Stefan Braum

Europäischer Datenschutz und europäisches Strafrecht

Der Zusammenhang von europäischem Datenschutz und europäischer Strafrechtsentwicklung ist ein juristisch und bürgerrechtlich beunruhigendes Thema. Das liegt daran, dass es ein europäisch vernetztes, technologisch aufgerüstetes Netzwerk der Erhebung, Speicherung, Verarbeitung und Weitergabe personenbezogener Daten gibt, es jedoch an einem kohärenten, wirksamen Schutzsystem dieser Daten in Europa fehlt. Stellt man die Frage nach der justizförmigen Kontrolle europäischer Datenverarbeitung im sogenannten Raum der Freiheit, der Sicherheit und des Rechts, kann man derzeit noch ohne Übertreibung sagen: sie existiert nicht. Umfassende Datensammlung ohne ebenso umfassenden Rechtsschutz: Das ist ein beunruhigender Zustand. Datenschutzprobleme in Europa lassen sich auf drei Ebenen entfalten. Es geht erstens um Maßstäbe, die grenzübergreifend gelten (A). Zweitens lassen sich drei Problembereiche europäischer Datenverarbeitung beschreiben, die grenzübergreifend wirken (B). Und schließlich – drittens – geht es um ein Konzept justizförmiger Kontrolle europäischer Datensammlung, das grenzübergreifend schützt (C).

A. Grenzübergreifende Maßstäbe

I. Das Recht auf Datenschutz – ein Freiheitsrecht

Prinzipien des Datenschutzes ergeben sich aus diversen Rechtsquellen: Sie leiten sich ab aus dem Recht auf Privatheit, verankert in Art. 8 der Europäischen Menschenrechtskonvention. Sie resultieren aus verfassungsrechtlichen Traditionen der Mitgliedstaaten, sind Bestandteil europäischer Richtlinien und werden Element des neuen europäischen Grundlagenvertrages sein. Art. 8 Abs. 1 der EMRK gibt jeder Person das Recht auf Achtung ihres Privatlebens, ihrer Wohnung und ihrer Korrespondenz. Betrachtet man die Verfassungstraditionen der Mitgliedstaaten, sticht die Konzeption des deutschen Bundesverfassungsgerichts hervor, das ein Recht auf informationelle Selbstbestimmung aus den allgemeinen Freiheitsrechten ableitet.[1] Der neue Grundlagenvertrag integriert grundsätzlich die Charta der Grundrechte der Union und sieht ein Recht auf Datenschutz vor,[2] das zudem durch einen neuen Artikel 15a ergänzt wird, der die Europäische Union verpflichtet, nach ordentlichem Gesetzgebungsverfahren Datenschutzvorschriften für die Zuständigkeitsbereiche der Europäischen Union zu erarbeiten. Ergänzt wird das Recht auf den Schutz personenbezogener Daten durch ein Recht, Auskunft über erhobene Daten zu erhalten und gegebenenfalls deren Berichtigung zu erwirken.[3]

1 So genanntes Volkszählungsurteil des Bundesverfassungsgerichts, BVerfGE 65, 1 ff.
2 Artikel 68 Abs. 1 EU-Grundrechtecharta.
3 Artikel 68 Abs. 2 EU-Grundrechtecharta.

Das Recht auf den Schutz personenbezogener Daten ist ein grundlegendes Freiheitsrecht. Es folgt aus dem Freiheitsgedanken der Selbstbestimmung, selbst zu entscheiden, welche persönlichen Lebenssachverhalte offenbart werden sollen und welche nicht.[4] Im Unterschied zu einer bloßen Regel ist dieses Recht politisch nicht ohne weiteres verfügbar. Angesichts der technischen Möglichkeiten, personenbezogene Daten zu registrieren und in Sekundenschnelle europa-, ja weltweit abzurufen, bedarf die für europäische und staatliche Institutionen damit verbundene Kontrollmacht eines Gegengewichts. Eine Gesellschaftsordnung, in welcher der Einzelne nicht weiß, wo, was und zu welchem Zweck über ihn bekannt ist, wäre mit diesem Gedanken persönlicher Autonomie nicht zu vereinbaren.[5] Eine demokratische Gesellschaft hängt wesentlich von der aktiven Partizipation ihrer Mitglieder ab: Nichtwissen über das Wissen der Mächtigen aber erzeugt Unsicherheit, die den Verzicht auf aktiven Gebrauch von Grundrechten zur Folge haben kann.[6]

Es ist daher wichtig, das Recht auf Datenschutz in seinem Inhalt und in seinen Grenzen zu definieren So enthält schon das Sekundärrecht der Europäischen Union Ansätze europäischen Datenschutzes: Artikel 6 der Richtlinie 95/46 vom 24. Oktober 1995[7] konkretisiert das Recht auf Datenschutz durch ein paar wichtige Kriterien: Personenbezogene Daten dürfen nur zweckgebunden erhoben werden. Der Zweck der Datenerhebung muss eindeutig sein und rechtmäßig. Jegliche Weiterverarbeitung einmal erhobener Daten darf nicht einfach einen anderen, als den ursprünglich festgelegten Zweck verfolgen. Vor allem: Die Dauer der Speicherung ist nicht unbegrenzt. Auch sie hängt von dem Zweck der Datenerhebung ab. Personenbezogene Daten dürfen nur solange gespeichert werden, als der Zweck der Datenerhebung es erfordert.

