Der Austausch von Strafverfolgungsdaten zwischen den Mitgliedstaaten der Europäischen Union*

Von Prof. Dr. **Mark A. Zöller**, Trier

I. Vorbemerkungen

Die inhaltliche Auseinandersetzung mit Fragen des europäischen Straf-, Strafprozess- und Polizeirechts ist ein unangenehmes Geschäft. Das gilt auf Tagungen wie dieser zunächst einmal für die Referenten, aber leider auch für die geschätzten Zuhörer. Die fehlende Greifbarkeit des Europäisierungsprozesses im Recht der Inneren Sicherheit beginnt bereits mit seiner Unübersichtlichkeit. Selbst für Spezialisten und unter Zuhilfenahme von Google und Datenbanken ist es kaum noch möglich, zuverlässig zu beurteilen, wie der derzeit geltende Rechtszustand aussieht, ob die einmal glücklich gefundenen Rechtsakte tatsächlich noch in Kraft sind oder ob nicht längst neue Dokumente von EU-Organen, Ausschüssen, Task Forces oder Working Groups in eine ganz andere Richtung weisen. Sowohl im wissenschaftlichen als auch im praktischen Umgang mit transnationalen Sachverhalten, also Kriminalitätsstrukturen, die mindestens eine Staatsgrenze überschreiten, bleibt daher oft ein ungutes Gefühl. Man ertappt sich immer wieder bei dem frommen Wunsch nach einfachen und klaren Entscheidungsstrukturen für Gefahrenabwehr und Strafverfolgung. Diese sollten nach Möglichkeit dem rechtlichen Rahmen entstammen, in dem wir auf nationaler Ebene ausgebildet worden sind, auf die wir im Zweifelsfall schnell zurückgreifen können und die – Dank den Juristen – zwar nicht immer sprachlich einwandfrei, aber immerhin in unserer Muttersprache formuliert sind.

Für solche Wünsche scheint der sprichwörtliche Zug längst abgefahren. Und damit sind wir beim Generalthema unserer Tagung und bin ich beim Thema meines Referats. Die Entwicklung der Zusammenarbeit zwischen den Strafverfolgungs- und Gefahrenabwehrbehörden in Europa lässt sich bildhaft durchaus als Expresszug begreifen, der mit Höchstgeschwindigkeit auf zwei ganz andere Ziele zusteuert: Das erste Ziel liegt in einer Harmonisierung oder – wo dies praktisch nicht durchsetzbar ist (z.B. im Bereich politischer Straftaten) – zumindest in einer gegenseitigen Akzeptanz rechtlicher Strukturen und justizieller Entscheidungen. Das dahinter stehende Prinzip der gegenseitigen Anerkennung ist, konkretisiert an den Beispielen des Europäischen Haftbefehls und der Europäischen Beweisanordnung, bereits Gegenstand dieser Tagung gewesen. Das zweite Ziel, man kann auch sagen: der zweite Grundpfeiler der Polizeilichen und Justiziellen Zusammenarbeit in Strafsachen liegt im Austausch von Informationen auf dem Boden des sog. Grundsatzes der Verfügbarkeit. Danach sollen Informationen den Strafverfolgungsbehörden aus einem anderen EU-Mitgliedstaat grundsätzlich in derselben Art und Weise zugänglich gemacht werden wie den inländischen Verfolgungsbehörden.[1]

Dieser Grundsatz der Verfügbarkeit personenbezogener Informationen zielt letztlich darauf ab, sämtliche nationalen und supranationalen Informationssysteme in Europa zu vernetzen. Die darin enthaltenen Daten sollen für die Angehörigen der Sicherheitsbehörden europaweit unmittelbar abrufbar, speicherbar und übermittelbar sein. In seiner Reinform bedeutet der Grundsatz – zumindest innerhalb der EU – den Abschied von allen Irrungen und Wirrungen des Rechtshilfeverkehrs, vor allem aber von Frustrationen durch unverhältnismäßige Wartezeiten oder gar vollkommen ausbleibenden Reaktionen auf Seiten der ersuchten Staaten. Deutsche Ermittler müssten somit nicht erst auf die Antwort der Kollegen in Frankreich, Luxemburg oder Polen warten, sondern könnten sich mit der erforderlichen Zugangsberechtigung direkt in die Datenbanksysteme der ausländischen Kollegen einloggen und dort selbst nach den gesuchten Informationen recherchieren. Das ist die Zukunftsversion der Polizeilichen und Justiziellen Zusammenarbeit, die vor allem der Europäischen Kommission vorschwebt: aus den „*Intra*nets“ der 27 EU-Mitgliedstaaten und europäischer Sicherheitsagenturen (z.B. von Europol) soll in nicht allzu ferner Zukunft ein „europaweites *Inter*net“ i.S.e. Informationsverbunds aller Sicherheitsbehörden entstehen. Die Vorteile solcher rechtlichen Instrumente liegen damit vor allem für eine effektive Strafverfolgung auf der Hand, die sich einem ständigen Wettbewerbsvorsprung krimineller Strukturen im Bereich von Technik, Mobilität, Personal und finanziellen Ressourcen ausgesetzt sieht. Aber es lauern eben auch Gefahren für den Schutz der Grund- und Menschenrechte und die sensible Balance zwischen individueller Freiheit und kollektiver Sicherheit in Europa. Die prinzipiell wünschenswerte Existenz eines modernen europäischen Netzwerks von Informationssystemen verlangt als Kehrseite der Medaille einen einheitlichen und wirksamen Schutz der darin enthaltenen Daten – also einen Zugführer, der den Zug auch sicher in Richtung Europa steuert.

