Bundeskriminalamt

Deutscher Bundestag
Innenausschuss

Ausschussdrucksache
17(4)585 D

Der Präsident

POSTANSCHRIFT Bundeskriminalamt · 65173 Wiesbaden

HAUSANSCHRIFT Thaerstraße 11, 65193 Wiesbaden

TEL +49(0)611 55-0

An den

Innenausschuss des deutschen
Bundestages
z.Hd. Ministerialrat Dr. Heyncks

Platz der Republik 1
11011 Berlin

DATUM **19.10.2012**

In der Einladung zur öffentlichen Anhörung im Innenausschuss des Deutschen Bundestages am 22. Oktober 2012 wurde um eine vorherige schriftliche Stellungnahme zu folgenden Punkten gebeten:

- Vorschlag für 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,
- Bericht der Kommission zum Rahmenbeschluss 2008/977/JI,
- Mitteilung der Kommission zum Schutz der Privatsphäre in einer vernetzten Welt- Ein europäischer Datenschutzrahmen für das 21. Jahrhundert,
- Antrag verschiedener Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN „EU Datenschutzreform unterstützen“.

Die Stellungnahme des Bundeskriminalamtes (**BKA**) hierzu lautet wie folgt:

I. Richtlinienvorschlag

Das Datenschutzrecht in Europa soll grundlegend neu geregelt werden: Zum Einen durch eine unmittelbar geltende Verordnung, die für private und öffentliche Stellen gelten soll; zum Anderen durch eine Richtlinie, welche die Verarbeitung von personenbezogenen Daten durch Polizei- und Justizbehörden zum Zwecke der Verfolgung und Verhütung von Straftaten regeln

soll. Die öffentliche Anhörung des Innenausschusses wird sich, ausweislich der Einladung, mit dem Richtlinienentwurf befassen.

1. Schaffung einheitlicher Mindeststandards

Grundsätzlich steht das BKA einer Harmonisierung des Datenschutzrechts der EU-Staaten im Polizei- und Justizbereich positiv gegenüber. Die grenzüberschreitende Datenverarbeitung hat nicht nur in der Privatwirtschaft, sondern auch bei den Strafverfolgungsbehörden zugenommen. Diese Entwicklung wird sich auch in Zukunft fortsetzen. Die deutsche Sicherheitsarchitektur muss von Europa her gedacht werden. Strafverfolgung darf nicht an Landesgrenzen halt machen und erfordert daher eine weitere Intensivierung der grenzüberschreitenden Zusammenarbeit der zuständigen Strafverfolgungsbehörden. Für eine intensive Zusammenarbeit der Strafverfolgungsbehörden ist ein einheitlich hohes Datenschutzniveau in den Mitgliedstaaten unerlässlich. Nur ein solches schafft Vertrauen in den Datenaustausch und ermöglicht eine gute und effektive Zusammenarbeit und letztlich erfolgreiche Strafverfolgung in Europa.

Der Richtlinienentwurf hat das Ziel, einen umfassenden Rechtsrahmen für den Datenschutz zu schaffen, der dem Schutz personenbezogener Daten zugute kommen und zu einem reibungslosen Informationsaustausch zwischen Polizei und Justizbehörden führen soll. Diese Ziele will die Richtlinie durch die einheitliche Regelung der innerstaatlichen Datenverarbeitung von Polizei und Justiz im Bereich der Verfolgung und Verhütung von Straftaten erreichen. In diesem Zusammenhang muss man sich die Frage stellen, ob wir überhaupt einen neuen Rechtsakt auf europäischer Ebene über die Verarbeitung personenbezogener Daten brauchen. Das kann mit guten Gründen bezweifelt werden. Immerhin haben wir noch keine ausreichenden Erfahrungen mit der Umsetzung des Rahmenbeschlusses 2008/977/JI zum Datenschutz gesammelt. Dieser Rahmenbeschluss ist in einigen Staaten, so z.B. in Deutschland, noch nicht vollständig in innerstaatliches Recht umgesetzt worden. Die Erforderlichkeit eines neuen Rechtsaktes ist darüber hinaus durch die Europäische Kommission weder empirisch belegt, noch ausreichend fachlich begründet worden.

