UNO & Europarat

28. Dezember 2009 – UN-Sonderberichterstatter zur Förderung und zum Schutz der Menschenrechte und Grundfreiheiten im Rahmen der Terrorismusbekämpfung veröffentlicht Bericht zum Schutz der Privatsphäre im Kampf gegen den Terrorismus

Dezember

Januar

Februar

März

April

Mai

Juni

Juli

August

29. September – Ministerkomitee des Europarates veröffentlicht Erklärungen über die digitale Agenda für Europa, über die Neutralität des Netzwerkes und die Verwaltung der Internet-Protokoll-Adressen im öffentlichen Interesse

September

Oktober

23. November – Ministerkomitee des Europarats veröffentlicht Empfehlung zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten im Zusammenhang mit *profiling*

November

Dezember

EU

Januar

Februar

9. März – EuGH interpretiert die Datenschutz-Richtlinie im Fall *Kommission gegen Deutschland*

März

April

Mai

15. Juni – Europäische Kommission veröffentlicht Mitteilung zum Gebrauch von Sicherheitsscannern in EU-Flughäfen

29. Juni – EuGH prüft Umfang des Datenschutzes im Zusammenhang mit dem Zugang zu EU-Dokumenten im Fall *Kommission gegen Bavarian Lager*

Juni

20. Juli – Europäische Kommission veröffentlicht Mitteilung zu Informations-Management im Bereich Freiheit, Sicherheit und Recht

Juli

August

21. September – Europäische Kommission veröffentlicht Mitteilung über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer

September

Oktober

4. November – Europäische Kommission veröffentlicht Mitteilung über Gesamtkonzept für den Datenschutz in der Europäischen Union

9. November – EuGH entscheidet im Fall *Volker und Markus Schecke GbR, Hartmud Eifert, Land Hessen gegen Bundesanstalt für Landwirtschaft und Ernährung*, dass verschiedene Vorschriften im EU-Sekundärrecht aufgrund ihrer Verletzung der EU-Datenschutzvorschriften ungültig sind

November

Dezember

3

Informationsgesellschaft und Datenschutz

Google Street View, Facebook und andere soziale Medien gehören seit einigen Jahren zum Alltag in der Informationsgesellschaft. Im Jahr 2010 wurden in Anbetracht dieser Entwicklungen in einer Reihe von EU-Mitgliedstaaten Datenschutzbedenken laut. Mit dem Hinweis auf die nationale Sicherheit und ihre mögliche Bedrohung wurden Sicherheitsmaßnahmen auf Flughäfen verschärft. Auch dies führte – im Zusammenhang mit der Einführung von Körperscannern – zu Debatten auf EU-Ebene und in einigen Mitgliedstaaten. Der Schutz personenbezogener Daten war 2010 ein Kernpunkt in vielen Grundrechtsdebatten in der EU, etwa wenn es um neue Technologien und Vorschläge für die Reform einschlägiger EU-Gesetzgebung unter Berücksichtigung des Vertrags von Lissabon und des Stockholmer Programms ging.

Das vorliegende Kapitel beschreibt, wie sich Strategien und Praktiken der Europäischen Union (EU) und ihrer Mitgliedstaaten im Bereich Informationsgesellschaft und Datenschutz im Jahr 2010 entwickelten. Zunächst legt es die Bedenken dar, die nationale Gerichte gegenüber dem einschlägigen EU-Recht äußerten. Dabei geht es insbesondere um die Frage, ob die Richtlinie über die Vorratsspeicherung von Daten mit den Grundrechten vereinbar ist; zudem wird auf die Forderungen nach einer Reform des EU-Rechtsrahmens eingegangen. Das Kapitel erörtert dann die Bedenken zu Unabhängigkeit, Befugnissen und Ressourcen der Datenschutzbehörden in den Mitgliedstaaten. Vor dem Hintergrund, dass Transparenz in jeder Informationsgesellschaft wichtig ist, beleuchtet das Kapitel dann das empfindliche Gleichgewicht, das es zwischen dem Datenschutz und dem Recht auf Information zu wahren gilt. Das Kapitel schließt mit Überlegungen zu der Frage, wie die Herausforderungen des Datenschutzes in den Bereichen der polizeilichen und sicherheitstechnischen Zusammenarbeit, des technologischen Fortschritts und der Flughafensicherheit im Jahr 2010 bewältigt wurden und in Zukunft bewältigt werden können.

Wichtige Entwicklungen im Bereich Informationsgesellschaft und Datenschutz:

- Neue Technologien gaben Anlass zu neuen Bedenken im Hinblick auf die Grundrechte und erfordern die Modernisierung der EU-Gesetzgebung zum Datenschutz.
- Zunehmend wurde klar, dass Datenschutz ein Kernanliegen internationaler Übereinkommen sein sollte, insbesondere wenn es um Fluggastdatensätze und SWIFT-Daten geht.
- Politische und rechtliche Bedenken wurden geäußert im Zusammenhang mit der obligatorischen Aufbewahrung von Daten der Telefon- und Internetkommunikation durch Unternehmen der Privatwirtschaft (so genannte Vorratsdatenspeicherung).
- Die Unabhängigkeit von Datenschutzbehörden wurde zum Thema – auch vor dem EuGH.
- Die politische Debatte über den sicherheitspolitisch motivierten Einsatz von Körperscannern an Flughäfen ging weiter.
- Das Verhältnis zwischen Datenschutz einerseits, und dem Recht auf Informationszugang andererseits, wurde zu einem Thema, dessen sich auch der EuGH annahm.

3.1. Überarbeitung des derzeitigen EU-Rechtsrahmens zum Datenschutz

Der Schutz personenbezogener Daten ist ausdrücklich in Artikel 8 der Charta der Grundrechte der Europäischen Union („Charta") als eigenständiges Grundrecht verankert. Tatsächlich ist die Charta das erste internationale Menschenrechtsinstrument, das solch eine explizite Festlegung enthält. Die Verarbeitung und der freie Verkehr personenbezogener Daten werden auf sekundärrechtlicher Ebene durch die Datenschutzrichtlinie geregelt.[1] Im Anschluss an die Annahme des Lissaboner Vertrags im Dezember 2009 erklärte die Vizepräsidentin der Europäischen Kommission, Viviane Reding, dass der Schutz der personenbezogenen Daten europäischer Bürger 2010 ein politischer Schwerpunktbereich sein werde.