Um dies näher zu begründen, möchte ich Ihnen zunächst den aktuellen Stand der Dinge für den Austausch von Strafverfolgungsdaten zwischen den EU-Mitgliedstaaten skizzieren. Auf dieser Grundlage sollen sodann einige kritische Bemerkungen zu den gegenwärtigen Defiziten des europäischen Datenschutzes[2] sowie ein kurzer Ausblick folgen.

II. Rechtliche Instrumente auf europäischer Ebene

1. Das Europäische Rechtshilfeabkommen

Noch bis vor wenigen Jahren wurde der Rechtsrahmen für den Informationsaustausch in Strafsachen vor allem durch das bereits 1962 in Kraft getretene Europäische Rechtshilfe-

---

* Der Beitrag gibt die Textfassung des Vortrages wieder, den der *Verf.* am 5.11.2010 im Rahmen des Ersten Trierer Forums zum Recht der Inneren Sicherheit (TRIFORIS) mit dem Generalthema „Transnationale Strafverfolgung“ gehalten hat. Der Vortragsstil wurde beibehalten.

[1] Vgl. *Böse*, Der Grundsatz der Verfügbarkeit von Informationen in der strafrechtlichen Zusammenarbeit der Europäischen Union, 2007, S. 17.

[2] Ausführlich hierzu *Braum*, KritV 2008, 82; vgl. auch *Meyer*, NStZ 2008, 188 (192 f.).

übereinkommen[3] und seine Zusatzprotokolle gebildet.[4] Hierbei handelt es sich um eine Konvention des Europarates und damit nicht um EU-Recht. Sie enthält eine Reihe von Verpflichtungen der Vertragsstaaten zum Informationstransfer, beispielsweise zur Übermittlung von Auszügen und Auskünften aus dem Strafregister (Art. 13) oder zur Benachrichtigung über strafrechtliche Verurteilungen von Staatsangehörigen anderer Vertragsstaaten (Art. 22). Das allgemeine Rechtshilferecht setzt dem Informationsaustausch in Strafsachen aber von vornherein deutliche Grenzen. Es lässt naturgemäß keine Rechtshilfehandlungen zu, die gegen innerstaatliches Recht verstoßen. Außerdem steht der Datenaustausch trotz der grundsätzlichen Kooperationspflicht letztlich stets im Ermessen der beteiligten Vertragsstaaten, so dass für den ersuchenden Staat kein verlässlicher Anspruch besteht.

2. Rahmenbeschlussvorschlag der Kommission

Vor allem die Europäische Kommission hat daher in den vergangenen Jahren erhebliche Anstrengungen unternommen, um solche Hindernisse für den Austausch von Strafverfolgungsdaten zu beseitigen. Basierend auf den Leitlinien des sog. Haager Programms vom November 2004[5] hat sie im Jahr 2005 einen Vorschlag für den Erlass eines Rahmenbeschlusses des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit vorgelegt.[6] Ziel war die Schaffung eines neuen Konzepts für den Austausch von strafverfolgungsrelevanten Informationen zur Stärkung des Raumes der Freiheit, der Sicherheit und des Rechts. Dieses Ziel sollte insbesondere dadurch erreicht werden, dass die Mitgliedstaaten gleichwertigen zuständigen Behörden anderer Mitgliedstaaten sowie Europol alle Informationen zur Verfügung stellen, die diese zur Erfüllung ihrer gesetzlichen Aufgaben im Hinblick auf die Verhütung, Aufdeckung und Untersuchung von Straftaten benötigen (Art. 6). Diese Behörden der anderen Mitgliedstaaten sollten unmittelbar online auf die jeweiligen elektronischen Datenbanken zugreifen können (Art. 9). In Bezug auf Daten, hinsichtlich derer ein Online-Zugriff technisch nicht möglich ist, werden die Mitgliedstaaten zudem verpflichtet, sog. Indexdaten einzurichten (Art. 10), mit deren Hilfe die anfragenden Behörden darüber informiert werden, ob Daten verfügbar sind und von welcher staatlichen Stelle sie verwaltet werden. Rechtsstaatlich problematisch an dieser Initiative der Kommission, die den Grundsatz der Verfügbarkeit nahezu in Reinform verwirklichen wollte, war neben ihrer inhaltlichen Unbestimmtheit und dem Fehlen ausreichender Datenschutzvorschriften vor allem die Tatsache, dass die Straftaten, zu deren Verfolgung ein unmittelbarer Zugriff auf Strafverfolgungsdaten anderer EU-Mitgliedstaaten zulässig sein sollte, in keiner Weise näher festgelegt waren. Damit wären sogar Abfragen zur Aufklärung von Bagatellstraftaten möglich gewesen. Angesichts der Tatsache, dass jeder Transfer personenbezogener Daten jedenfalls aus deutscher Sicht als Grundrechtseingriff zu bewerten ist, dessen Rechtfertigung neben dem Bestimmtheitsgrundsatz auch dem Verhältnismäßigkeitsprinzip genügen muss, hat sich dieser Vorschlag zu Recht nicht durchgesetzt. Er wurde mit dem Inkrafttreten des Lissaboner Vertrages auch ausdrücklich aufgegeben.

