

Terrorismus – Bestandsaufnahme durch Europol

Von Wolfgang Bogensberger

Nach den Terroranschlägen von Madrid (2004) und London (2005) konnten in der EU im vergangenen Jahr weitere Anschläge vor allem in Dänemark, Frankreich, Deutschland und im Vereinigten Königreich vereitelt werden. Laut Angaben von Europol¹ waren in der EU im Jahr 2007 dennoch insgesamt 583 Terroranschläge zu verzeichnen; davon entfielen allerdings 91% auf den separatistischen Terrorismus (vor allem im Baskenland und in Korsika). Die Zahl der wegen Terrorismus inhaftierten Tatverdächtigen stieg in der EU von 706 im Jahr 2006 auf 1044 im Jahr 2007. Das Internet hat sich zum zentralen Forum für die Verbreitung von ideologischer Propaganda bzw. von Bauanleitungen für Bomben entwickelt. Bei den terroristischen Aktivitäten in der EU gelangten – dem entsprechend - zunehmend selbstfabrizierte Bomben zum Einsatz. Eine signifikante Anzahl an EU-Bürgern und in der EU ansässigen Drittstaatsangehörigen wird zudem alljährlich für terroristische Zwecke in Drittstaaten rekrutiert (etwa für die Teilnahme am Jihad in Afghanistan, Irak und Somalia).

Anti-Terror-Rechtsetzungsaktivitäten der EU

Mit Blick auf das terroristische Bedrohungsszenario präsentierte die Kommission am 6. November 2007 mehrere Anti-Terror-Maßnahmen für die EU²:

Strafbarkeit der terroristischen Propaganda, des Anwerbens und der Ausbildung

Der Rahmenbeschluss zur Terrorismusbekämpfung aus 2002³ soll dahin ergänzt werden, dass er die Mitgliedstaaten - in Anlehnung an die Tathandlungen des Europaratübereinkommens zur Verhütung des Terrorismus vom 16. Mai 2005 - dazu verpflichtet, die „öffentliche Aufforderung zur Begehung einer terroristischen Straftat“ sowie die „Anwerbung für terroristische Zwecke“ und die „Ausbildung“ unter Strafe zu stellen. Der Zweck der Überführung dieser Europaratverpflichtungen in den Unions-Acquis liegt darin, den EU-eigenen Rechtsrahmen zu nutzen, der sich von jenem des Europarates vor allem durch ein höheres Maß an Schnelligkeit, Verbindlichkeit und Einheitlichkeit bei der innerstaatlichen Umsetzung und Anwendung unterscheidet⁴. Der Rat der Justiz- und Innenminister erzielte am 18. April 2008 eine *allgemeine Ausrichtung*⁵ zu diesem den Rahmenbeschluss zur Terrorismusbekämpfung ergänzenden Rahmenbeschluss; seine formelle Annahme sollte noch vor dem Jahresende 2008 erfolgen.

Präventionsmaßnahmen zur Verbesserung der Sicherheit von Explosivstoffen

Der „EU-Aktionsplan zur Verbesserung der Sicherheit von Explosivstoffen“ ergreift eine Reihe von präventiven Maßnahmen, welche die Sicherheit von Sprengstoffen, chemischen Grundstoffen und Sprengzündern verbessern und die Herstellung von Sprengkörpern für illegale Zwecke erschweren sollen. Dazu zählen unter anderem die Einrichtung eines Europäischen Netzes für die Entschärfung und Deaktivierung von Explosivstoffen, die Schaffung eines Frühwarnsystems für verlorengangene oder gestohlene Explosivstoffe sowie der Aufbau eines Euro-

päischen Bombendatensystems. Dieser EU-Aktionsplan ist vom Rat der Justiz und Innenminister am 18. April 2008 angenommen worden.

Verwendung von Fluggastdatensätzen (PNR-Daten)

PNR-Daten („Passenger Name Record“) sind Daten eines Passagiers zu seinen Flugreisebewegungen; sie beziehen sich auf die vom Fluggast bei der Buchung gemachten und bei der Abfertigung und beim Einstieg erfassten Angaben⁶. Durch die Erfassung und Auswertung von PNR-Daten sollen Strafverfolgungsbehörden Personen mit hohem Gefährdungspotenzial herausfiltern und sodann geeignete Maßnahmen ergreifen können.

