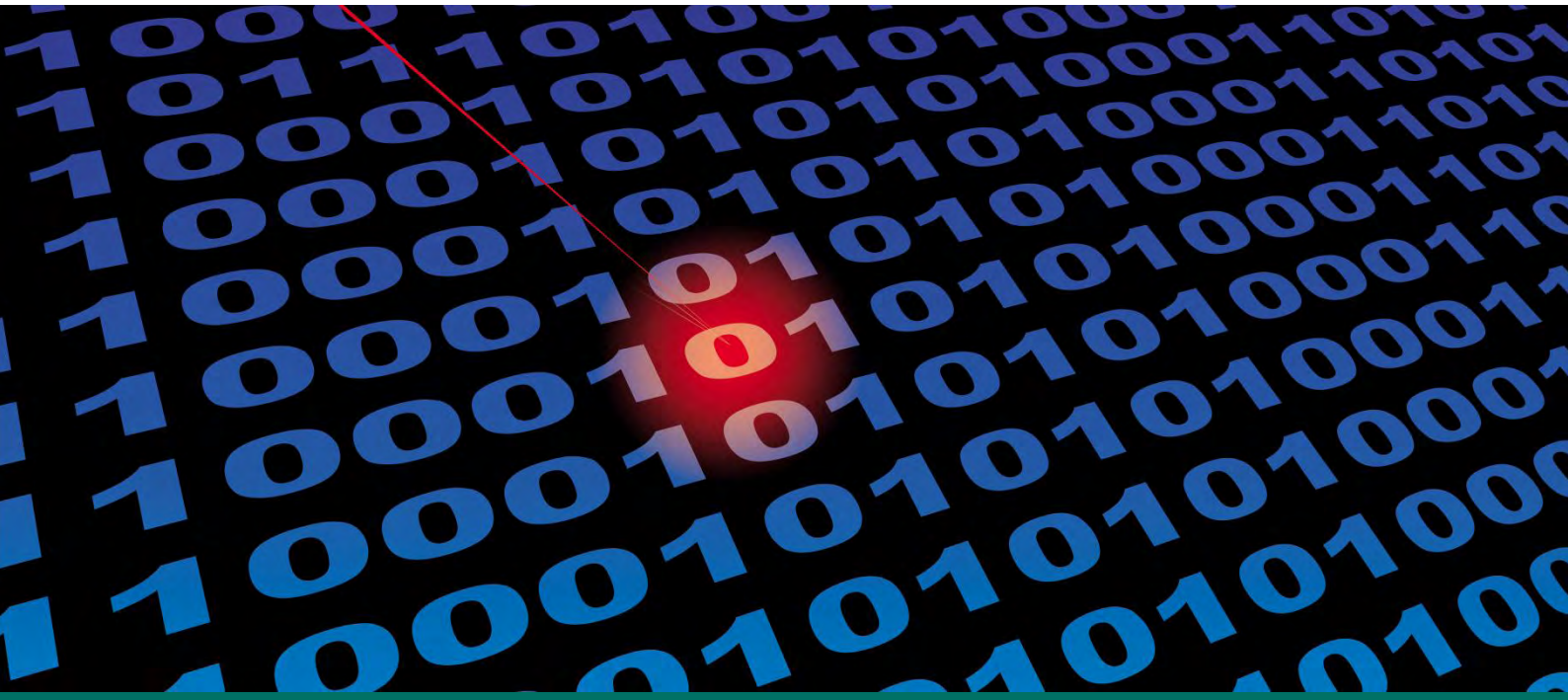
Max-Planck-Institut
für ausländisches und
internationales Strafrecht

Schutzlücken durch Wegfall der Vorratsdatenspeicherung?

Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten



Gutachten

der kriminologischen Abteilung des
Max-Planck-Instituts für ausländisches
und internationales Strafrecht

im Auftrag des Bundesamtes für Justiz

zu möglichen Schutzlücken durch den Wegfall
der Vorratsdatenspeicherung

2., erweiterte Fassung

Freiburg i.Br., Juli 2011

Beteiligte Mitabeiter und Autoren:

Prof. Dr. Dr. h.c. Hans-Jörg Albrecht (Gesamtverantwortung)
Dr. Phillip Brunst
Dr. Els De Busser
Dr. Volker Grundies
Dr. Michael Kilchling
Dr. Johanna Rinceanu, LL.M.
Brigitte Kenzel
Nina Nikolova
Sophie Rotino
Moritz Tauschwitz

Gesamtredaktion:

Dr. Michael Kilchling

Titelbild:

ilco / stock.xchng

Vorbemerkungen

Bei dem vorliegenden Bericht handelt es sich um die zweite, erweitere Version einer Untersuchung, die zunächst zwischen Mai 2010 und August 2010 durchgeführt worden ist. Der Bericht enthält eine Bestandsaufnahme der Situation im Bereich der Verkehrsdatenabfrage seit dem Urteil des BVerfG vom 2.3.2010 zur Vorratsdatenspeicherung. Der Schwerpunkt liegt dabei auf der Ermittlung praktischer Probleme auf dem Gebiet der Strafverfolgung und der Gefahrenabwehr infolge des – zumindest partiellen – Wegfalls auswertungsfähiger Verkehrsdaten. Wichtigste Erkenntnisquelle waren qualitative Interviews mit den an der Vorbereitung, Durchführung und Auswertung von Verkehrsdatenabfragen beteiligten Praktikern. Die Untersuchung enthält sich rechtlicher Bewertungen der geschilderten Vorgänge, insbesondere auch im Hinblick auf die Ideen und Vorschläge der zahlreichen Interviewpersonen für eine mögliche gesetzliche Neugestaltung des Bereichs der Vorratsdatenspeicherung.

Der unterschiedliche Umfang der Interview-Kapitel in Teil F ist nicht das Produkt ungleicher Gewichtung der verschiedenen Gesprächsrunden. Die Unterschiede sind vielmehr als Abbild des jeweiligen Ertrags der Gespräche zu interpretieren. Sie spiegeln damit insbesondere auch die operative Nähe der Ermittler wider, die ganz unmittelbar mit den Konsequenzen aus dem Wegfall der Vorratsdatenspeicherung konfrontiert sind. Entsprechend ausführlich und detailreich fielen ihre Schilderungen aus. Keines dieser Gespräche dauerte weniger als eineinhalb Stunden, mehrere hingegen zwei bis zweieinhalb Stunden. Weniger Informationsgehalt lieferten hingegen, dies war im Hinblick auf die schon in den vorbereitenden Gesprächen geäußerten Bedenken nicht unerwartet, die Beiträge der befragten Richter.

Ergänzt wurde der Bericht 2011 neben weiteren Interviews und Materialien der Bundesnetzagentur zur aktuellen Speicherpraxis der Telekommunikations-Anbieter insbesondere durch Untersuchungen zur Entwicklung der Gesetzgebung in Österreich und Schweden, eine Bewertung des Evaluationsberichtes der Europäischen Kommission zur Vorratsdatenspeicherung in der EU sowie eine Analyse der Auswirkungen der Vorratsdatenspeicherung auf der aggregierten Ebene der Aufklärungsquoten.