> *„Ich möchte (...) Schwerpunktbereiche herausstellen, bei denen wir nach meinem Dafürhalten nachdrücklich zeigen müssen, dass sich die Politik Europas mit dem Vertrag von Lissabon ändert. Als erstes müssen wir in all den verschiedenen EU-Politiken den Einsatz der EU für den Schutz der Privatsphäre unserer Bürger wesentlich stärken."*
>
> *Viviane Reding, Vizepräsidentin der Europäischen Kommission, 11. Januar 2010*

Die rasante technologische Entwicklung und der erhöhte Datenaustausch in der heutigen Informationsgesellschaft haben zu einer umfassenden Debatte über die Überarbeitung der derzeitigen Datenschutzregelungen der EU geführt, die von 1995 datieren. Die Europäische Kommission unternahm den ersten Schritt in dieser Debatte, indem sie 2009 eine öffentliche Konsultation über den künftigen Rechtsrahmen für den Schutz personenbezogener Daten in der EU auf den Weg organisierte.[2] Im November 2010 veröffentlichte die Europäische Kommission ihren Standpunkt zum Schutz personenbezogener Daten in der EU. Darin identifizierte sie neue Herausforderungen und wies darauf hin, dass die Datenschutz-Vorschriften für die polizeiliche und justizielle Zusammenarbeit in Strafsachen geändert werden müssten.[3] Einen Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht hatte die Europäische Kommission bereits zuvor in einer Mitteilung veröffentlicht.[4] Auch der Europarat eröffnete eine Debatte über die Modernisierung seines Datenschutz-Übereinkommens 108 zum Schutz des Menschen bei der automatischen Verarbeitung von personenbezogenen Daten.[5] Um den legitimen Erwartungen von Einzelnen und betroffenen Berufsgruppen im Bereich des Datenschutzes gerecht werden zu können, möchte der Europarat herauszufinden, ob die Vorgaben des Übereinkommens 108 geändert und ergänzt werden müssen. So startete er anlässlich des 30. Jahrestages des Übereinkommens 108 eine öffentliche Konsultation, um allen Interessensvertretern und interessierten Einzelpersonen die Möglichkeit zur Stellungnahme zu geben. Die Modernisierung des Übereinkommens 108 sollte auch dazu führen, dass seine tatsächliche Umsetzung besser überwacht wird.

3.2. Vereinbarkeit der Richtlinie zur Vorratsdatenspeicherung mit den Grundrechtsprinzipien

Die Europäische Kommission gab 2010 bekannt, dass sie die Richtlinie aus dem Jahr 2006 zur Vorratsdatenspeicherung überarbeiten werde,[6] die in ihrer bisherigen Fassung Telefon- und Internetunternehmen verpflichtet, unterschiedslos Daten über sämtliche Verbindungen ihrer Kunden zu erheben.[7] In vielen EU-Mitgliedstaaten wurden Bedenken laut, dass die Richtlinie nicht mit den Grundrechten vereinbar sei. In einem gemeinsamen Schreiben vom 22. Juni 2010 forderten mehr als 100 Nichtregierungsorganisationen (*non-governmental organisations*, NGOs) aus 23 EU-Mitgliedstaaten die EU-Kommissionsmitglieder Malmström, Reding und Kroes auf, eine Änderung vorzuschlagen: Die EU-Auflagen zur Vorratsdatenspeicherung sollten durch ein System zur schnellen Sicherstellung und gezielten Aufzeichnung von Verkehrsdaten ersetzt werden. Das Schreiben argumentiert, dass eine flächendeckende Vorratsdatenspeicherung für vertrauliche Tätigkeiten und Kontakte wie sie z. B. Journalisten, Telefonseelsorger oder Geschäftsleute pflegen, Gefahren berge. Im Falle eine derartigen Sammlung und Speicherung könnten Daten durchsickern oder missbraucht werden.[8] In **Belgien**, **Bulgarien**, **Deutschland** und **Österreich** gab es nationale Kampagnen gegen die Umsetzung der Richtlinie, die breiten Widerhall in den Medien fanden. Entsprechende Bedenken über die schrittweise Aushöhlung des Schutzes der Privatsphäre konstatierte Ende 2009 auch der Sonderberichterstatter der Vereinten Nationen (*United Nations*, UNO) zur Förderung und zum Schutz der Menschenrechte und Grundfreiheiten im Rahmen der Terrorismusbekämpfung.[9]

Eine Reihe von Verfassungsgerichtsurteilen in EU-Mitgliedstaaten heizte die Debatte über die Vereinbarkeit der Richtlinie zur Vorratsdatenspeicherung mit den Grundrechten weiter an. Im Dezember 2009 erklärte das **rumänische** Verfassungsgericht die auf der Grundlage der Richtlinie

1 Richtlinie 95/46/EG, ABL. 1995 L 281, S. 31-50.
2 Für eine Zusammenfassung der Ergebnisse dieser Konsultation siehe Europäische Kommission (2010a).
3 Europäische Kommission (2010b).
4 Europäische Kommission (2010c).
5 Europarat (2010).
6 Europäische Kommission (2010d).
7 Richtlinie 2006/24/EG, ABL. 2006 L 105, S. 54.
8 Gemeinsame Erklärung von über 100 NROs vom 22. Juni 2010, www.vorratsdatenspeicherung.de/images/DRletter_Reding.pdf.
9 Scheinin, M. (2009).

erlassene Umsetzungsmaßnahme für verfassungswidrig.[10] Im März 2010 hob das **deutsche** Bundesverfassungsgericht das Gesetz zur Umsetzung der Richtlinie auf und stellte fest, dass es das Recht auf Privatsphäre erheblich bedroht.[11] Im Anschluss an dieses Urteil forderte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit die deutschen Unternehmen auf, alle gemäß dem verfassungswidrigen Gesetz gesammelten Daten zu löschen. Dieser Forderung kamen alle Unternehmen nach.[12] In einer gemeinsamen Entschließung forderten die Datenschutzbeauftragten des Bundes und der Länder die deutsche Bundesregierung auf, sich für eine Aufhebung der Richtlinie zur Vorratsspeicherung von Daten einzusetzen.[13]

„Für die Gefahrenabwehr ergibt sich aus dem Verhältnismäßigkeitsgrundsatz, dass ein Abruf der vorsorglich gespeicherten Telekommunikationsverkehrsdaten nur bei Vorliegen einer durch bestimmte Tatsachen hinreichend belegten, konkreten Gefahr für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr zugelassen werden darf."

Bundesverfassungsgericht, Pressemitteilung, 2. März 2010

In **Irland** focht die NGO *Digital Rights Ireland* (DRI) 2006 beim *High Court* die Richtlinie selbst und auch die entsprechende Umsetzung an. Im Juli 2008 ließ das Gericht die *Irish Human Rights Commission (*IHRC*)* als *amicus curiae* (sachverständigen Berater) in diesem Fall zu. Einer Pressemitteilung der IHRC zufolge wirft der „Fall wichtige Fragen darüber auf, inwieweit Gesetze und Maßnahmen, die die Überwachung des Privatlebens durch den Staat zum Zwecke der Kriminalitätsbekämpfung regeln, in ausreichendem Maße Menschenrechtsgarantien beinhalten".[14] Im Mai 2010 entschied der *High Court*, dass die NGO DRI klagebefugt sei, und legte den Fall dem Gerichtshof der Europäischen Union (EuGH) vor.[15]

Unterdessen haben die Zweifel an der Vereinbarkeit der Richtlinie zur Vorratsdatenspeicherung mit den Grundrechten auch die Umsetzung in einigen Mitgliedstaaten verzögert. Obgleich der EuGH im Juli 2010 entschied, dass **Österreich** mit der nicht fristgerechten Umsetzung der Richtlinie (diese war bis zum 15. März 2009 umzusetzen) gegen den EU-Vertrag verstoßen hat,[16] verzögerte sich die Umsetzung in Österreich weiter.[17] Vor dem EuGH äußerte Österreich Bedenken, ob die Richtlinie mit den Grundrechten vereinbar sei, insbesondere mit Artikel 8 der Charta.[18] Auch in **Schweden** verzögerte sich die Umsetzung der Richtlinie wegen Grundrechtsbedenken.

