

Parlamentarisches Treffen des Europäischen Parlaments vom 2. bis 3. Oktober 2006 zum Thema "From Tampere to the Hague: Moving Forward? Progress and Shortcomings in the Area of Freedom, Security and Justice"

Vortrag des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, Peter Schaar, zum Thema

“Data exchange and data protection: What are the obstacles to the implementation of the principle of availability?”

Anrede,

die Themenüberschrift über der ersten Sitzung dieses parlamentarischen Treffens, suggeriert, dass der Datenschutz einen verstärkten Informationsaustausch zwischen den Polizei- und Strafverfolgungsbehörden der EU-Mitgliedstaaten behindere und damit einer effektiven Bekämpfung des internationalen Terrorismus und anderer Kriminalitätsformen, die die Bürger der Europäischen Union bedrohen, entgegenstehe.

Ich sehe dies anders. Auf nationaler Ebene findet bereits seit vielen Jahren zwischen den Strafverfolgungsbehörden ein intensiver Datenaustausch statt. Niemand wird ernsthaft behaupten, dass datenschutzrechtliche Anforderungen diesen unangemessen behindert hätten. Das Gegenteil ist der Fall: Regelungen zum Datenschutz bilden

vielmehr einen für alle Beteiligten verlässlichen Rechtsrahmen, innerhalb dessen es möglich ist, personenbezogene Daten zu Zwecken der Verhütung und Verfolgung von Straftaten zu erheben und zu verarbeiten. Sie bewirken zudem, dass bei Maßnahmen zur Gewährleistung von Sicherheit die bürgerlichen Freiheitsrechte angemessen berücksichtigt werden.

Auch auf EU-Ebene behindert der Datenschutz nicht den Informationsaustausch zwischen den Polizei- und Strafverfolgungsbehörden der EU-Mitgliedstaaten.

Das Schengener Durchführungsübereinkommen von 1990, das Europol-Übereinkommen von 1995 sowie diverse Rechtshilferegeln ermöglichen bereits seit langem einen umfangreichen personenbezogenen Datenaustausch. Die Rechtsakte enthalten umfassende Datenschutzregelungen, ohne dass dadurch die Zusammenarbeit beeinträchtigt würde. Dies zeigt sich auch daran, dass bei nachträglichen Änderungen der Übereinkommen und ganz aktuell, im Zusammenhang mit den Beratungen zu einem Schengener Informationssystem der 2. Generation, die Absicht besteht, die datenschutzrechtlichen Regelungen an die neuen Bedingungen und Funktionalitäten anzupassen, um damit den einmal erreichten Datenschutzstandard zu wahren.

Weitere Beispiele hierfür sind Eurojust und das Zollinformationssystem.

Der Informationsaustausch zwischen den Polizei- und Strafverfolgungsbehörden der EU-Mitgliedstaaten vollzieht sich jedoch mehr und mehr außerhalb der genannten Vertragswerke.

Nach den Terroranschlägen vom 11. September 2001 in den USA und vom 11. März 2004 in Madrid wurden zahlreiche Maßnahmen auf EU-Ebene zur Erhebung und Verarbeitung personenbezogener Daten zum Zwecke der Bekämpfung des Terrorismus und anderer schwerwiegender Straftaten beschlossen. Zu nennen wären hier u.a. der Rahmenbeschluss über den Europäischen Haftbefehl, die Verordnung zur Einführung biometrischer Daten in Pässen der EU-Bürgerinnen und -Bürger, die Richtlinie zur Fluggastdatenübermittlung zum Zwecke der Kontrollen an den EU-Außengrenzen, die – datenschutzrechtlich umstrittene - Richtlinie zur Vorratsdatenspeicherung von Telekommunikationsdaten sowie der auf Vorschlag der schwedischen Regierung gefasste Rahmenbeschluss zum erleichterten Informationsaustausch zwischen den Strafverfolgungsbehörden.