Ausweislich des Wortlauts des Richtlinienentwurfs[1] ist die nichtstraftatenbezogene Gefahrenabwehr vom Anwendungsbereich der Richtlinie ausgenommen und würde somit durch die Verordnung, die für private und öffentliche Stellen gelten soll, erfasst. Dies würde dazu führen, dass die Polizei zweierlei Datenschutzregime anwenden muss. Das BKA müsste z.B. im Rahmen der Abwehr von Gefahren des internationalen Terrorismus im Bereich der allgemeinen Gefahrenabwehr (§ 4 a Abs. 1 S. 1 BKAG) die Verordnung anwenden, im Bereich der straftatbezogenen Gefahrenabwehr (§ 4 a Abs. 1 S. 2 BKAG) hingegen die Richtlinie anwenden. Problematisch erscheint diese Zweiteilung auch im Bereich der gemeinsamen Datensammlungen, die für die straftaten- und nichtstraftatenbezogene Gefahrenabwehr existieren.[2] Zudem ist zu bedenken, dass die Verordnung nicht mit Blick auf die allgemeine polizeiliche Gefahrenabwehr, sondern die Privatwirtschaft und allgemeine Verwaltung geschrieben wurde und so die Gefahr besteht, dass Besonderheiten der Polizeiarbeit nicht ausreichend berücksichtigt wurden.

---

[1] Art. 1 und 2.

[2] Z.B. nach § 483 Abs. 3 StPO.

Aus Sicht des BKA wäre es wünschenswert, dass für alle Mitgliedstaaten einheitliche Mindeststandards geschaffen werden, von denen nationale Regelungen jedoch abweichen können. Eine Vollharmonisierung des innerstaatlichen Bereichs der polizeilichen Datenverarbeitung ist abzulehnen. Mit einer solchen Vollharmonisierung bestünde die Gefahr, dass eine schleichende Harmonisierung des Polizei- und Strafprozessrechts stattfindet. Bei einer isoliert aus datenschutzrechtlicher Perspektive geführten Diskussion ist zu befürchten, dass wichtige Aspekte des dahinterliegenden Fachrechts nicht ausreichend berücksichtigt werden. Zudem ist zu bedenken, dass es zum Teil erhebliche Unterschiede im Polizei- und Strafprozessrecht der Mitgliedstaaten gibt und mit einer Vollharmonisierung funktionierende und über Jahrzehnte erprobte und gewachsene Systeme gegebenenfalls geändert werden müssten.

Deutschland z.B. verfügt über ein ausdifferenziertes System, das die Grundrechte des Einzelnen auf der einen und die Interessen der Strafverfolgung auf der anderen Seite berücksichtigt. So finden sich detaillierte Regelungen zu Überwachungsmaßnahmen und Datenverarbeitungsprozessen in der Strafprozessordnung (**StPO**) und den Polizeigesetzen. Zudem gibt es eine umfangreiche Rechtsprechung des Bundesverfassungsgerichts (**BVerfG**), die sich mit Themen wie der Rasterfahndung, Onlinedurchsuchung oder Vorratsdatenspeicherung beschäftigt und den Schutz des Kernbereichs privater Lebensgestaltung definiert hat.[3] Dieses etablierte System sollte durch eine Vollharmonisierung auf europäischer Ebene nicht zerstört werden.

Außerdem haben Mindeststandards gegenüber einer Vollharmonisierung den Vorteil, dass nationale Regelungen sich weiterentwickeln können und so auf nationaler Ebene neue Standards erproben können.

2. Ausgewählte Probleme des Richtlinienentwurfs für die Strafverfolgungsbehörden

Aus polizeilicher Sicht enthält der Richtlinienentwurf verschiedene Problemkreise, welche die Effektivität der Strafverfolgung tangieren und die Arbeit der Polizei unnötig formalisieren könnten. Besonders anzusprechen sind die folgenden Punkte:

a) Die Regelungen zur Verarbeitung von „besonderen Kategorien von Daten“, wie z.B. Religion, politische Meinung, Gesundheit oder auch genetische Daten;
b) Die Regelung zum Profiling und auf automatischer Datenverarbeitung basierender Maßnahmen;
c) Die umfangreichen Informations- und Auskunftsrechte des Betroffenen;
d) Die Dokumentationspflichten;
e) Die Möglichkeit der datenschutzrechtlichen Überprüfung und die Kontrollbefugnisse der Aufsichtbehörde;
f) Die Koppelung der Datenübermittlung an Drittstaaten an Kommissionsbeschlüsse.