3. Die „Schwedische Initiative"

Ein deutlich moderaterer Schritt stellt demgegenüber der Rahmenbeschluss des Rates vom 18.12.2006 über die Vereinfachung des Austausches von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union[7] dar. Dieser Rahmenbeschluss geht zurück auf einen Vorschlag des Königreichs Schweden aus dem Jahr 2004[8] und ist daher in der Praxis besser unter dem Stichwort „Schwedische Initiative" bekannt. Er enthält die Regeln, nach denen die Strafverfolgungsbehörden der Mitgliedstaaten wirksam und rasch bestehende Informationen und Erkenntnisse zum Zwecke der Durchführung strafrechtlicher Ermittlungen oder polizeilicher Erkenntnisgewinnungsverfahren austauschen können (Art. 1 Nr. 1). Neben den 27 EU-Staaten wollen sich auch Island, Norwegen und die Schweiz beteiligen. Kernbestand des Konzepts ist die Verpflichtung, Informationen und Erkenntnisse von einzelnen nationalen Strafverfolgungsbehörden auch den zuständigen Behörden der anderen Kooperationspartner auf deren Ersuchen hin zur Verfügung zu stellen. Der Fortschritt dieser Lösung gegenüber dem bisherigen Rechtshilferecht besteht vor allem in zwei Aspekten: zum einen dürfen die Bedingungen für die Zurverfügungstellung von Informationen und Erkenntnissen gegenüber den zuständigen Behörden der anderen EU-Mitgliedstaaten nicht strenger sein als die vergleichbaren Bedingungen auf nationaler Ebene (Art. 3 Nr. 3). Für den Informationsaustausch mit dem EU-Ausland müssen also grundsätzlich die gleichen Regelungen angewandt werden, wie für den innerstaatlichen Informationsaustausch. Diese Voraussetzung wird daher auch als Gleichbehandlungsgrundsatz bezeichnet. Zum anderen wird die Effektivität von Ersuchen durch strenge Fristen abgesichert (Art. 4). Sofern die gewünschten Informationen in einer Datenbank enthalten sind, muss die Antwort auf dringende Ersuchen innerhalb von acht Stunden erfolgen – eine für den Bereich der Rechtshilfe geradezu astronomische Geschwindigkeit. Keinesfalls darf sich der ersuchte Mitgliedstaat für die Mitteilung der erbetenen Information mehr als 14 Tage Zeit lassen. In der Praxis durchaus vorkommende Wartezeiten von 10 bis 20 Monaten würden somit der Vergangenheit angehören. Dennoch ist der Fortschritt durch die hoch gelobte „Schwedische Initiative" begrenzt: Der Sache geht es nicht um eine gegenseitige Verfügbarkeit von Daten, sondern nur um einen gleichberechtigten Zugang zu Informationen nach dem geltenden Recht des jeweiligen Mitgliedstaats.[9] Vor allem aber wird bei allen Vorschusslorbeeren und Vorbereitungsmaßnahmen in technischer und organisatorischer Hin-

[3] SEV Nr. 30.
[4] *Meyer*, NStZ 2008, 188 (189).
[5] Dazu *Meyer*, NStZ 2008, 188.
[6] KOM (2005) 490 endg.; dazu *Böse* (Fn. 1), S. 46 ff.; *Meyer*, NStZ 2008, 188 (190 f.).
[7] ABl. EG 2006 Nr. L 386, S. 89.
[8] Zur Entwurfsfassung *Böse* (Fn. 1), S. 39 ff.
[9] *Böse* (Fn. 1), S. 40; *Meyer*, NStZ 2008, 188 (190).

sicht immer wieder übersehen, dass der zugrunde liegende Rahmenbeschluss bis heute nicht in nationales Recht umgesetzt wurde, obwohl die Umsetzungsfrist am 19.12.2006 abgelaufen ist.[10] Die geltenden Vorschriften des Gesetzes über die internationale Rechtshilfe in Strafsachen decken die geplanten Neuerungen nicht ab, so dass derzeit jedenfalls in Deutschland keine gesetzliche Grundlage für ein Vorgehen nach den Grundsätzen der „schwedischen Initiative" besteht.

