rahmenbeschlusses entsprächen. In den übrigen Mitgliedstaaten wurde der Rahmenbeschluss – zumeist aus Gründen des nationalen Gesetzgebungsverfahrens – bislang nicht in nationales Recht umgesetzt.[3]

Der RbDatA stellt einen weiteren Schritt bei der Realisierung des nunmehr in Art. 67 Abs. 1 AEUV formulierten Ziels der Schaffung eines Raumes der Freiheit, der Sicherheit und des Rechts dar. Nach dem erstmals im Haager Programm 2004 formulierten „Grundsatz der Verfügbarkeit“ *(principle of availability)* soll „der bloße Umstand, dass Informationen Grenzen überschreiten, nicht länger von Bedeutung sein.“[4] In den folgenden Jahren war eine rasante Entwicklung durch die Verabschiedung einer Vielzahl von Programmen und Rechtsakten zu verzeichnen, welche den Informationsaustausch zur Ermöglichung einer effektiven Strafverfolgung im europäischen Raum vereinfachen und beschleunigen sollen. Begrenzende Sicherungs-

* Dank für ihre wertvolle Hilfe bei der Erarbeitung der Stellungnahme gebührt Frau Ass. iur. *Désirée Glanzer*, Wiss. Mitarbeiterin am Fachbereich Rechtswissenschaft der Freien Universität Berlin.

1 Rahmenbeschluss 2006/960/JI, Abl. L 386 vom 29.12.2006, S. 89.

2 Commission staff working paper, Operation of the Council Framework Decision 2006/960/JHA of 18 December 2006 (“Swedish Initiative”), SEC (2011) 593 final, 13.5.2011.

3 Ebenda, S. 5 (Österreich, Belgien, Deutschland, Estland, Griechenland, Frankreich, Italien, Luxemburg und Polen).

4 Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union, Abl. C 53/1 vom 3.3.2005 S. 7; vgl. hierzu auch Satzger, Internationales und Europäisches Strafrecht, 4. Auflage, Baden-Baden 2010, § 10 Rn. 47 ff.; Meyer, Der Grundsatz der Verfügbarkeit, NStZ 2008, S. 188 f.

mechanismen zum Schutz der Betroffenen vor Erhebung, Übermittlung und Verwendung ihrer Daten sind jedoch bislang nicht harmonisiert.

Mit dem Vertrag von Lissabon wurde die Polizeiliche und Justizielle Zusammenarbeit in Strafsachen (PJZS) aus der 3. Säule herausgelöst und als neuer, nunmehr supranational ausgestalteter Politikbereich in eine einheitliche und mit Rechtspersönlichkeit ausgestattete Europäische Union überführt. Dennoch fand eine vollständige Integration in den Rechtsrahmen der ehemaligen europäischen Gemeinschaft bisher nicht statt. Eine Vielzahl von Rechtsakten bleiben nach wie vor den „originären Politikbereichen" vorbehalten, so auch die Richtlinie 95/46 des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DSRL) vom 24.10.1995 (Abl. L 281, S. 31). Wie sich die PJZS unter dem Vertrag von Lissabon - als nunmehr den Politikfeldern der früheren ersten Säule gleichwertiger Bereich – entwickeln wird und welche Angleichungen hierdurch erforderlich werden, ist derzeit Gegenstand rechtswissenschaftlicher Diskussionen[5]. Die weitere Entwicklung ist jedoch auch nach Annahme des Stockholmer Programms (2010-2014) durch den Europäischen Rat weitgehend offen. Eine Analyse und Bewertung des Gesetzesvorhabens setzt voraus, dass dieser Hintergrund mitberücksichtigt wird.

Hiervon ausgehend gilt es zu untersuchen, ob der vorliegende Gesetzentwurf – insbesondere unter datenschutzrechtlichen Gesichtspunkten – eine angemessene Umsetzung des ihm zugrunde liegenden Rahmenbeschlusses darstellt, oder ob weiterer Regelungs- bzw. Konkretisierungsbedarf zur Sicherstellung einer ausreichenden Beachtung von nationalen und unionalen (Grund-) Rechten besteht.

Dazu soll zunächst der Regelungsbedarf mit Blick auf die systematische Einordnung betrachtet werden. Sodann ist auf den Grundsatz der Normen-

5 Braum, Europäischer Datenschutz und Europäisches Strafrecht, KritV 2008, S. 82, 91 f.; Heger, Perspektiven des Europäischen Strafrechts nach dem Vertrag von Lissabon, ZIS 2009, S. 406, 417; Jokisch/Jahnke, in: Sieber/Brüner/Satzger/Heintschell-Heinegg (Hrsg.), Europäisches Strafrecht, Baden-Baden 2011, § 2, Rn. 1 f.; Kaiafa-Gbandi, Das Strafrecht in der Unionsgrundordnung, KritV 2011, S. 153 f.; Meyer, Das Strafrecht im Raum der Freiheit, der Sicherheit und des Rechts, EuR 2011, S. 169, 174; Selinger, Erstes Trierer Forum zum Recht der Inneren Sicherheit „Transnationale Strafverfolgung", ZIS 2011, S. 50 f.

klarheit einzugehen, um anschließend das Verhältnis von Gleichstellungsgebot und Datenschutz zu analysieren.

II. Regelungsbedarf und Systematik

Der Gesetzentwurf hat die Änderung einer Reihe von Gesetzen (IRG, StPO, BKAG, BPolG, ZFdG, ZollVG, SchwarzArbG, SGB X und der AO) zum Gegenstand. Regelungsbedarf besteht insbesondere hinsichtlich der Übermittlung von Informationen. Hierfür sieht der RbDatA in Art. 3 Abs. 3 ein Gleichstellungsgebot vor. Das Ersuchen eines EU–Mitgliedstaates hat zwar weiterhin nach den nationalen Rechtsvorschriften des Übersenderstaates zu erfolgen; hierfür dürfen jedoch keine strengeren Vorschriften als bei der Übermittlung an eine innerstaatliche Behörde gelten. Diesen Vorgaben entspricht die geltende nationale Rechtslage nicht. Derzeit existiert eine Reihe von Sondervorschriften für ausländische Ersuchen. So regelt beispielsweise § 14 BKAG die „Befugnisse bei der Zusammenarbeit im internationalen Bereich“. Darunter fallen derzeit auch Informationsersuchen der Mitgliedstaaten der Europäischen Union. Für derartige Ersuchen gelten strengere Voraussetzungen als bei einem rein innerstaatlichen Informationsaustausch. Aus diesem Grund sollen nach den Vorgaben des RbDatA neue Tatbestände für die Übermittlung von Informationen in EU- bzw. Schengen assoziierte Staaten geschaffen werden. In systematischer Hinsicht sind die Vorschriften im Gesetzentwurf nahezu identisch ausgestaltet, so dass im Folgenden die wichtigsten Änderungen anhand des BKAG-E beispielhaft dargestellt und bewertet werden.