In der Rechtsprechung des Europäischen Gerichtshofs werden diese Kriterien praktisch definiert. In seinem Urteil »Europäischer Rechnungshof vs. Österreichischer Rundfunk ua«[8], beharrt das Gericht im Anschluss an die Richtlinie 95/46 und die Bindung der Europäischen Union an Grundrechte auf einer strengen Zweckbindung der Datenverarbeitung und ergänzt sie um das Prinzip der Verhältnismäßigkeit und das allgemeine Bestimmtheitsgebot.

Verhältnismäßigkeit: Nicht nur der Zweck der Informationserhebung muss danach klar, eindeutig und rechtmäßig sein, auch die Datensammlung als Mittel, um diesen Zweck zu erreichen, muss sich als geeignet, erforderlich und angemessen darstellen. Ein Kriterium der Verhältnismäßigkeit besteht in der Wahrung eines öffentlichen Interesses, dem die Datensammlung zu dienen bestimmt ist, etwa wichtige Steuerungsaufgaben des europäischen Binnenmarkts.[9]

Allgemeines Bestimmtheitsgebot: Erfolgt ein Eingriff in das Recht auf Datenschutz, kann dieser nur aufgrund eines Gesetzes erfolgen, das Art und Ausmaß des Eingriffs

4 BVerfGE 65, 1 ff. (S. 40).
5 BVerfGE 65, 1 ff. (S. 41).
6 AaO.
7 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995, ABl. Nr. L 281/31 vom 23.11.1995.
8 Urteil vom 20. Mai 2004, Rs. C-465/2000, C-138/01 und C-139/01.
9 EuGH, aaO., Rz. 66 f. HH

für den Bürger objektiv vorhersehbar werden lässt.[10] Datenschutz und allgemeines Bestimmheitsgebot gehören eng zusammen. Soweit das Ideal. Indes: Es erweckt nur den Anschein eines wirksamen Konzepts europäischen Datenschutzes.

II. Datenschutz und Allgemeininteresse

Wo im Einzelfall die Grenzen des Rechts auf Datenschutz verlaufen, bleibt noch unklar. Schon die genannte Datenschutzrichtlinie 95/46 hat den groben Schönheitsfehler, dass deren Maßstäbe nur für den Bereich der noch existenten ersten Säule, also vor allem im Hinblick auf die Grundfreiheiten des Binnenmarktes, gelten. Für die polizeiliche und justizielle Zusammenarbeit gelten diese Maßstäbe nicht.[11] Beschränkungen des Datenschutzes ergeben sich bereichsspezifisch: Je nachdem, um welchen Bereich europäischen Rechts es sich handelt, können sie ganz verschieden sein. Für den Bereich der ersten Säule sind sie anders als im Bereich automatisierter Datensverarbeitung anlässlich polizeilicher Zusammenarbeit[12] und wiederum anders bei der Kontrolle von Immigration und wieder anders bei der justiziellen Zusammenarbeit im Bereich von Eurojust[13].

Vor allem aber kann es sein, dass Eingriffe in den Datenschutz durch ein überwiegendes Allgemeininteresse gerechtfertigt werden. Betrachtet man sich neuere Entwicklungen europäischer Datenverarbeitung, gewinnt man leicht den Eindruck, dass das Verhältnis von Allgemeininteresse und Datenschutzrechten längst aus der Balance ist – zum Nachteil des Individualrechts. Die folgenden Beispiele sollen dieses Problem verdeutlichen.

B. Probleme europäischer Datenverarbeitung

Die Probleme europäischer Datenverarbeitung sind unter anderem mit drei Stichworten verbunden: Schengen, Prüm und Vorratsdatenspeicherung. Alle Bereiche zeigen das Defizitprofil europäischen Datenschutzes deutlich. Sie symbolisieren aber auch einen wichtigen politischen Grundsatz der Europäischen Union bei der Definition des Datenschutzes. Ausgangspunkt ist der Grundsatz der Verfügbarkeit personenbezogener Daten in ganz Europa.[14] Daten sollen europaweit unmittelbar abrufbar, speicherbar und übermittelbar sein.

---

10 EuGH, aaO., Rz. 77.

11 Vgl. dazu Simitis, NJW 2006, 2011 (S. 2012).

12 Vgl. etwa Rechtsakt des Rates vom 12. März 1999 zur Festlegung der Bestimmungen über die Übermittlung von personenbezogenen Daten durch Europol an Drittstaaten und Drittstellen, ABl. C 88/1 vom 30.3. 1999.

13 Vgl. Beschluss des Rates vom 28. Februar 2002 über die Errichtung von Eurojust zur Verstärkung der Bekämpfung der schweren Kriminalität, ABl. Nr. L 63 vom 6.3.2002, dort Art. 14 – 27.