Vielversprechende Praktik

Öffentliche Anhörung zur Umsetzung der Richtlinie zur Vorratsdatenspeicherung

Vom 15. November 2009 bis 15. Januar 2010 veranstaltete die österreichische Bundesregierung eine öffentliche Anhörung zum Entwurf des Gesetzes, das die Richtlinie zur Vorratsdatenspeicherung umsetzen soll. Öffentliche Institutionen, private Einrichtungen und Personen reichten insgesamt 189 Kommentare ein – die höchste Zahl, die jemals bei der öffentlichen Kommentierung einer Gesetzesvorlage in Österreich erreicht wurde. Die meisten Stellungnahmen kritisierten die in der Richtlinie festgelegte Pflicht zur Speicherung von Verkehrs-, Standort- und Teilnehmerdaten, die bei der Nutzung öffentlich zugänglicher elektronischer Kommunikationsdienste oder -netze verarbeitet werden.[19]

3.3. Datenschutzbehörden: Unabhängigkeit, Befugnisse und Ressourcen

Nach Artikel 28 der bereits erwähnten Datenschutzrichtlinie müssen in jedem Mitgliedstaat eine oder mehrere Kontrollstellen die Anwendung der Richtlinie überwachen. Unabhängigkeit, Befugnisse und Ressourcen der Datenschutzbehörden wurden 2010 zu einem wichtigen Anliegen, dem die FRA ihren im Mai 2010 veröffentlichten Bericht „Datenschutz in der Europäischen Union: Die Rolle der nationalen Datenschutzbehörden" widmete.

3.3.1. Unabhängigkeit

Im Fall *Kommission gegen Deutschland* befasste sich der EuGH erstmals mit der Frage der Unabhängigkeit der Datenschutzbehörden. Der EuGH legte einen strengen Maßstab an und vertrat die Auffassung, dass die Datenschutzbehörden, die auf Landesebene die Verarbeitung personenbezogener Daten überwachen sollen, staatlicher Aufsicht unterstellt und somit nicht ausreichend unabhängig seien.[20] In dem Fall ging es um die Auslegung von Artikel 28 Absatz 1 der Datenschutzrichtlinie, in dem es heißt, „die Kontrollstellen

10 Rumänien, Curtea ConstituÐionalÐ a României (2009) Gerichtsentscheidung Nr. 1258, 8. Oktober 2009.
11 Deutschland, Bundesverfassungsgericht (2010) 1 BvR 256/08, 2. März 2010.
12 Deutschland, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BFDI).
13 Deutschland, Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder.
14 European Digital Rights (2008).
15 Irland, Oberster Gerichtshof, *Digital Rights Ireland Ltd. gegen Minister für Kommunikation, Marine und Natürliche Ressourcen und Anderes* (2010), McKechnie J., nicht veröffentlicht, 5. Mai 2010.
16 Gerichtshof der Europäischen Union (EuGH) C-189/09 *Kommission gegen Österreich*, 29. Juli 2010.
17 Österreichische Bundesministerium für Justiz (2010) „Vorratsdaten: Justizministerium prüft Vorschlag", Pressemitteilung, 27. Juli 2010.
18 EuGH, C-189/09, *Kommission gegen Österreich*, 29. Juli 2010.
19 Übersichtsliste aller Kommentare, siehe Österreich, Telekommunikationsgesetz 2003, Änderung (117/ME).
20 EuGH, C-518/07, *Kommission gegen Deutschland*, 9. März 2010.

für den Datenschutz nehmen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahr." Der Generalanwalt bezeichnete in seinen Schlussanträgen den Begriff „Unabhängigkeit" als relativ, da der Gesetzgeber das nötige Maß an Unabhängigkeit definieren müsse, was aber unterblieben sei. Gemäß dieser Logik gelangte der Generalanwalt zu dem Schluss, dass die deutschen Datenschutzbehörden sehr wohl ausreichend unabhängig seien, obwohl sie einer staatlichen Aufsicht unterliegen.[21] Der Gerichtshof lehnte diese Argumentation jedoch ab: Er betonte, dass die Richtlinie gemäß des allgemeinen Wortsinns zu interpretieren sei, und sprach sich somit für eine strikte Auslegung der „Unabhängigkeit" aus. Der EuGH wies ferner darauf hin, dass der Begriff „Unabhängigkeit" in der Richtlinie durch das Adjektiv „völlig" verstärkt werde und daher im Sinne einer weitgehenden Unabhängigkeit zu lesen sei.

> *„Richtlinie 95/46 [ist] dahin auszulegen, dass die für die Überwachung der Verarbeitung personenbezogener Daten im nichtöffentlichen Bereich zuständigen Kontrollstellen mit einer Unabhängigkeit ausgestattet sein müssen, die es ihnen ermöglicht, ihre Aufgaben ohne äußere Einflussnahme wahrzunehmen. Diese Unabhängigkeit schließt nicht nur jegliche Einflussnahme seitens der kontrollierten Stellen aus, sondern auch jede Anordnung und jede sonstige äußere Einflussnahme, sei sie unmittelbar oder mittelbar, durch die in Frage gestellt werden könnte, dass die genannten Kontrollstellen ihre Aufgabe, den Schutz des Rechts auf Privatsphäre und den freien Verkehr personenbezogener Daten ins Gleichgewicht zu bringen, erfüllen."*
>
> *EuGH, C-518/07* Kommission gegen Bundesrepublik Deutschland*, 9. März 2010, Randnummer 30*

Im Dezember 2010 brachte die Europäische Kommission **Österreich** wegen unzureichender Unabhängigkeit seiner Datenschutzbehörde vor den EuGH. Zwar verlangt das österreichische Datenschutzgesetz, dass die Datenschutzkommission ihr Amt unabhängig ausübt und an keine Weisungen gebunden ist. Der Kommission zufolge ist jedoch eine „vollkommene Unabhängigkeit" nicht gewährleistet, da die Datenschutzkommission Teil des Bundeskanzleramts ist und der Bundeskanzler somit das Recht hat, sich jederzeit über alles informieren zu lassen, was die tägliche Arbeit der Datenschutzkommission betrifft.[22]

3.3.2. Befugnisse

Am 24. Juni 2010 forderte die Europäische Kommission das **Vereinigte Königreich** auf, dem EU-Recht nachzukommen und die Befugnisse seiner nationalen Datenschutzbehörde, des *Information Commissioner's Office* (ICO), zu stärken.[23] Zu den Kompetenzen der Datenschutzbehörde solle die Möglichkeit gehören, Stichproben zur Einhaltung des Datenschutzrechts durchzuführen, gegebenenfalls Strafen zu verhängen und vor der Übermittlung von Daten an Drittländer nachprüfen zu können, ob der dort gebotene Datenschutz angemessen ist.[24] Derzeit analysiert die Kommission die Antworten des Vereinigten Königreichs auf die erhobene Kritik.

