Professor Dr. Matthias Bäcker, LL.M.
Universität Mannheim, Abt. Rechtswissenschaft
D 7, 27
68159 Mannheim

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)585 B

Stellungnahme

zur öffentlichen Anhörung des Innenausschusses des Deutschen Bundestages
am 22. Oktober 2012, 14.00 Uhr

über

den Entwurf einer EU-Richtlinie über die Datenverarbeitung bei Polizei und Strafjustiz
vom 25. Januar 2012 [KOM(2012) 10 endg.]

Gliederung

Thesen

Im Folgenden fasse ich die wesentlichen Ergebnisse meiner Stellungnahme vorab thesenartig zusammen:

1. Die EU hat nach Art. 16 Abs. 2 AEUV die Kompetenz, den Datenschutz bei Polizei und Strafjustiz auch für rein innerstaatliche Sachverhalte ohne grenzüberschreitenden Bezug zu regeln.

2. Allerdings muss hinsichtlich des zulässigen Harmonisierungsniveaus differenziert werden:

    a. Die EU darf auch für Polizei und Strafjustiz umfassende und abschließende Regelungen über Kernfragen des Datenschutzrechts wie die Rechte des Betroffenen einer Datenverarbeitung, die Datenschutzaufsicht, die Datensicherheit, die datenschutzrechtliche Verantwortlichkeit, prozedurale Vorkehrungen zur Gewährleistung von Datenschutz und Datensicherheit, die Folgen von Datenschutzverstößen sowie Datenübermittlungen in Drittstaaten schaffen.

    b. Hingegen darf die EU grundsätzlich nur Mindestvorgaben für die materiellen Voraussetzungen von Datenverarbeitungen der mitgliedstaatlichen Kriminalbehörden errichten. Im Übrigen bleibt das Eingriffsrecht der Kriminalbehörden Sache der Mitgliedstaaten, sofern nicht andere Kompetenztitel als Art. 16 Abs. 2 AEUV der EU eine Regelungsbefugnis zuweisen.

3. Der Richtlinienentwurf wahrt diese Grenzen der Rechtsetzungskompetenz der EU. Insbesondere enthält er lediglich Mindestanforderungen für Datenverarbeitungsermächtigungen und gibt die mitgliedstaatlichen Befugnisregelungen nicht umfassend und abschließend vor.

4. Die Regelungen über Datenübermittlungen in Drittstaaten und an internationale Organisationen sind der größte Schwachpunkt des Entwurfs. In ihrer gegenwärtigen Fassung täuschen sie lediglich vor, solche Datenübermittlungen zu regulieren, setzen ihnen aber letztlich kaum Grenzen. Diese Regelungen sind damit regelungstechnisch misslungen und rechtsstaatlich unerträglich.

Ich beschränke meine Stellungnahme auf Aspekte des Richtlinienentwurfs (im Folgenden: RL-E), die nach meiner Einschätzung für eine parlamentarische Beratung in einem Mitgliedstaat der EU besonders bedeutsam sind. Ich befasse mich daher zunächst näher mit der Frage, ob die EU die Kompetenz hat, ein Regelungswerk über den Datenschutz bei Polizei und Strafjustiz zu erlassen, wenn die beabsichtigten Regelungen auch auf rein innerstaatliche Sachverhalte ohne grenzüberschreitenden Bezug anwendbar sein sollen (unten I). Danach behandle ich noch wenige ausgewählte Einzelfragen, welche der Entwurf aufwirft (unten II).

Es würde hingegen den Rahmen dieser Stellungnahme sprengen, die vorgeschlagenen Regelungen im Einzelnen durchzugehen und zu bewerten. In vielen Punkten stimmt der Entwurf ohnehin weitgehend mit dem Entwurf einer Datenschutz-Grundverordnung (im Folgenden: VO-E) überein, der Gegenstand einer gesonderten Anhörung ist. Im Einzelnen ergeben sich allerdings durchaus bedeutsame Unterschiede, die insbesondere das Schutzniveau zum Teil absenken. Insoweit verweise ich auf die Stellungnahme von Gerrit Hornung, in der einige dieser Unterschiede näher herausgearbeitet und bewertet werden.

I. Regelungsbefugnis der EU

Die EU ist befugt, die geplante Richtlinie zu erlassen. Der Entwurf stützt sich zutreffend auf den Kompetenztitel des Art. 16 Abs. 2 AEUV. Allerdings muss diese Ermächtigung teils restriktiv ausgelegt werden, um zu vermeiden, dass die EU das Eingriffsrecht der Kriminalbehörden[1] weitgehend an sich zieht. Auf der Grundlage dieser restriktiven Interpretation des Kompetenztitels bestehen auch unter den Gesichtspunkten der Subsidiarität und der (kompetenzrechtlichen) Verhältnismäßigkeit keine Bedenken gegen eine unionsweite Regelung des Datenschutzes bei Polizei und Strafjustiz, die sich auch auf rein innerstaatliche Sachverhalte erstreckt.

