MATTHIAS BÄCKER / GERRIT HORNUNG

EU-Richtlinie für die Datenverarbeitung bei Polizei und Justiz in Europa

Einfluss des Kommissionsentwurfs auf das nationale Strafprozess- und Polizeirecht

Anforderungen an Ermittlungsbefugnisse
Benachrichtigungspflichten
Datenübermittlung in Drittstaaten
Anwendungsbereich
Freier Datenverkehr

■ Der am 25.1.2012 veröffentlichte Vorschlag der EU-Kommission für eine grundlegende Reform des europäischen Datenschutzrechts besteht aus zwei Teilen. Neben eine „Datenschutz-Grundverordnung" soll als zweites grundlegendes Regelungsinstrument eine Richtlinie für die Datenverarbeitung bei Polizei und Justiz treten, die nach dem Willen der Kommission den Rahmenbeschluss 2008/977/JI ersetzen wird. Der Beitrag stellt den Richtlinienentwurf im Kontext des Gesamtvorhabens vor und vertieft Fragen zum Anwendungsbereich, zu den Voraussetzungen der Datenverarbeitung, Benachrichtigungspflichten und der Datenübermittlung in Drittstaaten.

■ The proposal by the EU-Commission published on January 25, 2012 regarding a fundamental reform of the European data protection law consists of two parts. In addition to a "data protection basic regulation", a regulation for data processing by the police and justice shall be introduced as a second basic regulatory instrument, which – according to the Commission's will – shall replace the framework resolution 2008/977/JI. This article introduces the draft regulation in the context of the entire plan and will detail individual aspects regarding area of application, the requirements for data processing, obligations to inform and transferring data to third party states.

I. Hintergrund

Der Datenschutz im Bereich des Sicherheitsrechts (also die Datenverarbeitung durch Polizei und Justiz in der früheren „Dritten Säule") ist in der EU bislang deutlich weniger reguliert als in den Bereichen der übrigen staatlichen Verwaltung und der Wirtschaft. Während dort mit der Datenschutzrichtlinie 95/46/EG[1] (im Folgenden: DS-RL) seit längerer Zeit ein einheitlicher Rahmen vorgegeben wird, erfolgte eine – teilweise – Konsolidierung für die Polizei- und Strafverfolgungsbehörden (Kriminalbehörden) erst mit dem Rahmenbeschluss 2008/977/JI, der allerdings lediglich für den grenzüberschreitenden Datenverkehr gilt.[2] Der Reformvorschlag der *Kommission* sieht nunmehr für beide Bereiche wichtige Änderungen vor, die sich in beiden Fällen sowohl auf die materiellen Regelungen als auch auf das Regelungsinstrument beziehen. Während der Bereich der bisherigen Richtlinie durch eine „Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung)"[3] (im Folgenden: DS-GVO-E) erfasst wird, soll eine „Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr"[4] (im Folgenden: RL-E; Artikelangaben ohne Bezeichnung beziehen sich auf diese) den Rahmenbeschluss ersetzen und dabei erstmals auch rein innerstaatliche Datenverarbeitungen regulieren.

Die Gesamtstrategie – die sich nunmehr auf Art. 16 AEUV stützt[5] – wird in einer übergreifenden Mitteilung „Der Schutz der Privatsphäre in einer vernetzten Welt. Ein europäischer Datenschutzrahmen für das 21. Jahrhundert"[6] erläutert. Eine vorläufige Fassung der drei Texte wurde im November 2011 bekannt.[7] Gegenüber dieser erweitert die RL-E durchweg den Spielraum für Datenverarbeitungen der Kriminalbehörden,[8] teils indem (problematisch) unbestimmte Formulierungen gewählt werden.[9]

Durch den Wechsel zum Instrument der Richtlinie erhält das *Europäische Parlament* erstmals eine Mitwirkungsmöglichkeit, während der bisherige Rahmenbeschluss durch (einstimmige) Entscheidung im *Rat* verabschiedet werden konnte. Ähnlich wie bei der DS-GVO-E wird durch die Richtlinie eine stärkere „Vergemeinschaftung" als bisher erreicht, die RL-E lässt den Mitgliedstaaten aber – teils ausdrücklich, teils implizit – deutlich mehr Regelungsspielräume. Zumindest an einigen Stellen handelt es sich deshalb nicht um eine Vollharmonisierung.

II. Struktur und Inhalt im Überblick

Der Entwurf gliedert sich in zehn Kapitel. Mit Ausnahme des Kapitels IX der DS-GVO-E (das sich mit der Datenverarbeitung in bestimmten Sondersituationen, v.a. in den Bereichen Journalismus, Beschäftigtendaten, Wissenschaft, Gesundheitsdaten und Religionsgemeinschaften beschäftigt) korrespondieren die Kapitel der beiden Instrumente miteinander. Das gilt auch für viele Regelungsinhalte.

■ Die Allgemeinen Bestimmungen der RL-E (Kapitel I) beschreiben Gegenstand und Ziele (Art. 1, der wie die DS-GVO-E zwei in

1 RL 95/46/EG, ABl. EG Nr. L 281 v. 23.11.1995, S. 31.
2 ABl. EU Nr. L 350/60 v. 30.12.2008.
3 KOM(2012) 11 endg; dazu ausf. *Hornung*, ZD 2012, 99.
4 KOM(2012) 10 endg.
5 Zu den primärrechtlichen Änderungen im Bereich des Datenschutzrechts durch den Lissabon-Vertrag s. *Spiecker gen. Döhmann/Eisenbarth*, JZ 2011, 169.
6 KOM(2012) 9 endg.
7 S. http://www.statewatch.org/eu-dp.htm; dazu *Hornung*, ZD 2012, 99 f.
8 Etwa bei den Verarbeitungsgrundsätzen in Art. 4, der Einschränkung der Informationspflichten (Art. 23), der Ausweitung der Befugnisse zur Übermittlung in Drittstaaten (Art. 33 ff., v.a. Art. 35, 36), der Einschränkung der Befugnisse der Aufsichtsbehörden (Art. 46), der Beschränkung der Rechtsschutzmöglichkeiten sowie der Streichung der gemeinsamen Aktionen der Aufsichtsbehörden (Art. 52 des Entwurfs) und der besonderen Regeln über genetische Daten (Art. 10 des Entwurfs, nunmehr in abgeschwächter Form noch in Art. 8).
9 Z.B. „nicht exzessiv" (Art. 4 lit. c), „so weit wie möglich" (Art. 5 Abs. 1, Art. 6 Abs. 1), „alle vertretbaren Schritte" (Art. 10 Abs. 1).