AKTIVITÄT DER FRA

Vergleich der Datenschutzbehörden in den Mitgliedstaaten

Im Mai 2010 veröffentlichte die FRA den Bericht *Data Protection in the EU: the role of National Data Protection Authorities (Datenschutz in der Europäischen Union: Die Rolle der nationalen Datenschutzbehörden)*. Der Bericht bietet einen vergleichenden Überblick über die Befugnisse und die Unabhängigkeit der Datenschutzbehörden in der EU und verweist auf den Mangel an Unabhängigkeit, Befugnissen und Ressourcen der Datenschutzbehörden in einigen EU-Mitgliedstaaten.

FRA (2010) *Data Protection in the EU: the role of National Data Protection Authorities – Strengthening the fundamental rights architecture in the EU II (Datenschutz in der Europäischen Union: Die Rolle der nationalen Datenschutzbehörden – Stärkung des Grundrechtesystems in der Europäischen Union II)*

3.3.3. Ressourcen

Die Ressourcen der Datenschutzbehörden sind entscheidend, damit diese ihrer Aufgabe, die Grundrechte zu bewahren, gerecht werden können. Dessen ungeachtet kürzten viele EU-Mitgliedstaaten 2010 infolge der Finanzkrise die entsprechenden Haushaltsmittel. Die folgenden Informationen sind nicht direkt vergleichbar, deuten jedoch auf bestimmte Tendenzen hin.

Folgende Länder meldeten eine erhebliche Kürzung der personellen und/oder finanziellen Ressourcen im Berichtszeitraum: **Estland** (Verringerung der finanziellen Ressourcen für den Zeitraum 2008-2010 um 12,5 %), **Irland** (2,04 Mio. EUR für 2008; 1,81 Mio. EUR für 2009; 1,21 Mio. EUR für 2010), **Lettland** (25 Mitarbeiter 2008; 16 Mitarbeiter 2009; 19 Mitarbeiter 2010; 730 984 EUR für 2008; 476 984 EUR für 2009; 381 295 EUR für 2010), **Litauen** (keine Angaben zum Personalabbau, aber Kürzung des Lohnfonds um 69 % von 2 929 000 LTL [848 690 EUR am 31. Dezember 2010] auf 1 886 000 LTL [546 477 EUR], Kürzung der finanziellen Ressourcen um 64,6 %), **Slowakei** (keine Änderung bei den personellen Ressourcen; 960 850 EUR für 2008, 728 696 EUR für 2010).

Dagegen meldeten **Deutschland** und **Frankreich** für den Zeitraum 2007-2010 eine erhebliche Aufstockung der personellen und finanziellen Ressourcen.[25] Eine ähnliche Tendenz war in **Spanien** zu verzeichnen, wo die Zahl der Mitarbeiter in der Datenschutzbehörde *(Agencia Española de Protección de Datos)* von 99 im Jahr 2007 auf 155 im Jahr 2009 erhöht wurde. Die Finanzmittel der spanischen Behörde

21 *Ibid.*
22 Europäische Kommission (2010e).
23 Europäische Kommission (2010f).
24 Vereinigtes Königreich, Information Commissioner's Office (2010).
25 Falls nicht anders angegeben, stammen diese Daten vom Fralex-Netzwerk.

wurden ebenfalls aufgestockt, von 13,44 Mio. EUR für 2008 auf 15,32 Mio. EUR für 2009.[26]

Keine oder nur geringfügige Änderungen bei den personellen und finanziellen Ressourcen im Jahr 2010 meldeten diese Länder: **Bulgarien, Finnland, Griechenland, Italien, Malta, Österreich, Polen, Rumänien, Slowenien, Ungarn, Vereinigtes Königreich** und **Zypern**.

3.4. Datenschutz und Transparenz in der Informationsgesellschaft

Im Grundrechte-Diskurs gilt es oftmals, ein sensibles Gleichgewicht zwischen konkurrierenden Interessen herzustellen. Beim Datenschutz ist dieser Balanceakt dort nötig, wo das Recht auf Schutz personenbezogener Daten und das Recht auf Information zusammentreffen. Mit dieser Problematik befasste sich der EuGH 2010 im Zusammenhang mit der Verpflichtung zur Transparenz.

Im Juni 2010 prüfte der EuGH in dem Fall *Kommission gegen Bavarian Lager*, in welchem Umfang personenbezogene Daten zu schützen sei, wenn gleichzeitig eine Pflicht besteht, Zugang zu Dokumenten zu gewähren.[27] Im konkreten Fall hatte die Kommission das Protokoll eines Treffens offengelegt, jedoch fünf Namen geschwärzt. Die Klägerin hatte beantragt, Zugang zum vollständigen Dokument zu erhalten, konnte jedoch nicht begründen, weshalb die Übermittlung der personenbezogenen Daten nötig sei. Der EuGH gelangte dementsprechend zu dem Ergebnis, dass die Kommission den Zugang zum vollständigen Protokoll zu Recht abgelehnt hatte.

Erwähnenswert sind auch die verbundenen Rechtssachen C-92/09 und C-93/09, die der Großen Kammer des EuGH im November 2010 vorgelegt wurden. EU-Gesetzgebung wurde hier wegen Unvereinbarkeit mit den Grundrechten angefochten.[28] Konkret ging es um agrarpolitische Vorschriften, die die Mitgliedstaaten dazu verpflichten, stets zu veröffentlichen, wer im vorangegangen Jahr Mittel aus dem Europäischen Garantiefonds für die Landwirtschaft (EGFL) und dem Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums (ELER) erhalten hatte.[29] Die Kläger hatten beim Verwaltungsgericht Wiesbaden beantragt, das Land Hessen zu verpflichten, die betreffenden Daten nicht zu veröffentlichen; und das Verwaltungsgericht Wiesbaden hatte den Fall dem EuGH vorgelegt. Der EuGH erklärte einerseits, dass in einer demokratischen Gesellschaft die Steuerzahler einen Anspruch haben, über die Verwendung öffentlicher Gelder informiert zu werden. Andererseits vertrat er jedoch die Auffassung, dass die Veröffentlichung der Namen der Empfänger und der genauen Beträge, die sie aus dem EGFL und dem ELER erhalten hatten, das Recht der betroffenen Empfänger auf Achtung ihrer Privatsphäre im Allgemeinen und auf Schutz ihrer personenbezogenen Daten im Besonderen verletze. Der EuGH gelangte zu dem Ergebnis, dass die Veröffentlichung der personenbezogenen Daten eines jeden Empfängers von EGFL- und ELER-Mitteln nicht dem Grundsatz der Verhältnismäßigkeit entspreche, da sie nicht unbedingt notwendig sei, um das Ziel der Transparenz zu erreichen. Daher stufte der EuGH einige Bestimmungen der Verordnung Nr. 1290/2005 und der Verordnung Nr. 259/2008 als ungültig ein – und erklärte somit EU-Gesetzgebung für nichtig, weil sie gegen die Grundrechte verstoße.