[3] Der Kernbereich der privaten Lebensgestaltung ist staatlicher Beobachtung absolut entzogen.

a) Besondere Kategorien von Daten

Der Richtlinienentwurf sieht vor, dass besondere Kategorien von personenbezogenen Daten (z.B. ethnische Herkunft, politische Meinung, Religion oder Überzeugung, Gesundheit, genetische Daten) grundsätzlich nicht verarbeitet[4] werden dürfen. Nur wenn die Verarbeitung durch eine „geeignete Garantie“ gestattet wird[5], die Verarbeitung zur Wahrung lebenswichtiger Interessen erforderlich ist, oder die Daten durch den Betroffenen offenkundig öffentlich gemacht wurden, soll eine Verarbeitung ausnahmsweise doch möglich sein.

Zweifelsohne sollten besonders sensible Daten einen besonderen Schutz genießen. Die Verarbeitung „besonderer Kategorien von Daten" ist für die polizeiliche Arbeit allerdings erforderlich.

Genetischen Daten sind zum einen für den eindeutigen Nachweis der Täterschaft, aber auch zum eindeutigen Ausschluss der Täterschaft und damit der frühzeitigen Einstellung von weiteren Ermittlungen gegen Unschuldige unerlässlich. So konnten mit der DNA-Analysedatei herausragende Ermittlungserfolge erzielt werden. Im Phänomenbereich Eigentumskriminalität z.B. spielt die DNA-Analysedatei bei der Fallaufklärung eine bedeutende Rolle und führt speziell beim automatisierten Spurenabgleich innerhalb der EU-Staaten immer wieder zu Fallzuordnungen oder Täteridentifizierungen. Beispielhaft sei hier ein Fall eines bewaffneten Juwelierraubs in Wien/Österreich genannt. Hier wurde eine DNA-Spur gesichert, zu der im automatisierten Datenabgleich ein Treffer mit einer deutschen DNA-Spur erzielt wurde, die bei einem bewaffneten Juwelierraub in Hagen/Deutschland gesichert wurde. Dadurch konnte zunächst ein Zusammenhang zwischen den beiden Straftaten festgestellt und, nachdem die Tat in Deutschland durch andere Maßnahmen geklärt werden konnte, auch die Tatverdächtigen für die österreichische Tat ermittelt werden. Ferner ist die Auswertung der DNA-Spuren ein wichtiges Instrument im Bereich der Zahlungskartenkriminalität.

Personengebundene Hinweise wie „bewaffnet“ oder „gewalttätig“ sind aus Eigensicherungsgründen und bei der Vorbereitung und Durchführung offener strafprozessualer Maßnahmen, wie z.B. bei der Entscheidung über die Einbindung Spezialkräfte, unerlässlich.

Im Bereich des islamistischen Terrorismus sind Kenntnisse über die Religion des Betroffenen unabdingbar. Es ist von erheblicher Bedeutung zu wissen, welcher religiösen Strömung eine Person angehört. Eine Person, die dem jihadistischen Salafismus anhängt, hat ein großes Gefährdungspotential. Das Wissen um eine mögliche Fanatisierung sensibilisiert für zukünftige Ermittlungsverfahren und offenbart Ansatzpunkte für die „Deradikalisierung“. Solche Informationen sind nötig, um das Gefahrenpotential eines Täters einschätzen zu können. Ähnliches gilt für den Bereich des Rechtsextremismus. Hier ist es erforderlich, auf Informationen über

---

[4] Verarbeitung umfasst nach der Richtlinie „jeden mit oder ohne Hilfe automatisierten Verfahren ausgeführten Vorgang oder jede Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Weitergabe durch Übermittlung, die Verarbeitung oder jede andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, das Löschen oder Vernichten der Daten sowie die Beschränkung des Zugriffs auf Daten“.

[5] Es ist unklar, was unter „geeigneten Garantien“ zu verstehen ist und wie solche Garantien umgesetzt werden sollen.

die politische Gesinnung eines Betroffenen zurückgreifen zu können, um rassistische, antisemitische oder fremdenfeindliche Täter- oder Gruppenstrukturen erkennen zu können.