Teilen konfligierende Ziele enthält, nämlich Grundrechts- und Datenschutz einerseits, ungehinderten Datenverkehr andererseits), legen den Anwendungsbereich fest (Art. 2) und enthalten Begriffsbestimmungen (Art. 3). Einige Definitionen wurden mit Blick auf die Zielrichtung der RL-E (Kriminalbehörden) angepasst bzw. gestrichen (v.a. Art. 4 Abs. 8, 13-17 DS-GVO-E). Kinder werden wie in der DS-GVO-E definiert, anders als dort enthält die RL-E aber keine besonderen Einschränkungen oder Anforderungen an die Verarbeitung ihrer Daten.[10]

- Kapitel II enthält die Grundsätze der Datenverarbeitung, nämlich allgemeine Anforderungen (Art. 4), Anforderungen an die Rechtmäßigkeit (Art. 7), Einschränkungen für sensible Arten von Daten (Art. 8) und für auf Profiling und automatischer Datenverarbeitung basierende Maßnahmen (Art. 9, der nationale Befugnistatbestände bei entsprechenden Garantien zulässt; s. deutlich detaillierter Art. 20 DS-GVO-E). Während diese Regelungen Entsprechungen in der DS-GVO-E haben, führt die RL-E zwei neuartige Unterscheidungen ein, nämlich die nach verschiedenen Kategorien betroffener Personen (Art. 5: Verdächtige, Straftäter, Opfer, Zeugen und Kontaktpersonen, andere) und nach „Richtigkeit und Zuverlässigkeit" der Daten (Art. 6: Differenzierung zwischen Daten, die „auf Fakten beruhen, und solchen, die auf persönlichen Einschätzungen beruhen", s. bisher Art. 8 Abs. 1 des Rahmenbeschlusses). Bemerkenswerterweise knüpft die RL-E an keiner Stelle direkte Rechtsfolgen an die Pflicht der Verantwortlichen, zwischen diesen Betroffenen und Datenkategorien zu unterscheiden; auch EG 23 schweigt hierzu. Art. 16 bezieht sich nicht auf diese Vorschriften, sodass ein Verstoß keinen Löschungsanspruch nach sich zieht. In Betracht kommt allerdings ein Recht auf Berichtigung (Art. 15), wenn eine betroffene Person einer falschen Kategorie zugeordnet wird. Im Übrigen handelt es sich um strukturelle Vorgaben für die Datenverarbeitungsprozesse der Kriminalbehörden, die von den Aufsichtsbehörden im Rahmen ihrer Befugnisse (Art. 46) überwacht werden können.
- Wie die DS-GVO-E enthält Kapitel III für die Rechte der betroffenen Personen zunächst Anforderungen an die Modalitäten und generelle Pflichten der Verantwortlichen (Art. 10, einschließlich einer grundsätzlichen Kostenfreiheit). Im Einzelnen regelt Art. 11 eine grundsätzliche Informationspflicht bei Datenerhebungen. Art. 12 enthält ein grundsätzliches Auskunftsrecht des Betroffenen (Gegenstand: die Tatsache der Verarbeitung, einzelne Daten und das Recht auf eine Kopie), das allerdings von den Mitgliedstaaten in erheblichem Umfang eingeschränkt werden kann (Art. 13). In diesem Fall können die Betroffenen nach Art. 14 die Aufsichtsbehörde um Prüfung ersuchen. Hier müssen die Mitgliedstaaten eine in camera-Prüfung einrichten, an deren Ende nach Art. 14 Abs. 3 zumindest über das Ergebnis zu informieren ist. Weiter ist ein Löschungsanspruch vorgesehen, wobei in bestimmten Fällen eine Markierung der Daten an die Stelle der Löschung tritt (Art. 16). Art. 17 enthält schließlich die Befugnis, die Betroffenenrechte im einzelstaatlichen Strafprozessrecht zu regeln, sofern es um strafrechtliche Ermittlungen oder Strafverfahren geht.
- Kapitel IV betrifft die Pflichten des für die Verarbeitung Verantwortlichen und von Auftragsdatenverarbeitern. Die allgemeinen Pflichten (Art. 18) sowie die Regeln zum Datenschutz durch Technik (Art. 19, der diesen wichtigen Bereich wie Art. 23 DS-GVO-E sehr zurückhaltend angeht),[11] zur gemeinsamen Datenverarbeitung mehrerer Verantwortlicher (Art. 20), zur Auftragsdatenverarbeitung (Art. 21, 22), zur Dokumentation (Art. 23) sowie zur Zusammenarbeit mit der Aufsichtsbehörde (Art. 25, 26, einschließlich einer Vorabkonsultation bei sensiblen Daten und besonderen Risiken) entsprechen in Zielrichtung und wesentlichen Inhalten der DS-GVO-E. Gesondert geregelt wird die Aufzeichnung von Vorgängen (Art. 24). Danach ist über Erhebung, Veränderung, Abfrage, Weitergabe, Kombination und Löschung von Daten „Buch zu führen". Im Rahmen dieser Protokollierung sind Zweck, Datum und Uhrzeit sowie „so weit wie möglich" die Identität der verarbeitenden Person festzuhalten; Art. 24 Abs. 2 enthält eine Zweckbindung der Protokolldaten. Demgegenüber sind die Vorschriften zur Datensicherheit (Art. 27-29, dabei werden die Informationspflichten bei „Datenpannen"[12] begrüßenswerterweise auch auf die Kriminalbehörden erstreckt) und zu internen Datenschutzbeauftragten (Art. 30-32) wieder an die DS-GVO-E angelehnt. Dabei wird teilweise (dem Charakter als Richtlinie entsprechend) offener formuliert, teilweise allerdings auch detaillierter (s. etwa den Maßnahmenkatalog in Art. 27 Abs. 2, der deutlich mit der Anlage zu § 9 BDSG korrespondiert).[13] Offenbar hat die *Kommission* hier Regelungen aufgenommen, die sie im Anwendungsbereich der DS-GVO-E erst nachträglich auf Grund ihrer Befugnis zum Erlass delegierter Rechtsakte erlassen will.[14] Eine Regelung zur Datenschutz-Folgenabschätzung (Art. 33 DS-GVO-E; s. noch Art. 31 des Entwurfs vom November 2011) fehlt in der RL-E ebenso wie Bestimmungen zum Einsatz zertifizierter Technologien (Art. 39 DS-GVO-E).
- Kapitel V enthält abschließende (Art. 33) Regelungen zur Übermittlung in Drittländer und an internationale Organisationen. Von diesen sind Übermittlungen zwischen den Mitgliedstaaten sowie an oder von Stellen der EU abzugrenzen. Letztere werden in der Systematik der RL-E nicht von Übermittlungen zwischen verschiedenen Behörden eines einzelnen Mitgliedstaats unterschieden, sodass sich die Zulässigkeit nach den allgemeinen Verarbeitungsgrundsätzen der RL-E und den Bestimmungen gesonderter Rechtsakte richtet, die nach Art. 59 unberührt bleiben.
- Die detaillierten Bestimmungen über Aufsichtsbehörden (Kapitel VI) entsprechen vielfach der DS-GVO-E, insbesondere die völlige Unabhängigkeit[15] und das Recht auf angemessene Ausstattung (Art. 40), Anforderungen an die Person (Art. 41) und die Errichtung der Aufsichtsbehörde (Art. 42). Bei den Aufgaben (Art. 45) besteht sogar praktisch Gleichlauf mit Art. 52 DS-GVO-E.[16] Die Befugnisse (Art. 46) sind demgegenüber deutlich eingeschränkt (der Entwurf hatte hier mehr Regelungen aus der DS-GVO-E übernommen), beinhalten aber „wirksame Einwirkungsbefugnisse", die auch die Beschränkung, Löschung oder Vernichtung der Daten oder das vorläufige oder endgültige Verbot einer Verarbeitung umfassen. Dies entspricht Art. 25 des Rahmenbeschlusses.
- Kapitel VII enthält Regeln zur Zusammenarbeit der Aufsichtsbehörden (Art. 48) und Aufgaben des Europäischen Datenschutzausschusses (Art. 49, s. Art. 64 ff. DS-GVO-E). Ein Kohärenzverfahren wie in Art. 57 ff. DS-GVO-E fehlt; dementsprechend ist auch die Rolle der *Kommission* deutlich schwächer als dort.[17] In Kapitel VIII sind die Rechte auf Beschwerde bei der Aufsichtsbehörde (Art. 50; einschließlich eines Verbandsklagerechts auch unabhängig von individuellen Beschwerden), Rechtsbehelfe gegen diese (Art. 51, einschließlich der Verpflichtung zum Tätigwerden, aber anders als in Art. 74 Abs. 4 DS-GVO-E ohne die Möglichkeit, die Aufsichtsbehörde des eigenen Mitgliedstaats um Klage gegen die Behörde eines anderen Staates zu ersuchen) sowie gegen die verantwortlichen Kriminalbehörden und Auftragsdatenverarbeiter geregelt (Art. 52; anders als nach Art. 75 Abs. 2 Satz 2 DS-GVO-E ist allerdings keine Kla-