1. Rechtsetzungskompetenz

Die Rechtsetzungskompetenz der EU aus Art. 16 Abs. 2 AEUV erstreckt sich auf Datenschutzvorschriften für die Verhütung und Verfolgung von Straftaten sowie für die Strafvollstreckung. Dies gilt selbst dann, wenn diese Vorschriften auch rein innerstaatliche Sachverhalte ohne grenzüberschreitenden Bezug regulieren. Allerdings ermächtigt Art. 16 Abs. 2 AEUV die EU nicht dazu, das Eingriffsrecht der Kriminalbehörden umfassend zu harmonisieren. Insbesondere dürfen die materiellen Vorgaben für Datenverarbeitungen solcher Behörden lediglich als Mindestanforderungen, nicht aber als abschließende und umfassende Eingriffsermächtigungen konzipiert werden.

a) Regelung rein innerstaatlicher Sachverhalte

Dass Art. 16 Abs. 2 AEUV die EU überhaupt ermächtigt, Datenschutzvorschriften für die Verhütung und Verfolgung von Straftaten zu schaffen, steht außer Frage. Erörterungsbedürftig ist jedoch, ob diese Vorschriften sich auch auf rein innerstaatliche Sachverhalte ohne grenzüberschreitenden Bezug erstrecken dürfen, wie dies der Richtlinienentwurf vorsieht.

[1] Dieser Begriff bezeichnet hier die Behörden, deren gesetzliche Aufgabe darin besteht, Straftaten zu verhindern oder auf Straftaten zu reagieren; er umfasst damit Polizeibehörden und Staatsanwaltschaften. Das Recht der Kriminalbehörden steht im Vordergrund dieser Stellungnahme. Der Entwurf reguliert allerdings auch die Tätigkeit von Strafgerichten und Strafvollzugsbehörden. Die hier herausgearbeiteten Probleme und Lösungsvorschläge lassen sich darauf weitgehend übertragen.

Denn Art. 16 Abs. 2 AEUV trägt Datenschutzvorschriften für die Mitgliedstaaten nur, wenn diese Vorschriften den freien Datenverkehr zum Gegenstand haben oder soweit die Mitgliedstaaten Tätigkeiten ausüben, die in den Anwendungsbereich des Unionsrechts fallen.

Der Begriff des freien Datenverkehrs beschreibt primär Regelungen mit einem grenzüberschreitenden Bezug; insoweit konkretisiert Art. 16 Abs. 2 AEUV die allgemeine Binnenmarktkompetenz des Art. 114 AEUV.[2]

Der Anwendungsbereich des Unionsrechts im Sinne von Art. 16 Abs. 2 AEUV kann weiter nur mit Blick auf die sonstigen Sachkompetenzen der EU bestimmt werden.[3] Danach fällt zwar die polizeiliche und justizielle Zusammenarbeit in Strafsachen in den Anwendungsbereich des Unionsrechts. Die EU hat jedoch keine Kompetenz, das innerstaatliche Verfahrensrecht der Kriminalbehörden umfassend zu harmonisieren. Ihre Rechtsetzungsbefugnisse haben vielmehr in erster Linie Regelungen über grenzüberschreitende Sachverhalte zum Gegenstand und dienen auch im Übrigen dazu, grenzüberschreitende Sachverhalte durch Harmonisierung innerstaatlicher Normen zu bewältigen (vgl. insbesondere Art. 82 Abs. 1 und Abs. 2, Art. 85, Art. 87 Abs. 1 und Abs. 2 AEUV).

Auf den ersten Blick scheint darum der Kompetenztitel des Art. 16 Abs. 2 AEUV für die Verhütung und Verfolgung von Straftaten im Wesentlichen nur solche Datenschutzregelungen abzudecken, die einen grenzüberschreitenden Sachverhalt voraussetzen. Vorbild könnte insoweit der derzeit geltende Rahmenbeschluss[4] (im Folgenden: RB) sein. Er ist nach Art. 1 Abs. 2 RB nur anwendbar, wenn personenbezogene Daten zwischen Mitgliedstaaten oder zwischen einem Mitgliedstaat und einer Einrichtung der EU ausgetauscht werden. Dementsprechend haben sowohl der Bundesrat[5] als auch der schwedische Reichstag[6] gegenüber der EU-Kommission gerügt, für die vorgeschlagene Richtlinie fehle eine kompetenzielle Grundlage, soweit sie auch rein innerstaatliche Datenverarbeitungen zum Gegenstand habe.[7]

Eine solche restriktive Auslegung von Art. 16 Abs. 2 AEUV verfehlt jedoch den Gegenstand des Kompetenztitels und trägt den Belangen der Einzelnen, die durch die erlassenen Regelungen geschützt werden sollen, nicht hinreichend Rechnung.