In Deutschland werden die besonderen Kategorien von Daten durch verschiedene Rechtsvorschriften besonders geschützt und dürfen auch nur in diesen gesetzlich normierten Fällen verarbeitet werden. Dieser Schutz ist sinnvoll und wichtig. Nichts desto trotz zeigen die oben genannten Beispiele, dass die besonderen Kategorien von Daten für die polizeiliche Arbeit zur eindeutigen Identifizierung von Tätern und zum Eigenschutz unerlässlich sind. Daher spricht sich das BKA gegen ein generelles Verbot der Verarbeitung dieser Daten aus. Zwar sind die vorgesehenen Ausnahmen zum Teil so weit gefasst, dass einige der oben genannten Fälle hierunter subsumiert werden könnten, es muss hierbei aber immer beachtet werden, dass es sich um Ausnahmeregelungen handelt. Dies dürfte es verbieten, dass alle Fälle extensiv unter diese Ausnahmen subsumiert werden, sodass sich das Verhältnis von Regel und Ausnahme verkehrt. Es bleibt daher festzuhalten, dass die Fälle zu vielfältig sind, in denen die besonderen Kategorien von Daten benötigt werden, um sie nur in Ausnahmefällen zuzulassen. Aus Sicht des BKA wäre es daher sinnvoller, die Schutzwürdigkeit dieser Daten besonders herauszustellen und spezielle Regelungen für den Umgang mit ihnen einzufordern; nicht jedoch deren Verarbeitung für die polizeiliche Arbeit generell zu verbieten.

b) Auf Profiling und automatischer Datenverarbeitung basierende Maßnahmen

Art. 9 Abs. 2 des Richtlinienentwurfs sieht vor, dass die automatisierte Verarbeitung zum Zweck der Auswertung bestimmter persönlicher Aspekte von personenbezogenen Daten sich nicht ausschließlich auf die vorher beschriebenen besonderen Kategorien von Daten stützen darf. Ausnahmen von diesem Verbot sind nicht vorgesehen.

Ein Verbot der automatisierten Verarbeitung erscheint besonders problematisch im Bereich der DNA-Spuren. Bei DNA-Spuren ist die automatisierte Auswertung schon allein aufgrund des Umfangs und der zeitlichen Dringlichkeit notwendig. Nur mit einer automatisierten Auswertung ist eine zeitnahe Erhebung und Übermittlung weiterführender Ergebnisse möglich. Bei der Verwendung des Ergebnisses ist zudem zu berücksichtigen, dass damit keine endgültige Entscheidung verbunden ist. Das Trefferergebnis der DNA-Analysedatei ist vielmehr durch weitere Ermittlungsmaßnahmen zu verifizieren. Insbesondere wird ein möglicher Treffer durch eine Überprüfung eines Sachverständigen verifiziert, bevor das Ergebnis für weitere Maßnahmen verwendet werden kann. Insofern werden die DNA-Daten trotz automatisierter Verarbeitung geschützt.

Es ist zu befürchten, dass sich Art. 9 Abs. 2 des Richtlinienentwurfs auf die Aufgabenerfüllung des BKA und der Strafverfolgungsbehörden insgesamt negativ auswirkt und die Ermittlungsarbeit behindern könnte.

c) Umfangreiche Informations- und Auskunftsrechte des Betroffenen

Das deutsche Recht kennt bereits umfangreiche und detaillierte Regelungen zu Informations-, Auskunfts- und Akteneinsichtsrechten, insbesondere bei grundrechtsintensiven Eingriffen wie der Telekommunikationsüberwachung.

Kritisch erscheint das im Richtlinienentwurf vorgesehene umfassende, aber undifferenzierte Informationsrecht über die Datenerhebung. Nach § 11 Abs. 3 des Richtlinienentwurfs sollen die Personen zum Zeitpunkt der Erhebung oder, wenn die Daten nicht bei der Betroffenen Person erhoben werden, zum Zeitpunkt der Erfassung oder innerhalb einer angemessenen Frist nach der Erhebung detailliert über die Datenerhebung und ihre damit verbundenen Rechte informiert werden. Solche Informationspflichten erscheinen bei verdeckten Ermittlungen mit intensiven Grundrechtseingriffen sinnvoll und sind im deutschen Recht auch vorgesehen.[6] Ihr Nutzen bei offenen Maßnahmen erscheint allerdings fragwürdig. Und auch die im Richtlinienentwurf vorgesehenen Ausnahmen zum Informationsrecht scheinen nur verdeckte Maßnahmen im Auge gehabt zu haben und offene Maßnahmen nicht zu erfassen. Von der Informationspflicht ausgenommen seien sollen z.B. Fälle, in denen der Ermittlungserfolg oder die Öffentliche Sicherheit und Ordnung durch die Informationsmitteilung gefährdet wäre.