10 Als einzige Rechtsfolge regelt Art. 45 Abs. 2 Satz 2, dass die Aufsichtsbehörden bei der Information der Öffentlichkeit spezifische Maßnahmen für Kinder besonders beachten müssen.

11 Dazu *Hornung*, ZD 2012, 99, 103.

12 Dazu *Gabel*, BB 2009, 2045; *Eckhardt/Schmitz*, DuD 2010, 390; *Ernst*, DuD 2010, 472; *Hanloser*, MMR 2010, 300; *Hornung*, NJW 2010, 1841.

13 S. bisher Art. 22 des Rahmenbeschlusses.

14 Zur Rolle der *Kommission* in der DS-GVO-E s. *Hornung*, ZD 2012, 99, 105 f.

15 S. bisher Art. 25 Abs. 1 des Rahmenbeschlusses.

16 Hinzu tritt nach Art. 45 Abs. 1 lit. c die Überprüfung von Art. 14, die es in dieser Form in der DS-GVO-E nicht gibt.

17 Dazu *Hornung*, ZD 2012, 99, 105 f.

ge im eigenen Mitgliedstaat gegen Verantwortliche möglich, die in einem anderen Mitgliedstaat ansässig sind; anders noch der Entwurf). Haftung und Schadensersatz (Art. 54) entsprechen der DS-GVO-E, während die Sanktionen für Verstöße in Art. 55 weithin der Regelungsbefugnis der Mitgliedstaaten überlassen werden. Diese bestimmen somit beispielsweise, ob wie nach Art. 79 DS-GVO-E verwaltungsrechtliche Sanktionen auch gegenüber Behörden zulässig sind.[18]

Kapitel IX enthält die Regeln zu delegierten Rechtsakten und Durchführungsakten, die sich aber nur noch auf Art. 28 Abs. 5 beziehen. Der Entwurf hatte hier noch deutlich mehr Bestimmungen enthalten. In den Schlussbestimmungen (Kapitel X) werden der Rahmenbeschluss aufgehoben, das Verhältnis zu weiteren Rechtsakten bestimmt und eine Evaluationspflicht der *Kommission* normiert.

III. Anwendungsbereich

Gem. Art. 2 Abs. 1 gilt die RL-E für die Datenverarbeitung durch die „zuständigen Behörden zu den in Art. 1 Abs. 1 genannten Zwecken". Der Begriff der Behörde ist sehr unglücklich gewählt,[19] weil die RL-E auch Gerichte erfasst, soweit sie im Sicherheitsbereich tätig sind. Dies stellt EG 55 ausdrücklich klar, und einige der Normen beziehen sich sogar direkt auf die gerichtliche Datenverarbeitung (z.B. Art. 11 Abs. 4 lit. a, Art. 13 Abs. 1 lit. a, Art. 17). Die nationalen Gerichte unterliegen also dem materiellen Datenschutzrecht und sind nach Art. 44 Abs. 2 lediglich in ihrer Stellung als Rechtsprechungsorgane von der Kontrolle der Aufsichtsbehörden ausgenommen.[20]

Nach Art. 2 Abs. 2 ist erforderlich, dass es sich entweder um eine (teil-)automatisierte oder dateimäßige Verarbeitung handelt. Erfasst sind zunächst Datenerhebungen mittels automatisierter Ermittlungsmethoden (Telekommunikationsüberwachung, Vorratsdatenspeicherung, Online-Durchsuchung, Videoüberwachung, Kfz-Kennzeichenerfassung etc.). Daneben unterfallen auch manuelle Maßnahmen dem Anwendungsbereich, wenn die gewonnenen Daten – wie beispielsweise erkennungsdienstliche Unterlagen – automatisiert oder in einer Datei verarbeitet werden sollen. Der Dateibegriff setzt dabei gem. Art. 3 Abs. 5 keine elektronische Verarbeitung voraus. Nach EG 15 soll er dementsprechend auch Akten und Aktensammlungen umfassen, wenn sie nach „bestimmten Kriterien" geordnet werden können. Je nachdem, welche Anforderungen an ein solches Ordnungskriterium gestellt werden, könnte es bereits ausreichen, wenn eine Akte ein Aktenzeichen trägt und etwa nach dem Deliktstyp oder dem Namen des Betroffenen umsortiert werden kann.[21] Jedenfalls dürften mit der absehbaren flächendeckenden Verbreitung elektronischer Vorgangsbearbeitungssysteme in naher Zukunft so gut wie alle Datenverarbeitungen der Kriminalbehörden in den Anwendungsbereich fallen. Spätestens dann wären nur noch rein manuelle Maßnahmen wie etwa eine Personenkontrolle ausgenommen, und auch dies nur, solange die erlangten Daten weder mit einer Datei (etwa dem Fahndungsbestand) abgeglichen noch gespeichert werden.