3.5. Neue Herausforderungen

3.5.1. Datenschutz in der polizeilichen und sicherheitstechnischen Zusammenarbeit

Der Vertrag von Lissabon beseitigte die vorherige Unterteilung der EU in drei Säulen und weitete das ordentliche Gesetzgebungsverfahren auf den Bereich der polizeilichen und justiziellen Zusammenarbeit in Strafsachen aus. Darüber hinaus stärkte er die Befugnisse des Europäischen Parlaments beim Abschluss internationaler Übereinkommen erheblich, was auch bedeutende Auswirkungen auf den Datenschutz hat: So nutzte das Europäische Parlament diese neuen Befugnisse im Februar 2010, um seine Zustimmung zu dem Interimsabkommen zwischen der Europäischen Union und den Vereinigten Staaten zur Verarbeitung und Übermittlung von Zahlungsverkehrsdaten von der Europäischen Union an die Vereinigten Staaten („Swift-I-Abkommen“) zu verweigern, das am 30. November 2009 unterzeichnet worden war. Das Parlament machte geltend, dass das Abkommen nicht genug Schutz für die personenbezogenen Daten der EU-Bürger biete.[30] Nachdem der Europäische Datenschutzbeauftragte (EDSB) eine Stellungnahme[31] abgegeben hatte, stimmte das Europäische Parlament am 8. Juli 2010 dem geänderten Abkommen zu,[32] das am 13. Juli 2010 förmlich abgeschlossen wurde.[33]

Grundrechtliche Bedenken wurden auch im Zusammenhang mit internationalen Abkommen über den Austausch von Fluggastdaten (PNR-Daten) laut. Am 1. März 2010 reichte eine belgische Menschenrechts-NGO (*Ligue des Droits de L´Homme*) Klage beim **belgischen** Verfassungsgericht ein und machte geltend, dass das belgische Gesetz vom 30. November 2009 zur Umsetzung des PNR-Abkommens zwischen der EU und den USA aus dem Jahr 2007 Daten-

26 Spanien, Agencia Española de Protección de Datos (2009) und (2008).
27 EuGH, C-28/08 P (2010), *Kommission gegen Bavarian Lager*, 29. Juni 2010.
28 EuGH, Verbundene Rechtssache C-92/09 und C-93/09 (2010), *Eifert, Schecke gegen Land Hessen*, 9. November 2010.
29 Verordnung (EG) des Rates Nr. 1290/2005, ABL. 2007 L 322, S. 1 und Verordnung der Kommission (EG) Nr. 259/2008, ABL. 2008 L 76, S. 28.
30 Europäisches Parlament (2010a).
31 Europäischer Datenschutzbeauftragter (EDSB) (2010).
32 Europäisches Parlament (2010b).
33 Ratsentscheidung 2010/412/EG, ABl. 2010 L 195, S. 3.

schutznormen verletze.[34] Am 5. Mai 2010 verabschiedete das Europäische Parlament eine Entschließung,[35] die besagt, dass bei jedem neuen Rechtsinstrument über die Übermittlung von PNR-Daten zunächst eine Abschätzung der Folgen für die Persönlichkeitsrechte und eine Prüfung der Verhältnismäßigkeit vorgenommen werden müssen.

Im September 2010 beschloss die Europäische Kommission ein Paket von Vorschlägen zum Austausch von Fluggastdatensätzen mit Drittstaaten,[36] bestehend aus einer allgemeinen EU-Außenstrategie zum Thema Fluggastdaten und Empfehlungen für Verhandlungsrichtlinien für neue PNR-Abkommen mit den Vereinigten Staaten, Australien und Kanada.[37] Die Strategie soll ein hohes Datenschutzniveau beim Austausch von PNR-Daten mit Drittländern sicherstellen.[38]

3.5.2. Technologische Herausforderungen

Bedrohungen für die Grundrechte im Zusammenhang mit neuen technologischen Herausforderungen standen im Berichtszeitraum auf der Agenda des Europarats weit oben. Das Ministerkomitee des Europarats verabschiedete 2010 ein ganzes Paket von einschlägigen Erklärungen und Empfehlungen: eine Erklärung über die digitale Agenda für Europa,[39] eine Erklärung zur Netzneutralität,[40] eine Erklärung über die Verwaltung der IP-Adressressourcen im öffentlichen Interesse[41] und eine Erklärung zum verstärkten Engagement der Mitgliedstaaten in Angelegenheiten der *internet governance*, etwa im Rahmen des Beratenden Ausschusses (*Governmental Advisory Committee*, GAC) des Verbandes für zugewiesene Bezeichnungen und Nummern (*Internet Corporation for Assigned Names and Numbers*, ICANN).[42] Zudem verabschiedete die Parlamentarische Versammlung des Europarats ihre Empfehlung 1906 (2010) zum Umdenken kreativer Rechte im Zeitalter des Internets.[43]

Neue technologische Herausforderungen gaben auch Anlass zu Grundrechtsdebatten auf nationaler Ebene. Google Street View ist ein von dem IT-Unternehmen Google angebotener Dienst, der Panorama-Ansichten aus verschiedenen Positionen entlang von Straßen in vielen Städten weltweit bereitstellt. Um diese Bilddaten zu sammeln, schickt Google speziell ausgerüstete Fahrzeuge durch Städte innerhalb und außerhalb der Europäischen Union. Allerdings zeichnete Google dabei – nach eigener Aussage unbeabsichtigt – Fragmente von personenbezogenen Daten aus ungesicherten WLAN-Netzen auf.

Deshalb verhängte die **Österreichische** Datenschutzkommission (DSK) am 21. Mai 2010 ein zeitweiliges Verbot gegen die Sammlung von Daten durch Fahrzeuge von Google Street View und leitete eine Untersuchung ein. Ende November 2010 wurde das zeitweilige Verbot aufgehoben, aber die Untersuchung des Vorgehens von Google Street View geht weiter.[44] Ähnliche Verfahren wurden in vielen Ländern eingeleitet, etwa in **Italien,**[45] **Slowenien**[46] und **Spanien.**[47]

In **Deutschland** konzentrierte sich die Debatte auf das Recht, Widerspruch gegen die Veröffentlichung von Fotos einzulegen, die von Google Street View aufgenommen wurden. Seit August 2010 räumt Google Deutschland die Möglichkeit ein, Einzelwidersprüche gegen die Veröffentlichung von Fotos von Privathäusern und Personen in Street View einzulegen; seit Ende 2010 kann online Einspruch erhoben werden.[48] Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit veröffentlichte ein Informationsblatt[49] und ein Einspruchsformular.[50] Darüber hinaus forderte der Bundesbeauftragte für Datenschutz und Informationsfreiheit ein zentrales Register für Widersprüche gegen die Veröffentlichung personenbezogener Daten im Internet, das auch Dienste wie Google Street View einschließt.[51] Der Bundesrat nahm einen Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes (BDSG) an, um einen besseren Schutz personenbezogener Daten im Zusammenhang mit Online-Geodiensten wie Google Street View zu gewährleisten.[52] Einer Presseerklärung vom 18. August 2010 zufolge befürwortete die Bundesregierung offenbar eine umfassende Reform des Bundesdatenschutzgesetzes mit Blick auf den Online-Datenschutz und wollte einen entsprechenden Vorschlag vorlegen.[53]

Am 7. Juli 2010 leitete der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ein Verfahren gegen Facebook ein, weil dieses E-Mail- und Handy-Kontaktdaten sammelt und zu Vermarktungszwecken aus den Adressbüchern seiner Nutzer Kontaktprofile von Nichtnutzern erstellt.[54] Dieses europaweit erste derartige Verfahren gegen Facebook kann zur Verhängung eines Bußgelds führen.

