Die Wirkung von „Schengen" nach innen

Polizeiliche Informationsnetzwerke ohne Grenzen?

Konrad Lachmayer

1. Vom Binnenmarkt zum Raum der Sicherheit

Das Übereinkommen von Schengen wurde als völkerrechtlicher Vertrag zwischen den Benelux-Staaten, Deutschland und Frankreich im Jahre 1985 abgeschlossen.1 Ziel des Übereinkommens war der Abbau von Grenzkontrollen zur Verwirklichung des Binnenmarktes. Die Verwirklichung des Binnenmarktes bedingte einen Raum der Sicherheit, was im Jahre 1985 noch niemand wusste, aber im Ansatz sehr wohl angedacht war. So wurden gem Art 17 Schengener Übereinkommen „langfristig durchzuführende Maßnahmen" vorgesehen, die unter anderem „ergänzende Maßnahmen zum Schutz der inneren Sicherheit" betrafen. Die diesbezüglich einzuleitenden Gespräche gem Art 18 Schengener Übereinkommen betrafen etwa die „Ausarbeitung von Vereinbarungen über die polizeiliche Zusammenarbeit im Bereich der präventiven Verbrechensbekämpfung und der Fahndung" oder die „Suche nach Mitteln zur gemeinsamen Verbrechensbekämpfung, unter anderem durch Prüfung der etwaigen Einführung eines Rechts der polizeilichen Nacheile".

Die visionäre Kraft von 1985 ist längst in effektive Organisation, Verfahren und Rechtsstrukturen umgewandelt. Dazu beigetragen hat vor allem das Schengener Durchführungsübereinkommen (SDÜ). Damit wurden erste polizeiliche Operativmaßnahmen vorgesehen, wie grenzüberschreitende Observation (Art 40 SDÜ) oder grenzüberschreitende Nacheile (Art 41 SDÜ). Zentral ist aber auch das Schengener Informationssystem (SIS) als Fahndungsdatenbank, das eine informationelle Vernetzung zwischen den Mitgliedsstaaten brachte.[2] Bereits Art 102 SDÜ sah davon Abweichungen vom Fahndungszweck vor und so kann die Datenbank auch für präventive Zwecke verwendet werden. Der Rechtsschutz des Einzelnen im Rahmen von SIS ist ebenso eingeschränkt, da Auskunftserteilungen[3] an den Betroffenen unterbleiben können, „wenn dies zur Durchführung einer rechtmäßigen Aufgabe im Zusammenhang mit der Ausschreibung oder zum Schutz der Rechte und Freiheiten Dritter unerlässlich ist".

Der entscheidende Schritt vom Schengener System in eine europäische Politik fand durch die Überführung der völkerrechtlichen Schengener Verträge[4] in das Recht der Europäische Union durch den Vertrag von Amsterdam von 1997 statt. Die EU hat ergänzend dazu ihre eigenen polizeilichen Aktivitäten im Rahmen der 3. Säule (polizeiliche und justizielle Zusammenarbeit in Strafsachen) durch den Vertrag von Maastricht gestartet und diese zum Teil (Asyl, Visa, Einwanderung und andere Politiken betreffend den freien Personenverkehr) durch den Vertrag von Amsterdam in die 1. Säule (vergemeinschaftete Politikbereiche) verlagert. Durch den Vertrag von Amsterdam wurde auch die neue politische Vision des Raums der Freiheit, der Sicherheit und des Rechts geschaffen und damit die Maßnahmen der inneren Sicherheit in ein größeres politisches Konzept eingebettet, in dem die „Integration" von Polizei, Staatsanwaltschaft und Gerichten verstärkt betrieben werden konnte. Damit verbunden wurden mit dem Beginn der 1990er Jahre verstärkt Netzwerke zwischen den nationalen Institutionen und eigene europäische Institutionen, wie Europol oder Eurojust, geschaffen. Mit dem 21. Jahrhundert ist die Innenwirkung von Schengen nicht mehr losgelöst von den Entwicklungen im Rahmen des Raums der Freiheit, der Sicherheit und des Rechts zu betrachten, sondern Teil des größeren Prozesses im Rahmen der Polizei- und Justizkooperation der EU.