Die *Kommission* nennt den begrenzten Anwendungsbereich des Rahmenbeschlusses – insbesondere die Ausklammerung der innerstaatlichen Datenverarbeitung der Kriminalbehörden in Art. 1 Abs. 2 – als einen wesentlichen Grund für das Reformvorhaben.[22] Dementsprechend klammert Art. 2 Abs. 3 lit. a lediglich Tätigkeiten aus, die wie die nationale Sicherheit prinzipiell nicht in den Anwendungsbereich des Unionsrechts fallen. Was genau der Bereich der nationalen Sicherheit i.S.d. RL-E umfasst, wird weder dort noch im einschlägigen EG 15 definiert. Neben dem Verteidigungsbereich wird man wohl auch die Tätigkeit der Inlands- und Auslandsgeheimdienste dazuzählen müssen. Das würde in Deutschland insbesondere die Datenverarbeitungsregelungen im G 10, BNDG, MADG, BVerfSchG und den entsprechenden Gesetzen der Länder betreffen.

Die Ausnahme für Organe, Einrichtungen, Ämter und Agenturen der Union in Art. 2 Abs. 3 lit. b ist regelungstechnisch verständlich, da insoweit andere Rahmenbedingungen gelten. Es ist allerdings kaum nachvollziehbar, dass die *Kommission* – die immerhin mit dem Anspruch eines „europäischen Datenschutzrahmens für das 21. Jahrhundert"[23] auftritt – nicht zugleich einen Vorschlag für die Institutionen der Union vorgelegt hat. Insbesondere die Datenschutzregeln für *Europol* sind in der Vergangenheit vielfach und zu Recht als ungenügend kritisiert worden.[24] Zumindest mittelfristig sind hier einheitliche Regeln für die nationalen Kriminalbehörden einerseits und für *Europol* und *Eurojust* andererseits erforderlich.

IV. Ausgewählte Regelungsfelder

1. Voraussetzungen einer Datenverarbeitung

Die RL-E regelt zumindest weitgehend[25] nicht selbst, welche Datenverarbeitungen erlaubt sein sollen. Sie setzt vielmehr Erlaubnisnormen im Unionsrecht und im Recht der Mitgliedstaaten voraus. Für mitgliedstaatliche Erlaubnistatbestände enthält die RL-E dabei materielle Mindestanforderungen. Diese fallen allerdings auf den ersten Blick ausgesprochen mager aus. Gerade an dieser Stelle wurde nämlich die RL-E gegenüber dem Entwurf erheblich entschärft, der im November 2011 bekannt wurde. Strenge Anforderungen ergeben sich allerdings, wenn die einschlägigen Normen grundrechtlich aufgeladen werden.

Der Entwurf vom November 2011 errichtete in Art. 4 und Art. 7 noch hohe Anforderungen an das mitgliedstaatliche Recht: Er enthielt detaillierte Vorgaben für den Inhalt von Normen, die Datenverarbeitungen der Kriminalbehörden regeln. Hinzu kamen prozedurale Vorkehrungen für Zugriffe der Kriminalbehörden auf Datenbestände, die nicht zu kriminalbehördlichen Zwecken angelegt wurden. Schließlich war ein umfassendes Verwendungsverbot für rechtswidrig verarbeitete Daten vorgesehen, das etwa die deutsche Dogmatik der strafprozessualen Beweisverwertungsverbote[26] weitgehend obsolet gemacht und durch eine radikale fruit of the poisonous tree-Doktrin ersetzt hätte.

Hingegen enthält die RL-E nur noch wenige Anforderungen an mitgliedstaatliche Datenverarbeitungen, die zudem recht vage formuliert sind. Immerhin ist die Einwilligung des Betroffenen im Katalog zulässiger Verarbeitungsgründe in Art. 7 nicht aufgeführt und damit kein Rechtfertigungsgrund für eine Datenverarbeitung der Kriminalbehörden. Die dahinter stehende Wertung, dass der Betroffene über eine Einwilligung gegenüber einer Sicherheitsbehörde niemals autonom entscheiden wird, entspricht Art. 7 Abs. 4 DS-GVO-E. Diese Norm schließt die Einwilligung aus, wenn zwischen dem Betroffenen und dem Verant-

18 Dies war im Entwurf noch ausdrücklich geregelt.
19 Der Begriff „authority" in der englischen Fassung ist hingegen offener.
20 KOM(2012) 10 endg, 12; s. z.B. *Klink*, Datenschutz in der elektronischen Justiz, 2010.
21 Vgl. zu § 3 Abs. 2 Satz 2 BDSG *Gola/Schomerus*, BDSG, § 3 Rdnr. 20.
22 KOM (2012) 10 endg., 2.
23 KOM(2012) 9 endg.
24 Näher *Böhm*, Information Sharing and Data Protection in the Area of Freedom, Security and Justice, 2011, S. 177 ff. (zu Europol), S. 214 ff. (Eurojust); s. zur Rechtslage vor dem 1.1.2010 auch *Matz*, Europol – Datenschutz und Individualrechtsschutz im Hinblick auf die Anforderungen der EMRK, 2003; *Beaucamp*, DVBl. 2007, 802; *Hilger/Ruthig/Schenke/Wolter/Zöller*, Alternativentwurf Europol und europäischer Datenschutz, 2008.
25 Ob die Mitgliedstaaten die in Art. 7 lit. b bis d enthaltenen Erlaubnisgründe zwingend aufgreifen müssen, geht aus der Norm nicht eindeutig hervor; jedenfalls sind diese Erlaubnisgründe ersichtlich nachrangig ggü. Art. 7 lit. a, der ausdrücklich auf anderweitig geregelte „gesetzliche Aufgaben" der zuständigen Behörden verweist.
26 Hierzu im Überblick *Eisenberg*, Beweisrecht der StPO, 7. Aufl. 2011, Rdnr. 356 ff., m.w.Nw.

wortlichen ein erhebliches Ungleichgewicht besteht. Praktisch wäre der Ausschluss der Einwilligung durchaus bedeutsam. Insbesondere dürfte eine Kriminalbehörde nicht den Betroffenen fragen, ob er bereit ist, eine Ermittlungsmaßnahme „freiwillig" zu dulden, deren gesetzliche Voraussetzungen nicht vorliegen („Sie haben doch nichts dagegen"-Fälle).

Hingegen scheint die RL-E gesetzliche Verarbeitungsbefugnisse fast vollständig in das Belieben der Mitgliedstaaten zu stellen. Art. 4 beschränkt sich nunmehr darauf, allgemeine Grundsätze für Datenverarbeitungen aufzustellen.[27] Art. 7 zählt hingegen die zulässigen Typen von Erlaubnistatbeständen auf. Art. 7 lit. a, der in der Praxis absehbar im Vordergrund stehen wird, erlaubt gesetzliche Datenverarbeitungsregelungen bereits dann, wenn die Verarbeitung zu den Zwecken der Kriminalprävention oder Strafverfolgung erforderlich ist. Nähere inhaltliche Vorgaben an solche Regelungen fehlen. Es drängt sich das Gefühl auf, dass seit dem ersten bekanntgewordenen Entwurf vom November 2011 massiv interveniert wurde, um zu verhindern, dass den informationellen Befugnissen der Kriminalbehörden wirksame Grenzen gesetzt werden.