Zwar ist damit noch kein Informationsverbund der europäischen Sicherheitsbehörden in dem Sinne entstanden, dass deren Kenntnisse allen Strafverfolgungsbehörden in den EU-Mitgliedstaaten zum unmittelbaren Zugriff zur Verfügung stehen. Die Entwicklung dahin hat der Europäische Rat jüngst aber selbst vorgegeben: In dem von ihm im November 2004 verabschiedeten Haager Programm wird der Aufbau eines Raumes der Freiheit, der Sicherheit und des Rechts als eines der prioritären Ziele der Europäischen Union bestätigt. Unter anderem soll dies durch den Ausbau des grenzüberschreitenden Informationsaustauschs nach Maßgabe des sog. „Grundsatzes der Verfügbarkeit“ erreicht werden. Verfügbarkeit bedeutet, dass die Strafverfolgungsbehörden in einem Mitgliedstaat zur Erfüllung ihrer Aufgaben Zugang auf die Informationen der Strafverfolgungsbehörden in den anderen EU-Mitgliedstaaten haben sollen und letztere diese Informationen bereitzustellen haben, also eine Art Binnenmarkt für Zwecke der Strafverfolgung.

- 7 -

Niemand wird ernsthaft die Notwendigkeit einer guten Zusammenarbeit der Polizeien und Strafverfolgungsbehörden der EU-Mitgliedstaaten bezweifeln, insbesondere vor dem Hintergrund der Bedrohung durch den internationalen Terrorismus in Europa. Doch stellt sich gerade in dieser Situation die Frage, wie dies geschehen soll.

Die Vorschläge reichen von der Schaffung einer gemeinsamen europäischen Datenbank, in die alle relevanten nationalen Daten einfließen sollen, über die Vernetzung nationaler Dateien bis – in Anlehnung an den Prümmer Vertrag - zur gegenseitigen Einräumung eines Direktzugriffsrechts auf bestimmte Datenarten im Hit/no Hit-Verfahren und dem anschließenden Austausch personenbezogener Daten im Wege der Rechtshilfe im Falle eines Treffers.

Aber unabhängig davon, welche Maßnahmen beschlossen werden: Die Umsetzung des Grundsatzes der Verfügbarkeit führt zu einem erheblichen Anstieg des grenzüberschreitenden Austausches personenbezogener Daten zwischen den Polizei- und Justizbehörden in Strafsachen. Eine derartige Zusammenarbeit erfordert jedoch einen gleichermaßen hohen Datenschutzstandard in den EU-Mitgliedstaaten bezüglich der personenbezogenen Datenerhebung und -verarbeitung bei den Polizei- und Strafverfolgungsbehörden.

Dass die Datenschutzrichtlinie (95/46/EG) nicht auf Verarbeitungen betreffend die öffentliche Sicherheit und die Tätigkeiten des Staates im strafrechtlichen Bereich, also die 3. Säule anwendbar ist, hat erst kürzlich der Europäische Gerichtshof mit seiner Entscheidung bestätigt, in der er die Regelungen zur Übermittlung von Fluggastdaten in die USA für nichtig erklärt hat.

Es ist zudem evident, dass auch die Datenschutzkonvention 108 des Europarates von 1981 sowie die Grundsätze der Europaratsempfehlung (87) 15 für die Nutzung perso-

nenbezogener Daten im Polizeibereich zu allgemein gehalten sind, um den spezifischen Anforderungen eines datenschutzkonformen Informationsaustausches zwischen den EU-Staaten Rechnung zu tragen.

Der Umstand, dass in der 3. Säule eine datenschutzrechtliche Regelungslücke besteht, hat auch der Europäische Rat gesehen, als er das Haager Programm verabschiedet hat, denn er hat nicht nur für einen grenzüberschreitenden Austausch von personenbezogenen Daten im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen plädiert, sondern die Kommission inzidenter aufgefordert, gleichzeitig mit den Vorschlägen zum Informationsaustausch auch die notwendigen Regelungen zum Datenschutz zu schaffen. Aus Sicht des Persönlichkeitsschutzes ist das Haager Programm eine echte Herausforderung, bietet es doch eine einmalige Chance, die bei der polizeilichen und justiziellen Zusammenarbeit in Europa noch bestehende datenschutzrechtliche Regelungslücke zu schließen. Diese Chance gilt es im Interesse der Bürger zu nutzen.

Die Datenschutzbeauftragten der EU-Mitgliedstaaten haben es daher begrüßt, dass die Kommission im Oktober 2005 einen Vorschlag für einen Rahmenbeschluss vorgelegt hat zum Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, in Anlehnung an die Datenschutzrichtlinie von 1995. Nach den bisherigen Beratungen dieses Vorschlags im Rat lässt sich noch nicht vorhersagen, mit welchem Ergebnis die Verhandlungen enden werden. Ich habe derzeit den Eindruck, dass die Beratungen auf EU-Ebene eher langsam vorangehen. Soweit ich das richtig beurteilen kann, besteht bei einigen Regierungen der EU-Mitgliedstaaten Skepsis bezüglich der Notwendigkeit eines ent-

sprechenden Rechtsaktes. Zudem wird offenbar befürchtet, dass ein entsprechender Rahmenbeschluss zusätzliche bürokratische Hürden errichten werde.