3. Der Prümer Vertrag

Die eigentliche Revolution für den Austausch von Strafverfolgungsdaten bleibt daher bislang dem Städtchen Prüm in der Eifel vorbehalten. Rund 60 km von unserem heutigen Tagungsort entfernt wurde dort im Mai 2005 mit dem sog. „Prümer Vertrag"[11] ein völkerrechtliches Abkommen unterzeichnet, dessen Auswirkungen auf die strafrechtliche Zusammenarbeit in Europa kaum überschätzt werden können. Inspiriert vom „Erfolgsmodell" der Schengener Abkommen hatten sich zunächst sieben europäische Staaten dazu entschlossen, in Fragen des Informationsaustauschs, aber auch in anderen Bereichen der grenzüberschreitenden Zusammenarbeit einen zusätzlichen Schritt voranzugehen. Unterzeichnerstaaten des Vertragswerks sind Belgien, Deutschland, Spanien, Frankreich, Luxemburg, die Niederlande und Österreich. Nach der Unterzeichnung sind dem Abkommen zudem auch Finnland, Slowenien und Ungarn beigetreten. Portugal, Italien, Bulgarien, Rumänien, Schweden und Griechenland hatten parallel dazu die Absicht zum Beitritt erklärt.

Der Prümer Vertrag leitet in der Ermittlungspraxis einen Paradigmenwechsel ein, weil er den Informationsaustausch nicht mehr von dem Erfordernis eines vorherigen Ersuchens um Auskunft abhängig macht. Er erlaubt vielmehr zum ersten Mal den direkten Online-Zugriff auf Indexdaten in den Datenbanken, die von den Behörden der anderen Vertragsstaaten geführt werden. Die Zugriffsberechtigung erstreckt sich dabei allerdings nicht unbeschränkt auf alle Datenbestände, sondern lediglich auf drei Datenkategorien, nämlich

- DNA-Analyse-Dateien (in Deutschland: die DNA-Datenbank des Bundeskriminalamts),
- Datenbanken mit elektronisch gespeicherten Fingerabdrücken (in Deutschland: das Automatisierte Fingerabdruckidentifizierungssystem AFIS) und
- elektronische Register mit Kraftfahrzeug- und Kraftfahrzeughalterdaten (in Deutschland: das Zentrale Fahrzeugregister des Kraftfahrt-Bundesamts).

Damit das Zugriffsrecht auf solche Datenkategorien nicht ins Leere läuft, werden alle Vertragsparteien verpflichtet, die dafür erforderlichen Daten selbst dann zu erheben und zu speichern, wenn diese nicht dem Zugriff der nationalen Gerichtsbarkeit unterliegen.

Sofern in Bezug auf DNA- und Fingerabdruckdaten der maximal einige Minuten in Anspruch nehmende Online-Zugriff im sog. „hit-/no hit-Verfahren" einen Treffer ergibt, ist im Übrigen auch die Übermittlung weiterer zu den Fundstellendatensätzen vorhandener personenbezogener Daten und sonstiger Informationen zulässig. Diese richtet sich dann aber in einem zweistufigen Verfahren nach dem innerstaatlichen Recht des ersuchten Vertragsstaates (Art. 5, 10). Der Prümer Vertrag erleichtert damit grundsätzlich nur die Beantwortung der Frage, *ob* in den Datenbanken der anderen Vertragsstaaten bestimmte Basisinformationen vorhanden sind. Für ausführlichere Inhalte bleiben die Behörden nach wie vor auf den mühsamen Weg des Rechtshilfeersuchens verwiesen.[12] Etwas anderes gilt lediglich für den Abruf von Daten aus Fahrzeugregistern. Hier soll die abrufende Vertragspartei nach Maßgabe ihres Rechts und unter Angabe einer vollständigen Fahrzeugidentifizierungsnummer oder eines vollständigen Kennzeichens einen direkten Lesezugriff auf Eigentümer-, Halter- und Fahrzeugdaten erhalten (Art. 12).

Sämtliche Daten- und Informationsübermittlungen werden in der Praxis durch so genannte „Nationale Kontaktstellen" durchgeführt (Art. 6 Abs. 1, 11 Abs. 1). Diese Aufgabe ist in der Bundesrepublik Deutschland für DNA-Analyse-Daten und Fingerabdrücke dem Bundeskriminalamt und für Kraftfahrzeugdaten dem Kraftfahrt-Bundesamt übertragen worden.

Deutschland befindet sich im Bereich des DNA-Datenabgleichs mittlerweile bereits mit Österreich (seit dem 6.12.2006), Spanien (seit dem 8.5.2007), Luxemburg (seit dem 23.5.2007), Slowenien (seit dem 16.6.2008) und den Niederlanden (seit dem 25.7.2008) im Wirkbetrieb.[13] Seit dem 1.6.2007 gleicht Deutschland auch daktyloskopische Daten mit Österreich ab. Im Bereich des Kfz-Register-Datenaustauschs hat Deutschland mittlerweile immerhin den Wirkbetrieb (mit Österreich, Spanien, Luxemburg, Niederlande und Frankreich) für vom Ausland eingehende Abfragen aufgenommen.