Derzeit übermitteln die Fluggesellschaften solche PNR-Daten an die amerikanischen Grenzschutz- und Zollbehörden systematisch bei allen Flügen in die USA (auf der Basis eines Abkommens zwischen der EU und den USA, vgl. eu-update 4/2006, S. 128). Diese Praxis hat zur absurdre rechtlichen Situation geführt, dass die Fluggesellschaften solche Informationen zwar den Behörden der USA weitergeben, für die inner-europäische Situation gibt es jedoch keinen vergleichbaren Informationsmechanismus. Wenn man so will: Die USA bekommen von den europäischen Fluggesellschaften weit mehr Informationen als die zuständigen Behörden in der EU.

Diese informationelle Schieflage möchte der Kommissionsvorschlag zu einem „Rahmenbeschluss über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken“ beenden. Dieser strebt die Harmonisierung der Vorschriften der EU-Mitgliedstaaten zur Handhabung der PNR-Daten an. Dabei müssen die Fluggesellschaften, die Flüge aus einem oder in einen EU-Mitgliedstaat durchführen, die PNR-Daten an eine für die Auswertung der Daten und Durchführung der Risikoanalyse zuständige mitgliedstaatliche PNR-Zentralstelle übermitteln. Diese soll die PNR-Daten sammeln, analysieren und gegebenenfalls an die zuständigen Strafverfolgungsbehörden zum Zwecke der Verhütung und Bekämpfung von terroristischen Straftaten und organisierter Kriminalität weiterleiten, wobei zahlreiche Regeln und Rahmenbedingungen datenschutzrechtlicher Natur zu beachten sind. Die Daten sollen grundsätzlich für fünf Jahre nach Übermittlung gespeichert werden (mit Verlängerungsmöglichkeit bei akuten Bedrohungsfällen und behördlicher Genehmigung).

Die Annahme dieses Rahmenbeschlusses ist mittlerweile allerdings eher unwahrscheinlich geworden, zieht man einerseits die komplexe datenschutzrechtliche Problematik dieses Vorhabens und andererseits das sehr knappe Zeitfenster für die Annahme dieses Rechtsaktes in Betracht⁷.

Richtlinienumsetzung: Die Vorratspeicherung von Daten

Mit dem Begriff „Vorratsdatenspeicherung“ wird die Speicherung mehrerer Kundendaten durch Telekommunikationsanbieter auf Vorrat (also ohne konkreten aktuellen Verdacht) bezeichnet. Harmonisiert wird diese Form der Datenspeicherung in den Mitgliedstaaten durch die Richtlinie über die Vorratsdatenspeicherung⁸, die Anfang 2006 (also noch unter dem Eindruck der Terroranschläge vom 7. Juli 2005 in London) von Rat und Europäischem Parlament angenommen worden ist. Das Europäische Parlament stimmte der Richtlinie mit großer Mehrheit zu und im Rat stimmten lediglich Irland und Slowakei dagegen, wurden aber überstimmt. Irland, unterstützt von der Slowakei, reichte im Juli 2006 beim EuGH in Luxemburg die Nichtigkeitsklage gegen diese Richtlinie ein.

Die Richtlinie versteht sich als eine notwendige Maßnahme für die nationale oder öffentliche Sicherheit, zur Aufrechterhaltung der Ordnung, zur Verhütung von Straftaten oder zum Schutz der Rechte

und Freiheiten anderer. Laut ihrem 9. Erwägungsgrund hat sich die Vorratsspeicherung von Daten in mehreren Mitgliedstaaten als notwendiges und wirksames Ermittlungswerkzeug für die Strafverfolgung, insbesondere in schweren Fällen wie organisierter Kriminalität und Terrorismus, erwiesen. Aus diesem Grund soll die Speicherung der Telekommunikationsdaten sicherstellen, dass die Verkehrs- und Standortdaten (nicht aber auch die Inhaltsdaten, wie etwa E-Mails oder Gesprächsinhalte bei Telefonaten) sowie die Geräteidentifikationen für einen bestimmten Zeitraum zum Zweck der Ermittlung und Verfolgung von schweren Straftaten aufbewahrt werden. Die Aufbewahrungsfrist beträgt mindestens sechs Monate und höchstens zwei Jahre ab dem Zeitpunkt der Kommunikation.