Es ist ein Hauptanliegen des Datenschutzrechts, den Umgang mit personenbezogenen Daten als komplexen Prozess rechtlich zu strukturieren.[8] Erst aufgrund einer solchen Strukturierung kann der Betroffene einzelne Datenverarbeitungsschritte in den Gesamtprozess einordnen und so beurteilen, ob und wie sie sich für ihn auswirken können. Datenschutzrechtliche Regelungswerke, die lediglich punktuell bestimmte Ausschnitte einer längeren Kette von Daten-

---

[2] *Kingreen,* in: Calliess/Ruffert, EUV/AEUV, 4. Aufl. 2011, Art. 16 AEUV Rn. 7; *Sobotta,* in: Grabitz/Hilf/Nettesheim, Das Recht der EU, Stand 2010, Art. 16 AEUV Rn. 32.

[3] So implizit wohl auch *Kingreen,* in: Calliess/Ruffert, EUV/AEUV, 4. Aufl. 2011, Art. 16 AEUV Rn. 5.

[4] Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. L 350 vom 30. Dezember 2008, S. 60.

[5] BR-Drs. 51/12.

[6] Stellungnahme 2011/12:JuU31, englischsprachige Übersetzung abrufbar unter http://www.ipex.eu/IPEXL-WEB/dossier/files/download/082dbcc535f09fa601366293d59e4985.do.

[7] Kritisch auch *Rogall-Grothe,* ZRP 2012, S. 193 f.

[8] Grundlegend und eingehend *Albers,* Informationelle Selbstbestimmung, 2005; *dies.,* in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 2, 2008, § 22.

verarbeitungen erfassen, können diese Strukturierungsleistung nicht erbringen. Die naheliegende Folge sind Inkonsistenzen bis hin zu Wertungswidersprüchen sowie empfindliche Schutzlücken.

Wenn insbesondere ein europäisches Regelungswerk für den Datenschutz bei der Verhütung und Verfolgung von Straftaten nur grenzüberschreitende Sachverhalte erfasst, bleibt der Datenschutz im Übrigen in der Hand der Mitgliedstaaten. Die Mitgliedstaaten können darum frei etwa darüber entscheiden, welche Rechte der Betroffene hat, wer für bestimmte Verarbeitungsschritte verantwortlich ist oder wie die Datenschutzaufsicht ausgestaltet wird. Dadurch kann es dazu kommen, dass grenzüberschreitende und innerstaatliche Datenverarbeitungen in ganz unterschiedliche prozedurale und institutionelle Sicherungsregime eingebettet sind.

Jedoch können weder der Betroffene noch die mitgliedstaatlichen Kriminalbehörden im Voraus zuverlässig beurteilen, ob bestimmte personenbezogene Daten später einmal an Behörden eines anderen Mitgliedstaats oder an eine Einrichtung der EU übermittelt werden. Der Betroffene kann vielfach auch nicht einschätzen, ob es zu einer solchen Übermittlung bereits gekommen ist. Zudem werden selbst in kriminalbehördlichen Verfahren mit grenzüberschreitendem Bezug in der Regel bestimmte Daten nur innerstaatlich verarbeitet.

In der Folge droht aus Sicht des Betroffenen schlimmstenfalls ein Chaos von Rechtsregimen und zuständigen Stellen, in dem seine Datenschutzrechte untergehen. Aus behördlicher Sicht entstehen zumindest in vielen Fällen Rechtsunsicherheit und Wertungsinkonsistenzen. So stellt sich die Frage, wie mit Daten umzugehen ist, deren Übermittlung ins europäische Ausland konkret möglich erscheint, aber noch nicht sicher abzusehen ist. Zudem kann ein funktional einheitlicher behördlicher Datenbestand (etwa eine elektronische Verfahrensakte) teilweise dem europäisierten und teilweise dem rein mitgliedstaatlichen Datenschutzrecht unterfallen. Bei unterschiedlichen Schutzniveaus beider Regime[9] kann dies zu erheblichen Effizienzverlusten führen.