Erste Erfolge scheinen dem Prümer Modell Recht zu geben: Bereits im Dezember 2006 wurden zwischen Deutschland und Österreich 112.000 DNA-Datensätze abgeglichen. Allein dieser Datenabgleich führte in den ersten sechs Wochen in Deutschland zu mehr als 1.500 Treffern mit österreichischen Datensätzen und umgekehrt zu 1.400 Treffern in Österreich.[14] Der in den darauf folgenden Monaten auch mit anderen Staaten durchgeführte DNA-Datenaustausch machte jedoch deutlich, dass für die Bundesrepublik Deutschland die weit überwiegende Zahl der Treffer im Bereich der Diebstahlsdelikte, d.h. bei minder schweren Erscheinungsformen der Kriminalität liegt.[15] Offizielle Zahlen liegen bislang le-

[10] Art. 11 des Rahmenbeschlusses; vgl. nun aber den Entwurf eines Gesetzes über die Vereinfachung des Austauschs von Informationen und Erkenntnissen zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union (BR-Drs. 853/10) v. 31.12.2010.

[11] BGBl. I 2006, S. 1458; allg. dazu *Böse* (Fn. 1), S. 42 ff.; *Hummer*, EuR 2007, 517; *Papayannis*, ZEuS 2008, 219.

[12] *Hummer*, EuR 2007, 517 (520).

[13] BT-Drs. 16/14150, S. 2.

[14] *Hummer*, EuR 2007, 517 (519).

[15] Diese nahmen bis zum Juni 2007 immerhin 1.257 von 1.508 Treffern ein.

diglich für den Zeitraum bis Ende September 2009 vor.[16]

Danach gab es beispielsweise im Bereich des DNA-Datenabgleichs bei den Sexualdelikten seit Beginn des jeweiligen Wirkbetriebs mit Österreich 40, mit Spanien 22, mit den Niederlanden 31, mit Slowenien 4 und mit Luxemburg keinen Treffer. Bei den sonstigen Straftaten, hinter denen sich vor allem Eigentumsdelikte verbergen, waren es zu diesem Zeitpunkt allein mit Österreich 3.005, mit den Niederlanden 1.105 und mit Luxemburg 18 Treffer.[17] Bei den daktyloskopischen Daten ergab der deutsche Online-Zugriff auf österreichische Daten insgesamt 325 Treffer. Hier lagen klare Schwerpunkte im Bereich von Eigentumsdelikten, Verstößen gegen das Aufenthaltsgesetz, Betäubungsmittelkriminalität, Betrug und Urkundenfälschung.

Der Prümer Vertrag war von Anfang an so konzipiert, dass er (gem. Art. 1 Abs. 4) innerhalb der ersten drei Jahre nach seinem Inkrafttreten in das Recht der EU überführt werden sollte. Dieses Ziel ist mittlerweile erreicht. Am 23.6.2008 hat der Rat den Beschluss zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität[18] angenommen. Damit sind die wesentlichen Teile des Prümer Vertrages in den Rechtsrahmen der Europäischen Union überführt worden. Zu diesen „wesentlichen Bestandteilen" zählen vor allem die Bestimmungen über den Austausch von Daten zur Erstellung von DNA-Profilen, die Abgleichung von Fingerabdrücken sowie die Identifizierung von Fahrzeugen und deren Haltern. Damit hat sich der Prümer Vertrag – wie zuvor schon das Schengener Vertragswerk – von der völkervertragsrechtlichen Zusammenarbeit einiger weniger Staaten zum Modell für ganz Europa entwickelt. Von einer europaweiten Funktionsfähigkeit ist dieses in der Zukunft vermutlich bedeutsamste Ermittlungswerkzeug für transnationale Ermittlungen aber derzeit noch ein gutes Stück entfernt. Im Gegensatz zu anderen Inhalten des Ratsbeschlusses Prüm müssen die Mitgliedstaaten die Vorschriften zum Datenabgleich erst bis zum 26.8.2011 praktisch umsetzen.[19] Der vollständige Wirkbetrieb des Systems dürfte daher noch geraume Zeit auf sich warten lassen.[20]

III. Kritische Bemerkungen

Dennoch klingt das alles nach einer Erfolgsgeschichte – und das ist es auch, wenn man lediglich die Effektivitätssteigerung im Bereich des Austauschs von Strafverfolgungsdaten betrachtet. Zwar wird durch den Prümer Vertrag – im Gegensatz zum Vorschlag der Kommission – der Grundsatz der Verfügbarkeit nicht in Reinform umgesetzt, da eben nur ein Teil des zur Strafverfolgung verwendeten Datenmaterials unmittelbar abrufbar ist. Zudem kann überwiegend nur auf Indexdaten, nicht aber auf die vollständigen Datensätze zugegriffen werden. Ein Quantensprung ist es jedoch allemal! Und es bedarf keiner hellseherischen Fähigkeiten für die Erkenntnis, dass Prüm nur eine Momentaufnahme, eine Zwischenetappe auf dem Weg zu einem umfassenden europäischen Netzwerk von Datenbanken sein wird.