In einzelnen Punkten weicht das Gutachten von der ursprünglichen Forschungskonzeption ab. Dies betrifft namentlich das Vorhaben, über die Landesjustizverwaltungen belastbare statistische Angaben zu der quantitativen Entwicklung der Abfragen und zu Einstellungen wegen nichtbeauskunfteter Verkehrsdatenabfragen zu erhalten. Dies war in dem engen Zeitrahmen und wegen des damit verbundenen organisatorischen Aufwandes nicht zu realisieren (siehe hierzu auch Teil A, Pkt. 3.2.1.). Belastbare Zahlen lassen sich nur in einer Echtzeiterhebung durchführen, die mit erheblichem

Aufwand verbunden ist, auch für die Praxis. Eine solche empirische Erhebung ist derzeit in Vorbereitung und wird vom Freiburger Max-Planck-Institut für ausländisches und internationales Strafrecht im Herbst 2011 gesondert, d.h. außerhalb des formalen und zeitlichen Rahmens des vorliegenden Gutachtens, in drei Bundesländern durchgeführt. Die Ergebnisse werden voraussichtlich zum Jahresende 2011 vorgelegt werden. In der Zusammenschau mit weiteren, bis dahin erwarteten statistischen Zahlen zu der Entwicklung der Maßnahmen gem. §§ 100g und 100a StPO wird dann eine umfassende Analyse der Situation der Verkehrsdatenabfrage in Deutschland möglich sein.

Über die Fragestellungen der vorliegenden Untersuchung hinaus fielen im Vergleich zu der MPI-Studie 2008 im Übrigen deutliche Veränderungen beim Phänomen des Enkeltricks auf. Während es sich dabei seinerzeit eher noch um eine Randerscheinung zu handeln schien, gab es im Zuge des vorliegenden Projektes nahezu kein Gespräch, in dem nicht die hohe Relevanz dieser von zahlreichen Gesprächspartnern mittlerweile sogar der OK zugeordneten oder gerade an der Grenze zur OK eingeordneten Deliktsform hervorgehoben wurde.

Das Max-Planck-Institut dankt den Mitarbeiterinnen und Mitarbeitern des Bundeskriminalamtes für ihre großzügige Unterstützung bei der Expertenbefragung. Ohne die effektive organisatorische und logistische Unterstützung wäre es nicht möglich gewesen, die Vertreterinnen und Vertreter der verschiedenen Polizeibehörden des Bundes und aller 16 Bundesländer so ausführlich in face-to-face-Interviews zu befragen. Entsprechender Dank gebührt auch den vielen Mitwirkenden, die die Reise nach Wiesbaden oder Berlin auf sich genommen haben, um an den Gesprächen persönlich teilzunehmen.

Inhaltsverzeichnis

Verzeichnis der Tabellen und Schaubilder

Literaturverzeichnis

Aebi, M.F. u. a.: European Sourcebook of Crime and Criminal Justice Statistics 2010. WODC, Den Haag 2010.

Ahlberg, J.: Crime clearance and efficiency. An analysis of the factors affecting trends in the clear-up rate. Stockholm 2002.

Albrecht, H.-J., Dencker, F. u. a. (Hrsg.): Organisierte Kriminalität und Verfassungsstaat. Deutsche Sektion der Internationalen Juristen-Kommission. Rechtsstaat in der Bewährung. Bd. 33. Heidelberg 1998.

Albrecht, H.-J., Dorsch, C., Krüpe, C.: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen. Freiburg 2003.

Albrecht, H.-J., Grafe, A., Kilchling, M.: Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO. Berlin 2008.

Altstötter, C.: Pornografie und neue Medien. Eine Studie zum Umgang Jugendlicher mit sexuellen Inhalten im Internet. Mainz 2006.

Alvaro, A.: Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus. Ausschuss für bürgerliche Freiheiten, Justiz und Inneres, Europäisches Parlament, Arbeitsdokument vom 21.1.2005.

Bär, W.: Handbuch zur EDV-Beweissicherung im Strafverfahren, Stuttgart 2007.

Blinkert, B.: Kriminalität als Modernisierungsrisiko? Das “Hermes-Syndrom” der entwickelten Industriegesellschaften. Soziale Welt 39(1988), S. 397-412.

Blunn, A.: Report of the Review of the Regulation of Access to Communications. Commonwealth of Australia 2005.
www.ag.gov.au/www/agd/rwpattach.nsf/VAP/%28CFD7369FCAE9B8F32F341DBE097801FF%29~xBlunn+Report+13+Sept.pdf/$file/xBlunn+Report+13+Sept.pdf.

Brunst, P.: Anonymität im Internet - rechtliche und tatsächliche Rahmenbedingungen: zum Spannungsfeld zwischen einem Recht auf Anonymität bei der elektronischen Kom-

munikation und den Möglichkeiten zur Identifizierung und Strafverfolgung. Strafrechtliche Forschungsberichte aus dem Max-Planck-Institut für ausländisches und internationales Strafrecht. Berlin 2009.

Brunst, P., Sieber, Ulrich: Cybercrime Legislation in Germany, in: Basedow, J., Kischel, U., Sieber, U. (Hrsg.): German National Reports to the XVIII. International Congress of Comparative Law. Tübingen 2010.

Büllingen, F.: Vorratsspeicherung von Telekommunikationsdaten im internationalen Vergleich, DuD 2005, S. 349-353.

Bund Deutscher Kriminalbeamter Landesverband Hessen: BDK-Verbandszeitschrift Nr. 10, Oktober 2010 – Onlineausgabe, S. 6.

Burgheim, J.: Stalking – Erklärungsansätze und neue Forschungsergebnisse. Die Kriminalpolizei 2007, S. 52-58, S. 57.

Cameron, D., Clegg, N.: The Coalition: our programme for government. Cabinet Office, London 2010. www.cabinetoffice.gov.uk/media/409088/pfg_coalition.pdf.

Crump, C.: Data Retention: Privacy, Anonymity, and Accountability Online. Stanford Law Review 56 (2003), S. 191-229.

Diekmann, A.: Empirische Sozialforschung. Reinbek 2007.

Dix, A.: Informations- und Kommunikationskriminalität. Kriminalistik 2004, S. 81-85.

Dölling, D., Meier, B.-D., Verrel, T., Götting, B. (Hrsg.): Verbrechen – Strafe – Resozialisierung. Festschrift für Heinz Schöch zum 70. Geburtstag. Berlin 2010.

Dölling, D.: Die Dauer von Strafverfahren vor den Landgerichten. Köln 2000.

Etzel, T.: §238 StGB (Nachstellen) in der anwaltlichen Praxis. Lawzone 1(2010), S. 17-22.

European Commission: Report From the Commission to the Council and the European Parliament Evaluation report on the Data Retention Directive. Brussels 18. 4. 2011.

Fabrizy, E.: Die österreichische Strafprozessordnung (StPO), Kurzkommentar, 10. Auflage. Wien 2009.

Feil, C.: Kinder und Internet – Chancen und Gefahren. Recht der Jugend und des Bildunsgwesens 58(2010), S. 410-415.

Fünfsinn, H.: Erste Erfahrungen mit dem Stalking-Bekämpfungsgesetz. Lawzone 1(2010), S. 13-16.