Angesichts dieser Folgeprobleme eines punktuell angelegten datenschutzrechtlichen Regelungswerks ist es angezeigt, den Kompetenztitel des Art. 16 Abs. 2 AEUV weiter zu interpretieren. Mitgliedstaatliche Datenverarbeitungen fallen bereits dann in den Anwendungsbereich des Unionsrechts und können reguliert werden, wenn die betroffene Sachmaterie überhaupt vom primären und sekundären Unionsrecht erfasst wird. Dies ist für die polizeiliche und justizielle Zusammenarbeit in Strafsachen der Fall. In der Folge darf die EU den Datenschutz bei Polizei und Strafjustiz auch für rein innerstaatliche Sachverhalte regeln, bei denen ein grenzüberschreitender Bezug zumindest noch nicht abzusehen ist.

Für die hier vertretene weite Auslegung von Art. 16 Abs. 2 AEUV spricht auch die Rechtsprechung des EuGH zu der geltenden Datenschutz-Richtlinie[10] (im Folgenden: DSRL). Diese Richtlinie stützte sich mangels besonderen Kompetenztitels lediglich auf die Binnenmarkt-

[9] Kritisch zum Schutzniveau des geltenden Rahmenbeschlusses etwa *Eisele*, in: Sieber u.a. (Hrsg.), Europäisches Strafrecht, 2011, § 50 Rn. 14: „Einigung auf dem kleinsten gemeinsamen Nenner".

[10] Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. L 281 vom 23. November 1995, S. 31, geändert durch Verordnung (EG) Nr. 1882/2003 des Europäischen Parlaments und des Rates vom 29. September 2003, ABl. 284 vom 31. Oktober 2003, S. 1.

kompetenz des damaligen Art. 100a EGV. Gleichwohl hat der EuGH bereits im Jahr 2003 in seinem ORF-Urteil ausgeführt, der Anwendungsbereich der Richtlinie erstrecke sich auch auf Datenverarbeitungen durch hoheitliche Stellen ohne grenzüberschreitenden Bezug; dies sei auch kompetenzrechtlich zulässig. Denn alle personenbezogenen Daten könnten zwischen den Mitgliedstaaten übermittelt werden. Eine Abgrenzung des Anwendungsbereichs der Richtlinie anhand eines grenzüberschreitenden Bezugs wäre ungewiss und hinge von Zufälligkeiten ab. Dies würde dem Hauptzweck der Richtlinie zuwiderlaufen, Binnenmarkthindernisse zu beseitigen, die sich aus unterschiedlichen Datenschutzregimes in den Mitgliedstaaten ergäben.[11] Es liegt fern, den Kompetenztitel des Art. 16 Abs. 2 AEUV, der den Befugniskreis der EU gegenüber der Binnenmarktkompetenz gerade erweitern soll, hinsichtlich des zulässsigen Anwendungsbereichs der erlassenen Regelungen restriktiver auszulegen.[12]

b) Keine Vollharmonisierung des Eingriffsrechts der Kriminalbehörden

Allerdings darf die Rechtsetzungskompetenz der EU inhaltlich nicht überdehnt werden. Darin liegt der zutreffende Kern der Bedenken, die gegen eine Regelungsbefugnis der EU für rein innerstaatliche Datenverarbeitungen vorgebracht werden.

Eine Überdehnung liegt bei dem Kompetenztitel des Art. 16 Abs. 2 AEUV nahe und hätte gewichtige Folgen. Denn der Datenschutz als Querschnittsmaterie erfasst praktisch alle behördlichen Tätigkeiten. Zudem hat annähernd jedes behördliche Handeln eine informationelle Komponente[13] und kann darum zumindest auch als Teil einer Kette von Datenverarbeitungen begriffen werden. Wäre die Regelungsbefugnis der EU so zu verstehen, dass jedes behördliche Handeln mit einem Datenverarbeitungsanteil im Anwendungsbereich des Unionsrechts umfassend sekundärrechtlich reguliert werden darf, so würde Art. 16 Abs. 2 AEUV gewissermaßen zum Kompetenzstaubsauger, der das Prinzip der begrenzten Einzelermächtigung (Art. 5 Abs. 1 Satz 1, Abs. 2 EUV) weitgehend unterliefe.[14]

Diese Entgrenzungsgefahr zeigt sich gerade auf dem hoheitlichen Tätigkeitsfeld, das Gegenstand des Entwurfs ist. Insbesondere das Strafverfahren hat in allen Verfahrensabschnitten primär das Ziel, Informationen über ein bestimmtes Geschehen zu gewinnen, damit dieses Geschehen schließlich strafrechtlich bewertet werden kann. Hierzu werden laufend personenbezogene Daten erhoben, in strukturierter Form gesammelt, ausgewertet und miteinander verknüpft. Auf manchen Kriminalitätsfeldern gilt für das präventivpolizeiliche Handeln zur Verhütung von Straftaten Ähnliches.[15] Auf der Grundlage einer weiten Interpretation von Art. 16 Abs. 2 AEUV dürfte die EU den Mitgliedstaaten folglich weite Teile des nationalen Strafprozess- und Polizeirechts vorgeben. So dürfte das Sekundärrecht regeln, welche technischen oder sozialen Ermittlungsmethoden die Kriminalbehörden unter welchen Voraussetzungen

---

[11] EuGH, Urteil vom 20. Mai 2003, Rs. 465/00 u.a., Slg. 2003, S. I-5014 - ORF, Tz. 40 ff.; bestätigt in EuGH, Urteil vom 6. November 2003, Rs. C-101/01, Slg. 2003, S. I-12992 - Lindqvist, Tz. 40 ff.