Die Frist für die innerstaatliche Umsetzung ist mit 15. September 2007 festgelegt; die Richtlinie gibt den Mitgliedstaaten allerdings die Möglichkeit, die Umsetzung für die bestimmten Dienste (Internetzugang, Internet-Telefonie, E-Mail) um eineinhalb Jahre hinauszuschieben - also bis zum 15. März 2009; die meisten Mitgliedstaaten nehmen diese längere Umsetzungsfrist in Anspruch. Zahlreiche Mitgliedstaaten warten überdies auch mit der (Basis-) Umsetzung zu, sei es aus verfassungsrechtlichen (datenschutzrechtlichen) Problemen, aus Problemen im Zusammenhang mit der Tragung der Kosten der Speicherung oder auch aus rechtlicher Unsicherheit über den Fortbestand der Umsetzungsverpflichtung (bedingt durch das anhängige Nichtigkeitsverfahren vor dem EuGH). Wegen der sehr zögerlichen innerstaatlichen Umsetzung der Richtlinie hat die Europäische Kommission zwischenzeitig aber bereits gegen die säumigen Mitgliedstaaten das Vorverfahren zum Vertragsverletzungsverfahren eingeleitet.

Zum Verfahren vor dem EuGH: Irland bezweifelt mit seiner Nichtigkeitsklage die Rechtmäßigkeit dieser Richtlinie und möchte erreichen, dass der EuGH sie für nichtig erklärt, weil sie nicht auf einer gemeinschaftsrechtlichen Rechtsgrundlage, sondern auf einer solchen der *Dritten Säule* erlassen hätte werden müssen. Der einzige Zweck der Richtlinie bestehe darin, die Ermittlung, Entdeckung und Verfolgung schwerer Verbrechen, einschließlich des Terrorismus, zu erleichtern; dies falle aber nicht in die Zuständigkeit des Gemeinschaftsrechts⁹. Die irische Klage hat somit nicht die Frage zum Gegenstand, ob die Vorratsspeicherung mit den Grundrechten vereinbar ist; dieselbe Grundrechtsproblematik würde ja auch bei Annahme des Rechtsaktes im Rahmen der *Dritten Säule* bestehen. Allerdings kann der EuGH die Frage der Grundrechtskonformität der Vorratsdatenspeicherung im Rahmen dieses Verfahrens auch von sich aus aufgreifen. Aber gerade daran hätte Irland wohl kein Interesse, speichert es doch selbst die Vorratsdaten weit über den durch die Richtlinie vorgegebenen Maximalzeitraum hinaus; Irland steht vielmehr vor dem Problem, bei einer richtlinientreuen Umsetzung die bisher geltenden nationalen Speicherfristen drastisch reduzieren zu müssen.

Konträr dazu werden derzeit in anderen Mitgliedstaaten zum Teil recht heftige Auseinandersetzungen über die grundrechtskonforme innerstaatliche Umsetzung dieser Richtlinie geführt; vielfach wird die verdachtunabhängige Speicherung des Telekommunikationsverhaltens der gesamten Aufenthaltsbevölkerung als exzessiv eingestuft. In Deutschland liegen beim Bundesverfassungsgericht in Karlsruhe bereits Verfassungsbeschwerden zum „Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG“ vor. In seiner einstweiligen Anordnung vom 11. März 2008 hat das Bundesverfassungsgericht die Speicherpflicht für Telekommunikationsanbieter nicht ausgesetzt, sondern die Verwendung der gespeicherten Daten zum Zweck der Strafverfolgung bis zur Entscheidung

in der Hauptsache modifiziert zugelassen. Diese Modifikation besteht darin, dass die Telekommunikationsanbieter die verlangten Daten nur dann an die Strafverfolgungsbehörde übermitteln dürfen, wenn Gegenstand des Ermittlungsverfahrens eine schwere Straftat ist, die auch im Einzelfall schwer wiegt, der Verdacht durch bestimmte Tatsachen begründet ist und die Erforschung des Sachverhalts auf andere Weise wesentlich erschwert oder aussichtslos wäre. Ferner trägt das Bundesverfassungsgericht der deutschen Bundesregierung auf, ihm bis zum 1. September 2008 über die praktischen Auswirkungen der Datenspeicherungen und der einstweiligen Anordnung zu berichten.