Der Eindruck, die RL-E errichte keine echten Hürden für solche Befugnisse, könnte jedoch trügen. Gehaltvollere Aussagen zu den unionsrechtlichen Grenzen für mitgliedstaatliche Verarbeitungsregelungen lassen sich treffen, wenn diese Regelungen und ihr Vollzug an dem unionsrechtlichen Grundrecht auf Datenschutz aus Art. 8 GRCh zu messen sind. Dafür kommt es nach Art. 51 Abs. 1 Satz 1 GRCh maßgeblich darauf an, ob die Mitgliedstaaten Unionsrecht durchführen, wenn sie solche Verarbeitungsregelungen schaffen und anwenden. Hiergegen lässt sich zwar einwenden, dass Art. 7 lit. a den Mitgliedstaaten lediglich ermöglicht, ihren Kriminalbehörden bestimmte Datenverarbeitungen zu erlauben, dies aber nicht gebietet. Auch errichtet die Norm dem Wortlaut nach nur rudimentäre Anforderungen an die mitgliedstaatlichen Erlaubnistatbestände und belässt den Mitgliedstaaten damit einen fast unbegrenzten Regelungsspielraum. Gleichwohl bewegen sich die Mitgliedstaaten auf Grund von Art. 7 im Anwendungsbereich des Unionsrechts, wenn sie von diesem Spielraum Gebrauch machen. Für eine Anwendung von Art. 8 GRCh spricht zudem, dass die Kompetenzregelung in Art. 16 AEUV, auf der die RL-E beruht, das Datenschutzgrundrecht ausdrücklich wiederholt. Es liegt in der Folge nahe, die Rechtsakte, die auf der Grundlage dieses Kompetenztitels ergehen, so auszulegen, dass dieses Grundrecht möglichst weitgehend zur Geltung kommt.[28] Schließlich weist die Rechtsprechung des *EuGH* zum Anwendungsbereich der Unionsgrundrechte, wenngleich sie durchaus noch Fragen offen lässt, einen deutlichen expansiven Zug auf.[29] Insbesondere hat der *Gerichtshof* bereits angedeutet, dass die Mitgliedstaaten bei der Richtlinienumsetzung auch insoweit an die Unionsgrundrechte gebunden sind, als sie Regelungsspielräume ausfüllen, die eine Richtlinie ihnen belässt.[30]

Sind die Mitgliedstaaten an Art. 8 GRCh gebunden, wenn sie im Anwendungsbereich der RL-E kriminalbehördliche Datenverarbeitungsbefugnisse schaffen, so bildet Art. 7 lit. a den Ausgangspunkt für eine umfassende Grundrechtsrechtsprechung des *EuGH* zum Datenschutz gegenüber Kriminalbehörden. Bei der Konkretisierung von Art. 8 GRCh wäre gem. Art. 52 Abs. 3 GRCh der partiell gleichläufige Art. 8 EMRK heranzuziehen.[31] Dabei könnte der *EuGH* auch an die Rechtsprechung des *EGMR* anknüpfen,[32] der bereits zahlreiche Entscheidungen zu kriminalbehördlichen Überwachungsmaßnahmen getroffen hat.[33] Da die Konventionsrechte zudem lediglich einen Mindeststandard errichten,[34] könnte der *EuGH* über die konventionsrechtlichen Anforderungen sogar noch hinausgehen. In der Folge könnte der *Gerichtshof* zur zentralen Institution des Grundrechtsschutzes im Sicherheitsrecht werden.

2. Benachrichtigung des Betroffenen einer heimlichen Datenerhebung

Das Recht des Betroffenen, davon zu erfahren, wer welche personenbezogenen Daten über ihn verarbeitet, ist das grundlegende Datenschutzrecht, weil er ohne diese Kenntnis seine weiteren Rechte praktisch nicht ausüben kann und eine strukturelle Unkenntnis über hoheitliche Datenverarbeitungen mit einem rechtsstaatlichen Gemeinwesen unvereinbar ist. Im Verhältnis zu den Kriminalbehörden ist dieses Recht für den Betroffenen besonders bedeutsam. Denn diese Behörden sind in großem Umfang befugt, personenbezogene Daten ohne Mitwirkung oder Kenntnis des Betroffenen zu erheben. Der Betroffene ist grundsätzlich darauf angewiesen, dass die zuständige Behörde ihn aktiv von heimlichen Datenerhebungen benachrichtigt, da er in der Regel keinen Anlass haben wird, sich aus eigener Initiative über solche Datenerhebungen zu informieren.

Art. 11 trägt dem Informationsinteresse des Betroffenen Rechnung, indem die Mitgliedstaaten verpflichtet werden, Informationspflichten bei offenen wie verdeckten Datenerhebungen zu schaffen. Dabei errichtet Art. 11 Abs. 1 detaillierte Anforderungen an den Inhalt der Information. Diese Anforderungen gehen über die bisherigen Benachrichtigungspflichten des deutschen Rechts – beispielsweise nach § 101 Abs. 4 StPO oder § 20w Abs. 1 BKAG – deutlich hinaus.

Hingegen enthält Art. 11 Abs. 4 einen Ausnahmevorbehalt, der die grundsätzliche Benachrichtigungspflicht nach seinem Wortlaut erheblich relativiert. Danach dürfen die Mitgliedstaaten die Unterrichtung des Betroffenen aus einer Vielzahl von Gründen hinauszögern, einschränken oder unterbinden. Die Ausnahmegründe sind zudem durchweg sehr offen formuliert. So ermöglicht Art. 11 Abs. 4 lit. b ein Absehen von der Benachrichtigung „zur Gewährleistung, dass die Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten nicht beeinträchtigt" wird. Nach dem Wortlaut ist damit nicht erforderlich, dass es um die Straftaten geht, die den Anlass der Datenerhebung gebildet haben. Es muss sich nicht einmal um Straftaten handeln, an denen der Betroffene beteiligt ist oder mit denen er sonst in irgendeiner Verbindung steht. Insbesondere bei Ermittlungen in komplexen Strukturen der organisierten Kriminalität oder des Terrorismus könnte auf dieser Grundlage die Benachrichtigungspflicht weitgehend ausgehebelt werden. Solche Ermittlungen sollen vielfach ein fortlaufendes kriminelles Geschehen längerfristig beobachten und analysieren, um die betroffenen

27 Die Norm stimmt weitgehend mit Art. 6 DS-RL überein, zum Gehalt dieser Regelung *Albers*, in: Hoffmann-Riem/Schmidt-Aßmann/Voßkuhle, GVwR II, § 22 Rdnr. 49; s. nunmehr in angepasster Form Art. 5 DS-GVO-E.

28 Eingehend zum Verhältnis von Art. 8 GRCh und Art. 16 AEUV *J.-P. Schneider*, Die Verwaltung 44 (2011), 499, 502 ff.

29 Ähnlich *Ruffert*, EuGRZ 2004, 466, 468: „aktivistische Tendenz"; *Calliess*, JZ 2009, 113, 115: „expansive Entwicklung".