Art. 3 des Gesetzentwurfs sieht die Einfügung von § 14a BKAG mit dem Titel „Übermittlung personenbezogener Daten an Mitgliedstaaten der Europäischen Union“ vor. In dessen Abs. 1 S. 2 heißt es mit Blick auf das Gleichstellungsgebot des Art. 3 Abs. 3 RbDatA: „Für die Übermittlung dieser Daten gelten die Vorschriften über die Datenübermittlung im innerstaatlichen Bereich entsprechend.“ Abs. 2 regelt die formalen Zulässigkeitsvoraussetzungen für die Übermittlung und setzt die in Art. 5 Abs. 1 und 3 RbDatA aufgeführten Anforderungen unter Berücksichtigung des Zweckbindungsgrundsatzes um. Abs. 3 sieht Regelungen für Spontanauskünfte bei Straftaten im Sinne des Rahmenbeschlusses über den Europäischen Haftbefehl (EuHB) vor: Eine Übermittlung setzt voraus, dass „im Einzelfall die

Gefahr der Begehung einer Straftat [im Sinne des Rahmenbeschlusses über den EuHB] besteht und zu erwarten ist, dass die Datenübermittlung geeignet ist, zur Verhütung einer solchen Straftat beizutragen." Abs. 5 verweist für die Bestimmung der zuständigen Strafverfolgungsbehörde auf Art. 2 lit. a RbDatA, nach dem die Mitgliedstaaten beim Generalsekretariat des Rates eine entsprechende Erklärung zu hinterlegen haben.[6] § 27 BKAG-E fügt in Abs. 2 obligatorische, in Abs. 3 fakultative Übermittlungs- und Verweigerungsgründe ein. Abs. 2 sieht vor, dass eine Übermittlung nach § 14a BKAG-E zwingend zu unterbleiben hat, wenn hierdurch wesentliche Sicherheitsinteressen des Bundes oder der Länder beeinträchtigt werden (Nr. 1; entspricht Art. 10 Abs. 1 lit. a RbDatA), die Übermittlung zu Art. 6 EUV in Widerspruch steht (Nr. 2; entspricht Art. 1 Abs. 7 RbDatA), die Daten nicht vorhanden sind und nur durch Zwangsmaßnahmen erlangt werden können (Nr. 3; entspricht Art. 1 Abs. 5 i.V.m. Art. 2 lit. d, ii RbDatA) sowie bei Unverhältnismäßigkeit der Übermittlung oder fehlender Erforderlichkeit (Nr. 4; entspricht Art. 10 Abs. 1 lit. c RbDatA).

§ 27 Abs. 3 BKAG-E stellt die Entscheidung über die Ablehnung bei nicht vorhandenen, aber ohne Ergreifung von Zwangsmaßnahmen verfügbaren Daten (Nr. 1; entspricht Art. 2 lit. d, i, ii RbDatA), der Gefährdung laufender Ermittlungen, der Gefährdung von Leib, Leben oder Freiheit einer Person (Nr. 2; entspricht Art. 10 Abs. 1 lit. b RbDatA) und bei Vorliegen einer Tat, die im Höchstmaß mit weniger als einem Jahr Freiheitsstrafe bedroht ist (Nr. 3; entspricht Art. 10 Abs. 2 RbDatA) in das Ermessen der übermittelnden Behörde. Die konkrete Ausgestaltung der Ablehnungsgründe befindet sich im Einklang mit dem RbDatA und sichert die Einhaltung des Verhältnismäßigkeitsprinzips.

Für die Datenverwendung sollen gemäß Art. 8 Abs. 2 RbDatA die nationalen Vorschriften des Empfängerstaates – einschließlich der nationalen Datenschutzbestimmungen – Anwendung finden. Nach § 27a Abs. 1 S. 1 BKAG dürfen die Daten nur zu dem Zweck, zu dem sie übermittelt wurden, oder zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit verwendet werden. Eine Verwendung zu einem anderen

6 Vgl. zum Übermittlungsstand (Dezember 2010): Rat der Europäischen Union, Vermerk betr. der Leitlinien zum Rahmenbeschluss 2006/960/JI, Anlage IV, Lists of competent authorities for FWD2006/960/JHA , 9512/3/10 vom 1.3. 2011, S. 1, 124, (http://register.consilium.europa.eu/pdf/de/10/st09/st09512-re03.de10.pdf).

Zweck oder als Beweismittel bedarf nach S. 2 der Zustimmung des Mitgliedstaates (entspricht Art. 8. Abs. 3 RbDatA). Abs. 2 sieht eine Auskunft des Übermittlerstaates über die erfolgte Verwendung auf dessen Ersuchen vor (entspricht Art. 8 Abs. 4 S. 2 RbDatA).

Auffällig ist, dass eine Umsetzung der in Art. 4 RbDatA festgeschriebenen Beantwortungsfristen bislang vollständig unterblieben ist. Auch nach Behebung der erforderlichen technischen Anpassungen sollen diese allenfalls in die Richtlinien für den Verkehr mit dem Ausland in strafrechtlichen Angelegenheiten (RiVASt) aufgenommen werden.[7] Dies ist im Hinblick auf die obligatorische Benachrichtigung des Mitgliedstaates bei Verzögerungen als problematisch anzusehen. Die Erreichung des Ziels eines „raschen Austauschs“[8] kann damit nicht als gesichert gelten.

III. Grundsatz der Normenklarheit

Im Zuge des Gesetzgebungsverfahrens wurden Bedenken hinsichtlich der gebotenen Normenklarheit geäußert.[9] Nach der Rechtsprechung des Bundesverfassungsgerichts müssen Anlass, Zweck und Grenzen des Eingriffs in das Recht auf informationelle Selbstbestimmung in der Ermächtigungsgrundlage präzise und normenklar festgelegt werden: „Die konkreten Anforderungen an die Bestimmtheit und Klarheit der Ermächtigung richten sich nach Art und Schwere des Eingriffs. Diese ergibt sich aus der Art der vorgesehenen Maßnahme und der von ihr für den Betroffenen ausgelösten Wirkung. Welchem Ziel die Maßnahme dient, etwa der Gefahrenabwehr oder der Gefahrenverhütung, ist für die Beurteilung ihrer Schwere für den Betroffenen ohne Belang.“[10]