14 Vgl. bereits Rat der Europäischen Union, Haager Programm zur Stärkung von Freiheit, Sicherheit und Recht in der Europäischen Union, 16054/04, S. 18; Mitteilung der Kommission an den Rat und das Europäische Parlament – Das Haager Programm: Zehn Prioritäten für die nächsten fünf Jahre (...). KOM(2005), 184 endg, S. 7 f; Vorschlag für einen Rahmenbeschluss des Rates über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit, KOM(2005) 490 endg.

Ziel ist es, sämtliche EU-Informationssysteme miteinander zu vernetzen. Umfassende Verfügbarkeit personenbezogener Daten – dies ist ein ernstgemeinter Grundsatz, mag er auch auf den ersten Blick als Persiflage auf den Datenschutz erscheinen. Was steckt dahinter?

I. Der Grundsatz der Verfügbarkeit personenbezogener Daten

Der Grundsatz der Verfügbarkeit personenbezogener Daten dreht den Grundgedanken des Datenschutzes um: Der Staat wie auch europäische Institutionen müssen sich nicht primär vor dem Recht auf Privatheit rechtfertigen. Der Eingriff in die informationelle Selbstbestimmung des Bürgers ist nicht die Ausnahme. Als Anti-Terror-Maßnahme oder als Maßnahme der »Verbrechensbekämpfung« sollen alle notwendigen Informationen grenzübergreifend und möglichst ohne jegliches Hindernis für staatliche und europäische Behörden zugänglich sein. Nach dem Vorschlag eines Rahmenbeschlusses über den Austausch von Informationen nach dem Grundsatz der Verfügbarkeit[15] wird ein Netzwerk grenzübergreifenden Datentransfers entfaltet: Zum einen hat dieses Netzwerk bilateralen Charakter, soll es Strafverfolgungsbehörden doch möglich sein, jederzeit online auf Daten anderer Strafverfolgungsbehörden zuzugreifen.[16] Zum anderen ist der Ausbau zentraler Datenverarbeitungssysteme geplant. Europolbedienstete sollen etwa die automatisierte Datenverarbeitung des Europäischen Polizeiamtes um Informationen der nationalen Strafverfolgungsbehörden jederzeit ergänzen können.[17]

Nicht justizförmige Kontrolle stellt sich dabei als primäres Interesse des Rahmenbeschlusses dar, sondern Wirksamkeit des Datenaustausches. Leitlinien der Politik sind:

- den direkten Informationsaustausch zwischen Behörden sicherzustellen,
- ein EU-weites Informationssystem zu etablieren, mit dessen Hilfe sich generell feststellen lässt, welche Informationen vorliegen und wo sie vorliegen,
- unterschiedliche Bedingungen des Informationstransfers zwischen den Mitgliedstaaten zu harmonisieren, und dabei vor allem
- dafür zu sorgen, dass unterschiedliche Datenschutzstandards den Informationstransfer nicht unnötig behindern.[18]

Kurz: Es geht um umfassende Sozialkontrolle mittels Datensammlung, Datenschutz ist nur ein Gegenrecht.[19] Das liegt fern vom Prinzip des Datenschutzes, konstitutives Element einer freiheitlich verfassten europäischen Gesellschaft zu sein.

---

15 KOM(2005) 490 endg.
16 KOM(2005) 490 endg., S. 2.
17 KOM(2005) 490 endg., S. 3.
18 KOM(2005) 490 endg., S. 3f.
19 So etwa bei Böse, Der Grundsatz der Verfügbarkeit von Informationen in der strafrechtlichen Zusammenarbeit der Europäischen Union, 2007, S. 51 ff. Böse versteht Grundrechte nur als »Informationshilfegegenrechte« (S. 51): Das Recht auf Privatheit ist aber als subjektives Recht als solches konstitutiv für die Legitimität einer europäischen Rechtsordnung. Ein von diesem Recht losgelöstes Informationsrecht des Staates oder transstaatlicher Institutionen als solchem, das durch Grundrechte lediglich eingehegt würde, lässt sich nicht begründen. Es gibt kein *Prinzip* der Verfügbarkeit, sondern bestenfalls ein *institutionelles Interesse* nach umfassender Datenerhebung. Betrachtet man dieses Interesse als Prinzip, nimmt man bereits die kriminalpolitische Kapitulation vor dem dominanten Sicherheitsparadigma vorweg.

Freilich erkennt die Kommission auch, dass angesichts dieses deutlich erweiterten Umfangs der Datenverarbeitung der Datenschutz in Frage steht. So soll der Grundsatz der Verfügbarkeit durch einen weiteren Rahmenbeschluss zum Schutz personenbezogener Daten ergänzt werden.[20] Dieser Rahmenbeschluss hat zum Ziel, für den Bereich der Dritten Säule ein ähnliches Datenschutzniveau zu schaffen, wie es die Datenschutz-Richtlinie 95/46 für die erste Säule bereits vorsieht.[21] Jedoch bleibt der Umfang des Datenschutzes ambivalent.