> *„Die meisten der 75 % der europäischen Jugendlichen, die sich im Internet bewegen, sind begeisterte Nutzer von sozialen Netzwerkplattformen. … Die Veröffentlichung persönlicher Informationen oder Fotos kann jedoch zu peinlichen oder gar traumatischen Situationen führen. Jungen Menschen ist die Gefahr nicht immer bewusst, dass Online-Fotos und -Videos jenseits ihrer Kontrolle und ohne ihr Wissen im Internet im Umlauf sein können."*
>
> *Viviane Reding, Vizepräsidentin der Europäischen Kommission, 9. Februar 2010*

34 Belgien, La Ligue des droits de l'Homme (2010).
35 Europäisches Parlament (2010c).
36 Europäische Kommission (2010g).
37 Europäische Kommission (2010h).
38 Siehe Agentur der Europäischen Union für Grundrechte (FRA) (2008).
39 Europarat, Ministerkomitee (2010a).
40 Europarat, Ministerkomitee (2010b).
41 Europarat, Ministerkomitee (2010c).
42 Europarat, Ministerkomitee (2010e).
43 Parlamentarische Versammlung des Europarats (2010).
44 Österreich, Österreichische Datenschutzkommission (2011).
45 Italien, Garante Per la Protezione Dei Dati Personali.
46 Slowenien, Informationsbeauftragter (*Informacijski Pooblascenec*).
47 Spanien, Agentur für Datenschutz (*Agencia Española de Protección de Datos*)
48 Deutschland, Hamburgischer Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) (2010a).
49 Deutschland, HmbBfDI (2010b).
50 Siehe Deutschland, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD).
51 Deutschland, BFDI (2010).
52 Deutschland, Bundestag (2010).
53 *Ibid.*, S. 15.
54 Hamburg.de (2010).

In **Bulgarien** wurde 2010 die Rolle von Facebook bei Wahlkämpfen intensiv diskutiert. Am 22. Juni 2010 schlugen mehrere Mitglieder der Regierungspartei Vorschriften vor, um den Internet-Wahlkampf zu beschränken. Dabei ging es vor allem darum, die über elektronische Medien, Blogger und soziale Netzwerke wie Facebook und Twitter verbreiteten Informationen mit den Informationen aus Zeitungen, Radio und Fernsehen gleichzustellen: Generell sollten für beide Arten von Medien die gleichen Regeln für die Wahlkampfberichterstattung gelten. Die Oppositionsparteien reagierten besorgt auf diesen Vorschlag und erklärten, dass er einen Verstoß gegen die freie Meinungsäußerung darstelle und auf eine Kontrolle des Internets hinauslaufe.[55]

3.5.3. Körperscanner

Maßnahmen zur Flughafensicherheit, insbesondere der Einsatz von Körperscannern, schienen die Debatten über den Datenschutz in der Europäischen Union 2010 zu dominieren. Nachdem am 25. Dezember 2009 versucht worden war, in einem Flugzeug von Amsterdam nach Detroit einen versteckten Sprengsatz zu zünden, rückte die Diskussion über verschiedene Arten von Körperscannern für Flughafenkontrollen auf der politischen Agenda nach oben. Dieses Thema stieß bei den Medien auf großes Interesse. Es wurde argumentiert, dass die nackte Darstellung der Personen, die den Scanner passieren, gegen das Recht auf Achtung der Privatsphäre verstoße. Am 15. Juni 2010 veröffentlichte die Kommission ihre Mitteilung über den Einsatz von Sicherheitsscannern auf EU-Flughäfen, in der es heißt, dass nur ein gemeinsames Vorgehen auf EU-Ebene gewähren könne, dass die Sicherheitsvorschriften und -standards einheitlich angewendet würden. Dies sei entscheidend, „um sowohl das höchste Sicherheitsniveau als auch den bestmöglichen Schutz der Grundrechte und der Gesundheit der EU-Bürger zu gewährleisten."[56]

In diesem Zusammenhang betonte die Europäische Kommission, wie wichtig verschiedene Vorschriften der EU-Grundrechte-Charta seien, etwa menschliche Würde (Artikel 1); Achtung des Privat- und Familienlebens (Artikel 7); Schutz personenbezogener Daten (Artikel 8); Gedanken-, Gewissens,- und Religionsfreiheit (Artikel 10); Nichtdiskriminierung (Artikel 21); Rechte des Kindes (Artikel 24) und ein hohes Gesundheitsschutz-Niveau bei der Festlegung und Durchführung aller Politiken und Maßnahmen der EU (Artikel 35).

Das Thema der Körperscanner wurde auch auf der Europäischen Konferenz der Datenschutzbeauftragten erörtert, die im April 2010 in Prag stattfand. Die Datenschutzbeauftragten forderten in einer Entschließung, dass Datenschutzprinzipien und -garantien berücksichtigt werden sollen und Datenschutz von vornherein technisch vorgesehen sein soll (*Privacy by Design*), wenn der Einsatz von Körperscannern in Erwägung gezogen wird.[57]

Der Europäische Gerichtshof für Menschenrechte (EGMR) beschäftigte sich im Fall *Gillan und Quinton gegen Vereinigtes Königreich* mit Sicherheitsmaßnahmen auf Flughäfen.[58] Der Fall betraf die Polizeikontrollen im Vereinigten Königreich, die nach Auffassung der Regierung nicht gegen das Recht auf Privatsphäre verstießen, da sie den Durchsuchungsmaßnahmen entsprächen, denen sich Personen regelmäßig an Flughäfen unterziehen.[59] Der EGMR wies dieses Argument zurück und unterstrich, dass ein Flugreisender bei der Entscheidung für die Reise wisse, dass solche Durchsuchungen stattfinden, und er sich dieser Prozedur somit freiwillig unterziehe. Bei Polizeikontrollen hingegen, die jederzeit und überall stattfinden können, bestehe diese Entscheidungsfreiheit nicht.[60] Fraglich ist, ob die obige Überlegung analog auf den Einsatz von Körperscannern angewandt werden kann, da dieser über die üblichen Durchsuchungen hinausgeht.

AKTIVITÄT DER FRA

Körperscanner und Grundrechts-Schutz

Im Juli 2010 veröffentlichte die FRA ein Diskussionspapier über den Einsatz von Körperscannern – *The use of body scanners: 10 questions and answers* (10 Fragen und Antworten zum Einsatz von Körperscannern). Die kurze Analyse nennt die Grundrechte, die möglicherweise durch den Einsatz von Körperscannern verletzt werden. Darüber hinaus geht sie auf Vorgaben und spezifische Gesichtspunkte ein, die bei der Diskussion über die Einführung von Körperscannern auf europäischen Flughäfen berücksichtigt werden sollten. Zudem wird erörtert, welche Bedingungen erfüllt sein müssen, um grundrechtlichen Bedenken Rechnung zu tragen. Die FRA präsentierte die Schlussfolgerungen des Papiers bei einer Anhörung vor dem Europäischen Wirtschafts- und Sozialausschuss im Januar 2011.

Die Debatte um Körperscanner und Datenschutzbedenken kam im Laufe des Jahres 2010 auch in anderen EU-Mitgliedstaaten wie **Deutschland,**[61] **Frankreich**[62] und **Spanien**[63] auf.