7 BT-Drucks. 17/5098, S. 16.

8 Vgl. Rahmenbeschluss 2006/960/JI, Abl. L 386 vom 29.12.2006, S. 89, Erwägungsgründe 6.

9 Plenarprotokoll 17/99, S. 11419 (B).

10 BVerfGE 110, 33, 55; vgl. BVerfGE 65, 1, 44 ff; BVerfGE 100, 313, 359f, 372; BVerfGE 113, 348, 375.

1. Bestimmung der zuständigen Strafverfolgungsbehörde

Die zuständige Strafverfolgungsbehörde ergibt sich nicht unmittelbar aus der gesetzlichen Regelung, sondern erst aus einem Verweis auf Art. 2 lit. a RbDatA (vgl. § 92 Abs. 5 IRG-E, § 14a Abs. 5 BKAG-E, § 32a Abs. 5 BPolG-E, § 34a Abs. 5 ZfdG-E, § 11a Abs. 7 ZollVG-E). Danach haben die Mitgliedstaaten die zuständige Stelle in einer beim Generalsekretariat des Rates zu hinterlegenden Erklärung zu benennen.[11] Diese Vorgehensweise stieß im Rahmen der Beratungen im Bundestag auf Kritik.[12]

Eine Verletzung des Bestimmtheitsgebots liegt jedoch insoweit nicht vor. Dies käme in Betracht, wenn durch zahlreiche Verweisungen „ein hohes Fehlerrisiko bei der Rechtsanwendung erzeugt“ würde.[13] Art. 2 lit. a RbDatA definiert den Begriff jedoch seinerseits als „eine nationale Polizei-, Zoll- oder sonstige Behörde, die nach nationalem Recht befugt ist, Straftaten oder kriminelle Aktivitäten aufzudecken, zu verhüten und aufzuklären und in Verbindung mit diesen Tätigkeiten öffentliche Gewalt auszuüben und Zwangsmaßnahmen zu ergreifen. Behörden oder Stellen, die sich speziell mit Fragen der nationalen Sicherheit befassen, fallen nicht unter den Begriff der zuständigen Strafverfolgungsbehörde.“ Der Vorschrift lässt sich damit sowohl eine gegenständliche Begrenzung des Anwendungsbereichs als auch die Vorgabe eines bereichsspezifischen Zwecks für die jeweilige Datenerhebung entnehmen.[14] Die zuständige Behörde ist erkennbar, eine weitere Konkretisierung der Norm nicht erforderlich.

2. Der Begriff der Zwangsmaßnahme

Nach dem RbDatA muss sich die Informationsübermittlung nur auf solche Informationen erstrecken, die entweder bereits beim Übermittlerstaat „vorhanden“, oder die für diesen ohne die Ergreifung von Zwangsmaßnahmen „verfügbar“ sind (vgl. Art. 1 Abs. 5 i.V.m. Art 2 lit. d, ii RbDatA). Es besteht damit ein gewisser Umsetzungsspielraum für den nationalen Gesetzgeber.

11 Zu den benannten Strafverfolgungsbehörden vgl. FN 7.

12 Plenarprotokoll 17/99, S. 11419 (B).

13 Vgl. BVerfGE 110, 33, 61 ff.

14 Vgl. zu den Anforderungen BVerfG,NJW 2007, 2464, 2467.

Der deutsche Gesetzentwurf sieht vor, dass eine Übermittlung unzulässig ist, wenn die ihr zugrunde liegenden Informationen, erst mittels Zwangsmaßnahme beschafft werden müssten. (vgl. § 92 Abs. 3 Nr. 2 IRG, § 27 Abs. 2 Nr. 3 BKAG, § 33 Abs. 3a Nr. 3 BPolG, § 35 Abs. 2 Nr. 3 ZfdG, § 11a Abs. 4 Nr. 3 ZollVG, § 6a Abs. 3 Nr. 3 SchwarzArbG). Für die Beurteilung der Zulässigkeit einer Informationsübermittlung kommt es entscheidend darauf an, ob es sich um vorhandene oder um bloß verfügbare, also noch zu beschaffende Informationen handelt. Liegen die Informationen bereits vor, ist es im Ergebnis unerheblich, ob ihre Erhebung mittels Zwangsmaßnahme oder auf andere Weise erfolgt ist. Damit steht auch das Instrument des Datenabgleichs, als eine bereits im deutschen Datennetzwerk vorhandene Information, grundsätzlich zur Verfügung, ohne dass es auf die Frage der Zwangsmaßnahme in diesem Zusammenhang entscheidend ankäme.[15] Der Bundesrat hatte in einer Stellungnahme zum gegenständlichen Gesetzentwurf um eine Definition des Begriffs gebeten, da er befürchtet, der Datenabgleich sei wegen seiner spezialgesetzlichen Ermächtigungsgrundlage vom Anwendungsbereich des RbDatA ausgeschlossen.[16]

Auch darüber hinaus besteht keine Notwendigkeit einer Legaldefinition. Was unter einer Zwangsmaßnahme zu verstehen ist, bestimmt sich gemäß Art. 1 Abs. 6 RbDatA nach innerstaatlichem Recht. Der Begriff ist auch in der Rechtsanwendung bestimmbar. Ausweislich der Gesetzesbegründung sind Zwangsmaßnahmen im Sinne des Gesetzentwurfs (im Bereich der Gefahrenabwehr) „Maßnahmen, die gegen oder ohne den Willen der betroffenen Person durchgesetzt werden und die aufgrund des damit einhergehenden wesentlichen Grundrechtseingriffs einer speziellen gesetzlichen Grundlage bedürfen, also nicht auf Generalklauseln oder vergleichbare Grundnormen (…) gestützt werden können.“[17] Für die innerstaatliche Handhabung im Anwendungsbereich des RbDatA ist der Begriff aufgrund des Verweises auf die nationale Rechtsordnung sowie Ausführungen in der Gesetzesbegründung hinreichend klar, so dass es einer Legaldefinition durch den Gesetzgeber nicht bedarf.

15 Vgl. Gegenäußerung der Bundesregierung, BT-Drucks. 17/5096, S. 38.

16 Stellungnahme des Bundesrates, BT-Drucks. 17/5096, S. 33.

17 BT-Drucks. 17/5096, S. 25, 27, 29 f.

3. „Zweifelsfallkompetenz“ der Staatsanwaltschaft

Der Gesetzentwurf sieht ferner eine Änderung der §§ 478 und 481 StPO vor. Bislang liegt die Entscheidungskompetenz für die Übermittlung personenbezogener Daten zum Zwecke der Strafverfolgung allein bei der übermittelnden Polizeibehörde. Der Entwurf sieht nun bei Zweifeln der ersuchten Polizeibehörde die Möglichkeit vor, die Staatsanwaltschaft anzurufen, um bei grenzüberschreitenden Sachverhalten eine justizielle Vorabprüfung durchzuführen.[18]

§ 481 StPO betrifft die Fälle der sogenannten „Umwidmung“ von personenbezogenen Daten aus Strafverfahren zu Zwecken der Gefahrenabwehr.[19] Dies ist den Polizeibehörden „nach Maßgabe der Polizeigesetze“ grundsätzlich gestattet. Der Gesetzentwurf sieht in Abs. 3 einen Verweis auf § 478 StPO vor, so dass bei Zweifeln über die Verwendung die Anrufung der Staatsanwaltschaft möglich ist. Die Auffassung des Bundesrates, dies stelle einen Eingriff in die ausschließliche Zuständigkeit der Polizei dar und sei daher unzulässig,[20] kann im Ergebnis nicht geteilt werden. Der Bundesregierung ist insoweit zuzustimmen, dass aufgrund des Verweises in § 481 Abs. 2 StPO weitere bundes- und landesrechtliche Verwendungsbeschränkungen zu prüfen sind.[21] Im Anwendungsbereich der Strafprozessordnung ist die Zuständigkeit der Staatsanwaltschaft gemäß § 161 Abs. 1 StPO eröffnet. Auch im Hinblick auf die gemäß § 477 Abs. 2 StPO juristisch anspruchsvolle „hypothetische Ersatzprüfung“[22] bei durch eingriffsintensive Maßnahmen erlangten Informationen, ist dies im Ergebnis auch sachgerecht.