Für den straf- und strafprozessrechtlichen Blickwinkel ist vor allem die Erkenntnis von Bedeutung, dass die Bemühungen um eine effektivere transnationale Strafverfolgung zum Schutz kollektiver Sicherheitsinteressen den Datenschutz und damit den Individualschutz der Unionsbürger weitgehend auf der Strecke lassen. Es ist schon erstaunlich, dass wir uns auf europäischer Ebene Abstriche im Bereich des Datenschutzes zumuten, die wir uns auf nationaler Ebene unter dem wachsamen Auge des Bundesverfassungsgerichts nie gefallen lassen würden. Es wiederholt sich ein Muster, das uns bereits in den 1990er Jahren bei der Schaffung des europäischen Polizeiamts Europol begegnet ist: erst fängt man einmal mit der Arbeit an und später legt man sich dann in aller Ruhe ein paar passende und die einmal begonnene Arbeit möglichst nicht allzu sehr einschränkende Rechtsgrundlagen zu.

Um es deutlich zu sagen: für den Austausch von Strafverfolgungsdaten innerhalb der EU-Mitgliedstaaten gibt es nach wie vor keine ausreichenden allgemeinverbindlichen Datenschutzstandards auf europäischer Ebene. Und das nationale deutsche Datenschutzrecht, das durch das Bundesverfassungsgericht vor allem im Recht der Inneren Sicherheit in jahrzehntelanger Detailarbeit letztlich aus dem allgemeinen Persönlichkeitsrecht des Grundgesetzes (Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG) zu einem hohen Schutzstandard ausgeformt wurde, verpufft infolge des Anwendungsvorrangs des Unionsrechts auf europäischer Ebene ohne Wirkung. Befürworter eines raschen Ausbaus europäischer Formen der Informationskooperation verweisen in diesem Zusammenhang zu Unrecht auf das angebliche Vorhandensein einschlägiger Rechtsakte.

Die europäische Datenschutzrichtlinie aus dem Jahr 1995[21] war nach ihrem ausdrücklichen Wortlaut[22] schon im Zeitpunkt ihres Erlasses nur im Bereich des Gemeinschafts-

[16] Vgl. dazu die Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Ulla Jelpke, Inge Höger, Jan Korte, weiterer Abgeordneter und der Fraktion DIE LINKE v. 22.10.2009 (BT-Drs. 16/14150).

[17] BT-Drs. 16/14150, S. 4.

[18] ABl. EG 2008 Nr. L 210, S. 1. In Deutschland wurde der Ratsbeschluss Prüm durch das Gesetz zur Umsetzung des Beschlusses des Rates 2008/615/JI vom 23.6.2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität v. 31.7.2009 (BGBl. I 2009, S. 2507) innerstaatlich umgesetzt. Es ist seit dem 5.8.2009 in Kraft.

[19] Vgl. Art. 23 des Beschlusses 2008/616/JI des Rates vom 23.6.2008 zur Durchführung des Beschlusses 2008/615/JI zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität (ABl. EG 2008 Nr. L 210, S. 12.

[20] Zum aktuellen Umsetzungsstand vgl. Ratsdok. 5904/6/10 REV 6 v. 13.10.2010.

[21] Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. EG 1995 Nr. L 281, S. 31).

[22] Vgl. Art. 3 Abs. 2 der Richtlinie.

rechts, also für die Rechtsmaterien der früheren ersten Säule der EU, anwendbar. Auch nach dem Inkrafttreten des Vertrags von Lissabon zum 1.12.2009 mit der dadurch veranlassten Auflösung der Säulenstruktur und der Vergemeinschaftung der Polizeilichen und Justiziellen Zusammenarbeit in Strafsachen hat sich an diesem ausdrücklichen Ausschluss des Strafrechts aus dem Anwendungsbereich der Datenschutzrichtlinie nichts geändert.[23] Keine Abhilfe schafft entgegen verbreiteter Auffassung auch der lange umkämpfte Rahmenbeschluss des Rates vom 27.12.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden.[24] Ausweislich der Vorbemerkung Nr. 39 zu diesem Rahmenbeschluss bleiben neben weiteren Rechtsakten aus der früheren dritten Säule der EU insbesondere auch die Datenschutzvorschriften des Prümer Ratsbeschlusses unberührt. Die Formulierung „bleiben unberührt" ist hier i.S.v. „nicht anwendbar" zu verstehen. Der Rahmenbeschluss aus dem Jahr 2008 bietet somit gerade keine allgemeine datenschutzrechtliche Grundlage für den Austausch von Strafverfolgungsdaten in Europa.