Gaspar, R.: NCIS Submission on Communications Data Retention Law: Looking to the Future. Clarity on Communications Data Retention Law. Submission to the Home Office For Legislation on Data Retention. London, 2000. http://cryptome.org/ncis-carnivore.htm.

Geppert, M., Piepenbrock, H.-J., Schütz, R.: Beck'scher TKG-Kommentar, 3. Auflage. München 2006.

Gercke, M., Brunst, P.: Praxishandbuch Internetstrafrecht. Stuttgart 2009.

Gilbert, D., Kerr, I., McGill, J.: The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunication Providers. Criminal Law Quarterly 51:4 (2006) S. 469-507. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1302544.

Greenwood, P. W., Chaiken, J., Petersilia, J.: The criminal investigation process. Lexington 1977.

Hebrok, T.: Strukturermittlungen im Spannungsfeld von Effizienz der Strafverfolgung zum Rechtsschutz des Einzelnen. Aachen 2007.

Henrichs, A.: Funkzellenauswertung. Rechtliche und taktische Aspekte der telekommunikativen Spurensuche. Die Kriminalpolizei 2010. www.kriminalpolizei.de/articles,funkzellenauswertung,1,275.htm

Hinduja, S.: Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future. International Journal of Cyber Criminology 1(2007), S. 1-26, S. 13.

Kilchling, M.: Die Neuregelung zur Auslandskopfüberwachung gemäß § 4 TKÜV auf dem verfassungsrechtlichen Prüfstand. Gutachten im Auftrag des VATM. Freiburg i. Br. 2006. www.mpicc.de/de/data/pdf/auslandskopf_publ-1.pdf.

Kinzig, J.: Die rechtliche Bewältigung von Erscheinungsformen organisierter Kriminalität. Berlin 2004.

Larnhof, K.: Data Retention - Zur aktuellen Rechtslage in einigen EU-Mitgliedsländern unter Berücksichtigung der EU-Richtlinie zur Vorratsdatenspeicherung. Diplomarbeit FH Eisenstadt 2006.

Lawrence, K.: Investigation into the Murder of Hell´s Angel Gerard Tobin on the M40: A Murder committed by an Organised Crime Group against another. The Journal of Homicide and Major Incident Investigation 5(2009), S. 39-52, S. 42.

Liederbach, J., Fritsch, E. J., Womack, C. L.: Detective workload and opportunities for increased productivity in criminal investigations. Police Practice and Research 12(2011), S. 50-65, S. 50.

Livingstone, S., Haddon, L., Görzig, A., Ólafsson, K.: Risks and Safety on the Internet. The perspective of European children. Initial findings from the EU Kids Online survey of 9-16 year olds and their parents. www.eukidsonline.net, 21. Oktober 2010, S. 11.

LKA Nordrhein-Westfalen: Kampagne gegen Enkeltrick. Düsseldorf 4. März 2009.

Long, C., Bratby, R. (Hrsg.): The International Comparative Legal Guide to telecommunication Laws and Regulations 2010, 3. Auflage. London 2010.

Ludwig Boltzmann Institut für Menschenrechte: Rechtsvergleichende Analyse im Hinblick auf die Umsetzung der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung. Wien 2008.

Ludwig, J.: Enkeltrick – Grenzen der Ermittlungen und der Prävention. der kriminalist 41(2009), S. 4-9.

Ludwig, J.: Enkeltrick – Kollektive Strafvereitelung durch Unzuständigkeit? der kriminalist 38(2006), S. 55- 60, S. 55, 59.

Malmström, C.: Member of the European Commission responsible for Home Affairs: Taking on the Data Retention Directive European Commission conference in Brussels. Brüssel, 3. Dezember 2010.

Meyer-Wieck, H.: Der Große Lauschangriff – eine empirische Untersuchung zu Anwendung und Folgen § 100c Abs. 1 Nr. 3 StPO. Berlin 2005.

Milford, P.: The retention of communications data: a view from industry. PLC IP& IT, 19. 11. 2008. www.ld.practicallaw.com/5-384-0822.

Mitchell, K.J., Finkelhor, D., Jones, L.M., Wolak, J.: Use of Social Networking Sites in Online Sex Crimes Against Minors: An Examination of National Incidence and Means of Utilization. Journal of Adolescent Health 47 (2010) S. 183–190.

Neagu, I.: Tratat de procedură penală, Partea generală, Ediția a II–a, revăzută şi adăugită. Bukarest 2010.

Pehl, D.: Die Implementation der Rasterfahndung – Eine empirische Untersuchung der gesetzlichen Regelungen zur operativen Informationserhebung durch Rasterfahndung. Berlin 2008.

Pujazon-Zazik, M., Park, M.J.: To Tweet, or Not to Tweet: Gender Differences and Potential Positive and Negative Health Outcomes of Adolescents' Social Internet Use. American Journal of Mens Health 4(2010), S. 77-85, S. 81.

Rau, L.: Phänomenologie und Bekämpfung von „Cyberpiraterie". Göttingen 2004.

Ringland, K.: The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model*, 5* Shidler J. L. Com. & Tech. 13 (2009). www.lctjournal.washington.edu/vol5/a13Ringland.html.

Roberts, L.: Cyber-Victimisation in Australia. Extent, Impact on Individuals and Responses. Hobart 2008.

Roßnagel, A.: Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung. NJW 2010, S. 1238-1242.

Rusch, S.: Das „Gesetz zur Strafbarkeit beharrlicher Nachstellung" – Allheilmittel polizeilicher Intervention bei Stalking? Lawzone 1(2010), S. 22-30.

Rowland, D.: Data Retention and the War Against Terrorism – A Considered and Proportionate Response? T*he Journal of Information, Law and Technology (JILT) 2004.* www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_3/rowland/.

Schramm, S., Wegener, C.: Neue Anforderungen an eine anlasslose Speicherung von Vorratsdaten – Umsetzungsmöglichkeiten der Vorgaben des Bundesverfassungsgerichts. MMR 2011, S. 9-13.

Schrock, A., Boyd, D.: Online Threats to Youth: Solicitation, Harassment, and Problematic Content. Literature Review Prepared for the Internet Safety Technical Task Force http://cyber.law.harvard.edu/research/isttf. Berkman Center for Internet & Society Harvard University, 31. Dezember, 2008, S. 17.

Sessar, K.: Rechtliche und soziale Prozesse einer Definition der Tötungskriminalität. Freiburg 1981.

Shannon, D.: Vuxnas kontakter med barn via Internet. Omfattning, karaktär, åtgärder (The online sexual solicitation of children by adults in Sweden). Report 11. Stockholm 2007.

Sierck, G. M., Schöning, F., Pöhl, M.: Wissenschaftliche Dienste des Deutschen Bundestages, Gutachten zur „Zulässigkeit der Vorratsdatenspeicherung nach europäischem und deutschem Recht". Berlin 2006.

Smith, A.: PEW Internet and American Life Project. 14.10.2007, www.pewinternet.org.

Spindler, G., Schuster, F. (Hrsg.): Recht der elektronischen Medien. München 2008.

Stahlmann-Liebelt, U.: § 238 StGB - Das Wundermittel der Zukunft? Gemeinsam gegen Stalking. Fachtagung am 31. Oktober 2007 im Landeshaus in Kiel.