18 BT-Drucks. 17/5096, S. 22 f.

19 Vgl. Hilger in Erb et al. (Hrsg.), Löwe-Rosenberg StPO, 26. Auflage, Berlin 2010, § 481, Rn. 1 f.

20 Stellungnahme des Bundesrates, BT-Drucks. 17/5096, S. 33.

21 BT-Drucks. 17/5096, S. 38.

22 Vgl. hierzu BT-Drucks. 16/5486, S. 66; Singelnstein, ZStW 2008, S. 854, 880.

Problematisch ist jedoch die Formulierung „bei Zweifeln“. Eine Begriffsbestimmung findet sich weder im Gesetz noch in der Gesetzesbegründung. Zwar ist die Verwendung unbestimmter Rechtsbegriffe grundsätzlich unbedenklich, solange sich ihr konkreter Inhalt durch Auslegung der betreffenden Norm bestimmen lässt.[23] Verbleibende Ungewissheiten dürfen jedoch nicht so weit gehen, dass die Vorhersehbarkeit und Justiziabilität des Verwaltungshandelns gefährdet wird.[24] Auch wenn ein unbestimmter Rechtsbegriff grundsätzlich bestimmbar ist und damit das Gebot der Normenklarheit nicht per se verletzt, bleibt fraglich, ob sich die Norm in der Praxis als effektiv erweisen wird. Eine mögliche, letztlich freiwillige justizielle Prüfung wird aller Voraussicht nach seltener als vom Gesetzgeber intendiert genutzt werden. Wünschenswert wäre insoweit eine weitere Präzisierung der Entscheidungszuständigkeit im Gesetz.

4. Garantieerklärung bei Übermittlung in Drittstaaten

Nach § 14 Abs. 7 S. 8 BKAG-E, § 33 Abs. 3 S. 3 BPolG-E, § 34 Abs. 5 S. 5 ZfdG-E, § 11 Abs. 2 S. 6 ZollVG-E zählt ein „angemessenes Datenschutzniveau im Empfängerstaat“ zu den schutzwürdigen Interessen der betroffenen Person.

Ausweislich der Gesetzesbegründung stellt der Begriff jedoch kein abstraktes Kriterium dar, sondern soll fortan erst im Rahmen einer Einzelfallabwägung ermittelt und berücksichtigt werden.[25] Der Begriff eines angemessenen Datenschutzniveaus ist jedoch weitgehend unbestimmt.[26] Es fehlt ein entsprechender Bezugsrahmen, der eine praxistaugliche Anwendung ermöglichen könnte. Schließlich sieht der Entwurf vor, dass die schutzwürdigen Interessen – zu denen das angemessene Datenschutzniveau gehört – fortan auch dadurch gewahrt werden können, dass der Empfängerstaat „im Einzelfall einen angemessenen Datenschutz gegenüber der übermittelnden Stelle garantiert“ (vgl. § 14a Abs. 7 S. 8 BKAG-E). Angaben bezüglich Inhalt, Form und Ausgestaltung dieser Garantieerklärung finden sich jedoch

23 BVerfGE 31, 255, 264; BVerfGE 83, 130, 145 (st. Rspr).

24 Vgl. BVerfGE 21, 73, 79.

25 Vgl. zu § 14 BKAG-E, BT-Drucks. 17/5096, S. 24.

26 Vgl. hierzu unter Punkt IV. 4.

weder im Gesetz selbst noch in der Gesetzesbegründung.

IV. Gleichstellungsgebot und Datenschutz

Mit der Umsetzung des in Art. 3 Abs. 3 RbDatA normierten Gleichstellungsgebots (vgl. § 92 Abs. 1 S. 2 IRG-E, § 14a Abs. 1 S. 2, § 32a Abs. 1 S. 2 BPolG-E, § 34a Abs. 1 S. 2 ZFdG-E, § 11a Abs. 1 S. 2 ZollVG-E) dürften in Zukunft an eine Übermittlung in einen EU-Mitgliedstaat keine strengeren Anforderungen gestellt werden als bei einem rein nationalen Sachverhalt. Eine Ablehnung der Übermittlung mit dem Argument, im Empfängerstaat sei ein angemessenes Datenschutzniveau nicht gewährleistet, ist fortan nur noch für den Informationsaustausch mit Drittstaaten vorgesehen. Es wird damit für den gesamten Raum der Europäischen Union unterstellt, dass personenbezogene Daten angemessen und vergleichbar geschützt werden. Damit stellt sich die Frage, ob der Vereinfachung des Datenaustauschs auch ein ausreichender kompensatorischer Schutz bei der Verwendung der Daten gegenübersteht.

1. Datenschutz nach dem RbDatA

Der RbDatA selbst enthält über das in Art. 9 normierte Gebot der Vertraulichkeit der Informationen hinaus keine spezifischen Datenschutzregelungen. Art. 8 Abs. 2 RbDatA verweist insoweit lediglich auf das Übereinkommen des Europarates zum Schutz personenbezogener Daten[27] nebst Zusatzprotokollen über Kontrollstellen und grenzüberschreitenden Datenverkehr[28] und die Empfehlung des Europarates über die Nutzung personenbezogener Daten im Polizeibereich.[29] Das Datenschutz-Übereinkommen stammt aus dem Jahr 1981 und enthält Vorschriften über Datenqualität und Zweckbindung (Art. 5), über die Gewährleistung der Datensicherheit (Art. 7) sowie allgemeine Bestimmungen über die Rechte des Betroffenen (Art. 8).

27 Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten des Europarates vom 28.1.1981, SEV 108.

28 Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung vom 8.11.2011, SEV 181.

29 Recommendation No. R (87) 15 of the commitee of ministers to member states regulating the use of personal data in the police sector, 17.9.1987.