Der einzig geltende Rechtsakt ist damit ein völkerrechtliches Abkommen der Mitglieder des Europarats aus dem Jahr 1981. Schließlich sind alle EU-Mitgliedstaaten gleichzeitig auch Mitglieder des Europarats. Konkret handelt es sich um das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten.[25] Es wurde zwar für die Praxis durch Empfehlungen des Ministerkomitees des Europarates aus den Jahren 1987 und 1992 konkretisiert.[26] Diese besitzen aber gerade keinen rechtsverbindlichen Charakter und ihr Schutzniveau liegt deutlich unter dem der EG-Datenschutzrichtlinie, die schon ihrerseits keinen überragend hohen Datenschutzstandard aufweist. Dass ein Rechtsakt aus Zeiten, in denen Begriffe wie Internet, E-Mail, Data Mining oder Data Profiling noch in ferner Zukunft lagen, keine geeignete Grundlage für den Umgang mit personenbezogenen Daten im 21. Jahrhundert sein kann, liegt auf der Hand.

Infolgedessen bleiben die von Datenspeicherungen Betroffenen zunächst auf das höchst heterogene nationale Datenschutzrecht für das jeweilige Datenbanksystem verwiesen. Hierin liegt zugleich eines der zentralen Probleme: für den Austausch von Strafverfolgungsdaten in Europa wird einfach ein nicht existierendes gemeinsames Datenschutzniveau unterstellt, anstatt es tatsächlich zu schaffen.[27]

Daneben gelten die jeweiligen bereichsspezifischen Datenschutzbestimmungen aus solchen Rechtsakten, auf deren Grundlage europäische Institutionen für die polizeiliche und justizielle Zusammenarbeit in Strafsachen etabliert worden sind. Gemeint sind diejenigen Bestimmungen, die nur für spezielle Anwendungsbereiche des Unionsrechts gelten, beispielsweise die Vorschriften zum Umgang mit personenbezogenen Daten im Europol-Ratsbeschluss, im Schengener Durchführungsübereinkommen oder eben im Prümer Ratsbeschluss. Gerade ein Blick in Letzteren zeigt jedoch, dass solche bereichsspezifischen Datenschutzregelungen allgemeinverbindliche Standards für sämtliche Bereiche der polizeilichen und justiziellen Zusammenarbeit oder gar des gesamten Unionsrechts nicht ersetzen können. Klare Bestimmungen über den Zweck der Erhebung und des Austausches von Daten, den von der Datenverarbeitung betroffenen Personenkreis und vor allem eine Eingrenzung der Straftaten, zu deren Aufklärung beispielsweise Informationen über genetische Merkmale genutzt werden dürfen, sucht man hier vergeblich.[28] Stattdessen bleibt eine Fülle von Fragen offen: Sind etwa erhebliche Eingriffe in das Recht auf informationelle Selbstbestimmung wie der Austausch und Abgleich von DNA-Daten zur Aufklärung von Bagatellstraftaten (z.B. Fahrrad- oder Ladendiebstählen) wirklich noch verhältnismäßig? Wie will man die materielle Rechtmäßigkeit einer transnationalen Informationsübermittlung insbesondere mit Blick auf den ordre-public-Vorbehalt überhaupt überprüfen? Ist nicht für eine Information, die sich einmal in einem national betriebenen, aber europäisch vernetzten Datenbanksystem befindet, der Grundsatz der Zweckbindung von personenbezogenen Daten und der damit verbundene Schutzgedanke für immer aufgehoben? Und lassen sich die nationalen Datenschutzvorschriften einfach dadurch aushebeln, dass man bestimmte Strafverfolgungsbehörden zwischen verschiedenen Staaten als vertrauenswürdig einstuft und danach für immer auf jegliche Kontrolle im Einzelfall verzichtet? Solchen Fragen kann man nicht durch bloßen Verweis auf den unabweisbaren europäischen Integrationsprozess ausweichen. Sie zu stellen hat nichts mit anti-europäischer Einstellung, sondern mit Rechtsstaatlichkeit zu tun.

Der Grundsatz der Verfügbarkeit dreht den Grundgedanken des Datenschutzes letztlich um. Staatliche Eingriffe in das Recht des Bürgers auf Privatheit bedürfen grundsätzlich nicht mehr der Rechtfertigung. Stattdessen werden wir in Zukunft wohl begründen müssen, warum wir im Einzelfall den Datenaustausch zum Schutz von Grund- und Menschenrechten blockieren wollen.

IV. Ausblick

Es bleibt somit die Frage, wie es weiter gehen wird mit dem Informationsaustausch auf europäischer Ebene. Ohne Zweifel ist dieser Informationsaustausch eines der wichtigsten Elemente der polizeilichen und justiziellen Zusammenarbeit. Die geltende Rechtslage – oder besser: Nicht-Rechtslage – hilft letztlich keinem Beteiligten weiter. Die Angehörigen der nationalen Sicherheitsbehörden werden in die unangenehme Lage versetzt, Eingriffe in Grund- und Menschenrechte der Bürger ohne ausreichende Rechtsgrundlage, also rechtswidrig

[23] *Hijmans*, ERA-Forum 2010, 219 (221).
[24] ABl. EG 2008 Nr. L 350, S. 60.
[25] SEV Nr. 108.
[26] Vgl. Empfehlung Nr. R (87) 15 des Ministerkomitees des Europarates vom 17.9.1987 über die Nutzung personenbezogener Daten im Polizeibereich sowie Empfehlung Nr. R (92) 1 des Ministerkomitees des Europarates vom 10.2.1992 über die Anwendung der DNS-Analyse im Rahmen der Strafrechtspflege.
[27] Vgl. auch *Braum*, KritV 2008, 82 (90).
[28] *Papayannis*, ZEuS 2008, 219 (247).