Eine umfassende, auch auf offene Maßnahmen anwendbare Informationspflicht würde vor allem die tägliche Arbeit der Landerpolizeien betreffen. So müsste nach der Richtlinie z.B. zukünftig jede Person, die im weiteren Umfeld eines Tatorts befragt wird, weil sie gegebenenfalls als Zeuge in Betracht kommt, unter anderem über folgende Dinge belehrt werden:

- Namen und Kontaktdaten des für die Verarbeitung Verantwortlichen und des zuständigen Datenschutzbeauftragten,
- die Zwecke der Verarbeitung, für welche die personenbezogenen Daten bestimmt sind,
- die Speicherfrist,
- Bestehen des Rechts auf Auskunft, Berichtigung oder Löschung der Daten,
- die Empfänger der Daten, auch in Drittländern oder in internationalen Organisationen (!).

(Aufzählung ist nicht abschließend)

Solche Regelungen können zu einem erheblichen administrativen Aufwand für die Beamten führen. Offene Maßnahmen, wie eine informelle Befragung eines potentiellen Zeugen, stellen naturgemäß einen geringeren Grundrechtseingriff in das Recht auf informelle Selbstbestimmung dar als verdeckte Maßnahmen. Es sollte daher überdacht werden, inwieweit, zusätzlich zu bereits bestehenden Belehrungspflichten, weitere Informationspflichten von Nöten sind, und ob bei informellen Befragungen Informationen über die gerade stattfindende Befragung aufgrund des nur geringen Grundrechtseingriffs und der Offensichtlichkeit der gerade stattfindenden Maßnahme überhaupt notwendig sind.

---

[6] § 101 StPO.

d) Dokumentationspflichten

Die Regelung in Art. 23 des Richtlinienentwurf zu Dokumentationspflichten könnte einen unnötigen bürokratischen Aufwand verursachen, da alle Datenverarbeitungsvorgänge – dies können auch nur marginale Daten-Eingaben durch einen Sachbearbeiter sein – einer gesonderten und erweiterten Dokumentation unterworfen werden. Bereits heute bestehen automatisierte, im Hintergrund laufende, umfängliche Protokollierungen bei den wichtigen polizeilich genutzten Datenbanken (z.B. INPOL, INPOL-Fall, ATD, RED). Ein Mehrwert für den Datenschutz des Betroffenen ist deshalb nicht erkennbar.

e) Befugnisse der Aufsichtbehörde

In Art. 46 des Richtlinienentwurfes ist vorgesehen, dass die Datenschutz-Aufsichtbehörde die Beschränkung, Löschung oder Vernichtung von Daten anordnen können soll. Ausgenommen von der Kontrolle und Anordnungsbefugnis soll die gerichtliche Datenverarbeitung sein. Die Datenverarbeitung von Polizei und Staatsanwaltschaft unterfällt hingegen der Kontrolle der Datenschutz-Aufsichtbehörde. Damit wäre es möglich, dass die Datenschutz-Aufsichtbehörde Daten im Ermittlungsverfahren löschen lässt. Das Löschen von Daten aus dem Ermittlungsverfahren kann jedoch einen Eingriff in die richterliche Beweiswürdigung und die Funktion des Strafverfahrens darstellen. Für den Richter können schließlich alle Informationen bei seiner Beweiswürdigung wichtig seien. Nur wenn dem Richter alle Informationen vorliegen, kann er sich ein umfassendes Bild vom jeweiligen Fall bilden. Die Befugnisse der Aufsichtbehörde sind daher unvereinbar mit dem deutschen System des einheitlichen Strafverfahrens.