2. Vertrag von Prüm und die zunehmende Überwachung

Die Entwicklungen im Rahmen der ersten Säule (Visa, Asyl und Einwanderung) und der dritten Säule (Justiz und Inneres) dynamisierten sich Anfang des 21. Jahrhunderts sehr rasch. Im Bereich der inneren Sicherheit fand der Prozess vom Binnenmarkt zum Raum der Sicherheit einen vorläufigen Höhepunkt im Vertrag von Prüm, der wiederum als völkerrechtlicher Vertrag über die Vertiefung der grenzüberschreitenden Zusammenarbeit abgeschlossen wurde.[5] Ursprüngliche Vertragspartner waren die Benelux-Staaten, Deutschland, Frankreich, Spanien und Österreich. Der rechtliche Fokus ist politisches Programm: Bekämpfung des Terrorismus, der grenzüberschreitenden Kriminalität und der illegalen Migration. Die im Prümer Vertrag vorgesehenen Maßnahmen reichen dabei vom grenzüberschreitenden, automationsunterstützten DNA-Datenabgleich und anderen informationellen Kooperationsmaßnahmen bis zu zahlreichen Formen operativer Zusammenarbeit (siehe Art 24 ff Prümer Vertrag). Etliche andere rechtliche Entwicklungen runden die Integra-

1) Der österreichische Beitritt zu den Abkommen erfolgte im zeitlichen Kontext des Beitritt zur Europäischen Union (BGBl III 1997/89; BGBl III 1997/90).
2) Siehe Art 92 ff SDÜ.
3) Art 109 Abs 2 SDÜ.
4) Sog „Schengener Besitzstand", siehe ABl 2000, L 239/1-473.
5) BGBl. III Nr. 159/2006.

tion des Polizeirechts ab und zeigen, dass der Europäische Raum der Sicherheit bereits besteht. Was als völkerrechtliches Projekt für sechs Vertragsstaaten begann, wird nun für alle 27 Mitgliedsstaaten der EU umgesetzt.[6]

Aus Schengener Perspektive sollte ein freier Binnenmarkt geschaffen werden. Als Gegengewicht zur Öffnung der Binnengrenze wurde die Kooperation der inneren Polizei und Justiz beschlossen, um steigende Kriminalität zu verhindern. Die neueren Entwicklungen gehen darüber hinaus. Die durch „Schengen" geschaffene Bewegungsfreiheit wird zunehmend durch Überwachung kontrolliert. Dabei ist etwa die Fluggastdatenweitergabe an Staaten wie Kanada, Australien oder die Vereinigten Staaten zu erwähnen,[7] ebenso wie die Pläne der EU einen eigenen EU Fluggastendaten-Rahmenbeschluss zu erlassen[8] Auf informationeller Ebene repräsentiert die Vorratsdatenspeicherung eine ähnliche Tendenz, Personen zu überwachen.[9]

Die menschenrechtlichen Schranken ergeben sich primär aus Art 6 EU und damit aus der allgemeine Bedeutung der Menschenrechte im Rahmen der Europäischen Union. Damit sind sowohl die Maßnahmen im Rahmen der 3. Säule, aber auch im Rahmen der 1. Säule – wie etwa die Vorratsdatenspeicherung – erfasst. Die Bindung an die Menschenrechte bringt wiederum die Berücksichtigung des Grundrechts auf Privatleben gem Art 8 EMRK und das darin zum Ausdruck kommende Grundrecht auf Datenschutz mit sich.[10] In der konkreten Abwägung der spezifischen Maßnahme und den Menschenrechten sind allerdings die Einschränkungen der Anrufbarkeit der Gerichte gem Art 35 EU zu berücksichtigen.