Jeder vorgesehene Datenschutzgrundsatz wird durch eine Ausnahme brüchig: So wird der Anwendungsbereich auf den Bereich der Dritten Säule ausgedehnt, gilt aber gemäß Artikel 3 Abs. 2 des Rahmenbeschluss-Vorschlages weder für Europol noch für Eurojust – zwei Instanzen, die an der automatisierten Datenverarbeitung grenzübergreifend in maßgeblicher Weise beteiligt sind. Zwar darf die Datenerhebung nur zu einem rechtmäßigen Zweck erfolgen (Art. 4 Abs. 1 lit. b Rahmenbeschluss-Vorschlag), dürfen Daten nicht unbegrenzt gespeichert werden, darf die Zweckbestimmung einmal erhobener Daten nicht einfach ausgetauscht werden und gibt es präzise definierte Pflichten, die automatische Übermittlung personenbezogener Daten genau zu protokollieren (Art. 10), so dass der Weg des Datentransfers zurückverfolgbar erscheint. Zugleich aber ist der Personenkreis, der von einer Datenerhebung betroffen sein kann, deutlich erweitert. Nicht nur personenbezogene Daten von Personen, die einer Straftat verdächtig sind (Art. 4 Abs. 3, 1. Spiegelstrich), können erhoben und verarbeitet werden, sondern auch von Personen, bei denen lediglich die Vermutung besteht, dass sie künftig Straftaten begehen könnten (Art. 4 Abs. 3, 3. Spiegelstrich), darüber hinaus von Personen, die Hinweise zu Straftaten geben können (Art. 4 Abs. 3, 6. Spiegelstrich), oder die zu potentiellen Straftätern und Hinweisgebern in Kontakt stehen (Art. 4 Abs. 3, 7. Spiegelstrich).

Wesentlicher Bestandteil der Zweckbindung ist aber zum einen, dass man Gefahrenabwehr und Strafverfolgung sorgfältig trennt.[22] Zum anderen muss die Datenverarbeitung auch auf diese Zwecke beschränkt bleiben. Setzt man den Verdacht einer Straftat voraus, genügt die Vermutung, jemand könne irgendwann eine Straftat begehen, nicht.[23] Je weiter die Datenerhebung in das Vorfeld der Straftat reicht, um so strenger müssen die Grenzen des Rechts auf Datenschutz interpretiert werden.[24] Eine Differenzierung nach Intensität und Ausmaß des Eingriffs in das Recht auf Datenschutz sieht der Rahmenbeschluss nicht vor. Schließlich: Informationsrechte der Betroffenen stehen stets unter starken Vorbehalten öffentlichen Interesses. Informationen über die

20 Vorschlag für einen Rahmenbeschluss des Rates über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden vom 4.10.2005, KOM(2005) 475 endg.

21 KOM(2005) 475 endg., S. 7.

22 Aus der Rechtsprechung des Bundesverfassungsgerichts etwa BVerfG, 1BvR 2226/94 vom 14.7.1999, Rz. 241.

23 Vgl. aus der Rechtsprechung des Bundesverfassungsgerichts zum Beispiel BVerfG, 1BvF 3/92 vom 3.3.2004, Rz. 129.

24 Vgl. BVerfG, 1BvF 3/92 vom 3.3.2004, Rz. 161; vgl. auch BVerfG 1BvR 2226/94 vom 14.7.1999, Rz. 277.

Verarbeitung personenbezogener Daten können verweigert werden, um laufende Ermittlungen nicht zu gefährden oder um die öffentliche Sicherheit in den Mitgliedstaaten zu schützen (Art. 19 Abs. 2 lit. b und lit c Rahmenbeschluss-Vorschlag). Das sind stets gewichtige Argumente. Legt man sie auf die Waagschale, verliert das Recht auf Datenschutz an Gewicht. Der Grundsatz der Verfügbarkeit personenbezogener Daten dürfte langfristig das Recht auf den Schutz personenbezogener Daten aushöhlen.

II. Das Schengener Informationssystem

Es ist der Kern polizeilicher und justizieller Zusammenarbeit. An die Stelle der Kontrolle an den Binnengrenzen der Europäischen Union tritt ein computergestütztes und zentralisiertes System der Datenverarbeitung. Es dient dem Ziel, Datensätze über Personen, die zur Fahndung ausgeschrieben sind, grenzübergreifend zu erfassen, zu speichern und behördlich europaweit zu nutzen. Das Schengener Durchführungsübereinkommen, ursprünglich als vertragliche Vereinbarung zwischen den sogenannten Schengen-Staaten geschlossen,[25] ist durch den Vertrag von Amsterdam in europäisches Recht überführt.[26] Bereits unmittelbar nach der Einführung des Schengener Informationssystems wurden bereits 3, 9 Millionen Datensätze gespeichert. Bis zum Jahre 2003 kletterte die Anzahl der elektronisch registrierten Datensätze auf 11, 3 Millionen.[27] Nun soll dieses Datenverarbeitungssystem weiter ausgebaut werden. Damit verbindet sich ein formelles und ein inhaltliches Problem:

Das formelle Problem besteht im Stile der Gesetzgebung, der sich nun auch bei der Einrichtung des Schengener Informationssystems II beobachten läßt. Regeln und technische Grundlagen dieses Systems werden auf Regierungsebene ausgehandelt. Die Verwaltung der Europäischen Union, insbesondere die Kommission, schafft technische Fakten. Bevor ein Parlament inhaltlich zu Art und Umfang des Datenschutzes im Schengener Informationssystem Stellung nehmen kann, werden Art und Umfang der Datenerhebung exekutivisch festgelegt und zudem technisch umgesetzt.[28] Ohne öffentliche Debatte hat die Europäische Kommission – gestützt auf ein Mandat des Rates und auf mehrere Machbarkeitsstudien – bereits im Jahre 2003 die öffentliche Ausschreibung zur Hard- und Softwareentwicklung des SIS II-System eingeleitet. Gegen solche Sachzwänge kommt kein Parlament mehr an – eine echte demokratische Mitsprache findet nicht statt. Dies gilt um so mehr als die Integration des Schengen Besitzstandes in das Recht der Europäischen Union das generelle Kompetenzproblem europäischer Gesetzgebung widerspiegelt.

Mangels eindeutiger Zuordnung zu den Sachbereichen der ersten Säule bzw. zu der Politik der Dritten Säule wurde die Kompetenzgrundlage für das Schengener Informa-

25 Übereinkommen zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985, ABl. Vom 22.9.2000, S. 19 ff.

26 Vgl. Protokol Nr. 2 zum Vertrag über die Europäische Union zur Einbeziehung des Schengenbesitzstandes in den Rahmen der Europäischen Union (1997); Beschluss des Rates 1999/34/EG vom 20. Mai 1999, ABl. Nr. L 176 vom 10. Juli 1999, S. 1.

27 Vgl. Leutheusser-Schnarrenberger, ZRP 2004, 97 ff. (S. 97).

28 Kritisch Leutheusser-Schnarrenberger, ZRP 2004, 97 ff. (S. 99).

tionssystem einfach geteilt. Geht es um Visa- und Immigrationsfragen stützt sich Schengen noch auf das Gemeinschaftsrecht, alle Bereiche der polizeilichen und justiziellen Zusammenarbeit zählen noch zu dem Bereich der Dritten Säule. Im Hinblick auf die Einrichtung des SIS II existieren daher auch zwei Gesetzgebungsvorschläge: Der Vorschlag für eine Verordnung eines Schengener Informationssystems der zweiten Generation betrifft Immigrationsfragen und andere Sachbereiche des Gemeinschaftsrechts.[29] Dagegen erfasst der Vorschlag für einen Beschluss des Rates über dasselbe System die polizeiliche und justizielle Zusammenarbeit.[30]

Daraus folgt: Es gibt zwei Gesetzgebungsprozeduren – mal mit, mal ohne Beteiligung des Europäischen Parlaments, es gibt auch zwei Arten des Datenschutzes – mal kohärent im Rahmen der Datenschutzrichtlinie, mal bereichsspezifisch zersplittert, je nachdem, wer, wo und wann an welche Information gelangen will. Vor allem: Mal unter der eindeutigen justiziellen Kontrolle einer europäischen Gerichtsbarkeit, mal aber nationalen Rechtsinstanzen mit heterogenem Datenschutzniveau unterstehend oder gar – soweit es Europol betrifft – ganz ohne europäische richterliche Kontrolle.[31] Wenn Datenschutz Transparenz voraussetzt, dann spiegelt sich im Schengener Informationssystem bereits in seiner Genese das genaue Gegenteil wider: Das ist dem Vertrauen in einen europäischen Datenschutz abträglich.

Wie so oft transportiert die Form auch den Inhalt. Das Demokratiedefizit zieht das Rechtsschutzdefizit nach sich – und umgekehrt. So drängt sich manchen Datenschützern der Eindruck auf, das Schengener Informationssystem der zweiten Generation gerate völlig außer Kontrolle.[32] Dies liegt unter anderem an der verstärkten Vernetzung des Systems und an der deutlichen Erweiterung der Ausschreibungskategorien.[33] So sollen Europol, Eurojust, Staatsanwaltschaften, Nachrichtendienste, Kfz-Zulassungsstellen, Finanzbehörden aber auch nicht staatliche Stellen wie Kreditinstitute oder Fluggesellschaften online Zugriff auf die in SIS II gespeicherten Daten haben.[34] Man schafft neue Speicher-, Übermittlungs-, und Abrufmöglichkeiten für biometrische Daten, wie Lichtbilder, Gesichtserkennungsmerkmale und Fingerabdrücke, ermöglicht europaweit computergestütze Personenprofilrecherchen.[35] Die Rasterfahndung wird

29 Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), KOM(2005) 236 endg.

30 Vorschlag für einen Beschluss des Rates über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II), KOM(2005) 230 endg.

31 Vgl. auch die Kritik aus dem Europäischen Parlament: Bericht über den Ersten Bericht über die Durchführung der Datenschutzrichtlinie (Berichterstatter Marco Cappato) vom 24. Februar 2004, A5-0104/2004 endg., S. 14 f.

32 So Leutheusser-Schnarrenberger, »Ein System gerät außer Kontrolle: Das Schengener Informationssystem«, ZRP 2004, 97.

33 Vgl. bereits VO (EG) Nr. 871/2004 des Rates vom 29. April 2004 über die Einführung neuer Funktionen für das Schengener Informationssystem, auch im Hinblick auf die Terrorismusbekämpfung.