Das Urteil des Bundesverfassungsgerichts über die Verfassungsbeschwerden zur innerstaatlichen Umsetzung sowie die Entscheidung des EuGH über die Nichtigkeitsklage zur Richtlinie werden frühestens Ende 2008/Anfang 2009 erwartet. Damit dauert die derzeitige rechtliche Unsicherheit in Bezug auf die Rechtmäßigkeit der Vorratsdatenspeicherung wohl noch einige Zeit an.

Dr. Wolfgang Bogensberger ist Leiter der Straflegislativektion im Bundesministerium für Justiz in Wien

Fußnoten:

- 1 TE-SAT Bericht für das Jahr 2008: <http://www.europol.europa.eu/publications/TESAT/TESAT2008.pdf>.
- 2 Abrufbar unter: http://eur-lex.europa.eu/LexUriServ/site/de/com/2007/com2007_0650de01.pdf, http://eur-lex.europa.eu/LexUriServ/site/de/com/2007/com2007_0651de01.pdf und http://eur-lex.europa.eu/LexUriServ/site/de/com/2007/com2007_0654de01.pdf.
- 3 Rahmenbeschluss 2002/475/JI des Rates vom 13. Juni 2002 zur Terrorismusbekämpfung (ABl. L 164, 22.6.2002, S. 3.)
- 4 Bei Rahmenbeschlüssen sind etwa – im Gegensatz zu Europaratserübereinkommen – keine langwierigen innerstaatlichen Ratifizierungsverfahren erforderlich; die zeitgerechte und rahmenbeschlußkonforme Umsetzung wird durch die Europäische Kommission überprüft und der EuGH legt die Vorschriften des Rahmenbeschlusses auf Ersuchen mitgliedstaatlicher Gerichte einheitlich aus.
- 5 Im Bereich der Dritten Säule hat sich die – vertraglich nicht vorgesehene – Übung eingebürgert, dass zwischen der politischen Einigung auf den Text eines Rahmenbeschlusses („allgemeine Ausrichtung“) und seiner förmlichen Annahme viel Zeit verstreicht. Denn in einzelnen Mitgliedstaaten ist die Zustimmung der jeweiligen Regierung zu einem EU-Rechtsakt an die Genehmigung des nationalen Parlamentes gebunden; davor prüft dieses aber zunächst den von der Regierung bereits fertig verhandelten Rechtsakt eingehend – in manchen Fällen kann das mehr als zwei Jahre dauern. Von einer solchen Prüfung sind derzeit mehrere Rahmenbeschlüsse betroffen, die „fertig“ verhandelt, aber noch nicht förmlich angenommen worden sind.
- 6 Dazu zählen im Einzelnen der PNR-Buchungscode, das Datum der Buchung/Flugscheinausstellung, das geplante Abflugdatum, der Name und die Anschrift des Fluggastes sowie Kontaktangaben (Telefonnummer, E-Mail-Adresse), alle Arten von Zahlungsinformationen einschließlich Rechnungsanschrift, der gesamter Reiseverlauf für eine Buchung, der Vielflieger-Eintrag, das Reisebüro/der Sachbearbeiter, der Reisestatus des Flugreisenden mit Angaben über Reisebestätigungen, Eincheckstatus, nicht angetretene Flüge (no show) und Flugreisende mit Flugschein, aber ohne Reservierung (go show), Angaben über gesplittete/geteilte Buchungen, allgemeine Hinweise, Flugscheindaten (Flugscheinnummer, Ausstellungsdatum, einfacher Flug (one-way), automatische Tarifanzeige, Sitzplatznummer, sonstige Sitzplatzinformationen, code-sharing, vollständige Gepäckangaben, Zahl und Namen von Mitreisenden im Rahmen einer Buchung).
- 7 Dritte-Säule-Rahmenbeschlüsse können nur noch bis zum Inkrafttreten des Lissabonner Vertrages angenommen werden, danach gibt es dieses Rechtsinstrument nicht mehr, weil auch die Dritte Säule abgeschafft wird.
- 8 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG (ABl. L 105, 13.4.2006, S. 54).
- 9 Damit befindet sich dieses Verfahren einmal mehr im Zentrum der europäischen Auseinandersetzung über die Reichweite der strafrechtlichen Zuständigkeiten im Gemeinschaftsrecht, vgl. eu-update NKP 2/2007, S. 79.