3. Informationelle Vernetzung

Von besonderer Bedeutung in der Polizeikooperation ist – wie dargestellt – die informationelle Ermittlung, Verarbeitung und Weitergabe von Daten. Die Datensammlungen im Rahmen der Polizeikooperation sind beachtlich. Dabei sind etwa das Schengener Informationssystem (SIS), dessen in Umsetzung befindliche Weiterentwicklung SIS II, die Europol-Datenbanken oder die Prümer Datenverbunde zu erwähnen. Andere Datenbanken im Bereich Asyl und Visa sind etwa die Fingerabdruckdatenbank Eurodac[11] oder die Visa-Datenbank VIS[12]. Problematisch ist allerdings der Verbund der Datenbanken untereinander.[13] Damit entsteht ein stärkerer Grundrechtseingriff als die Summe der Eingriffe der beiden Datenbanken. Das staatliche Informationspotential gegenüber den Einzelnen nimmt unproportional zu. Insoweit ist die Schaffung neuerer Datenbanken ebenso wie die Verknüpfung derselben grundrechtlich und rechtsstaatlich höchst bedenklich. Durch die Verknüpfung der Datenbanken geht die Zuordnung zu einem spezifischen Zweck verloren. Damit unmittelbar verbunden sind die Rechtsschutzdefizite im Rahmen der polizeilichen Informationsverwaltung. Diese liegen primär in einem Informationsdefizit der betroffenen Person hinsichtlich des Wissens, dass personenbezogene Daten verarbeitet werden, sowie in zu extensiven Möglichkeiten der Behörden zur Auskunftsverweigerung.

4. Defizitärer Rechtsschutz: der Rahmenbeschluss zum Schutz personenbezogener Daten als Beispiel

Der neue Rahmenbeschluss zum Datenschutz (RB)[14] kann als Beispiel für die Problematik der Rechtsschutzdefizite im Datenschutz dienen. Der RB soll den Schutz personenbezogener Daten regeln. Er erstreckt sich auf Daten, die aufgrund von Kooperationen der Mitgliedstaaten untereinander oder mit Informationssystemen der EU übermittelt werden sowie auf Daten, die aufgrund europäischer Rechtsakte übermittelt werden sollen. Dabei ist als erstes Defizit vorab festzuhalten, dass der RB bestehende zentrale Datenbanken wie Europol-Datenbanken oder SIS aus seinem Anwendungsbereich ausnimmt.[15]

Auch in Hinblick auf die Weiterverwendung von Daten für andere Zwecke geht der RB denkbar weit. So ist gem

6) Siehe den Beschluss 2008/615/JI des Rates vom 23.6.2008 zur Vertiefung der grenzüberschreitenden Zusammenarbeit, insbesondere zur Bekämpfung des Terrorismus und der grenzüberschreitenden Kriminalität, ABl 2008, L 210/1.

7) Siehe den Beschluss des Rates 2006/230/EG über den Abschluss eines Abkommens zwischen der Europäischen Gemeinschaft und der Regierung Kanadas über die Verarbeitung von API/PNR-Daten, ABl 2006, L 82/14; Abkommen zwischen der Europäischen Union und den Vereinigten Staaten von Amerika über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) und deren Übermittlung durch die Fluggesellschaften an das United States Department of Homeland Security (DHS), ABl 2007, L 204/18; Abkommen zwischen der Europäischen Union und Australien über die Verarbeitung von Fluggastdatensätzen (Passenger Name Records – PNR) aus der Europäischen Union und deren Übermittlung durch die Fluggesellschaften an die australische Zollbehörde, ABl 2008, L 213/49.

8) Siehe den Vorschlag der Kommission für einen Rahmenbeschluss über die Verwendung von Fluggastdatensätzen (PNR-Daten) zu Strafverfolgungszwecken, KOM 2007/0654 endg. Dazu kritisch die Stellungnahme des Europäischen Datenschutzbeauftragten (EDSB), ABl 2008, C 110/1.

9) Richtlinie 2006/24/EG über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, ABl 2006, L 105/54. Vgl auch die jüngst zur Vorratsdatenspeicherungs-Richtlinie ergangene Entscheidung des EuGH 10.2.2009, Rs C 301/06, *Irland/Parlament und Rat*.

10) Siehe *Siemen*, Datenschutz als europäisches Grundrecht (2006)

11) Siehe die VO (EG) 2725/2000 über die Einrichtung von „Eurodac" für den Vergleich von Fingerabdrücken zum Zwecke der effektiven Anwendung des Dubliner Übereinkommens, ABl 2000, L 316/1.

12) Siehe VO (EG) 767/2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung), ABl 2008, L 218/60.