vornehmen zu müssen. Das schadet nicht nur der Legitimität und der gesellschaftlichen Akzeptanz ihrer Arbeit, mit der für uns alle ein Raum der Freiheit, der Sicherheit und des Rechts geschaffen werden soll. Vielmehr birgt es auch ein erhebliches Frustrationspotential für die Beamten, wenn die Nutzung neuer Ermittlungswerkzeuge nicht zu rechtsstaatlichen und damit nicht zu gerichtsfesten Beweismitteln führt. Schon im eigenen Interesse sollten Polizei und Staatsanwaltschaft hier massiv auf Nachbesserungen drängen. Auf der anderen Seite wird der Strafverteidiger zu peniblen Nachforschungen, teilweise auch im Ausland, hinsichtlich der Herkunft und Qualität von Informationen und Beweismitteln gezwungen, die möglicherweise zum Nachteil seines Mandanten verwertet werden. Erbitterte Kämpfe um Beweisanträge und über Beweisverwertungsverbote erscheinen damit vorprogrammiert. Und ganz nebenbei: Strafverteidigung mit derartigem Aufwand und dieser Güteklasse können sich ohnehin nur die wenigsten Beschuldigten tatsächlich leisten. Am wenigsten zu beneiden sind aber vermutlich die nationalen Gerichte, die solche Verwertungsfragen letztlich zu entscheiden haben werden. Hier dürfte auch der Grundsatz der freien richterlichen Beweiswürdigung an seine faktischen Grenzen stoßen.

Gerade der Vertrag von Lissabon hat die Bedeutung des Datenschutzes auf europäischer Ebene für die individuelle Freiheit der EU-Bürger noch einmal deutlich verstärkt. Gemäß Art. 16 Abs. 1 des neuen Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten. Und in Absatz 2 werden das Europäische Parlament und der Rat ausdrücklich dazu verpflichtet, Vorschriften über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union sowie durch die Mitgliedstaaten im Rahmen der Ausübung von Tätigkeiten, die in den Anwendungsbereich des Unionsrechts fallen, zu erlassen. Eine dem Art. 16 AEUV vergleichbare Regelung findet sich auch in Art. 8 der EU-Grundrechtecharta. Und schließlich wird derzeit durch den Rat und die Kommission auch der nach Art. 6 Abs. 2 des neuen EU-Vertrags vorgesehene Beitritt der EU zur Europäischen Menschenrechtskonvention (EMRK) vorbereitet. Mit dem Abschluss dieses Beitrittsverfahrens gelten damit auch unmittelbar auf EU-Ebene menschenrechtliche Gewährleistungen wie Art. 8 EMRK. Dieser schützt als Teilbereich des Rechts auf Achtung der Privatsphäre eben auch den Datenschutz im Sinne einer ungerechtfertigten staatlichen Erhebung, Speicherung und Verarbeitung von personenbezogenen Daten.[29]

Dass vor diesem Hintergrund gerade im Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen ein datenschutzrechtlicher Nachholbedarf besteht, wird durchaus auch in Brüssel erkannt. Insofern ist auch das sog. Stockholmer Programm[30] von der Überzeugung geprägt, dass Strafverfolgungsmaßnahmen und Maßnahmen zur Sicherung individueller Rechte, Rechtsstaatlichkeit und internationale Schutzregelungen miteinander der gleichen Richtung folgen und einander gegenseitig verstärken müssen. Teil dieses am 11.12.2009 verabschiedeten neuen Fünfjahresprogramms in der Nachfolge des Haager Programms ist auch eine umfassende Bestandsaufnahme der gegenwärtigen Rechtsinstrumente, Informationskanäle und technischen Lösungen, der eine grundlegende Evaluation folgen soll. In diesem Rahmen sollen sowohl die Schwedische Initiative als auch das Prümer Rechtsregime überprüft werden. Konkrete Empfehlungen sind im Laufe des Jahres 2011 zu erwarten. Wie auch immer diese ausfallen mögen, ob für eine neue allgemeine Datenschutzrichtlinie oder für eine Stärkung des bereichsspezifischen Datenschutzes in den bestehenden Rechtsakten[31]: im Vergleich zum gegenwärtigen Rechtszustand kann es nur besser werden.

[29] Vgl. nur *Grabenwarter*, Europäische Menschenrechtskonvention, 4. Aufl. 2009, § 22 Rn. 10; *Breitenmoser*, Der Schutz der Privatsphäre gemäß Art. 8 EMRK, 1986, S. 245.

[30] Ratsdok. 17024/09.

[31] Eine klare Festlegung lässt sich bislang auch der Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen über ein Gesamtkonzept für den Datenschutz in der Europäischen Union v. 4.11.2010 (KOM [2010] 609 endg.) nicht entnehmen.