Stanley J.: The Surveillance-Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society. American Civil Liberties Union. New York 2004.

Tinnefeld, M.-T., Ehmann, E., Gerling, R.: Einführung in das Datenschutzrecht, 4. Auflage. München 2005.

U.S. Department of Justice, Office of the Inspector General Audit Division: The Federal Bureau of Investigation´s Efforts to Combat Crimes Against Children. Washington 2009.

de Vries, K., Bellanova, R., De Hert, P.: Proportionality overrides Unlimited Surveillance. The German Constitutional Court Judgment on Data Retention. European Center for Policy Studies, Brüssel 2010.

Walker, C., Akdeniz, Y.: Anti-Terrorism Laws and Data-Retention: War is Over? Northern Ireland Legal Quarterly 2003, H. 2, S. 159-182.

Walker, C.: Data retention in the UK: Pragmatic and proportionate, or a step too far? Computer law & security review 25 (2009), S. 325-334.

Wolak, J., Finkelhor, D., Mitchell, K.: Internet-initiated Sex Crimes against Minors: Implications for Prevention Based on Findings from a National Study. Journal of Adolescent Health 35(2004), S. 424.e11– 424.e20.

Wolak, J., Mitchell, K., Finkelhor, D.: Unwanted and Wanted Exposure to Online Pornography in a National Sample of Youth Internet Users. Pediatrics 119(2007), S. 247-257.

Hinweise zu Gender Mainstreaming:

Zur leichteren Lesbarkeit der Texte wurde die männliche Form von personenbezogenen Hauptwörtern gewählt. Eine Benachteiligung des weiblichen Geschlechts ist damit nicht beabsichtigt.

Ferner erscheinen in Teil F zur Vermeidung einer Reidentifikation einzelner Personen anhand des Geschlechts alle Interviewpartner in der männlichen Form.

Teil A: Einleitung

1. Einführung

Die vorliegende Untersuchung befasst sich mit der Frage, welche Auswirkungen das Fehlen von auf Vorrat gespeicherten Verkehrsdaten der Telekommunikation für Strafverfolgung und Gefahrenabwehr hat. Anlass ist die Entscheidung des Bundesverfassungsgerichts vom März 2010, in der die durch die deutsche Umsetzung der Richtlinie 2006/24 (Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG (BT-Drs. 16/545) modifizierten bzw. eingeführten §§113a, 113b TKG sowie §100g StPO, soweit er sich auf §113a TKG bezieht, wegen Verstoßes gegen Art. 10 GG für nichtig erklärt wurden und die sofortige Löschung der bis dahin auf dieser gesetzlichen Grundlage gespeicherten Verkehrsdaten angeordnet wurde[1].

Die Untersuchung greift die Frage der Auswirkungen fehlender Speicherung von Telekommunikationsverkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr aus verschiedenen Perspektiven auf. Dabei werden vorhandene empirische Studien, darunter auch die Evaluation zu der Richtlinie 2006/24/EG[2], auf Hinweise zu besonderen Nutzen gespeicherter Telekommunikationsdaten sowie besonderen Problemen, soweit solche Daten nicht zur Verfügung stehen, überprüft. In einem weiteren Schritt werden die Debatten und Erfahrungen in solchen Ländern betrachtet, in denen die Richtlinie bislang nicht umgesetzt bzw. die Transformation noch nicht in Kraft ist (insbesondere Österreich und Schweden), bzw. in (außereuropäischen) Regionen, in denen bislang eine Politik der Vorratsspeicherung von Telekommunikationsdaten nicht implementiert worden ist (Nordamerika – USA, Kanada –, Australien, Neuseeland).

Den Kern der Untersuchung bilden Interviews mit Ermittlungs- und Polizeibeamten aus allen Bundesländern sowie den Bundesbehörden, die verschiedene Ebenen der Hierarchie, unterschiedliche Zuständigkeiten und Erfahrungen (Drogen, Wirtschaftskriminalität, politische Kriminalität und Terrorismus etc.), Praxisbereiche (Technik etc.) und Ausrichtungen (Gefahrenabwehr, Strafverfolgung) repräsentieren.

2. Abwägungen zwischen Persönlichkeitsschutz, Sicherheit und Strafverfolgungseffizienz: verfassungsrechtliche Praxis

Die Verkehrsdatenspeicherung hat europaweit rechtspolitische und verfassungsrechtliche Kontroversen ausgelöst, geführt durch Nichtregierungsorganisationen, Datenschutzbeauftragte und Sicherheits- bzw. Polizeibehörden sowie Innen- und Justizministerien und ausgetragen

---

1 BVerfG, 1 BvR 256/08, vom 2.3.2010.

2 Europäische Kommission: Bewertungsbericht zur Richtlinie 2006/24/EG über die Vorratsdatenspeicherung, KOM(2011) 225 endgültig vom 18.4.2011.

teilweise vor Verfassungs- oder Obersten Gerichten. Es geht um strategische Abwägungen zwischen Strafverfolgungseffizienz, Sicherheit und dem Schutz des Privaten. Angesichts der beträchtlichen Datenmengen werden darüber hinaus besondere Herausforderungen aus der Perspektive des Datenschutzes gesehen, der auch aus der Sicht der Europäischen Kommission innerhalb der Europäischen Union herausragende Beachtung finden soll[3]. Eine Vorratsdatenspeicherung, wie in der EU Richtlinie vorgesehen und in dem nun vom Bundesverfassungsgericht für nichtig erklärten Gesetz umgesetzt, ist aus Datenschutzgesichtspunkten heraus auch deshalb problematisch[4], weil sie als anlassunabhängige und verdachtslose Überwachung des Telekommunikations- und Internetverkehrs einen intensiven Eingriff in Art. 8 der EMRK bzw. des Fernmeldegeheimnisses mit sich bringt[5] und sich in Deutschland jedenfalls nur schwer mit den Vorgaben des – allerdings lange zurück liegenden – Volkszählungsurteils des Bundesverfassungsgerichts in Einklang bringen lässt.[6] In der Beurteilung der Vorratsdatenspeicherung wird die Bedeutung des Telekommunikationsgeheimnisses als zentrales Menschenrecht in der Informationsgesellschaft betont und ferner darauf hingewiesen, dass Kommunikationsnetze nicht zu „Plattformen der Verdachtsschöpfung“ werden dürften. Praktische Bedenken gegen die Vorratsspeicherung berufen sich auf Zweifel an der Kosten-Nutzen-Effizienz[7] und an der Beherrschbarkeit von Datenmengen, die aus der Telekommunikation von etwa 400 Millionen Menschen resultieren[8]. Gezweifelt wird darüber hinaus an der Existenz eines hinreichenden datenschutzrechtlichen Konzepts, mit dem den Gefahren einer missbräuchlichen Verwendung der Daten angemessen begegnet werden kann[9].

Aus der Perspektive der Sicherheits- und Strafverfolgungsbehörden wird betont, dass Veränderungen im Kommunikationsverhalten sowie in der Technik der Kommunikation unabweisliche Bedürfnisse nach Zugriffsmöglichkeiten auf zurückliegende Verbindungs- bzw. geogra-

---

3 European Commission: Communication From the Commission To the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Delivering an area of freedom, security and justice for Europe's citizens Action Plan Implementing the Stockholm Programme Brussels, COM(2010) 171, S. 3.