Diese Befürchtung möchte ich entkräften.

Ein Rahmenbeschluss zum Datenschutz wirkt nicht bürokratisch, sondern trägt zur Vereinheitlichung des Verfahrens bei. Er führt dazu, dass das beim grenzüberschreitenden Informationsaustausch erforderliche gegenseitige Vertrauen entsteht, indem er für die Erhebung und Verarbeitung personenbezogener Daten durch die Polizei- und Strafverfolgungsbehörden der EU-Mitgliedstaaten sowie für die Wahrung des informationellen Selbstbestimmungsrechts der von der Verarbeitung Betroffenen einheitliche Standards vorgibt. Der grenzüberschreitende Datenaustausch würde durch einen Rahmenbeschluss zum Datenschutz damit eher erleichtert. Hindernisse für die Verwirklichung des Informationsaustausches nach dem Verfügbarkeitsgrundsatz ergeben sich vielmehr aus dem Fehlen harmonisierter Rechtsvorschriften in den EU-Mitgliedstaaten, insbesondere auf dem Gebiet des Strafrechts und des Strafverfahrensrechts.

Zudem gilt es, einen angemessenen Ausgleich zu den bereits bestehenden und künftig zu verwirklichenden Formen des Informationsaustausches zwischen den Strafverfolgungsbehörden in der Europäischen Union zu verankern und das derzeitige unausgewogene Verhältnis zwischen Gewährleistung von Sicherheit für die EU-Bürgerinnen und Bürger und Wahrung ihrer bürgerlichen Freiheitsrechte in einem „Raum der Freiheit, der Sicherheit und des Rechts“ wieder in das richtige Maß zu bringen.

Die Frage nach einem angemessenen Verhältnis zwischen diesen beiden Komponenten, die auf der jeweiligen nationalen Ebene längst ausdiskutiert und entschieden ist, muss auch auf europäischer Ebene einer befriedigenden Lösung zugeführt werden.

Der Rahmenbeschluss sollte die gesamte Informationsverarbeitung auf nationaler Ebene und beim Informationsaustausch mit andern Mitgliedstaaten, Drittstaaten und -stellen umfassen. Ziel ist ein einheitlicher Datenschutzstandard für die polizeiliche und justizielle Informationsverarbeitung in der gesamten EU, damit eine Divergenz der anzuwendenden Datenschutzregelungen vermieden wird. Insbesondere die tragenden Grundsätze der Zweckbindung, der Datenqualität und der Erforderlichkeit sind dabei zu wahren. Die Rechte des Betroffenen bei der Informationsverarbeitung müssen auf möglichst einheitlicher Grundlage gewährleistet sein. Das Recht auf Auskunft muss dabei Regelfall sein und darf nicht durch zu viele Ausnahmetatbestände ausgehöhlt werden. Neben der Gewährleistung einer unabhängigen Datenschutzkontrolle in jedem Mitgliedstaat muss zudem eine unabhängige Beratung des Rates durch die Vertreter der nationalen Datenschutzkontrollstellen sichergestellt werden.

Die Einsicht in die Notwendigkeit eines Datenschutzregimes in der 3. Säule wächst auf EU-Ebene erst langsam. Dabei sehe ich auch die Parlamente – sowohl das Europäische Parlament als auch die nationalen Volksvertretungen – in der Pflicht, auf die Regierungen der EU-Mitgliedstaaten entsprechend Einfluss zu nehmen. Auf gar keinen Fall darf es dazu kommen, dass auf europäischer Ebene immer neue Datenverarbeitungsbefugnisse für die Sicherheitsbehörden mit immer tieferen Einschnitten in Grundrechte beschlossen werden, ohne dass die Grundrechte der in der EU lebenden Bürgerinnen und Bürger mindestens in gleicher Weise gestärkt und geschützt werden.

Ich würde mich deshalb freuen, wenn die jetzige finnische und die kommende deutsche Ratspräsidentschaft das Projekt „Rahmenbeschluss zum Datenschutz in der 3. Säule“ zügig voran und zu einem guten Abschluss bringen könnten.