30 Vgl. bereits vor Verbindlichkeit der GRCh *EuGH*, EuZW 2006, 566, 570 – Parlament gegen Rat (Familienzusammenführung); eingehend *Matz-Lück*, in: dies./Hong, Grundrechte und Grundfreiheiten im Mehrebenensystem, 2012, S. 161, 179 ff.

31 In diese Richtung das Urteil *EuGH* MMR 2011, 122 – Schecke und Eifert, das sich allerdings kumulativ auf Art. 7 und Art. 8 GRCh stützt; a.A. *Kingreen*, in: Calliess/Ruffert, EUV/AEUV, 4. Aufl. 2011, Art. 8 GRCh Rdnr. 5; *J.-P. Schneider*, Die Verwaltung 44 (2011), 499, 501.

32 Der Stellenwert der Rspr. des *EGMR* i.R.v. Art. 52 Abs. 3 GRCh ist noch weitgehend ungeklärt, hierzu *Jarass*, GRCh, 2010, Art. 52 Rdnr. 65.

33 Vgl. zu TK-Überwachungen etwa *EGMR*, U. v. 6.9.1978 – 5029/71 – Klass u.a. gegen Deutschland; U. v. 16.2.2000 – 27798/95 – Amann gegen Schweiz; zu sonstigen Ermittlungsmaßnahmen etwa U. v. 25.9.2001 – 44787/98 – P.G und J.H. gegen Großbritannien – heimliche Aufzeichnung des gesprochenen Worts; U. v. 4.12.2008 – 30562/04 und 30566/04 – S. und Marper v. Großbritannien – Speicherung von DNA-Profilen und Fingerabdrücken; U. v. 2.9.2010 – 35623/05 – Uzun v. Deutschland – Überwachung mittels eines GPS-Empfängers. Eingehend *S. Schiedermair*, Der Schutz des Privaten als internationales Grundrecht, Habilitationsschrift Mainz 2011, Teil 3, A. VI. 5) c) und 6) d).

34 Näher *Naumann*, EuR 2008, 424, 430 ff.

Strukturen möglichst umfassend zu zerschlagen.[35] Es wird sich nahezu stets begründen lassen, dass eine Benachrichtigung dieses „operative" Ziel gefährdet. Auch die Ausnahmevorbehalte „zur Gewährleistung, dass behördliche oder gerichtliche Ermittlungen, Untersuchungen oder Verfahren nicht behindert werden" (Art. 11 Abs. 4 lit. a) und „zum Schutz der öffentlichen Sicherheit" (Art. 11 Abs. 4 lit. c) sind ausgesprochen weit gefasst.

Weiter dürfen die Mitgliedstaaten nach Art. 11 Abs. 5 Kategorien von Datenverarbeitungen festlegen, auf welche die Ausnahmeregelung nach Abs. 4 ganz oder teilweise anzuwenden ist. Dies dürfte so zu verstehen sein, dass für bestimmte Datenverarbeitungsarten eine Information des Betroffenen abstrakt-generell und damit ohne Rücksicht auf den Einzelfall ausgeschlossen werden kann.

Allerdings steht die Einschränkung der Benachrichtigung nach Art. 11 Abs. 4 unter dem Vorbehalt, dass sie verhältnismäßig ist. Die Anforderungen des Verhältnismäßigkeitsgrundsatzes sind wiederum auf der Grundlage der Unionsgrundrechte zu konkretisieren. Einschlägig ist auch insoweit Art. 8 GRCh. Hinzu tritt möglicherweise die Rechtsschutzgarantie des Art. 47 GRCh. Dazu müsste dieses Grundrecht – analog zur Rechtsprechung des *BVerfG* zu Art. 19 Abs. 4 GG[36] – Anforderungen an das behördliche Verfahren errichten, um einen wirksamen gerichtlichen Rechtsschutz zu ermöglichen.[37]

Wegen der zentralen Bedeutung der Benachrichtigung des Betroffenen nach einer heimlichen Ermittlungsmaßnahme sind die Ausnahmetatbestände des Art. 11 Abs. 4 daher restriktiv auszulegen. So wäre es unverhältnismäßig, die Benachrichtigung über einen längeren Zeitraum oder dauerhaft nur deshalb auszuschließen, weil ansonsten bestimmte Informationsquellen nicht mehr genutzt werden könnten[38] oder der Betroffene irgendwelche Rückschlüsse auf Arbeitsweise und Erkenntnisinteressen der Behörde ziehen könnte. Vielmehr ist grundsätzlich zu fordern, dass das Benachrichtigungsinteresse des Betroffenen mit den Geheimhaltungsbelangen der Behörde auf Grund aller relevanten Umstände des Einzelfalls abgewogen wird.[39] In der Folge dürfte Abs. 5, der den Mitgliedstaaten ermöglicht, die Benachrichtigung ohne solche Einzelfallabwägung auszuschließen, nur einen schmalen Anwendungsbereich haben.

Für das deutsche Recht relevant ist schließlich, dass Art. 11 eine Ausnahme von der Benachrichtigung des Betroffenen nicht bereits deshalb ermöglicht, weil die Datenerhebung seine Belange nur geringfügig berührt hat oder weil die Benachrichtigung aufwändig wäre. Der von beiden Senaten des *BVerfG* gebilligte[40] Ausschlusstatbestand in § 101 Abs. 4 Satz 4 StPO, nach dem Drittbetroffene bestimmter Ermittlungsmaßnahmen nicht zu benachrichtigen sind, wenn sie von der Maßnahme nur unerheblich betroffen wurden und anzunehmen ist, dass sie kein Interesse an einer Benachrichtigung haben, wäre daher mit der RL-E nicht vereinbar.

3. Datenübermittlungen in Drittländer

Art. 13 des Rahmenbeschlusses enthielt bislang lediglich eine Regelung für die Weiterleitung in Drittstaaten, wenn die Sicherheitsbehörden eines Mitgliedstaates personenbezogene Daten von Behörden eines anderen Mitgliedstaates erhalten hatten.[41] Art. 33 ff. sind demgegenüber bei jeder Übermittlung in ein Drittland zu beachten. Die Frage ist von besonderer Bedeutung, weil die so übermittelten Daten dort anderen – typischerweise weniger strengen – Verarbeitungsregeln unterworfen sind und beispielsweise bei Auslandsaufenthalten persönliche Nachteile mit sich bringen können. Grundvoraussetzung für alle Übermittlungen ist gem. Art. 33 lit. a, dass die Übermittlung zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Strafvollstreckung erforderlich ist. Hinzutreten muss nach Art. 33 lit. b ein Erlaubnistatbestand, nämlich Angemessenheitsbeschluss (Art. 34), geeignete Garantien (Art. 35) oder weitere Ausnahmetatbestände (Art. 36).