4 Vgl. *Sierck, G. M., Schöning, F., Pöhl, M.*: Wissenschaftliche Dienste des Deutschen Bundestages, Gutachten zur „Zulässigkeit der Vorratsdatenspeicherung nach europäischem und deutschem Recht“. Berlin 2006, S. 21.

5 *Dix, A.*: Informations- und Kommunikationskriminalität. Kriminalistik 2004, S. 81-85, S. 81.

6 Stenographischer Bericht des BT, 19. Sitzung in der 16. Wahlperiode, 16.2.2006, S. 1428.

7 Vgl. zu Kostenschätzungen *Larnhof, K.*: Data Retention - Zur aktuellen Rechtslage in einigen EU-Mitgliedsländern unter Berücksichtigung der EU-Richtlinie zur Vorratsdatenspeicherung. Eisenstadt 2006, S. 64f.; *Sierck, G. M., Schöning, F., Pöhl, M.*: a.a.O., 2006, S. 14; Stenographischer Bericht des BT, 19. Sitzung in der 16. Wahlperiode, 16.2.2006, S. 1420.

8 BT-Drs. 16/128, S. 2; vgl. auch *Alvaro, A.*: Entwurf eines Rahmenbeschlusses über die Vorratsspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus. Ausschuss für bürgerliche Freiheiten, Justiz und Inneres, Europäisches Parlament, Arbeitsdokument vom 21.1.2005, S. 3f.

9 Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Stellungnahme zum Gesetzentwurf der Bundesregierung BT-Drucksache 275/07 vom 23.8.2007, www.datenschutzzentrum.de/polizei/20070627-vorratsdatenspeicherung htm, S. 28 [Juni 2011].

fische Daten der Telekommunikation mit sich bringen. Insbesondere Straftaten, die mittels eines Telekommunikationsgeräts begangen werden, bieten im Wesentlichen nur Verkehrsdaten als Anknüpfungspunkt für erfolgreiche Ermittlungen. Auch die typische Transaktionskriminalität, wie sie beispielsweise im Drogenhandel und im Handel mit Menschen oder Kinderpornografie zum Ausdruck kommt, sowie der internationale Terrorismus, der grenzüberschreitende Netzwerke zur Grundlage hat, integrieren moderne Kommunikationstechnologie und lassen damit digitale Spuren entstehen, die für Prävention und Repression grundsätzlich geeignet sind. Die häufige Nutzung von Prepaid SIM-Karten sowie die Flatrate-Praxis der Telekommunikationsunternehmen führen entweder zu einer nurmehr kurzen Speicherungsdauer der Verkehrsdaten oder gar dazu, dass bestimmte Daten gar nicht mehr gespeichert werden (und gespeichert werden dürfen), wodurch sich die Zugriffsmöglichkeiten auf kurze Zeitfenster und selektive Datenbestände begrenzen und Aufklärungs- und Präventionsmöglichkeiten reduzieren.

Nur wenige Informationen liegen über die öffentliche Meinung zur Vorratsspeicherung von Verkehrsdaten vor. Eine FORSA-Umfrage aus dem Jahr 2008[10], kurz nach der Implementierung der Richtlinie 2006/24 in Deutschland durchgeführt, ergab, dass etwa 10% der Befragten auf eine Kommunikation, die speicherungsfähige Daten hinterlassen hätte, verzichtet hat. Etwa die Hälfte gab an, Kontakte zu sensiblen Einrichtungen (Drogenberatung etc.) wohl nicht über Mobiltelefon oder Internet herzustellen. Gespalten ist die öffentliche Meinung darüber, ob die Vorratsspeicherung eine notwendige und verhältnismäßige Maßnahme zur Kriminalitätsbekämpfung ist.

Die Entscheidung des Bundesverfassungsgerichts vom März 2010 (BVerfG, 1 BvR 256/08, 2.3.2010) hat für Deutschland insoweit Klarheit geschaffen, als eine Vorratsdatenspeicherung von Telekommunikationsdaten im Grundsatz als verfassungsgemäß angesehen wird. Das Gericht betonte freilich, dass eine solche Vorratsspeicherung nicht als Schritt hin zu einer Gesetzgebung verstanden werden dürfe, die auf eine möglichst flächendeckende vorsorgliche Speicherung aller für die Strafverfolgung oder Gefahrenprävention nützlichen Daten zielt. Eine solche Gesetzgebung wäre – so führte das Bundesverfassungsgericht aus – unabhängig von der Gestaltung der Verwendungsregelungen von vornherein mit der Verfassung unvereinbar. Die verfassungsrechtliche Unbedenklichkeit einer vorsorglich anlasslosen Speicherung der Telekommunikationsverkehrsdaten setzt demnach voraus, dass die anlasslose Telekommunikationsverkehrsdatenspeicherung eine Ausnahme bleibt (Nr. 218). Besonders hervorgehoben wird dann das Erfordernis der gesetzlichen Vorgabe eines besonders hohen, klaren und verbindlichen Sicherheitsstandards (Nr. 225). Das Gericht unterscheidet die Verwendung der durch eine anlasslos systematische Speicherung aller Telekommunikationsverkehrsdaten gewonnenen Datenbestände von der Abfrage von Telekommunikationsverkehrsdaten, die die Diensteanbieter in Abhängigkeit von den jeweiligen betrieblichen und vertraglichen Umständen – von den Kunden teilweise beeinflussbar – nach § 96 TKG spei-

---

10 FORSA: Meinungen der Bundesbürger zur Vorratsdatenspeicherung. 27. bis 28. Mai 2008, www.forsa.de/ [Juli 2010].

chern dürfen (die also in einem weitgehend durch einen Vertrag zwischen Unternehmen und Kunden gestalteten Prozess entstehen). Die Unterscheidungsbedürftigkeit (zwischen anlasslos und umfassend gespeicherten Daten und den im Rahmen der zivil-, telekommunikations- und datenschutzrechtlich begründeten Datenspeicherung) ergibt sich nach den Urteilsgründen aus der Unausweichlichkeit, Vollständigkeit und damit gesteigerten Aussagekraft der über sechs Monate systematisch vorsorglich erhobenen Verkehrsdaten. Den auf Vorrat gespeicherten Verkehrsdaten wird ein im Verhältnis zu den bei den Telekommunikationsunternehmen zu Abrechnungs- und Kontrollzwecken gespeicherten Verkehrsdaten ungleich größeres Gewicht wegen der tief in das Privatleben eindringenden Rückschlussmöglichkeiten und der Erstellbarkeit unter Umständen detaillierter Persönlichkeits- und Bewegungsprofile zugemessen. Die auf Vorrat gespeicherten Verkehrsdaten werden deshalb der inhaltsbezogenen Telekommunikationsüberwachung gleichgestellt. Hieraus ergibt sich dann, dass die Verwendung solcher Daten dem Verhältnismäßigkeitsgrundsatz nur genügt, wenn sie besonders hochrangigen Gemeinwohlbelangen dient. Eine Verwendung der Daten kommt deshalb nur für überragend wichtige Aufgaben des Rechtsgüterschutzes in Betracht, das heißt zur Ahndung von Straftaten, die überragend wichtige Rechtsgüter bedrohen oder zur Abwehr von Gefahren für solche Rechtsgüter (Nr. 227). Deshalb setzt der Datenabruf zumindest den durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraus. Diese Straftaten können durch den Gesetzgeber in einem eigenständigen und abschließenden Katalog oder durch Bezugnahme auf einen bestehenden Katalog festgelegt werden. Die Schwere der Straftat ist anhand objektivierbarer Kriterien zu bestimmen, insbesondere der Strafdrohungen (vgl. BVerfGE 109, S. 279, S 343 ff., S. 347 f.); die verfolgte Straftat muss auch im Einzelfall schwer sein. Ein Beurteilungsspielraum des Gesetzgebers besteht, jedoch sind Generalklausel oder Verweis auf Straftaten von erheblicher Bedeutung ausgeschlossen (Rdnr. 229).