Bei diesen Regelungen wird in besonderem Maße deutlich, dass eine EU weite Harmonisierung des Strafprozess- und Polizeirechts bisher aus guten Gründen nicht vorgenommen wurde. Die bereits erwähnte Ausnahmeregelung, dass nur die gerichtliche Datenverarbeitung von den Kontrollbefugnissen ausgenommen sein soll, schützt die Ermittlungsdaten in Systemen, in denen der Ermittlungsrichter eine starke Rolle hat (z.B. Frankreich), nicht jedoch Systeme, wie sie in Deutschland bestehen, in denen die Ermittlungen durch Staatsanwaltschaft und Polizei geführt werden. Eine Stelle außerhalb des Strafverfahrens sollte jedoch, unabhängig davon ob die Ermittlungen von einem Ermittlungsrichter oder von einem an Recht und Gesetz gebundenen Staatsanwalt durchgeführt werden, keine Befugnisse haben, die Beschränkung, Löschung oder Vernichtung von Daten im Ermittlungsverfahren anordnen zu können. Es muss sichergestellt sein, dass dem Richter im Strafverfahren alle Daten zu einer umfassenden Beweiswürdigung zu Verfügung stehen.

Diese erweiterten Kompetenzen der Datenschutz-Aufsichtbehörde könnte man zudem als unnötig ansehen, da Betroffenen in Deutschland der Rechtsweg offen steht, um eine rechtswidrige Datenverarbeitung zu unterbinden.

f) Datenübermittlung an Drittstaaten

Nach den Art. 33 ff. des Richtlinienentwurfes sollen personenbezogene Daten in Zukunft grundsätzlich nur an Empfänger in Drittstaaten oder an eine internationale Organisation übermittelt werden, deren Datenschutzniveau seitens der Kommission per Beschluss für angemessen erachtet worden ist. Stellt die Kommission hingegen fest, dass kein angemessenes Datenschutzniveau besteht, müssen die Mitgliedstaaten sicherstellen, dass eine Übermittlung personenbezogener Daten unterbleibt. In Abweichung zu den Vorgaben der Art. 34 und 35 soll eine Übermittlung in den in Art. 36 beschriebenen Fällen ausnahmsweise zulässig sein. Vorgesehen ist hierbei unter anderem, dass eine Übermittlung ausnahmsweise zulässig sein soll, wenn dies „zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten oder der Strafvollstreckung erforderlich ist“. Unter diese weitgefasste Ausnahme könnten viele Fallkonstellationen subsumiert werden, da Datenübermittlung zwischen Strafverfolgungsbehörden in aller Regel die Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten zum Zweck haben wird. Allerdings muss hier bedacht werden, dass es sich um eine Ausnahmevorschrift handelt, und es durch extensive Nutzung einer solchen Vorschrift nicht zur Umkehrung von Regel und Ausnahme kommen darf. In konsequenter Anwendung der Richtlinie und unter Berücksichtigung des Ausnahmecharakters dieser Vorschrift wäre eine Datenübermittlung daher im Regelfall an die Vorgaben der Listen gebunden.

Aus Sicht des BKA scheinen starre Listen in der schnelllebigen und sich ständig verändernden Welt kein taugliches Mittel, um schnell und effektiv auf Straftaten reagieren zu können. Politische Schwankungen in den Staaten widersprechen zudem einer „starren Liste“ und ermöglichen keine zeitnahen Anpassungen.

Die vorgesehene Regelung würde beispielsweise den internationalen Nachrichtenverkehr im Bereich des internationalen Terrorismus oder der OK-Kriminalität erheblich schwächen. Das BKA führt täglich im Rahmen der weltweiten INTERPOL-Personenfahndung in großem Umfang Schriftverkehr mit Drittländern. Im Jahr werden rund 2000 deutsche Interpol Personenfahndungen durchgeführt. Hierbei werden auch personenbezogene Daten übermittelt. Es ist davon auszugehen, dass von den 190 INTERPOL-Staaten ein großer Teil über keinen im Sinne der EU ausreichenden Datenschutzstandard verfügt bzw. diesen weit unterschreitet.[7] Dennoch ist für eine effektive Bekämpfung von Schwerkriminalität im Einzelfall eine Übermittlung personenbezogener Daten an diese Staaten erforderlich, wie es gegenwärtig auf der Grundlage des § 14 Abs. 7 BKAG auf der Basis einer Abwägungsentscheidung möglich ist. Hier werden im konkreten Fall jeweils die Interessen des Betroffenen gegen die öffentlichen Interessen abzuwägen sein. Eine von der EU-Kommission erstellte (starre) "Verbotsliste" von Staaten, an die (in aller Regel) mangels ausreichenden Datenschutzstandards personenbezogene Daten nicht übermittelt werden dürften, würde dieser Anforderung hiesigen Erachtens nicht ausreichend Rechnung tragen.