Die Regelungen sind jedoch insgesamt allgemeiner Natur und enthalten keine präzisen Bestimmungen, wie beispielsweise Löschungs- und Prüffristen. Kapitel V des Übereinkommens enthält Bestimmungen über die Errichtung eines beratenden Ausschusses. Dieser besitzt jedoch keine weitergehenden Kontrollbefugnisse. Das Zusatzprotokoll, das die Einrichtung nationaler Kontrollstellen vorsieht, wurde bis zum heutigen Zeitpunkt nicht von allen Mitgliedstaaten unterzeichnet bzw. ratifiziert.[30]

Aufgrund seiner sehr allgemeinen Formulierung stellt sich die Frage, ob das Datenschutzabkommen des Europarates aus dem Jahr 1981 geeignet ist, einen ausreichenden Datenschutz zu gewährleisten. Klärungsbedürftig ist, ob ausreichende Sicherungsmaßnahmen im Hinblick auf den hohen Stellenwert des Schutzes personenbezogener Daten (als nationales sowie als Unionsgrundrecht) bestehen.

2. Grundrechtsstatus des Schutzes personenbezogener Daten

Der Schutz personenbezogener Daten besitzt auch auf Ebene der europäischen Union Grundrechtsstatus. Gemäß Art. 8 Abs. 2 S. 1 der Grundrechtecharta (GRCh) darf die Verarbeitung nur nach Treu und Glauben erfolgen. Ferner schreibt Art. 8 Abs. 2 S. 2 GRCh einen Anspruch der betroffenen Person auf Auskunft sowie Berichtigung ihrer personenbezogenen Daten fest. Abs. 3 sieht die Überwachung dieser Vorschriften durch eine unabhängige Stelle vor. Mit dem Vertrag von Lissabon wurde Art. 16 AEUV eingeführt, der den früheren Art. 286 EG ersetzt und ergänzt. Dessen Abs. 1, der wörtlich mit Art. 8 GRCh übereinstimmt, enthält einen primärrechtlichen Individualanspruch auf Achtung des Datenschutzes, auch gegenüber und in den Mitgliedstaaten (Art. 51 Abs. 1 S. 1 GRCh), und umfasst alle Politikbereiche.[31] Abs. 2 enthält eine allgemeine Rechtssetzungsbefugnis der EU zum Erlass von Schutzvorschriften sowie die Anordnung, dass deren Einhaltung durch unabhängige Behörden überwacht wird. Weiterhin haben die Mitgliedstaaten nach Art. 6 Abs. 3 EUV auch Art. 8 EMRK zu beachten, der

30 Siehe zum Ratifikationsstand im August 2011: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=181&CM=1&DF=23/08/2011&CL=GER.

31 Zerdick, in: Lenz/Borchardt (Hrsg.) EU-Verträge, 5. Auflage, Köln 2010, Art. 16 AEUV, Rn. 7.

durch das Datenschutz-Übereinkommen des Europarates zum Schutz personenbezogener Daten (SEV 108) nebst Zusatzprotokollen über Kontrollstellen und grenzüberschreitenden Datenverkehr (SEV 181) ergänzt wird. Auf Sekundärrechtsebene konnte insbesondere durch die allgemeine Datenschutzrichtlinie der EG[32] (DSRL) über die Verarbeitung personenbezogener Daten im Rahmen der 1. Säule eine weitgehende Harmonisierung der nationalen Datenschutzbestimmungen erzielt werden.[33] Aufgrund des hohen Schutzniveaus der DSRL wird diese häufig als Maßstab zur Konkretisierung des EU-Grundrechts auf Datenschutz herangezogen.[34]

3. Datenschutzdefizit im Bereich der PJZS

Die Geltung der Allgemeinen Datenschutzrichtlinie, die im Bereich der 1. Säule einen weitgehend einheitlichen Datenschutzstandard sichert, ist gemäß Art. 3 Abs. 2 DSRL auf den Anwendungsbereich des Gemeinschaftsrechts beschränkt. Der Bereich der polizeilichen und justiziellen Zusammenarbeit war damit als Teil der ehemals 3. Säule von Anfang an nicht erfasst. Auch nach Auflösung des klassischen Säulenmodells und der „Vergemeinschaftung“ dieser Politikbereiche fallen diese nicht in den Geltungsbereich der Richtlinie.[35] Ein entsprechendes Gegenstück zur DSRL für die übrigen Politikbereiche existiert bislang nicht. Dadurch entsteht ein Datenschutzdefizit.

4. Fiktion eines vergleichbaren Datenschutzniveaus in den Mitgliedstaaten

Art. 8 Abs. 2 RbDatA bestimmt, dass bei der unmittelbaren Informationsübermittlung zwischen zwei Mitgliedstaaten die nationalen Datenschutzbestimmungen des Empfängerstaates Anwendung finden sollen. Es wird da-

32 Richtlinie 95/45 EG, Abl. L 281 vom 23.11.1995, S. 31-50.

33 EuGH, Rs. C-101/01, Bodil Lindquvist, Slg. 2003, I-1297, Rn. 96, 97; vgl. auch Gabel, in: Taeger/Gabel (Hrsg.), Kommentar zum BDSG, Frankfurt am Main 2010, § 4b, Rn. 21 f.

34 Holznagel/Werthmann in: Schulze/Zuleeg/Kadelbach (Hrsg.), Europarecht, 2. Auflage, Baden-Baden 2010, § 37, Rn. 10.

35 Sobotta, in: Grabitz/Hilf/Nettesheim (Hrsg.), Das Recht der Europäischen Union, München, 41. EL Juli 2010, Art. 16 AEUV, Rn. 27.

mit unterstellt, dass die Verarbeitung in allen Mitgliedstaaten soweit vergleichbar ist, dass stets ein angemessenes Datenschutzniveau gewährleistet wird. Dies ergibt sich in systematischer Hinsicht daraus, dass neben den neu eingeführten Bestimmungen zum Informationsaustausch innerhalb der Europäischen Union die alten Regelungen für die Übermittlung in Drittstaaten fortgelten.

Für den Übersenderstaat endet mit der Übermittlung nahezu jegliche Kontrollmöglichkeit über die Verwendung der Daten. Dies ist insbesondere deshalb problematisch, weil der Datenschutzstandard in den einzelnen Mitgliedstaaten im Bereich der PJZS mangels europäischer Vorgaben tatsächlich “höchst heterogen“ und keineswegs vergleichbar ist.[36] Auch die europäische Kommission selbst sieht Handlungsbedarf, wie sich aus dem im vergangenen Jahr vorgelegten Gesamtkonzept für Datenschutz in der Europäischen Union ersehen lässt; darin hat sie ebenfalls auf die Notwendigkeit einer Harmonisierung im Bereich der polizeilichen Zusammenarbeit, insbesondere auch in Bezug auf die innerstaatliche Datenverarbeitung, hingewiesen.[37]

36 Zöller, Der Austausch von Strafverfolgungsdaten zwischen Mitgliedsstaaten der Europäischen Union, ZIS 2011, S. 64, 68; vgl. Braum Europäischer Datenschutz und europäisches Strafrecht, KritV 2008, S. 82, 90; Holznagel/Werthmann in Schulze/Zuleeg/Kadelbach (Hrsg.), Europarecht, 2. Auflage, Baden-Baden 2010, § 37, Rn. 8.