55 Bulgarisches Helsinki-Komitee (Български хелзинкски комитет) (2010).
56 Europäische Kommission (2010i).
57 Europäische Datenschutzbeauftragte (2010).
58 Europäischer Gerichtshof für Menschenrechte (EGMR), *Gillan und Quinton gegen Vereinigtes Königreich,* Nr. 4158/05, 12. Januar 2010.
59 *Ibid.*, siehe Absatz 60.
60 *Ibid.*, siehe Absatz 64.
61 Deutschland, Datenschutzbeauftragte des Bundes und der Länder (2010) *Entschließung der 79. Konferenz der Datenschutzbeauftragten des Bundes und der Länder*.
62 Siehe Frankreich, Nationale Kommission für Informationstechnologie und bürgerliche Freiheiten (*Commission nationale de l'informatique et des libertés*, CNIL) (2010).
63 Siehe Website der Madrider Datenschutzagentur www.dataprotectionreview.eu/ zur Expertendebatte über die Benutzung von Körperscannern an Flughäfen.

Ausblick

Neue technische Entwicklungen prägen unser Leben auch weiterhin und lassen immer wieder grundrechtliche Bedenken aufkommen. Man kann davon ausgehen, dass Facebook, Google Street View und Körperscanner weiterhin auf der Tagesordnung bleiben und auch in der übergreifenden Debatte über die Modernisierung des EU-Rechts zum Datenschutz eine Rolle spielen werden. Vor dem Hintergrund des Vertrags von Lissabon werden in naher Zukunft zwei Themen von zentraler Bedeutung sein: die Einhaltung der Grundrechtsnormen (etwa im Zusammenhang mit der Vorratsdatenspeicherung) und die mögliche Ausweitung des Geltungsbereichs des derzeitigen EU-Datenschutzes auf polizeiliche und justizielle Angelegenheiten. Dies dürfte Auswirkungen darauf haben, wie man innerhalb und außerhalb der EU mit dem Datenschutz umgeht. So wird die Debatte über den Datenschutz in den kommenden Jahren vermutlich immer weiter ins Zentrum des Grundrechte-Diskurses in der EU rücken.

Bibliografie

Agentur der Europäischen Union für Grundrechte (FRA) (2008) *Stellungnahme der Agentur der Europäischen Union für Grundrechte über den Vorschlag zu einem Rahmenbeschluss des Rates zur Verwendung von Passagierdaten zu Zwecken der Rechtsdurchsetzung*, Wien, 28. Oktober 2008.

Agentur der Europäischen Union für Grundrechte (2010) *Datenschutz in der EU: Die Rolle von nationalen Datenschutzbehörden: Stärkung der Grundrechtsarchitektur in der EU II,* Wien, 7. Mai 2010.

Agentur der Europäischen Union für Grundrechte (2010) *Der Einsatz von Körperscannern: 10 Fragen und Antworten*, Luxemburg, Amt für Veröffentlichungen der Europäischen Union, Wien, Juli 2010.

Belgien, La Ligue des droits de l'Homme (2010) *PNR, l'oeil de Washington*.

Bulgarien, Български хелзинкски комитет (2010) *ДПС е против опитите да се наложи чрез изборното законодателство контрол върху Интернет*, 22. Juni 2010.

Deutschland, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI) (2010a) *„Vorratsdatenspeicherung*", Bonn.

Deutschland, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (2010b) „Google Street View: Schaar fordert Schaffung eines Widerspruchsregisters und Profilbildungsverbot", Pressemitteilung, 18. August 2010.

Deutschland, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (2010c) *„Diskretionszone für Köperscanner gewährleisten!"*, Bonn, 24. November 2010.

Deutschland, Bundestag (2010) Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes, Publikation/Bt-Drs. 17/2765, 18. August 2010.

Deutschland, Bundesverfassungsgericht (2010) „Konkrete Ausgestaltung der Vorratsdatenspeicherung verfassungswidrig", Pressemitteilung Nr. 11/2010, 2. März 2010.

Deutschland, Hamburgischer Beauftragte für Datenschutz und Informationsfreiheit (HmbBfDI) (2010a) „Vorab-Widerspruch gegen Veröffentlichungen in Google Street View: So funktioniert's", Pressemitteilung, Hamburg, 13. August 2010.

Deutschland Hamburgischer Beauftragte für Datenschutz und Informationsfreiheit (2010b) *„Aus den Augen, aus dem Sinn ... Information zur Umsetzung des Vorab-Widerspruchs gegen Abbildungen im Internetdienst Google Street View"*, Hamburg.

Deutschland, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Website: www.datenschutzzentrum.de/geodaten/20100310-google-streetview-musterwiderspruch.pdf.

Europarat (2010) *Antworten des Europarates zu Herausforderungen im Bereich der Privatssphäre, Modernisierung des Übereinkommens 108, Positionspapier, 32. Internationale Konferenz von Beauftragten für Datenschutz und Privatssphäre,* Jerusalem, 27.-29. Oktober 2010.

Europarat, Ministerkomitee (2010a) *Erklärung des Ministerrates zur Digitalen Agenda für Europa*, Straßburg, 29. September 2010.

Europarat, Ministerkomitee (2010b) *Erklärung zur Netzneutralität*, Straßburg, 29. September 2010.

Europarat, Ministerkomitee (2010c) *Erklärung zur Verwaltung von Internet-Protokoll-Adressen im öffentlichen Interesse*, 29. September 2010.

Europarat, Ministerkomitee (2010d) *Declaration of the Committee of Ministers on enhanced participation of Member States in Internet Governance matters – Government Advisory Committee (GAC) of the Internet Corporation for Assigned Names and Numbers (ICANN)*, Straßburg, 26. Mai 2010.

Europarat, Ministerkomitee (2010e) *Empfehlung CM/Rec(2010)13 des Ministerkomitees an die Mitgliedstaaten über den Schutz des Menschen bei der automatischen Ver-*

arbeitung personenbezogener Daten im Zusammenhang mit Profiling, Straßburg, 23. November 2010.

Europarat, Parlamentarische Versammlung (2010) *Empfehlung 1906 (2010) zu Rechten des geistigen Eigentums in der digitalen Gesellschaft,* Straßburg, 12. März 2010.

Europäische Kommission (2010a) *Zusammenfassung der Antworten der öffentlichen Konsultation über den künftigen Rechtsrahmen für den Schutz von persönlichen Daten*, Brüssel, 4. November 2010.

Europäische Kommission (2010b) *Gesamtkonzept für den Datenschutz in der Europäischen Union*, KOM(2010) 609 endg., Brüssel, 4. November 2010.

Europäische Kommission (2010c) *Überblick über das Informationsmanagement im Bereich Freiheit, Sicherheit und Recht*, KOM(2010) 385 endg., Brüssel, 20. Juli 2010.

Europäische Kommission (2010d) „Stärkung des EU-Datenschutzrechts: Europäische Kommission stellt neue Strategie vor", Presseerklärung, IP/10/1462, Brüssel, 4. November 2010.

Europäische Kommission (2010e) „Datenschutz: Kommission verklagt Österreich wegen unzureichender Unabhängigkeit seiner Datenschutzbehörde", Presseerklärung, IP/10/1430, Brüssel, 28. Oktober 2010.