Das Gericht hat sich auch zur Verwendung gespeicherter Daten für Zwecke der Gefahrenabwehr und nachrichtendienstlicher Aufgaben geäußert und auch für diese Bereiche eine wirksame Begrenzung eingefordert (Rdnr. 230). Zur Begrenzung wird hier verständlicherweise nicht an Straftatenkataloge gedacht. Vielmehr soll eine unmittelbare Bezugnahme auf hochrangige Rechtsgüter, deren Schutz mit Hilfe gespeicherter Verkehrsdaten angestrebt wird, erfolgen. Hinzutreten soll die Intensität der Gefahr. Ein Abruf gespeicherter Telekommunikationsverkehrsdaten wird auf dieser Grundlage nur zur Abwehr von Gefahren für Leib, Leben oder Freiheit einer Person, für den Bestand oder die Sicherheit des Bundes oder eines Landes oder zur Abwehr einer gemeinen Gefahr zulässig sein (Rdnr. 231). Für die Bestimmung der Gefahr reichen nach den Ausführungen des Gerichts Vermutungen und allgemeine Erfahrungssätze nicht aus. Bestimmte Tatsachen müssen die Prognose einer konkreten Gefahr begründen. Dies bedeutet, dass im Einzelfall die hinreichende Wahrscheinlichkeit besteht, dass in absehbarer Zeit ohne Eingreifen des Staates ein Schaden für die Schutzgüter der Norm durch bestimmte Personen verursacht wird. Gefordert sind ein konkretisierbares und zeitlich absehbares Geschehen sowie Informationen zu potentiellen Gefahrverursachern, gegen die die Abfrage gezielt eingesetzt werden kann. Eingriffe im Vorfeld von Gefahren müssen unterbleiben. Eine Differenzierung zwischen Polizeibehörden und Nachrichtendiensten kommt

im Hinblick auf die Eingriffsvoraussetzungen nach den Gründen des Urteils nicht in Betracht (Rdnr. 232).

Nach Inkrafttreten der rumänischen Vorratsdatenspeicherung hat sich das rumänische Verfassungsgericht mit dem die Speicherung von Telekommunikations- und Internetverbindungsdaten anordnenden Gesetz befasst und in einer Entscheidung vom 8. Oktober 2009 ausgeführt, dass das Gesetz in Gänze verfassungswidrig und deshalb nichtig sei[11].

Am 22. März 2011 erklärte das tschechische Verfassungsgericht das Gesetz Nr. 127/2005 sowie die Verordnung Nr. 485/2005, mit denen die Richtlinie 2006/24/EG in der tschechischen Republik umgesetzt worden war, für verfassungswidrig. Das Verfassungsgericht hob dabei auf die Unbestimmtheit der Zugangsvoraussetzungen für auf Vorrat gespeicherte Telekommunikationsdaten durch Strafverfolgungsbehörden und Sicherheitsdienste ab. Ferner wies das Gericht auf den unzureichenden Schutz vor Missbrauch gespeicherter Daten hin. Schließlich werden Zweifel angemeldet, ob eine Vorratsdatenspeicherung, auch angesichts der Möglichkeiten, die Erfassung durch den Gebrauch anonymer Prepaid-Dienste zu umgehen, Verhältnismäßigkeitsgrundätzen genügt.

Das bulgarische Oberste Verwaltungsgericht hat in einer Entscheidung vom 11.12.2008 einen wesentlichen Teil der bulgarischen Transformationsgesetzgebung für verfassungswidrig erklärt[12]. In der Begründung verwies das Gericht auf einen unverhältnismäßigen Eingriff in das durch die bulgarische Verfassung gewährleistete Persönlichkeitsrecht sowie in Art. 8 der EMRK wegen fehlender gesetzlicher Klarstellungen der Bedingungen, unter denen Sicherheits- und Strafverfolgungsbehörden auf gespeicherte Verkehrsdaten zugreifen können. Die bulgarische Neuregelung berücksichtigt nunmehr die Vorgaben des Obersten Verwaltungsgericht durch eine gesetzliche Festlegung von Voraussetzungen für die Abfrage.

In Ungarn ist bereits seit längerer Zeit eine Verfassungsbeschwerde beim Verfassungsgericht anhängig[13], über die noch nicht entschieden ist. Ein konkretes Datum für die Entscheidung des Verfassungsgerichts ist derzeit noch immer nicht absehbar.

Irland hatte im Juli 2006 zunächst vor dem EuGH (Nichtigkeits-) Klage gegen die Richtlinie erhoben. Die Irische Regierung vertrat die Auffassung, dass die Richtlinie als Rahmenbeschluss hätte erlassen werden müssen, nahm freilich nicht zu substantiellen Fragen Stellung.[14] Der Europäische Gerichtshof hat daraufhin entschieden, dass die Materie in Form einer Richtlinie geregelt werden durfte[15]. In einem Beschwerdeverfahren der Digital Rights Ireland Limited gegen das im Juli 2009 eingebrachte Reformgesetz (Communications (Reten-

---

11 Entscheidung Nr.1258 vom 8. Oktober 2009: www.legi-internet ro/fileadmin/editor_folder/pdf/decision-constitutional-court-romania-data-retention.pdf [Juni 2011].

12 Siehe dazu unten Teil G, Pkt. 4.2.

13 Constitutional Complaint Filed by HCLU Against Hungarian Telecom Data Retention Regulations; http://tasz.hu/en/node/826 [Juni 2011].

14 *Sierck/Schöning/Pöhl*, 2006, S. 21; Pressemitteilung von Digital Rights Ireland vom 14.9.2006, abrufbar unter www.digitalrights.ie/2006/09/14/dri-brings-legal-action-over-mass-surveillance/ [Juni 2011].

15 EuGH, Urteil vom 10. Februar 2009, C-301/06.

tion of Data) Bill 2009), das die Speicherung von Telefonverkehrsdaten auf 2 Jahre und die von Internetverbindungen auf 1 Jahr festsetzt[16], hat das Oberste Gericht am 5. Mai 2010 eine Vorlage zum Europäischen Gerichtshof zugelassen[17], die voraussichtlich im Laufe des Jahres 2012 zu einer erneuten Überprüfung der Richtlinie führen wird, dieses Mal unter inhaltlichen Gesichtspunkten, insbesondere der Vereinbarkeit mit der EU-Grundrechtecharta. Die Vorlage zielt auf die Aufhebung des Gesetzes u.a. wegen Verstoßes der EU-Richtlinie 2006/24/EG gegen Art. 7, 8, 11 und 41 der Grundrechtecharta, gegen den Grundsatz der Verhältismäßigkeit (Art. 5 EUV) sowie gegen die Europäische Menschenrechtskonvention (Art. 8).