13) Siehe etwa den Beschluss 2008/633/JI des Rates vom 23. Juni 2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten, ABl 2008, L 218/129.

14) Siehe den Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl 2008, L 350/60 (im Folgenden: RB).

15) Siehe den 39. Erwägungsgrund des RB: „Verschiedene auf der Grundlage von Titel VI des Vertrags über die Europäische Union erlassene Rechtsakte enthalten spezifische Vorschriften über den Schutz personenbezogener Daten, die gemäß den Bestimmungen dieser Rechtsakte ausgetauscht oder anderweitig verarbeitet werden. Diese Vorschriften bilden in einigen Fällen ein vollständiges, in sich geschlossenes Regelwerk, das alle relevanten Datenschutzaspekte […] erfasst, und regeln diese Fragen ausführlicher als dieser Rahmenbeschluss. Die einschlägigen Datenschutzvorschriften dieser Rechtsakte, […] bleiben von dem vorliegenden Rahmenbeschluss unberührt."

Art 3 Abs 2 RB die Weiterverarbeitung zu anderen Zwecken bei Notwendigkeit und Verhältnismäßigkeit zulässig.[16] Dies bedeutet aber, dass auf Ebene des RB keine konkreten Einschränkungen erfolgen, sondern der Vollziehung ein (zu) großer Spielraum eröffnet wird. Die Zwecke der Weiterverarbeitung werden durch Art 11 RB geregelt[17] und sind ebenso denkbar weit, etwa „die Verhütung, Ermittlung, Feststellung oder Verfolgung von Straftaten […]; die Abwehr einer unmittelbaren und ernsthaften Gefahr für die öffentliche Sicherheit; oder jede[r] andere Zweck [!] nur mit der vorherigen Zustimmung des übermittelnden Mitgliedstaats oder mit Einwilligung der betroffenen Person, die sie im Einklang mit dem innerstaatlichen Recht erteilt hat." Der RB schützt damit personenbezogene Daten nicht, sondern legitimiert deren Weitergabe. Es reicht dabei die Zustimmung des übermittelnden Staates aus. Die Betroffenen müssen grundsätzlich nicht zustimmen, ja sie erfahren nicht einmal von der Weiterverarbeitung der personenbezogenen Daten.

Informationspflichten – also die Voraussetzung für effektiven Rechtsschutz – werden nur nach innerstaatlichen Vorgaben erteilt (Art 16 Abs 1 RB). Diese bestehen allerdings regelmäßig nicht. Überdies legitimiert Art 16 Abs 2 RB dazu, dass jeder Mitgliedstaat – nach innerstaatlichen Vorgaben – einen anderen Mitgliedsstaat ersuchen kann, die betroffene Person nicht zu informieren.

Das Gegenstück zur Informationspflicht ist die Auskunftspflicht, die in Art 17 RB geregelt ist. Dabei kommt der einzelnen Person grundsätzlich das Recht zu, frei und ungehindert und ohne unzumutbare Verzögerung oder übermäßig hohe Kosten, Auskunft zu erhalten. Das Mindestmaß an Auskunft stellt eine „Bestätigung von der nationalen Kontrollstelle" (etwa der Datenschutzkommission) dar, dass „alle erforderlichen Überprüfungen durchgeführt wurden".[18] Eine Information über den Gegenstand der Datenverarbeitung, also den Grund weshalb überhaupt Daten polizeilich verarbeitet werden, kann bei Notwendigkeit und Verhältnismäßigkeit entfallen, um „behördliche oder gerichtliche Ermittlungen, Untersuchungen oder Verfahren nicht zu behindern; die Verhütung, Feststellung, Ermittlung oder Verfolgung von Straftaten nicht zu beeinträchtigen oder um strafrechtliche Sanktionen zu vollstrecken; die öffentliche Sicherheit zu schützen; die Sicherheit des Staates zu schützen oder die betroffene Person und die Rechte und Freiheiten anderer zu schützen."[19] Die betroffene Person ist zwar über die Verweigerung der Auskunft schriftlich zu informieren; ihr sind auch „die tatsächlichen oder rechtlichen Gründe, auf die die Entscheidung gestützt wird, mitzuteilen"[20]. Diese Mitteilung kann aber aus denselben Gründen entfallen, die zu einer Verweigerung der Auskunft geführt haben. In diesen Fällen hilft auch der Hinweis der Beschwerde bei der zuständigen nationalen Kontrollstelle wenig.