[12] Implizit wie hier *Schneider*, in: Wolff/Brink (Hrsg.), Beck'scher Online Kommentar Datenschutzrecht, Syst. B Rn. 53, 55, der nunmehr eine einheitliche Regelung des Datenschutzrechts für möglich hält, die auch die polizeiliche und justizielle Zusammenarbeit in Strafsachen erfasste.

[13] Zugespitzt *Vesting*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle (Hrsg.), Grundlagen des Verwaltungsrechts, Bd. 2, 2008, § 22 Rn. 2: Alle Operationen der Verwaltung seien *ausschließlich* solche der Informationsverarbeitung [Hervorhebung im Original].

[14] In der Diagnose ähnlich wie hier, aber mit anderen - überschießenden - Schlussfolgerungen *Rogall-Grothe*, ZRP 2012, S. 193 f.

[15] Zum „neuen" Polizeirecht als Informationsrecht statt vieler *Möstl*, DVBl 2007, S. 581.

und zu welchen Zwecken einsetzen oder welche Datensammlungen die Kriminalbehörden unterhalten können.

Eine solche Interpretation von Art. 16 Abs. 2 AEUV würde die Kompetenztitel in Art. 82 Abs. 1 und Abs. 2, Art. 85, Art. 87 Abs. 1 und Abs. 2 AEUV unterlaufen, die sekundärrechtliche Vorgaben für das Eingriffsrecht der mitgliedstaatlichen Kriminalbehörden nur in engen Grenzen ermöglichen und sich weitgehend auf grenzüberschreitende Sachverhalte beschränken. Schon daran zeigt sich, dass der Gegenstand der Rechtsetzungsbefugnis aus Art. 16 Abs. 2 AEUV enger zu fassen ist. Meiner Ansicht nach bietet sich insoweit folgende Differenzierung an:

Die EU darf auf der Grundlage von Art. 16 Abs. 2 AEUV für alle erfassten Sachbereiche umfassende und abschließende Regelungen über datenschutzspezifische Regelungsgegenstände schaffen, die den Kern des Datenschutzrechts ausmachen. Hierzu zählen die Rechte des Betroffenen einer Datenverarbeitung, die Datenschutzaufsicht, die Datensicherheit, die datenschutzrechtliche Verantwortlichkeit, prozedurale Vorkehrungen zur Gewährleistung von Datenschutz und Datensicherheit sowie die Folgen von Datenschutzverstößen. Insoweit sind einheitliche Regelungen für grenzüberschreitende und innerstaatliche Sachverhalte angezeigt, um die oben dargestellten Nachteile für den Schutz des Einzelnen und für die Effektivität des behördlichen Handelns zu vermeiden.

Hingegen ergibt sich aus Art. 16 Abs. 2 AEUV grundsätzlich keine Kompetenz der EU, die materiellen Anforderungen an behördliche[16] Datenverarbeitungen umfassend und abschließend zu regeln. Prinzipiell sind insoweit lediglich Mindestregelungen kompetenzgemäß, die gewährleisten, dass grundlegende Schutzstandards in allen Mitgliedstaaten erfüllt werden. Im Übrigen ist es Sache der Mitgliedstaaten festzulegen, für welche behördlichen Aufgaben welche Daten benötigt werden, mit welchen Methoden diese Daten erhoben werden dürfen und zu welchen Zielen sie innerstaatlich weiterverarbeitet werden können. Eine Ausnahme gilt im Interesse eines einheitlichen europäischen Datenschutzniveaus „nach außen“ für Regelungen über Datenübermittlungen an Staaten oder internationale Organisationen außerhalb der EU; ansonsten drohten wiederum erhebliche Rechtsunsicherheit und Wertungswidersprüche, die mit dem Ausbau des „europäischen Datenverkehrsraums“[17] noch erheblich zunehmen könnten.