Die bisherigen Entscheidungen europäischer Verfassungs- und Obergerichte lassen bei grundsätzlich vergleichbarem Zugang über eine Verhältnismäßigkeitsprüfung unterschiedliche Bewertungen der Vorratsspeicherung erkennen[18]. Während das bulgarische Oberste Verwaltungsgericht eine klare gesetzliche Regelung der Voraussetzungen für die Nutzung gespeicherter Daten angemahnt hat und im Übrigen davon ausgeht, dass eine Vorratsdatenspeicherung grundsätzlich verhältnismäßig ist, geht das rumänische Verfassungsgericht von einer ebenso grundsätzlichen Nichtvereinbarkeit der Vorratsdatenspeicherung mit der rumänischen Verfassung sowie Art. 8 aus. Auch das tschechische Verfassungsgericht hat entsprechende Bedenken geäußert. Das Bundesverfassungsgericht weist demgegenüber darauf hin, dass eine Vorratsdatenspeicherung von Telekommunikationsdaten zwar grundsätzlich noch verfassungskonform ist, gleichzeitig aber das Äußerste an Vorratsdatenspeicherung für Zwecke der Strafverfolgung und Gefahrenabwehr repräsentiert.[19] Zusätzlich wird in einer Abschichtung von im regulären Betrieb von Telekommunikationsunternehmen anfallenden Verkehrsdaten und deren Abfrage unterschieden von systematisch gespeicherten Verkehrsdaten und ihrer Nutzung. In der Entscheidung des Bundesverfassungsgerichts wird hiermit ein grundsätzlicher Wandel angesprochen, der beispielsweise auch im australischen Blunn-Bericht[20] Erwähnung findet. Es geht hier um die Bewegung weg von einer punktuellen Überwachung der Kommunikation, über Telefon, Briefwechsel oder direkten Austausch, hin zum Zugang zu gespeicherten Daten der Kommunikation und hin zum Aufbau von Informationssystemen, die über Kommunikation Auskunft geben.

---

16 Kritisch hierzu Irish Council for Civil Liberties: Submission on the Communications (Retention of Data) Bill 2009, as initiated November 2009, Dublin 2009, insbesondere aus der Perspektive von Art. 8 der EMRK sowie der Entscheidung des EGMR S. und Marper v. UK, Application nos. 30562/04 und 30566/04, 4. Dezember 2008.

17 Digital Rights Ireland Ltd. vs. Minister for Communications and Others, [2010] IEHC 221.

18 Vgl. hierzu auch *de Vries, K., Bellanova, R., De Hert, P.*: Proportionality Overrides Unlimited Surveillance. The German Constitutional Court Judgment on Data Retention. European Center for Policy Studies, Brüssel 2010.

19 Hierzu ausführlicher *Roßnagel, A.*: Die „Überwachungs-Gesamtrechnung" – Das BVerfG und die Vorratsdatenspeicherung, NJW 2010, S. 1238ff., *Schramm, S., Wegener, C.*: Neue Anforderungen an eine anlasslose Speicherung von Vorratsdaten – Umsetzungsmöglichkeiten der Vorgaben des Bundesverfassungsgerichts, MMR 2011, S. 9ff.

20 *Blunn, A.S.*: Report of the Review of the Regulation of Access to Communications. Commonwealth of Australia 2005, S. 14ff.

3. Anlage der Untersuchung

3.1. Methodische Erwägungen

Die verfassungsrechtlichen Debatten verweisen auf Abwägungen zwischen dem Interesse an der effizienten Aufklärung von Straftaten und dem Schutz des Fernmeldegeheimnisses bzw. des Persönlichkeitsrechts sowie auf Fragen der Verhältnismäßigkeit, damit auf Fragestellungen, die eine Einschätzung bedingen, ob eine Vorratsdatenspeicherung zum Schutz von Rechtsgütern notwendig ist. Das grundlegende Problem, das sich der Evaluationsforschung in diesem Zusammenhang stellt, besteht darin, dass eine experimentelle Untersuchung der Fragen nicht möglich ist. Sichtbar wird dies in dem als Entwurf vorliegenden Evaluationsbericht der Europäischen Union. Dort wird auf zwei Informationsquellen Bezug genommen. Zum einen geht es um eine einfache Statistik zur Häufigkeit des Zugriffs von auf Vorrat gespeicherten Verkehrsdaten in den Mitgliedsländern. Zum anderen wird in dem Bericht auf von Strafverfolgungsbehörden der Mitgliedsländer mitgeteilte Fälle zurückgegriffen, in denen der Zugriff auf Verkehrsdaten zur erfolgreichen Strafverfolgung beigetragen hat. Beide Informationsquellen sind streng genommen für eine Evaluation nicht geeignet. Denn sie ermöglichen lediglich Aussagen darüber, wie häufig eine Ressource der Strafverfolgung genutzt wurde und welche Einschätzung bei Ermittlungsbeamten hinsichtlich der Bedeutung einer bestimmten Ermittlungsmaßnahme bei nicht nachvollziehbarer Selektion der Fälle vorliegt. Da ein Kontrollgruppenansatz nicht realisierbar ist und deshalb eine Suche nach Unterschieden in Aufklärungsmöglichkeiten und Gefahrenabwehrpotenzial im Vergleich unterschiedlicher Ermittlungsmöglichkeiten nicht umgesetzt werden kann, muss demnach auf andere Indikatoren zurückgegriffen werden. Diese sollten allerdings über die bloße Häufigkeit der Nutzung und selektive Mitteilung von Fällen hinausgehen.

3.2. Datenzugänge

3.2.1. Auswertung statistischer Informationen und Sekundäranalysen

Eine erste wichtige Komponente der eigenen Erhebungen ist zunächst die quantitative Eingrenzung der aktuellen Größenordnungen zur Verkehrsdatenabfrage insgesamt sowie möglicher Problemfälle. Hierzu wurden die amtliche Statistik zur Verkehrsdatenabfrage aus dem Jahr 2008 sowie die Listen mit Daten aus den drei Sonderhebungen, die im Zusammenhang mit dem beim BVerfG anhängigen Verfahren durchgeführt wurden, einer näheren Analyse unterzogen. Siehe hierzu Teil C, Pkt. 1 und 2. Ferner wurden Informationen zu der Speicherdauer von Verkehrsdaten berücksichtigt, die die Bundenetzagentur im ersten Quartal 2011 erhoben hat (siehe Teil C, Pkt. 5).