Dies bedeutet zusammenfassend, dass die Einzelne aufgrund des RB zum Schutz (!) personenbezogener Daten über die Datenverwendung im Rahmen der Polizei und Justiz in vielen Fällen nicht informiert wird und auch keine Auskunft erhält. Die Gründe der Verweigerung der Auskunft sind dabei beinahe ebenso weit gefasst wie die Gründe zur Weiterverwendung der Daten für andere Zwecke. Die rechtlich-inhaltlichen Möglichkeiten betroffener Personen sind stark beschränkt, womit die prozeduralen Kontrollmöglichkeiten ins Leere laufen. Die Kontrolle der gesetzeskonformen Ausübung der Befugnisse der Behörde verbleibt damit in der innerstaatlichen Organisation und gibt dem Einzelnen nicht die Möglichkeit, sich effektiv zu wehren. All dies wird durch die Regeln zum europäischen Datenschutz in den Bereichen Justiz und Inneres ermöglicht, bestätigt und legitimiert.

Ähnliche Bestimmungen wie im neuen Rahmenbeschluss finden sich in den Datenschutzregeln des Vertrags von Prüm[21] oder in der Europol-Konvention.[22] Auch die österreichische Auskunftsregelung gem § 26 DSG sieht entsprechende Einschränkungen der Auskunftspflicht vor.[23] Im Gesamten zeigt sich ein Rechtsschutzdefizit bei der informationellen Verarbeitung in den Polizeikooperationen. Maximalfristen, nach denen zwingend Informationen an betroffene Personen zu geben sind, und Rechtsschutzmechanismen, die es der Einzelnen ermöglichen, sich effektiv gegen die europäischen Informationsverbünde zu wehren, bestehen nicht.

5. Ein Ausblick zur Außenwirkung der inneren Sicherheit

Zum Abschluss führt „der Blick nach innen" in die andere Richtung, nämlich nach außen. Sicherheitskooperationen wie sie durch Schengen begonnen wurden, lassen sich längst nicht mehr auf die Kooperation der Mitgliedsstaaten der Europäischen Union beschränken. Zahlreiche bi- und multilaterale Abkommen externalisieren Maßnahmen zur inneren Sicherheit über die Grenzen der europäischen Union hinaus. Das bekannteste Beispiel stellt die Weitergabe der Fluggastdaten an die Vereinigten Staaten dar.[24] Dabei bleibt es allerdings nicht. Die Weitergabe von Informationen und der Aufbau von Informationskooperationen mit Drittstaaten befinden sich in voller Entwicklung. Internationale Polizeikooperation in bezug auf Informationen (also auch personenbezogene Daten) befindet sich dabei im Ausbau. Diese erfolgt auf Ebene der Europäischen Union ebenso wie innerstaatlich.

Abschließend sei daher auf die von Europol abgeschlossenen internationalen Verträge hingewiesen: Operative Abkommen bestehen mit Australien, Kanada, Kroatien, Island, Norwegen, der Schweiz, den Vereinigten Staaten; strategische Übereinkommen bestehen mit Albanien, Bosnien und Herzegowina, Kolumbien, Mazedonien, Russland und der

16) Als weitere Vorgaben normiert Art 3 Abs 2 RB, dass „die Weiterverarbeitung zu einem anderen Zweck […] zulässig [ist] soweit diese Verarbeitung mit den Zwecken, zu denen die Daten erhoben worden sind, nicht unvereinbar ist [und] die zuständigen Behörden nach den für sie geltenden Rechtsvorschriften zur Verarbeitung solcher Daten zu einem anderen Zweck befugt sind". Damit sind aber keine wesentlichen Eingrenzungen vorgenommen, die über das Legalitätsprinzip hinausreichen.

17) In diesem Zusammenhang ist auch die Bestimmung des Art 13 RB relevant, die „eine Weiterleitung an die zuständigen Behörden in Drittstaaten oder an internationale Einrichtungen" unter ebenso allgemeinen Kriterien generell ermöglicht.