Zudem sollte bedacht werden, dass die Gefahr besteht, dass sich Straftäter in Staaten, die kein angemessenes Datenschutzniveau haben „verstecken“. Die Listen werden wohl öffentlich sein, und die Straftäter werden wissen, dass in diese Staaten in der Regel keine Daten über-

[7] Nur 80 Staaten werden auf einer Positivliste des Auswärtigen Amtes geführt.

mittelt werden und so eine erfolgreiche Fahndung unter Umständen nur schwer möglich sein würde.

Länderlisten der EU könnten allenfalls in Form von Empfehlungen an Stelle rein formaler, starrer Vorgaben durchaus ein hilfreiches Instrument bei der Beurteilung der schutzwürdigen Interessen sein und überdies dazu beitragen, ein einheitliches Niveau der Übermittlung an Drittstaaten innerhalb der EU zu erreichen. Es sollte jedoch weiterhin anhand des Einzelfall abgewogen werden können, ob eine Übermittlung in einen Drittstaat stattfindet oder nicht; dies dient sowohl dem Schutz des Betroffenen als auch der Wahrung des öffentlichen Interesses.

3. Zusammenfassung

Das Ziel einer Verbesserung des Datenschutzes ist generell zu begrüßen, und die EU-Datenschutzreform sollte als Anlass genommen werden, die deutschen Regelungen im Polizei- und Justizbereich zu untersuchen und auf ihre Aktualität hin zu überprüfen.
Abzulehnen ist allerdings eine Vollharmonisierung des innerstaatlichen Polizei- und Strafprozessrechts, die mit dem deutschen System unvereinbar ist, in die Beweiswürdigung des Gerichts eingreift, die Arbeit der Beamten unnötig formalisiert und eine internationale Strafverfolgung erschwert.

Zu begrüßen wäre die Schaffung von europaweiten Mindeststandards für die staatliche Datenverarbeitung. Die Mitgliedstaaten sollten aber die Möglichkeit haben, über diese Mindeststandards hinauszugehen und Regelungen einzuführen, die ihrem jeweiligen Strafverfolgungssystem entsprechen. Die derzeit vorgesehenen Regelungen der Richtlinie bieten eine solche Möglichkeit jedoch nicht. Sie sind zu starr und nicht ohne weiteres mit dem über Jahrzehnte gewachsenen deutschen System vereinbar.

II. Bericht der Kommission zum Rahmenbeschluss 2008/977/JI

Der Bericht befasst sich mit der Frage, ob und wie die Mitgliedstaaten ihrer Umsetzungspflicht aus dem Rahmenbeschluss 2008/977/JI nachgekommen sind. Deutschland hat den Rahmenbeschluss bisher noch nicht gesetzlich umgesetzt. Es existieren lediglich Verwaltungsvorschriften in Form von Anwendungshinweisen. Das BKA hat keine besonderen Anmerkungen zu diesem Bericht.

III. Mitteilung der Kommission „Der Schutz der Privatsphäre in einer vernetzten Welt - Ein europäischer Datenschutzrahmen für das 21. Jahrhundert

Die Mitteilung erläutert einerseits die Beweggründe und stellt zudem die Ziele der EU Datenschutzreform vor. Sie geht nur kurz auf den das BKA betreffenden Richtlinienentwurf ein und beschreibt, dass es das Ziel der Richtlinie ist, den Schutz der personenbezogenen Daten zu verbessern und einen reibungslosen Informationsaustausch zwischen den Polizei- und Justizbehörden zu gewährleisten. Diese Ziele sind zu begrüßen und sollten, wie oben bereits be-

schrieben, mittels Festsetzung von Mindeststandards, von denen nationale Regelungen abweichen können, angestrebt werden.

IV. Antrag Bündnis 90/DIE GRÜNEN: EU Datenschutzreform unterstützen (BT-Drs. 17/9166)

Der Antrag stellt klar, dass europäische Regelungen im Polizei- und Justizbereich aufgrund des zunehmenden grenzüberschreitenden Datenaustauschs nötig sind, eine Absenkung des deutschen Schutzniveaus allerdings verhindert werden muss. Dem stimmt das BKA entsprechend den unter I. angesprochenen Punkten zu. Die Kommission sollte hierbei nicht in die Kompetenz der Mitgliedstaaten eingreifen, die Details des nationalen Strafverfahrens selbst zu regeln.

Jörg Ziercke