Eine weitergehende Befugnis zur Harmonisierung des mitgliedstaatlichen Verwaltungs- und Prozessrechts kann sich im Übrigen aus anderen Kompetenztiteln als Art. 16 Abs. 2 AEUV ergeben, die sich in der Regel auf einen bestimmten hoheitlichen Tätigkeitsbereich beschränken. Insbesondere kann die EU aufgrund solcher Kompetenztitel regelmäßig die Voraussetzungen und das Verfahren von grenzüberschreitenden Datenverarbeitungen innerhalb der EU festlegen. Auch die Anforderungen an rein innerstaatliche Datenverarbeitungen können je nach Sachbereich in mehr oder weniger großem Ausmaß sekundärrechtlich vorgegeben werden. Derartige Regelungen sind jedoch nicht Gegenstand der geplanten Richtlinie, die sich

[16] Anderes gilt für Datenverarbeitungen Privater, die im Entwurf einer Datenschutz-Grundverordnung reguliert werden. Insoweit sind abschließende Regelungen über die Zulässigkeit von Datenverarbeitungen erlaubt, um das Befugnisziel des freien Datenverkehrs zu erreichen. Zudem droht hier kein übermäßiger Regelungszugriff auf das mitgliedstaatliche Verwaltungs- und Prozessrecht.

[17] *Schneider*, in: Wolff/Brink (Hrsg.), Beck’scher Online-Kommentar Datenschutzrecht, 2012, Syst. B Rn. 162.

ausschließlich auf Art. 16 Abs. 2 AEUV stützt; sie finden sich hingegen insbesondere im europäischen Strafverfahrensrecht.[18] Beispielhaft sei der Rahmenbeschluss über die Europäische Beweisanordnung genannt.[19]

2. Subsidiarität und Verhältnismäßigkeit

Auf der Grundlage der hier vorgeschlagenen Interpretation von Art. 16 Abs. 2 AEUV stehen auch die Grundsätze der Subsidiarität und der (kompetenzrechtlichen) Verhältnismäßigkeit (Art. 5 Abs. 1, 3 und 4 EUV) einem sekundärrechtlichen Regelungswerk des Datenschutzes bei Polizei und Strafjustiz nicht entgegen, selbst wenn die darin enthaltenen Regelungen auch für rein innerstaatliche Datenverarbeitungen gelten. Denn danach darf die EU nur solche Fragen umfassend und abschließend regeln, bei denen Rechtsunsicherheit, Ineffizienzen und Wertungswidersprüche drohen, wenn sie in der Hand der Mitgliedstaaten belassen werden. Im Übrigen ist sie darauf beschränkt, ein unionsweit einheitliches Mindestschutzniveau für kriminalbehördliche Datenverarbeitungen zu gewährleisten, das unabdingbar ist, um einen rechtsstaatskonformen europäischen Datenverkehrsraum bei der Verhütung und Verfolgung von Straftaten einzurichten.

II. Einzelfragen

Im Folgenden gehe ich auf zwei Einzelfragen des Entwurfs ein, die ich für besonders bedeutsam halte: Zum einen möchte ich darlegen, welche Regelungsspielräume der Entwurf den Mitgliedstaaten für die Voraussetzungen einer Datenverarbeitung belässt. Solche Regelungen machen den Kern des Eingriffsrechts der Kriminalbehörden aus. Zum anderen möchte ich die Regelungen des Entwurfs über Datenübermittlungen in Drittstaaten besonders kritisch hervorheben. Diese Regelungen sind völlig misslungen und müssen unbedingt überarbeitet werden.

1. Voraussetzungen einer Datenverarbeitung

Die Regelungen dazu, unter welchen Voraussetzungen personenbezogene Daten verarbeitet werden dürfen, entscheiden maßgeblich darüber, wie weitgehend die Richtlinie auf das mitgliedstaatliche Strafprozess- und Polizeirecht zugreift. Bedauerlicherweise sind diese Regelungen verkürzt geraten und wenig klar formuliert. Letztlich ergibt sich zwar hinreichend deutlich, dass lediglich Mindeststandards gesetzt werden. Es erscheint aber geboten, den Entwurf auszubauen und zu präzisieren.

Die zentrale Vorgabe für die Voraussetzungen einer Datenverarbeitung findet sich in Art. 7 Buchstabe a RL-E. Danach dürfen die Mitgliedstaaten eine Datenverarbeitung zulassen, wenn diese Verarbeitung erforderlich ist, damit eine zuständige Behörde eine gesetzliche Aufgabe auf den Gebieten der Verhütung oder Verfolgung von Straftaten oder der Strafvollstreckung wahrnehmen kann.

---

[18] Vgl. zum derzeitigen Stand dieser Rechtsmaterie die Beiträge in *Sieber u.a.* (Hrsg.), Europäisches Strafrecht, 2011, §§ 31-50.