34 Vgl. KOM(2005) 230 endg., Art. 18, Art. 24, Art. 28, Art. 33, Art. 37, Art. 48, Art. 56 ff.

35 KOM(2005) 230 endg., Art. 39, 40 ff. Art. 46 (Verknüpfung zwischen Ausschreibungen).

europäisiert. Schließlich: Es wird Personen- und Sachfahndungen geben zwecks verdeckter Registrierung und gezielter Kontrolle.[36] Das betrifft Personen, bei denen konkrete Anhaltspunkte vorliegen, dass sie schwere Straftaten planen.[37] Schon hier weiß man nicht, ob das noch Verdacht oder schon Abwehr einer konkreten Gefahr ist. Zudem ist die verdeckte Registrierung erlaubt, wenn eine Gesamtbeurteilung des Betroffenen erwarten lässt, dass er auch künftig Straftaten begehen wird.[38] Das liegt jenseits der begrenzenden Kategorien Verdacht und konkrete Gefahr. Hier geht es um die Zuschreibung von Risiken, die ohne eindeutiges Kriterium politischer Definitionsmacht überlassen werden: Es gibt Verdächtige, Straftäter, Gefährliche und »Risikobürger«, die es zu erfassen gilt.[39] Das ist soziale Kontrolle um ihrer selbst willen – nicht weit entfernt von Orwell.

III. Vertrag von Prüm

Auch der Vertrag von Prüm[40] folgt derselben Gesetzgebungstechnik. Der Vertrag soll nicht Bestandteil des Schengen-Vertragswerks werden. Am 12. Juni 2007 haben sich die Innenminister der EU bei ihrer Ratstagung in Luxemburg darauf geeinigt, wesentliche Teile des Vertrages in europäisches Recht zu überführen – eine passende Rechtsgrundlage wird sich schon finden. Der inhaltliche Kern der Vereinbarung indes wurde zwischen den beteiligten Staaten (Belgien, Deutschland, Spanien, Frankreich, Luxemburg, Niederlande und Österreich) ausgehandelt. Auf dieser exekutiven Ebene haben weder nationale Parlamente und schon gar nicht das Europaparlament etwas zu sagen. Bevor der Vertrag in europäisches Recht überführt wird, werden – wie schon beim Schengener Informationssystem – technische Fakten geschaffen, wie etwa die Einrichtung von Kontaktstellen, die technische Verknüpfung von Datenbanken oder Form und Ausmaß zusätzlicher Datenübermittlung.

Inhaltlich fokussiert der Vertrag von Prüm vor allem auf den Abgleich von DNA-Profilen.[41] Generell verpflichten sich die Vertragsstaaten, forensische DNA-Datenbanken einzurichten. Art. 2 des Vertrages beschreibt die inhaltlichen Anforderungen an die nationalen DNA-Datenbanken, ohne jedoch Datenschutzbestimmungen festzulegen. Gemäß Artikel 4 Abs. 1 des Vertrages ist ein automatisierter Abgleich von DNA-Profilen möglich. Einzige Schranke ist, dass die DNA-Analyse-Dateien nur zum Zwecke der Strafverfolgung eingerichtet und geführt werden dürfen. Im 7. Kapitel des

36 KOM(2005) 230 endg. Art. 31 ff.
37 AaO., Art. 31 Abs. 1 lit. a.
38 AaO., Art. 31 Abs. 1 lit. b.
39 Kritisch auch Leutheusser-Schnarrenberger, ZRP 2004, 97 ff.
40 Vertrag zwischen dem Königreich Belgien, der Bundesrepublik Deutschland, dem Königreich Spanien, der Französischen Republik, dem Großherzogtum Luxemburg, dem Königreich der Niederlande und der Republik Österreich über die Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration. Vgl. BGBl. 2007, II, Nr. 20 vom 16. Juli 2007.
41 Vgl. zur Kritik das Papier von Weichert, »Wo liegt Prüm? Der polizeiliche Datenaustausch in der EU bekommt eine neue Dimension«, download unter www.datenschutzzentrum.de.

Vertrages werden ein paar Datenschutzbestimmungen statuiert. Deutlich wird, dass es einerseits einen weichen gesamteuropäischen Datenschutz gibt und dass andererseits die Garantie des Rechts auf den Schutz personenbezogener Daten den Vertragstaaten überlassen wird. Im Hinblick auf Mindeststandards eines gemeinsamen europäischen Datenschutzes verweist der Vertrag auf die Empfehlungen des Europarates aus dem Jahre 1987[42], die zum einen keinen rechtsverbindlichen Charakter haben und zum anderen unter dem Niveau der europäischen Datenschutzrichtlinie liegen. Mangels europäischen Datenschutzes gibt es nur einen nationalstaatlichen Datenschutz mit höchst heterogenen Anforderungen: Ein bereits existentes gemeinsames Datenschutzniveau lässt sich nicht einfach unterstellen. Erneut überwiegt das Bestreben nach umfassender, beschleunigter, europäisch zentralisierter Datenverarbeitung, das Bemühen um einen gemeinsamen, justizförmig überprüfbaren europäischen Datenschutz.