Angemessenheitsbeschlüsse können entweder auf der Basis von Art. 41 DS-GVO-E oder – dann sektorspezifisch für den Bereich des Sicherheitsrechts – nach Art. 34 Abs. 2–4 ergehen; Art. 34 Abs. 5 lässt auch die Feststellung des Fehlens eines angemessenen Schutzes zu. An die Stelle eines Angemessenheitsbeschlusses können nach Art. 35 Abs. 1 lit. a „geeignete Garantien" treten, wenn diese in einem rechtsverbindlichen Instrument vorgesehen sind. Anders als in Art. 42 Abs. 2 DS-GVO-E[42] werden weder diese Instrumente noch rechtliche Anforderungen an sie definiert, sodass ihr Effekt im Vagen bleibt. Art. 35 Abs. 2 lit. b lässt es sogar ausreichen, dass der Verantwortliche „alle Umstände beurteilt hat, die bei der Übermittlung personenbezogener Daten eine Rolle spielen, und zu der Auffassung gelangt ist, dass geeignete Garantien zum Schutz personenbezogener Daten bestehen". Dieses Vorgehen muss nach Art. 35 Abs. 2 zwar dokumentiert und die Dokumentation der Aufsichtsbehörde zur Verfügung gestellt werden. Eine normative Sicherung ist damit aber kaum noch verbunden: Ein rechtsverbindliches Instrument wird nicht verlangt, und die Garantien müssen überdies nach dem Wortlaut von lit. b nur in der ex ante-Perspektive der handelnden Personen bestehen.

Art. 36 ist schließlich mit „Ausnahmen" betitelt, enthält der Sache nach aber Vorschriften für die gesamte Tätigkeit der Sicherheitsbehörden. Allein Art. 36 lit. d lässt alle übrigen Übermittlungsvorschriften von Kapitel V überflüssig werden. Danach soll es als „Ausnahme" möglich sein, Daten in ein Drittland oder an eine internationale Organisation zu übermitteln, wenn dies zur „Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder zur Strafverfolgung erforderlich ist". Dies ist jedoch bereits nach dem wortgleichen Art. 33 lit. a erforderlich, sodass Art. 33 lit. a und lit. b (über Art. 36 lit. d) denselben normativen Inhalt haben. Die übrigen Regelungen des Kapitels sind daneben regelungstechnisch überflüssig und rechtsstaatlich schädlich, da sie vorgeben, ein Sicherungsmittel zu sein, das de facto nicht besteht. Der Schutzstandard bleibt damit letztlich sogar noch hinter der aktuellen Rechtslage zurück, da Art. 13 Abs. 3 lit. a des Rahmenbeschlusses eine Datenübermittlung ohne entsprechende Garantien des Drittstaats nur wegen „überwiegender berechtigter Interessen, insbesondere wichtiger öffentlicher Interessen" zulässt.

Im Ergebnis verzichtet die RL-E damit auf echte materielle Anforderungen an die datenschutzrechtlichen Regelungen in den Drittländern, an die die Sicherheitsbehörden personenbezogene Daten übermitteln. Dies sollte durch eine Beschränkung der Ausnahmeregelungen in Art. 36 geändert werden. Auch Art. 35 sollte deutlich restriktiver gefasst werden, um den Schutz des Betroffenen nicht weitgehend in das Belieben der übermittelnden Behörde zu stellen.

---

35 Näher zu solchen „operativen" oder „proaktiven" Ermittlungskonzepten *Weßlau*, Vorfeldermittlungen, 1989, S. 25 ff.; *Albers*, Die Determination polizeilicher Tätigkeit in den Bereichen der Straftatenverhütung und der Verfolgungsvorsorge, 2001, S. 108 ff.; *Kinzig*, Die rechtliche Bewältigung von Erscheinungsformen organisierter Kriminalität, 2004, S. 125 ff.

36 BVerfGE 100, 313, 361, 364; 109, 279, 363 f. = MMR 2004, 302; 118, 168, 207 f.; 125, 260, 334 ff.

37 Dafür *Jarass* (o. Fußn. 32), Art. 47 Rdnr. 48.

38 Vgl. zum deutschen Recht BVerfGE 109, 279, 366 f. = MMR 2004, 302; 113, 348, 390 = MMR 2005, 674; anders jedoch *BVerfG*, B. v. 12.10.2011 – 2 BvR 236/08 u.a. = ZD 2012, 123, Rdnr. 234 ff.

39 Vgl. zum deutschen Recht BVerfGE 120, 351, 375 f. = MMR 2008, 450.

40 BVerfGE 125, 260, 337; *BVerfG*, B. v. 12.10.2011 – 2 BvR 236/08 u.a. = ZD 2012, 123, Rdnr. 232.

41 Für den Datenaustausch zwischen den Mitgliedstaaten s. ausf. *Böhm* (o. Fußn. 24).

42 Dort wird insb. auf verbindliche unternehmensinterne Vorschriften, Standardschutzklauseln und genehmigte Vertragsklauseln verwiesen.

V. Ausblick: Zukunft des Grundrechtsschutzes im Sicherheitsrecht

Insgesamt enthält die RL-E neben einer Vielzahl von Verbesserungen und Präzisierungen für den Datenschutz im Sicherheitsrecht auch eine Reihe offener Fragen, insbesondere im Bereich der Übermittlungsvorschriften. Die grundlegenden materiellrechtlichen Vorgaben der RL-E sind überwiegend bereits im deutschen Recht enthalten, sodass sich bei der Verabschiedung des Entwurfs zwar in Teilbereichen, nicht aber grundsätzlich ein Anpassungsbedarf ergeben würde.

Mittelfristig ergibt sich das größte Veränderungspotenzial für die Bundesrepublik ausgerechnet im Hinblick auf Fragen, die auf den ersten Blick in der RL-E gar nicht geregelt sind. Diese könnte das Sicherheitsrecht der Mitgliedstaaten nämlich vor allem dann erheblich beeinflussen, wenn sie dazu führt, dass mitgliedstaatliche Normen an den Unionsgrundrechten zu messen sind. Auf Grund der bisherigen Rechtsprechung des *EuGH* zum Anwendungsbereich der Unionsgrundrechte[43] erscheint wahrscheinlich, dass der *EuGH* eine solche Grundrechtsbindung im Anwendungsbereich der RL-E bejahen wird. Damit würden die Unionsgrundrechte in weitem Umfang einen besonders sensiblen Regelungsbereich erfassen, der als Lackmustest für die rechtsstaatliche Schlagkraft einer Grundrechtsordnung dienen kann. Dies könnte weitreichende inhaltliche und vor allem institutionelle Konsequenzen haben.

Inhaltlich steht zwar nicht zu erwarten, dass der Schutz der Unionsgrundrechte flächendeckend über die Grundrechte des Grundgesetzes hinausginge. Denn zumindest der *Erste Senat des BVerfG* hat in jüngerer Zeit bereits hohe Anforderungen an kriminalbehördliche Datenverarbeitungsbefugnisse errichtet.[44] Hingegen könnten sich aus den Unionsgrundrechten durchaus einzelne Anforderungen ergeben, die den Schutzstandard des Grundgesetzes überschreiten. So hat der *EuGH* aus Art. 8 GRCh eine Pflicht der Gesetzgebungsorgane der EU hergeleitet, die Grundrechte der Betroffenen im Gesetzgebungsverfahren umfassend gegen die kollidierenden öffentlichen Belange abzuwägen.[45] Vergleichbare Berücksichtigungspflichten und Abwägungslasten des Gesetzgebers finden sich in der sicherheitsrechtlichen Rechtsprechung des *BVerfG* nicht.[46] Das *Gericht* prüft allein, ob das Gesetz als Ergebnis des Gesetzgebungsverfahrens materiell grundrechtskonform ist.