[19] Rahmenbeschluss 2008/978/JI des Rates vom 18. Dezember 2008 über die Europäische Beweisanordnung zur Erlangung von Sachen, Schriftstücken und Daten zur Verwendung in Strafsachen, ABl. L 350 vom 30. Dezember 2008, S. 72; zu dem weitergehenden Plan einer Europäischen Ermittlungsanordnung *Gleß*, in: Sieber u.a. (Hrsg.), Europäisches Strafrecht, 2011, § 38 Rn. 92.

Auf den ersten Blick scheint es möglich, diese Norm als umfassende und abschließende Grundlage kriminalbehördlicher Ermächtigungen zu lesen. Die Vorschrift würde danach die Trennung von Aufgaben und Befugnissen aufgreifen, die das deutsche Sicherheitsrecht prägt.[20] Die Mitgliedstaaten könnten nur noch festlegen, welche Behörden die Aufgabe haben, Straftaten zu verhüten und zu verfolgen. Die Datenverarbeitungsbefugnisse dieser Behörden wären hingegen unionsrechtlich vorgegeben: Diese Behörden dürften grundsätzlich alle Daten mit allen denkbaren Mitteln erheben und verarbeiten. Nur das Gebot der Erforderlichkeit begrenzte die Reichweite der Ermächtigung.

Eine solche Interpretation von Art. 7 Buchstabe a RL-E wäre jedoch verfehlt. Zunächst wäre die Norm in dieser Auslegung mit höherrangigem Recht nicht vereinbar: Zum einen wäre sie kompetenzwidrig. Zum anderen stünde sie mit den Grundrechten der Betroffenen und dem rechtsstaatlichen Bestimmtheitsgrundsatz nicht in Einklang. Eine derartige Interpretation von Art. 7 Buchstabe a RL-E liegt weiter auch aus systematischen Gründen fern. Eine sehr ähnliche Vorgabe findet sich bereits jetzt in Art. 7 Buchstabe e DSRL, ohne dass diese Norm bislang als abschließende und umfassende Befugnisregelung für behördliche Datenverarbeitungen gelesen worden wäre.[21] Weiter findet sich eine annähernd wortlautgleiche Vorgabe in Art. 6 Abs. 1 Buchstabe e des Entwurfs einer Datenschutz-Grundverordnung (VO-E). Aus Art. 6 Abs. 3 VO-E ergibt sich, dass diese Norm die Verarbeitungsbefugnisse mitgliedstaalicher Behörden nicht abschließend und umfassend festlegt, sondern mitgliedstaatliche Befugnisregelungen voraussetzt und begrenzt.[22]

Der Begriff der behördlichen Aufgabe im Sinne von Art. 7 Buchstabe a RL-E muss daher unionsrechtlich so interpretiert werden, dass den Mitgliedstaaten grundsätzlich überlassen wird, welche Verarbeitungsmethoden ihre Kriminalbehörden aus welchem Anlass und mit welchem Ziel einsetzen dürfen. Das Eingriffsrecht der Kriminalbehörden bleibt also primär Sache der Mitgliedstaaten.

Art. 7 Buchstabe a RL-E wird damit nicht funktionslos. Die Vorschrift errichtet vielmehr mit dem Gesetzlichkeitsprinzip und dem Grundsatz der Erforderlichkeit zwei wesentliche (Mindest-)Anforderungen an mitgliedstaatliche Befugnisregelungen. Zudem eröffnet sie über Art. 51 Abs. 1 Satz 1 GRCh den Anwendungsbereich der Unionsgrundrechte. In der Folge ist das mitgliedstaatliche Sicherheitsrecht umfassend am Maßstab dieser Grundrechte zu überprüfen.[23]

Es erscheint allerdings wünschenswert, den Regelungsgehalt von Art. 7 Buchstabe a RL-E klarer zu formulieren. Dazu ist zumindest erforderlich, eine ähnliche Vorschrift wie Art. 6 Abs. 3 VO-E auch in den Richtlinienentwurf aufzunehmen. Noch besser wäre es, die Vorga-

---

[20] Hierzu *Denninger*, in: Lisken/ders. (Hrsg.), Handbuch des Polizeirechts, 5. Aufl. 2012, Rn. D 67 f.

[21] Vgl. *Schneider*, in: Wolff/Brink (Hrsg.), Beck'scher Online-Kommentar Datenschutzrecht, 2012, Syst. B Rn. 93: Art. 7 Buchstabe e DSRL bedürfe der „Ausgestaltung" durch mitgliedstaatliches Recht. Die Rechtsprechung des EuGH, nach der Art. 7 Buchstabe e DSRL unmittelbar anwendbar ist, steht hierzu nicht im Widerspruch, da es dort um eine unmittelbare Anwendbarkeit des dort niedergelegten Schutzstandards zugunsten des Einzelnen geht. In der Folge darf mitgliedstaatliches Recht, das diesen Standard verfehlt, nicht angewandt werden, EuGH, Urteil vom 20. Mai 2003, Rs. 465/00 u.a., Slg. 2003, S. I-5014 - ORF, Tz. 100.