IV. Speicherung von Vorratsdaten

Kommen wir schließlich zum Albtraum des Datenschutzes: die Speicherung von Vorratsdaten. In der Richtlinie 2006/24 vom 15. März 2006[43] will die Europäische Union die Mitgliedstaaten verpflichten, Verkehrs- und Standortdaten elektronischer oder öffentlicher Kommunikationsnetze auf Vorrat zu speichern. Verkehrs- und Standortdaten umfassen auch jegliche damit in Zusammenhang stehende Daten, die zur Feststellung jedes Teilnehmers an elektronischer Kommunikation oder auch jedes Benutzers von elektronischen Kommunikationsmitteln dienen.[44] Hier kulminieren die formellen und materiellen Probleme europäischen Datenschutzes. Sie kulminieren in formeller Hinsicht, weil es einmal mehr ein Kompetenzproblem gibt. Die Europäische Kommission stützt die Richtlinie auf Art. 95 EG-Vertrag und betrachtet die Vorratsdatenspeicherung als ein Problem der Binnenmarktharmonisierung. Freilich weist schon die Begründung der Richtlinie eher darauf hin, dass es um eine Maßnahme im Rahmen strafrechtlicher Ermittlungen geht. Die Republik Irland hat daher auch Nichtigkeitsklage vor dem Europäischen Gerichtshof erhoben.[45]

Indes mögen die Probleme der Vorratsdatenspeicherung weniger formeller als vielmehr inhaltlicher Natur sein. Die Speicherung von Daten auf Vorrat verstößt so ziemlich gegen alle datenschutzrechtlichen Grundsätze. Sie konterkariert die Zweckbindung, weil sie unabhängig von Verdacht und Gefahr aus allgemeinen Erwägungen künftiger Strafverfolgung jedermann betreffen kann. Sie ignoriert den Bestimmtheitsgrundsatz, weil die wesentlichen Voraussetzungen und der Umfang der Datenerhe-

42 Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen des Europarates vom 28. Januar 1981); Empfehlung Nr. R(87)15 des Ministerkomitees des Europarates vom 17. September 1987.

43 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten (...), ABl. L 105/54 vom 13.4.2006.

44 Richtlinie 2006/24/EG, Artikel 2 Abs. 2 lit. a.

45 Rechtssache C-301/06: Irland gegen den Rat der Europäischen Union und das Europäische Parlament.

bung unklar bleiben. So sieht Artikel 5 der Richtlinie beinahe ausnahmslose Kategorien der Vorratsdatenspeicherung vor. Erfasst werden können unter anderem:

- alle Daten, die zur Rückverfolgung und Identifizierung der Nachrichtenquelle dienen können, wie etwa die Rufnummer des anrufenden Anschlusses, Name und Anschrift des Teilnehmers,
- alle Daten, die Aufschluss über Datum und Uhrzeit des Kommunikationsvorganges betreffen, wie etwa Datum und Uhrzeit der Anmeldung zu Internetdiensten,
- alle Daten, die Aufschluss über die Art der Nachrichtenübermittlung geben, wie etwa der benutzte Telefondienst,
- Daten schließlich, die Auskunft über den Standort eines mobilen Gerätes geben können, so etwa die Standortkennung (Cell-Id) bei Beginn der Verbindung.

Diese Datenerhebung kann jedermann an jedem Ort betreffen. Sie bedeutet die dichte Kontrolle des normalen Kommunikationsalltags. Vorratsdatenspeicherung schließlich verletzt den Verhältnismäßigkeitsgrundsatz, weil sie verdachtsunabhängig und flächendeckend Grundrechte berührt, ohne dass Grenzen dieser Rechtsbeschränkung auch nur annähernd sichtbar werden. Die Sammlung nicht anonymisierter Daten auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken ist unzulässig. Das ist gute und richtige verfassungsrechtliche Tradition in diversen Mitgliedstaaten.[46] Dies war im Übrigen auch festes Prinzip der europäischen Datenschutzrichtlinie. Die Speicherung von Daten auf Vorrat ist nach Maßstäben europäischen Rechts – den Grundsätzen des Datenschutzes und deren Umsetzung im Sekundärrecht – materiell rechtswidrig.[47]

C. Perspektiven des Datenschutzes in Europa

Man kann die Beispiele, die eine Erosion des Datenschutzes in Europa illustrieren, fortsetzen. Man könnte die Europol-Konvention und den Umstand, dass Europol-Bedienstete bei der Verarbeitung personenbezogener Daten richterlich unkontrolliert sind, anführen, man könnte thematisieren, dass Europol bei Bedarf Daten auch zu anderen Zwecken als den ursprünglich vorgesehenen an Dritte weiterleiten darf, man könnte letztlich die Erhebung, Speicherung und Übermittlung von Fluggastdaten skandalisieren, die an ein Drittland – die Vereinigten Staaten – transferiert werden, bei dem es zumindest sehr zweifelhaft ist, ob das dortige Datenschutzniveau europäischen Maßstäben wirklich äquivalent ist.[48]