Für die Bundesrepublik besonders bedeutsam erscheinen die absehbaren institutionellen Auswirkungen, wenn Datenverarbeitungsregelungen im deutschen Sicherheitsrecht an den Unionsgrundrechten zu messen wären. Diese Auswirkungen beträfen zum einen das Verhältnis von *BVerfG* und Fachgerichten, zum anderen die Stellung des *EuGH* im Gefüge des europäischen Grundrechtsschutzes.

Jedes deutsche Gericht könnte und müsste in der Folge eine streitentscheidende Befugnisregelung unangewandt lassen, wenn sie ein Unionsgrundrecht verletzt. Das Verwerfungsmonopol des *BVerfG* aus Art. 100 Abs. 1 GG bliebe danach zwar rechtlich bestehen, würde aber faktisch deutlich relativiert. Unionsrechtlich wären die deutschen Gerichte hingegen nicht zwingend verpflichtet, den *EuGH* zu befassen, bevor sie eine deutsche Norm unangewandt lassen. Unterinstanzliche Gerichte müssten dies nie, und selbst für letztinstanzlich entscheidende Gerichte bestünde eine Vorlagepflicht nach Art. 267 Abs. 3 AEUV nur, wenn die maßgebliche Grundrechtsfrage noch nicht geklärt ist und sich auch nicht eindeutig beantworten lässt.[47] Zumindest hätte das Gericht in der Regel die Wahl, ob es ein Vorabentscheidungsersuchen an den *EuGH* oder eine Gültigkeitsvorlage an das *BVerfG* richtet.[48] In dieser Situation erschiene es aus fachgerichtlicher Perspektive angesichts der sehr restriktiven Rechtsprechung des *BVerfG* und der sehr großzügigen Rechtsprechung des *EuGH* zur Zulässigkeit von Richtervorlagen[49] durchaus attraktiv, zunächst den Weg über Art. 267 AEUV einzuschlagen.

Insgesamt wertet die RL-E den *EuGH* institutionell erheblich auf. Der *Gerichtshof* würde anders als die nationalen Verfassungsgerichte grundrechtliche Schutzgehalte für die ganze oder jedenfalls für den größten Teil der EU[50] festlegen. In der Folge dürften Bedeutung und faktischer Entscheidungsspielraum der nationalen Verfassungsgerichte in diesem zentralen Grundrechtsbereich deutlich schrumpfen. Zwar blieben die nationalen Grundrechte anwendbar, soweit die RL-E keine zwingenden Vorgaben macht.[51] Eine schlagkräftige Grundrechtsjudikatur des *EuGH* würde aber mittelfristig die Frage aufwerfen, welchen Sinn eine mehrfache Kontrolle des nationalen Sicherheitsrechts anhand unterschiedlicher Grundrechtskataloge ergibt. Zur Auslegung der Unionsgrundrechte müsste der Gerichtshof weiter zwar die EMRK und wohl auch die Rechtsprechung des *EGMR* heranziehen. Wie eng der *EuGH* nach Art. 52 Abs. 3 GRCh letztlich an die Konvention gebunden ist, ist aber bislang wenig geklärt.[52] Jedenfalls würde der *EuGH* regelmäßig vor dem *EGMR* befasst und könnte so die Initiative ergreifen. Zudem verfügt der *EuGH* anders als der *EGMR* wegen des Anwendungsvorrangs des Unionsrechts über quasi-kassatorische Befugnisse. Der *Gerichtshof* könnte so die Schlagkraft der Konvention mittelbar erhöhen, ihre unmittelbare Bedeutung jedoch zugleich vermindern.

Die RL-E installiert damit den *EuGH* als maßgeblichen Akteur des Grundrechtsschutzes im Sicherheitsrecht. Ob der *EuGH*, sollte die Richtlinie in Kraft treten, diese Rolle tatsächlich offensiv ausfüllt, dürfte allerdings auch davon abhängen, ob er sich zutraut, die damit verbundene Arbeitslast zu bewältigen.

Prof. Dr. Matthias Bäcker
ist Juniorprofessor für Öffentliches Recht an der Universität Mannheim.

Prof. Dr. Gerrit Hornung, LL.M.
ist Inhaber des Lehrstuhls für Öffentliches Recht, IT-Recht und Rechtsinformatik an der Universität Passau, der auch in das Institute of IT-Security and Security Law (ISL) der Universität eingebunden ist.

43 S.o. IV.1.
44 Vgl. etwa BVerfGE 107, 299; 109, 279; 110, 33; 113, 348; 115, 320; 120, 378; 125, 260.
45 *EuGH* MMR 2011, 122 – Schecke und Eifert; ähnliche Interpretationen des Urteils bei *Brink/Wolff*, JZ 2011, 206, 207; *Guckelberger*, EuZW 2011, 126, 130; *J.-P. Schneider*, Die Verwaltung 44 (2011), 499, 515.
46 Vgl. hingegen zu öffentlich-rechtlichen Leistungsansprüchen die dichten prozeduralen Vorgaben in BVerfGE 125, 175, 226 – Hartz IV; *BVerfG*, U. v. 14.2.2012 – 2 BvL 4/10, Rdnr. 163 ff. – Professorenbesoldung.
47 St. Rspr. seit *EuGH*, Slg. 1984, 1257 – CILFIT.
48 So für Art. 100 Abs. 1 GG BVerfGE 116, 202, 214 f.
49 Vgl. einerseits *Schlaich/Korioth*, Das Bundesverfassungsgericht, 8. Aufl. 2010, Rdnr. 145 ff., andererseits *Wegener*, in: Calliess/Ruffert (o. Fußn. 31), Art. 267 AEUV Rdnr. 21 ff., beide m.w.Nw.
50 Vgl. zur Geltung bzw. Bindungswirkung der RL-E für Dänemark, Irland und das Vereinigte Königreich EG 75 f.; zur Geltung der Unionsgrundrechte für Polen und das Vereinigte Königreich das Protokoll über die Anwendung der Charta der Grundrechte der Europäischen Union auf Polen und das Vereinigte Königreich v. 31.12.2007, ABl. Nr. C 306, S. 154.
51 So jedenfalls die st. Rspr. des *BVerfG*: BVerfGE 118, 79, 95 ff.; 125, 260, 306 f.; *BVerfG* NJW 2011, 3428, 3432 m. Anm. *Ritter*.
52 Näher *Kingreen* (o. Fußn. 31), Art. 52 GRCh Rdnr. 31 ff., m.w.Nw.