[22] Ähnlich *Gola*, EuZW 2012, S. 332 (335): Art. 6 Abs. 3 VO-E als „Öffnungsklausel".

[23] Näher hierzu und zu den möglichen institutionellen Auswirkungen einer Anwendung der Unionsgrundrechte *Bäcker/Hornung*, ZD 2012, S. 147 (150, 152).

ben für das mitgliedstaatliche Recht präziser und detaillierter zu fassen. Konkretere Vorgaben fanden sich etwa in Art. 4 Abs. 3 des Arbeitsentwurfs der Richtlinie, der im November 2011 bekannt wurde.[24]

Schließlich wäre es sinnvoll, das derzeit weitgehend unklare systematische Verhältnis von Art. 7 Buchstabe a RL-E zu den weiteren Verarbeitungstatbeständen in Art. 7 Buchstaben b-d RL-E zu erhellen; nach meiner Vermutung sind diese weiteren Regelungen zumindest überwiegend entbehrlich.

2. Datenübermittlung in Drittstaaten

Regelungstechnisch misslungen und rechtsstaatlich unerträglich sind die Vorschriften über die Übermittlung personenbezogener Daten in Drittländer in Art. 33 ff. RL-E. Diese Normen scheinen zwar auf den ersten Blick durchaus hohe Anforderungen an solche Übermittlungen zu errichten. Bei näherer Betrachtung bleibt von diesen Anforderungen jedoch so gut wie nichts übrig.[25]

Art. 33 RL-E nennt zwei Voraussetzungen einer Datenübermittlung in einen Drittstaat: Die Übermittlung muss erforderlich sein, um Straftaten zu verhüten, aufzudecken, zu untersuchen oder zu verfolgen oder um eine Strafe zu vollstrecken (Buchstabe a). Zudem muss ein Erlaubnistatbestand hinzutreten (Buchstabe b). Solche Erlaubnistatbestände sind ein Angemessenheitsbeschluss (Art. 34 RL-E) oder geeignete Garantien des Datenschutzniveaus im Empfangsstaat (Art. 35 RL-E). Art. 36 RL-E enthält als Auffangregelung Ausnahmen von dem grundsätzlichen Übermittlungsverbot im Einzelfall.

Dieses im Ansatz plausible Regelungskonzept wird im Einzelnen praktisch vollständig verwässert: Bereits die Erlaubnistatbestände des Art. 35 RL-E sind sehr vage formuliert und errichten letztlich kaum materielle Anforderungen an die Datenübermittlung. Schließlich ist der Anwendungsbereich der Ausnahmevorschrift in Art. 36 RL-E so weit, dass die Kriminalbehörden letztlich Daten praktisch nach Belieben in Drittstaaten übermitteln dürfen. Dies gilt insbesondere für den „Ausnahmetatbestand“ in Art. 36 Buchstabe d RL-E. Danach soll die Datenübermittlung pauschal zulässig sein, wenn dies zur „Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Strafverfolgung erforderlich ist“. Dies ist jedoch bereits nach dem wortlautgleichen Art. 33 Buchstabe a RL-E erforderlich. Als Voraussetzung der Datenübermittlung bleibt so nur der Erforderlichkeitsgrundsatz übrig, irgendwelche Datenschutzgarantien in dem Drittland werden nicht verlangt. Der Schutzstandard der Übermittlungsvorschriften bleibt damit letztlich noch hinter dem geltenden Art. 13 Abs. 3 Buchstabe a RB zurück, der eine Datenübermittlung ohne entsprechende Garantien des Drittstaats immerhin nur wegen „überwiegender berechtigter Interessen, insbesondere wichtiger öffentlicher Interessen“ zulässt.

Die Übermittlungsregelungen erweisen sich damit insgesamt als Augenwischerei ohne Schutzgehalt für den Betroffenen. Rechtsstaatlich ist dies nicht hinnehmbar. Es ist dringend geboten, die Anforderungen an eine Datenübermittlung in Drittstaaten zu erhöhen. Dazu sollte Art. 35 RL-E deutlich restriktiver gefasst werden, um den Schutz des Betroffenen nicht weit-

[24] Abrufbar unter http://www.statewatch.org/eu-dp.htm; hierzu *Hornung*, ZD 2012, S. 99 f.
[25] Näher zum Folgenden *Bäcker/Hornung*, ZD 2012, S. 147 (151).

gehend in das Belieben der übermittelnden Behörde zu stellen. Zudem müssen die Ausnahmeregelungen in Art. 36 RL-E auf echte Krisensituationen beschränkt werden.