Indem man das Negative resümiert, mag sich das Positive zwangsläufig ergeben:

- der Grundsatz der Verfügbarkeit von Informationen ist ein Gegenprogramm zum Europäischen Datenschutz,
- die Zweckbindung – zentraler Grundsatz des Datenschutzes – erodiert,

46 Vgl. zur Kritik u.a. Blakeney, Computer and Telecommunication Law Review(C.T.L.R.) 2007, S. 152 ff.; Gitter/Schnabel, MMR 2007, 411 ff.; Leutheusser-Schnarrenberger, ZRP 2007, S. 9 ff.;

47 So auch Gitter/Schnabel, MMR 2007, 411 ff. (S. 416); Leutheusser-Schnarrenberger, ZRP 2007, 9 ff. (S. 11 u. S. 13).

48 Vgl. zur Kritik Simitis, NJW 2006, 2011 ff.

- die Datenerhebung wird auf Kategorien ausgedehnt, die jenseits von Verdacht und Gefahr liegen, also über Strafverfolgung und polizeilicher Prävention noch hinausgehen,
- generell: Die Möglichkeiten einer automatisierten und vernetzten europäischen Datenverarbeitung werden systematisch erweitert, ohne dass in gleich kohärenter Weise effektiver Datenschutz gewährleistet wird. Der Datenschutz erreicht kaum noch die technische und politische Intensität automatisierter Datenverarbeitung.

Aus diesem Negativprofil ergibt sich bereits, was zu tun ist. Es gilt das Verhältnis von Datenschutz und Informationsinteresse europäischer und staatlicher Institutionen wieder umzukehren. Dem Recht auf den Schutz personenbezogener Daten gebührt der Vorrang und deren Erhebung kann nur – wohlbegründete – Ausnahme sein.

Mit dem Vertrag von Lissabon verbinden sich Hoffnungen, dem Recht auf den Schutz personenbezogener Daten wieder den ihm gebührenden Rang einzuräumen. Diese Hoffnung kann sich auf verschiedene Erwägungen stützen. So entfällt mit dem Vertrag von Lissabon die bisherige »Säulenstruktur« der Europäischen Union. Datenschutz wird dann Gegenstand einer zwischen der Europäischen Union und den Mitgliedstaaten geteilten Kompetenz. Diese wird indes angesichts einer zunehmend europäisch zentralisierten Datenverarbeitung die Tendenz haben, auf gesamteuropäischer Ebene ausgeübt zu werden. Zugleich gilt das Recht auf Datenschutz aus der EU-Grundrechtecharta unmittelbar und verlangt nach Beachtung. Damit erhöht sich der Druck auf den europäischen Gesetzgeber, eine für alle Sachbereiche der europäischen Politik geltende verbindliche Datenschutzregelung zu entwickeln. Die europäische Grundrechtsbindung, der Maßstab von Artikel 8 der Europäischen Menschenrechtskonvention und die gemeinsamen Verfassungstraditionen der Mitgliedstaaten verhindern, dass eine Harmonisierung auf niedrigem oder auch nur mittlerem Niveau erfolgt. Vorrang für den Datenschutz bedeutet europäische Harmonisierung auf höchstem Niveau. Schon die Datenschutzrichtlinie 95/46 sah dieses vor.

Vor allem gilt: In jedem Sachbereich europäischer Politik, die den Datenschutz betrifft, gilt die Zuständigkeit des Europäischen Gerichtshofs als Hüter des Rechts auf den Schutz personenbezogener Daten. Sicher bedarf es hierzu organisatorischer Veränderungen: Soweit das Strafrecht betroffen ist, gilt es eine Fachgerichtsbarkeit in Strafsachen zu etablieren, die auch für den Datenschutz im Strafrecht zuständig wäre. Es geht aber auch um inhaltliche Veränderungen. Der Europäische Gerichtshof wird sich dem materiellen Datenschutzrecht und der Entwicklung von Schutzbereich und Schranken dieses Rechts widmen müssen. Längst dürfte es nicht mehr damit getan sein, eigentlich materiell-rechtliche Probleme hinter formellen Fragen der Kompetenzausübung zu verstecken, wie etwa im Fluggastdatenfall geschehen.[49] So ist die Richtlinie zur Vorratsdatenspeicherung möglicherweise schon aufgrund einer falsch gewählten Ermächtigungsnorm nichtig. Sie ist aber in ihrem materiellen Kern nichtig, weil sie gegen elementare Grundsätze des Datenschutzes verstößt. Diese Grundsätze zu definieren, sie kräftig auszubauen und ihre Einhaltung zu überwachen, wird die vornehmste Aufgabe europäischer Judikatur sein. Von Karl Raimund Popper stammt

49 EuGH, Urteil vom 23. Oktober 2007, Rs. C-440/05.

der Satz: »Wir können zwar vieles wissen, nur nicht das, was wir in Zukunft wissen werden«. Die Menge der Daten, die erhoben werden können, scheint unendlich. Die Informationsphantasien erscheinen grenzenlos. Eine freie Gesellschaft muss dem aber Grenzen setzen. Wir sollten wissen, dass wir nicht alles wissen dürfen.