37 Gesamtkonzept für den Datenschutz in der Europäischen Union, 4.11.2010, KOM (2010) 609, S. 15 f.

5. Zusammenfassende Bewertung und Lösungsansätze

Ein gleichwertiger Schutz personenbezogener Daten in den Mitgliedstaaten ist nicht hinreichend sicher gewährleistet. Gleichzeitig sieht der RbDatA einen nahezu ungehinderten Austausch von Informationen vor, welche dann nach den Datenschutzbestimmungen des Empfängerstaates verarbeitet werden. Dies führt zu einem weitgehenden Kontrollverlust des Übersenderstaates in Bezug auf den Verwendungsvorgang. Es stellt sich somit die Frage, wie dies auf europäischer und nationaler Ebene zu kompensieren ist.

a) Notwendigkeit eines europäischen Regelungswerks

Da ein entsprechender unionaler Rechtsakt im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen fehlt, besteht nach wie vor eine datenschutzrechtliche Regelungslücke. Ein Schutzniveau, das im Einklang mit dem deutschen sowie unionsrechtlichen Grundrecht auf informationelle Selbstbestimmung steht, ist nicht garantiert. Das Erfordernis eines unionsweit gültigen allgemeinen Rechtsaktes, der einen vergleichbaren Standard im Umgang mit personenbezogenen Daten schafft, ist im Ergebnis unbestritten.[38] So formuliert auch das „Stockholmer Programm“ die Einführung eines einheitlichen unionsrechtlichen Datenschutzes bis zum Jahr 2014 als Zielvorgabe der Union.[39] Die Kommission wies in ihren Mitteilungen über die Umsetzung des Stockholmer Programms sowie in dem hierzu ergangenen Aktionsplan darauf hin, dass es einer einheitlichen unionsrechtlichen Regelung zum Schutz personenbezogener Daten in allen Zuständigkeitsbereichen einschließlich der Bereiche der Strafverfolgung und Kriminalprävention bedarf.[40]

38 Braum, Europäischer Datenschutz und Europäisches Strafrecht, KritV 2008, 82 f.; Meyer, Der Grundsatz der Verfügbarkeit, NStZ 2008, S.188, 193; Zerdick in Lenz/Borchardt (Hrsg.) EU-Verträge, 5. Auflage, Köln 2010, Art. 16 AEUV, Rn. 6; Zöller, Der Austausch von Strafverfolgungsdaten zwischen den Mitgliedsstaaten der Europäischen Union, ZIS 2011 S. 64, 67 f.

39 Rat der Europäischen Union, Vermerk Betr.: das Stockholmer Programm – Ein offenes und sicheres Europa im Dienste und zum Schutz der Bürger, 17024/09 vom 2.12.2009, S. 18 f., 37 f.

40 Mitteilung der Kommission, Ein Raum der Freiheit der Sicherheit und des Rechts im Dienste der Bürger KOM (2009) 262 endg. vom 10.6.2009 S. 33; Mitteilung der Kommission Aktionsplan zur Umsetzung des Stockholmer Programms KOM (2010) 171 endg. vom 20.4.2010. S. 3.

Mit Einführung von Art. 16 AEUV (als Ermächtigungsgrundlage zum Erlass von Rechtsakten im Bereich des Datenschutzes) besitzt die Union zwar die Kompetenz zum Erlass eines umfassenden Regelungswerkes. Es ist jedoch bislang nicht ersichtlich, wann sie hiervon Gebrauch macht.

b) Erfordernis eines Bezugsrahmens auf nationaler Ebene

Da einheitliche europäische Datenschutzvorschriften fehlen, birgt jede Übersendung die Gefahr eines Grundrechtsverstoßes. Der Gesetzgeber ist gemäß Art. 6 Abs. 2 EUV zur Beachtung der Unionsgrundrechte sowie gemäß Art. 20 Abs. 3 GG der nationalen Grundrechte verpflichtet. Insoweit definieren die Grundrechte Reichweite und Grenzen der Umsetzungspflicht.[41] Da einer Übersendung von Daten keine ihre Verwendung verbindlich begrenzenden Unionsrechtsakte gegenüberstehen, ist die Schaffung eines Bezugsrahmens auf nationaler Ebene erforderlich.

Es obliegt damit dem deutschen Gesetzgeber, den Datenschutzstandard jedenfalls dahingehend zu konkretisieren, welche Mindestanforderungen der Empfängerstaat bei der Verarbeitung erfüllen muss. Dies ist bislang nicht geschehen. Zwar hat das Umsetzungsgesetz vermeintlich nur die Übermittlung der Daten zum Gegenstand, d.h. es regelt den Vorgang vom Ersuchen bis zur Ablehnung oder Übermittlung der Daten; die Frage der Verwendung der Daten könnte davon gedanklich getrennt werden. Jedoch sind die Begriffe der Übermittlung und der Verwendung durch die drohende Grundrechtsverletzung untrennbar miteinander verknüpft. Es ist mithin erforderlich, einen Mindeststandard festzulegen, dessen Einhaltung die Übermittlung bedingt.

c) Mindestschutz nach dem Rahmenbeschluss 2008/977/JI

Es existiert ein Rahmenbeschluss (2008/977/JI) des Rates zum Schutz personenbezogener Daten, die im Rahmen der PJZS verarbeitet werden

41 So auch Böse, Grundsatz der Verfügbarkeit von Informationen in der strafrechtlichen Zusammenarbeit der Europäischen Union, Göttingen 2007, S. 54. Böse bezeichnet die Grundrechte in diesem Zusammenhang als „Informationshilfegegenrechte."