Europäische Kommission (2010f) „Datenschutz: Kommission fordert das Vereinigte Königreich auf, dem EU-Recht nachzukommen und die Befugnisse der nationalen Datenschutzbehörde zu stärken", Presseerklärung, IP/10/811, Brüssel, 24. Juni 2010.

Europäische Kommission (2010g) *Mitteilung der Kommission über das sektorübergreifende Konzept für die Übermittlung von Fluggastdatensätzen (PNR) an Drittländer*, KOM(2010) 492 endg., Brüssel, 21. September 2010.

Europäische Kommission (2010h) „Europäische Kommission schlägt EU-Außenstrategie zur Übermittlung von Fluggastdaten (PNR) vor", Presseerklärung, IP/10/1150, Brüssel, 21. September 2010.

Europäische Kommission (2010i) *Mitteilung der Kommission an das Europäische Parlament und den Rat über den Einsatz von Sicherheitsscannern auf EU-Flughäfen*, KOM(2010) 311 endg., Brüssel, 15. Juni 2010.

Europäischer Gerichtshof für Menschenrechte (EGMR), *Gillan und Quinton gegen Vereinigtes Königreich*, Nr. 4158/05, 12. Januar 2010.

Europäischer Datenschutzbeauftragter (2010) *Stellungnahme des Europäischen Datenschutzbeauftragten zum Vorschlag für einen Beschluss des Rates über die Unterzeichnung des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus* (TFTP II), ABl. 2010 C 355, 22. Juni 2010.

Europäisches Parlament (2010a) „Innenausschuss empfiehlt das SWIFT-Abkommen mit den USA abzulehnen", Presseerklärung, 5. Februar 2010.

Europäisches Parlament (2010b) *Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung für die Zwecke des Programms der USA zum Aufspüren der Finanzierung des Terrorismus*, Prozessakte, NLE/2010/0178.

Europäisches Parlament (2010c) *Entschließung des Europäischen Parlaments vom 5. Mai 2010 zum Start der Verhandlungen über Abkommen über Fluggastdatensätze mit den USA, Australien und Kanada,* P7_TA-PROV(2010)0144, Brüssel, 5. Mai 2010.

Europäischer Datenschutzbeauftragter (2010) Entschließung *zum Einsatz von Körperscannern für die Sicherheit an Flugplätzen verabschiedet von der Europäischen Konferenz der Datenschutzbeauftragten*, Prag, 29.–30. April 2010.

European Digital Rights (2008) *Irish Human Rights Commission added to data retention challenge*, Newsletter *EDRI-gram*, Nr. 6.14, 16. Juli 2008.

Frankreich, Nationale Kommission für Informationstechnologie und bürgerliche Rechte (*Commission nationale de l'informatique et des libertés,* CNIL) (2010) *Body scanner: quel encadrement en France et en Europe*, 8. Juni 2010.

Gerichtshof der Europäischen Union (EuGH), C-189/09, *Kommission gegen Österreich,* 29. Juli 2010.

Gerichtshof der Europäischen Union, C-518/07, *Kommission gegen Deutschland,* 9. März 2010.

Gerichtshof der Europäischen Union, C-28/08 P, *Kommission gegen Bavarian Lager*, 29. Juni 2010.

Gerichtshof der Europäischen Union, Verbundene Rechtssache C-92/09 und C-93/09, *Schecke und Eifert gegen Land Hessen,* 9. November 2010.

Hamburg.de (2010) *Bußgeldverfahren gegen Facebook wegen Speicherung der Daten Dritter*, 7. Juli 2010.

Irland, Hoher Gerichtshof von Irland (An Ard-Chúirt) (2010) *Digital Rights Ireland Ltd. gegen Minister für Kommunikation, Marine und Natürliche Ressourcen und Anderes*, 5. Mai 2010.

Italien, Garante Per la Protezione Dei Dati Personali (2010) „Auszüge aus der Entscheidung der italienischen Datenschutzbehörde bezüglich Google Streetview Informationsverpflichtungen, die Google Inc. Obliegen", Pressemitteilung, 15. Oktober 2010.

Österreich, Bundesministerium für Justiz (2010) *Vorratsdaten: Justizministerium prüft Vorschlag*, Pressemitteilung, 27. Juli 2010.

Österreich, Österreichische Datenschutzkommission (2011) *Neue Entwicklungen betreffend Google Street View?*

Österreich, Telekommunikationsgesetz 2003, Änderung (117/ME) (2009).

Rat der Europäischen Union (2005) Verordnung (EG) Nr. 1437/2007 des Rates vom 26. November 2007 zur Änderung der Verordnung (EG) Nr. 1290/2005 über die Finanzierung der gemeinsamen Agrarpolitik, ABL. 2007 L 322, 26. November 2005.

Rat der Europäischen Union (2010) Beschluss des Rates vom 13. Juli 2010 über den Abschluss des Abkommens zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Zahlungsverkehrsdaten und deren Übermittlung aus der Europäischen Union an die Vereinigten Staaten für die Zwecke des Programms zum Aufspüren der Finanzierung des Terrorismus, Brüssel, ABl. 2010 L 195, 13. Juli 2010.

Reding V. (2010) *Eröffnungsrede bei der Anhörung vor dem Ausschuss für bürgerliche Freiheiten, Justiz und Inneres* (LIBE),11. Januar 2010.

Reding V. (2010) *Think before you post! How to make social networking sites safer for children and teenagers?,* Safer Internet Day, Straßburg, 9. Februar 2010.

Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. 1995 L 281.

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. 2006 L 105.

Rumänien, Curtea Constituionala (2009) Gerichtsentscheidung Nr. 1258 vom 8. Oktober 2009 bezüglich der Verfassungswidrigkeitsausnahmeklausel der Verordnungen von Gesetz Nr. 298/2008.

Scheinin, M. (2009) *Bericht zum Schutz des Rechts auf Privatssphäre im Kampf gegen Terrorismus*, A/HRC/13/37, Menschenrechtsrates, Büro des Hohen Kommissars für Menschenrechte, 28. Dezember 2009.

Slovenien, Informacijski Pooblascenec (2010) *Kommunikation bezüglich Google Street View*.

Spanien, Agencia Española de Protección de Datos (2008) *Jahresbericht 2008*, Madrid.

Spanien, Agencia Española de Protección de Datos (2009) *Jahresbericht 2009*, Madrid.

Vereinigtes Königreich, Büro des Informationskommissars (2010) "European data protection Commission's call for the UK to strengthen the powers of its national data protection authority", Presseerklärung, London, 28. Juni 2010.

Vereinigtes Königreich, Justizministerium (2010) "Call for Evidence on the data protection legislative framework", Presseerklärung, London, 6. Juli 2010.

Verordnung (EG) Nr. 259/2008 der Kommission vom 18. März 2008 mit Durchführungsbestimmungen zur Verordnung (EG) Nr. 1290/2005 des Rates hinsichtlich der Veröffentlichung von Informationen über die Empfänger von Mitteln aus dem Europäischen Garantiefonds für die Landwirtschaft (EGFL) und dem Europäischen Landwirtschaftsfonds für die Entwicklung des ländlichen Raums, ABl. 2008 L 76 (ELER).