18) Art 17 Abs 1 lit b RB.

19) Art 17 Abs 2 RB.

20) Art 17 Abs 3 RB.

21) Siehe Art 33 ff Prümer Vertrag und im Besonderen Art 40 Abs 1 leg cit.; siehe zur Einschränkung gem § 26 DSG sogleich.

22) Siehe Art 19 Europol-Konvention.

23) Siehe § 26 Abs 2 iVm Abs 5 DSG.

24) Siehe dazu bereits in FN 5.

Türkei. In Österreich bestehen bilaterale Abkommen mit allen Nachbarstaaten sowie etwa mit Albanien, Aserbaidschan, Bosnien und Herzegowina, Bulgarien, Kroatien, Lettland, Montenegro, Polen, Serbien, Südafrika und Usbekistan.[25]

Der Austausch personenbezogener Daten ist dabei die Regel. Als Beispiel dient etwa der bilaterale Vertrag zwischen Österreich und Bulgarien.[26] Dessen Art 2 Abs 3 legt fest: „Informationen […] teilt die zuständige Behörde jeder Vertragspartei nach Maßgabe ihres nationalen Rechts der zuständigen Behörde der anderen Vertragspartei auch ohne Ersuchen mit, wenn sie für die andere Vertragspartei für die Abwehr von Gefahren für die öffentliche Sicherheit und Ordnung oder die Vorbeugung und Aufklärung von Straftaten von Bedeutung sein können. Die Vertragsparteien unterstützen einander hiebei insbesondere dann, wenn im Staatsgebiet einer Vertragspartei eine Straftat vorbereitet oder begangen wird und Anzeichen dafür bestehen, dass dies Auswirkungen auf dem Staatsgebiet der anderen Vertragspartei haben könnte." Die Regelung ist denkbar allgemein und gibt großen Spielraum bei der Anwendung. Die regelmäßig vorgesehenen Datenschutzbestimmungen sehen eine Zweckbindung vor und das Verbot der Verwendung dieser Daten für andere Zwecke. Die effektive Überprüfung, was mit den Daten wirklich geschieht, ist aber für die betroffenen Personen nicht gewährleistet. Hier müssen die Vertrag schließenden Staaten einander vertrauen: ein sehr problematischer Zustand, besonders für jene Personen, deren Daten übertragen werden.

Über die unterschiedlichen völkerrechtlichen Verträge beginnen EU-Staaten Informationen zu verteilen und geben diese – je nach Vertrag – auch an Drittstaaten weiter. Die Informationspflicht von Betroffenen als datenschutzrechtliche Mindestbedingung wird dabei nicht gewährleistet. Der Einzelne weiß also von alledem nichts und wird auch nicht informiert. Als Mindestmaß eines adäquaten Umgangs mit personenbezogenen Daten ist die Information des Einzelnen und dies sobald als möglich zu sehen; jedenfalls muss es einen Zeitpunkt geben, in dem die Einzelne von der Verarbeitung ihrer Daten erfährt.

Dr. Konrad Lachmayer ist Assistent am Institut für Staats- und Verwaltungsrecht der Universität Wien und Redaktionsmitglied des juridikum; konrad.lachmayer@univie.ac.at

25) BGBl III 2002/206 (Bulgarien), BGBl III 2004/19 (Lettland), BGBl III 2004/143 (Südafrika), BGBl III 2005/10 (Montenegro), BGBl III 2006/44 (Aserbaidschan), BGBl III 2007/99 (Bosnien-Herzegowina), BGBl III 2007/134 (Albanien), BGBl III 2001/120 (Schweiz/Liechtenstein), BGBl III 2005/72 (Slowakei), BGBl III 2008/141 (Kroatien), BGBl III 2005/20 (Serbien), BGBl III 2003/193 (Polen), BGBl III 2000/52 (Italien), BGBl III 2005/51 (Slowenien), BGBl III 2005/210 (Deutschland), BGBl III 2006/121 (Tschechien), BGBl III 2006/99 (Ungarn), BGBl III 2002/91 (Usbekistan).
26) BGBl III 2002/206.