(Datenschutzrahmenbeschluss).[42] Mit seinen Mindestanforderungen für die Verwendung der übermittelten Daten stellt er das Gegenstück zum RbDatA dar.[43] So sieht der Datenschutzrahmenbeschluss im Hinblick auf die Datenqualität die Beifügung von Hintergrundinformationen vor, um eine Überprüfung durch den Empfängermitgliedstaat zu ermöglichen (Art. 8). Auch enthält er Regelungen über die Vertraulichkeit und bezüglich der technischen Anforderungen an die Sicherheit der Verarbeitung (Art. 22). Jede Übermittlung ist nach Art. 10 zum Zweck der Überprüfung ihrer Rechtmäßigkeit zu protokollieren oder zu dokumentieren. Ferner enthält Art. 4 detaillierte Regelungen über Berichtigung, Löschung und Sperrung von Daten. Zudem kann die übermittelnde Behörde gemäß Art. 9 entsprechende Fristen angeben. Die betroffene Person ist grundsätzlich über die Übermittlung zu unterrichten (Art. 16). Ihr steht zudem nach Art. 17 ein Auskunftsrecht zu. Gemäß Art. 18 besteht ein Anspruch auf Berichtigung und Löschung; im Falle von dessen Ablehnung ist die Möglichkeit der Einlegung von Rechtsmitteln eröffnet. Art. 19 normiert das Recht auf Schadenersatz. Art. 20 sichert dem Betroffenen die Gewährung von Rechtsschutz zu, Art. 25 sieht die Errichtung unabhängiger Kontrollstellen mit Untersuchungs- und Einwirkungsbefugnissen vor. Schließlich ist eine Weiterleitung von Daten an Drittstaaten grundsätzlich nur mit Zustimmung des übersendenden Mitgliedstaates zulässig (Art. 13 Abs. 1 lit. c).

Allerdings ist der Anwendungsbereich des Rahmenbeschlusses auf den zwischenstaatlichen Bereich beschränkt. Auf die innerstaatliche Informationsverarbeitung ist er nicht anwendbar. Dennoch beinhaltet er eine Reihe von Kontrollmechanismen sowohl für den Übersenderstaat (durch Protokollierungs-, Übermittlungs- und Löschungsfristen) als auch für den Betroffenen (durch die Gewährleistung von Informationsrechten, Rechtsschutz und Schadenersatz). Zwar bleibt auch der Rahmenbeschluss deutlich hinter den Bestimmungen der DSRL zurück und sichert lediglich einen Mindeststandard.[44] Trotz berechtigter Kritik an Umfang und Reichweite des Datenschutzrahmenbeschlusses[45] bleibt aber festzuhalten, dass dieser der der-

42 Rahmenbeschluss 2008/977/JI, Abl. L 350 vom 30.12.2008, S. 60-71.

43 Vgl. Erwägungsgründe 4 und 5 des Rahmenbeschlusses.

44 Zerdick, in: Lenz/Borchardt (Hrsg.), EU-Verträge, 5. Auflage, Köln 2010, Art. 16 AEUV, Rn. 50.

45 Zur Kritik vgl: Eisele in Sieber/Brüner/Satger/Heintschell-Heinegg (Hrsg.), Europäisches Strafrecht, Baden-Baden 2011, § 50 Rn.14; Europäische Kommission,

zeit einzige unionsrechtliche Rechtsakt ist, der für den relevanten Bereich verbindliche Mindestanforderungen festschreibt. Jedenfalls für den zwischenstaatlichen Informationsaustausch trägt dieser im Vergleich zum Europaratsabkommen zu einer deutlichen Verbesserung des Schutzes personenbezogener Daten bei. Insgesamt stellt der Rahmenbeschluss damit einen „wichtigen Schritt“ bei der Schaffung eines datenschutzrechtlichen Ausgleichs dar.[46]

Obwohl die Umsetzungsfrist am 27. November 2010 abgelaufen ist, ergab eine Anfrage beim Generalsekretariat des Rates, dass bisher lediglich zwei Mitgliedstaaten (Dänemark und Schweden) nationale Kontrollstellen im Sinne von Art. 25 benannt haben.[47] Die Schweiz hat – soweit ersichtlich – als bisher einziges Land den Rahmenbeschluss in nationales Recht umgesetzt.[48] Eine Evaluierung der Europäischen Kommission über die Umsetzung des Rahmenbeschlusses erfolgt bis zum 27. November 2011. Die Bundesrepublik Deutschland hat bislang kein nationales Umsetzungsgesetz erlassen. Nach Auskunft des Bundesjustizministeriums befindet sich aktuell ein erster Diskussionsentwurf in der Ressortabstimmung.

Gesamtkonzept für den Datenschutz in der Europäischen Union, 4.11.2010, KOM (2010) 609, S. 15.

46 So auch Satzger, Europäisches und Internationales Strafrecht, 4. Auflage, Baden-Baden 2010, § 10, Rn. 50.

47 Rat der Europäischen Union, Vermerk betr. Rahmenbeschluss 2008/977/JI, 7299/11 vom 7.3.2011; ders. 8361/11 vom 29.3.2011.

48 Bundesgesetz über die Umsetzung des Rahmenbeschlusses 2008/977/JI über den Schutz von Personendaten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen vom 19.März 2010, SR 142.20, AS S. 3387.

d) Handlungsmöglichkeiten des Gesetzgebers

Zu untersuchen sind die Möglichkeiten des Gesetzgebers, Verstöße gegen nationale bzw. unionsrechtliche Grundrechte zu vermeiden.

(1) Aussetzung des Gesetzgebungsverfahrens

Die Aussetzung des Gesetzgebungsverfahrens bis zum Zeitpunkt, in dem ein unionsrechtlicher Rechtsrahmen geschaffen wurde, der ein ausreichendes Schutzniveau sicherzustellen vermag, ist abzulehnen. Die Mitgliedstaaten sind zur Umsetzung des Rahmenbeschlusses verpflichtet.

(2) Anknüpfung an den ordre public-Vorbehalt in Art. 1 Abs. 7 RbDatA

Naheliegend ist eine Anknüpfung an den ordre public-Vorbehalt in Art. 1 Abs. 7 RbDatA. Dieser wurde als zwingender Ablehnungsgrund für die Übermittlung in den Gesetzentwurf aufgenommen (vgl. § 27 Abs. 2 Nr. 2 BKAG-E, § 33a Nr. 2 BPolG-E, § 35 Abs. 2 Nr. 2 ZFdG-E, § 11 a Abs. 4 Nr. 2 ZollVG-E). Danach hat eine Übermittlung zu unterbleiben, wenn diese einen Verstoß gegen Art. 6 EUV und damit gegen Unionsgrundrechte darstellen würde. Dies schließt das Grundrecht auf informationelle Selbstbestimmung mit ein, so dass grundsätzlich auch nach der derzeitigen Rechtslage eine Ablehnung mit Berufung auf den ordre public-Vorbehalt möglich wäre. Indes würde dies bedeuten, dass jeder Übermittlung eine Analyse des Datenschutzniveaus des Empfängerstaates vorzuschalten wäre. Dies ist angesichts der Komplexität der Regelungsmaterie praktisch nicht umsetzbar und widerspräche zudem der Intention des Rahmenbeschlusses.

Denkbar wäre aber (am Beispiel von § 27 Abs. 2 Nr. 2 BKAG-E) folgende Formulierung:

> „Die Übermittlung nach § 14 a Abs. 1 und 3 unterbleibt auch dann, wenn
>
> (….)
>
> Nr. 2 „die Übermittlung der Daten zu den in Art. 6 des Vertrages über die Europäische Union enthaltenen Grundsätzen im Widerspruch stünde, insbesondere, wenn ein entsprechender Mindestschutz bei der Verwendung der personenbezogenen Daten im Sinne des Rahmenbeschlusses 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der po-

> lizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350 vom 30.12.2008, S. 60), nicht gewährleistet ist."

Mit dem Rahmenbeschluss als Anknüpfungspunkt würde – im Gegensatz zum Begriff des angemessenen Datenschutzniveaus – auf einen konkreten Mindestschutz Bezug genommen.[49] Dieser Standard wäre einer wirksamen Kontrolle zugänglich. Auch wäre eine Übermittlung selbst dann nicht ausgeschlossen, wenn der ersuchende Mitgliedstaat den Rahmenbeschluss (noch) nicht umgesetzt hätte. In diesem Fall erfolgte eine Prüfung, ob ein entsprechender Mindestschutz, wie er in diesem Rechtsakt vorgesehen ist, auf andere Weise gewährleistet werden könnte, wobei der Rahmenbeschluss den Bezugsrahmen stellen würde.

(3) Berücksichtigung des Rahmenbeschlusses 2008/977/JI bei der Auslegung des ordre public-Vorbehalts

Des Weiteren kommt in Betracht, den Wortlaut der oben genannten Bestimmungen unverändert zu übernehmen, allerdings die Mindestanforderungen im Hinblick auf die Verwendung der personenbezogenen Daten im Empfängerstaat im Rahmen der ordre public-Klausel zu prüfen. In diesem Fall böte es sich jedoch an, eine entsprechende Passage in die Gesetzesbegründung einzufügen, die zur Auslegung und Anwendung herangezogen werden könnte.

(4) Bewertung der Ansätze

Entscheidend ist insbesondere die Schaffung ausreichender Transparenz. Eine Konkretisierung von Mindeststandards ist deshalb von besonderer Bedeutung. Ein bloßer Verweis auf die Achtung der Grundrechte vermag einen effektiven Grundrechtsschutz nicht zu gewährleisten. Vorzugswürdig ist der weiter konkretisierende Verweis auf den Rahmenbeschluss 2008/977/JI als Mindeststandard.

Auch wenn der Rahmenbeschluss kein optimales Schutzniveau gewährleistet, so stellt er doch einen praktisch handhabbaren Mindestschutz bei der Datenverarbeitung dar. Durch die Umsetzung in den Mitgliedstaaten wäre auch eine Sicherung der von der Bundesrepublik in einen EU-Mitgliedstaat übermittelten Informationen möglich. Zumindest muss die Beachtung der im

49 Bei dieser „Außenverweisung" müssen die Normgeber nicht identisch sein, vgl. Bundesministerium der Justiz (Hrsg.), Handbuch der Rechtsförmlichkeit, 3. Auflage 2008, Rn. 235.

Rahmenbeschluss postulierten Anforderungen für eine Übermittlung der Daten vorausgesetzt werden können.

Zwar erklärt der RbDatA explizit, dass hinsichtlich der Verwendung der Daten die nationalen Datenschutzbestimmungen des Empfängerstaates anwendbar sein sollen; dies schließt jedoch nicht aus, dass die Übermittlung als solche an Voraussetzungen geknüpft wird.

V. Resümee

Die Umsetzung des RbDatA vermag einen wichtigen Schritt hin zu einem Raum der Freiheit, der Sicherheit und des Rechts (Art. 67 Abs. 1 AEUV) zu gehen. Dieser Raum soll aber nicht nur offen für einen erleichterten Datenaustausch zwischen Strafverfolgungsbehörden, sondern auch mit einem angemessen hohen Datenschutzniveau ausgestaltet sein.

Durchaus konsequent wird die Normierung des Gleichstellungsgebots umgesetzt, nach dem bei einer Informationsübermittlung in einen EU- bzw. Schengen-assoziierten Staat keine strengeren Voraussetzungen gelten dürfen als bei einer Übersendung an eine innerstaatliche Strafverfolgungsbehörde. Ein weiteres Kernstück der Vereinfachung, die Beschleunigung des Informationsaustauschs, wurde jedoch bislang nicht in den Gesetzentwurf aufgenommen. Fristenregelungen fehlen bislang vollständig und sollen auch nach Vornahme der erforderlichen technischen Anpassungen allenfalls in die RiVASt aufgenommen werden.[50]

Der Begriff der zuständigen Strafverfolgungsbehörde ist zwar ebenso hinreichend bestimmt wie der Begriff der Zwangsmaßnahme. Wünschenswert wäre jedoch eine Konkretisierung des Begriffs des „Zweifels“ für das Eingreifen der Entscheidungskompetenz der Staatsanwaltschaft. Die Komplexität der juristischen Prüfungen im Rahmen der §§ 478 und 481 StPO und die erschwerte Möglichkeit der Erlangung nachträglichen Rechtsschutzes im Empfängerstaat, erfordern eine justizielle Vorabprüfung der Zulässigkeit der Übermittlung. Hierzu ist es jedoch unumgänglich, dass die Entscheidungskompetenzen präzise und transparent ausgestaltet sind.

50 Vgl. BT-Drucks. 17/5096, S. 14, 16.

Ein umfassender Schutz personenbezogener Daten im Sinne der unionsrechtlichen sowie nationalen Grundrechte ist nicht ausreichend gewährleistet, da ein entsprechender unionaler Rechtsakt fehlt und die Datenschutzvorschriften in den Mitgliedstaaten voneinander abweichen. Das einzige existierende verbindliche Regelungswerk in diesem Bereich stellt das sehr allgemein formulierte Europaratsabkommen aus dem Jahr 1981 dar. Die fragmentarischen Bestimmungen legen lediglich allgemeine Grundsätze für den Datenschutz fest, können eine umfassende Kontrolle jedoch nicht gewährleisten.

Zu empfehlen ist daher eine Bezugnahme auf den Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 zum Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden. Zwar weist auch der Rahmenbeschluss 2008/977/JI Schwächen auf und kann, wegen fehlender Anwendbarkeit auf die innerstaatliche Datenverarbeitung, nicht als umfassendes Regelwerk bezeichnet werden. Er ist jedoch geeignet, einen einheitlichen Mindestschutz für personenbezogene Daten zu gewährleisten. Wesentliche Kontrollmechanismen, wie beispielsweise Informations- und Auskunftspflichten, sind darin vorgesehen. Aus diesem Grund ist zum einen eine Umsetzung dieses Rahmenbeschlusses in deutsches Recht notwendig, um die Einhaltung dieser unerlässlichen Sicherungsmechanismen auch innerstaatlich zu gewährleisten. Zum anderen sollten die Mindestanforderungen des Rahmenbeschlusses durch den ordre public-Vorbehalt des RbDatA als Bezugsrahmen für die Bestimmung des Datenschutzniveaus herangezogen werden.

Berlin, den 14. September 2011