Weiterhin war geplant, eine ergänzende Erhebung bei den Landesjustizverwaltungen nach aktuelleren Daten durchzuführen. Ziel dieses Moduls sollte die Ermittlung von belastbaren Zahlen zu solchen Fällen sein, die für die Dauer des Verfahrens beim BVerfG zunächst vorläufig eingestellt worden waren und nach der in dem Urteil verfügten endgültigen Löschung auf der Basis der neuen Rechtslage eingestellt wurden. Die Landesjustizverwaltungen sahen sich aber außerstande, die erforderlichen Erhebungen in dem kurzen Zeitraum, der hierfür zur

Verfügung gestanden hätte, durchzuführen. Die Ministerien der größeren Bundesländer verwiesen ergänzend auf die Personalintensität entsprechender Recherchen. Mangels Fortführung der Sondererhebung nach der dritten Welle wäre hierfür eine nachträgliche händische Durchsicht zehntausender seither eingestellter Verfahren erforderlich gewesen.

In Ergänzung zu den aggregierten statistischen Daten wurden die im Rahmen der Aktenanalyse zu der ersten Verkehrsdatenuntersuchung des MPI[21] generierten Daten reaktiviert. Diese haben einen konkreten Fallbezug und beruhen auf einer repräsentativen Stichprobe von Verfahren mit Beschlüssen gem. § 100g/h a.F. StPO aus den Jahren 2003 und 2004. Für die Sekundärauswertung wurden ausgesuchte Variablen zu einem neuen Datensatz zusammengefasst, um vertiefende Analysen zu den zeitlichen Aspekten der Verkehrsdatenabfrage sowie zu den Effekten erfolgloser Abfragen (nicht bzw. nicht mehr verfügbare sowie nicht verwertbare Verkehrsdaten) auf den Ausgang von Ermittlungs- bzw. Strafverfahren durchführen zu können. Siehe zu den Ergebnissen Teil C, Pkt. 4.

3.2.2. Interviews

Im Mittelpunkt der inhaltlichen Problemanalyse stehen sodann qualitative Interviews mit Praktikern aus Polizei und Justiz. Auf der Basis von Gesprächsleitfäden, die den befragten Personen zur Vorbereitung der Gespräche vorher zur Verfügung gestellt worden waren, sollten die Interviewpersonen zu allen rechtlichen und praktischen Aspekten der nach dem Urteil vom 2.3.2010 eingetretenen Lage Stellung beziehen. Die Analyse berücksichtigt dabei explizit auch mögliche, aus Ermittlersicht praktikable Substitute, mit denen nicht mehr erreichbare Verkehrsdaten eventuell ersetzt werden können. Auf der Grundlage einer Gesamtschau aus allen genannten Aspekten sollten dann die konkreten Schutzlücken identifiziert werden.

Aufgrund der kurzen Projektlaufzeit konnten für die einzelnen Berufsgruppen keine repräsentativen Stichproben gebildet werden. Sachliches Auswahlkriterium war die aktuelle berufliche Befasstheit mit Fragen der Verkehrsdatenabfrage. Die individuelle Auswahl erfolgte durch die Behörden selbst.

Im Einzelnen wurden die folgenden Gruppen befragt:

- Justiz: Mindestens ein Sachbearbeiter als ermittelnder Staatsanwalt aus den OLG-Bezirken mit Ausnahme der OLG Koblenz, München und Naumburg sowie ein Bundesanwalt. Die Auswahl kann regionale Besonderheiten zumindest auf OLG-Ebene weitgehend erfassen und erscheint geeignet, die wesentlichen Problemlagen ebenso zu erfassen wie Unterschiede in der Bewertung bzw. der Implementierung konkreter Problemlösungsstrategien. Lediglich Sachsen-Anhalt ist in diesem Sample nicht vertreten.[22] Die Interviewergebnisse liefern in der Zusammenschau ein Gesamtbild, das die Praxisperspektive hinreichend detailliert erfasst, um rechtspolitisch belastbare

21 *Albrecht/Grafe/Kilchling* 2008.

22 Die Perspektive der Strafverfolgung wird freilich durch die befragten Polizeibeamten repräsentiert; in Sachsen-Anhalt ist die Verkehrsdatenabfrage ausschließlich zu repressiven, nicht zu präventiven Zwecken zulässig.

Schlussfolgerungen zu ziehen. Die ursprünglich geplante ergänzende Befragung von Personen auf der Ebene der Generalstaatsanwaltschaften erwies sich als unpraktikabel, da keine ausreichende Zahl von Interviewpersonen mit hinreichenden Detailkenntnissen zu der aktuellen Situation benannt werden konnten. Insgesamt wurden auf dieser Ebene 26 Personen befragt. In die Analyse einbezogen wurden auch die Stellungnahmen sämtlicher Behördenleiter der Staatsanwaltschaften im OLG-Bezirk Karlsruhe, die die dortige Generalstaatsanwaltschaft zur Unterstützung der vorliegenden Untersuchung angefordert hatte. Siehe zu den Ergebnissen ausführlich Teil F, Pkt. 2.

Eine systematische Einbeziehung von Richtern wurde in diesem speziellen Kontext für weitgehend entbehrlich erachtet. Die untersuchungsgegenständlichen Fragestellungen sind im Wesentlichen ermittlungstechnischer und kriminaltaktischer Natur und liegen außerhalb der Entscheidungsroutine der Richter, die vorwiegend auf die rechtliche Prüfung der Beschlussvoraussetzungen ausgerichtet ist. Um ihren rechtlichen Blickwinkel gleichwohl in die Bewertung einfließen zu lassen, wurden ergänzend einige wenige Richter mit Ermittlungsrichtererfahrung als kleine Kontrollgruppe befragt. Die Auswahl beschränkte sich aus forschungsökonomischen Gründen auf die beiden OLG-Bezirke in Baden-Württemberg und ist unter keinem Aspekt repräsentativ. Insgesamt konnte mit 5 Personen gesprochen werden. Vgl. hierzu Teil F, Pkt. 3.

- Polizei: Eine einheitliche, der justiziellen Organisation vergleichbare Struktur existiert im Polizeibereich nicht. Aus Zeit- und Kapazitätsgründen konnten nicht alle Polizeibehörden in den Ländern systematisch einbezogen werden. Die Auswahl orientierte sich daher vor allem an der operativen Nähe zur Verkehrsdatenabfrage. Um weiter verschiedene Delikts- und Aufgabenbereiche (Allgemeinkriminalität, IuK-Kriminalität, organisierte Kriminalität, Wirtschaftskriminalität sowie die jeweiligen Sonderzuständigkeiten des Bundeskriminalamtes und der Bundespolizei) zu berücksichtigen, wurden pro Bundesland jeweils zwischen drei und fünf Experten befragt. Hinzu kamen das Bundeskriminalamt sowie die Bundespolizei. Um die Gespräche zeit- und mengenmäßig bewältigen zu können, wurden sie mit organisatorischer Unterstützung des Bundeskriminalamtes gebündelt. Die Gespräche mit den Vertretern aus jedem Land sowie der beiden Bundesbehörden wurden jeweils zusammen geführt, und zwar je eine Woche in den Räumlichkeiten des BKA in Wiesbaden (Baden-Württemberg, Bayern, Hessen, Nordrhein-Westfalen, Rheinland-Pfalz, Saarland, Thüringen sowie das Bundeskriminalamt selbst) und in Berlin (Berlin, Brandenburg, Bremen, Hamburg, Niedersachsen, Mecklenburg-Vorpommern, Sachsen, Sachsen-Anhalt, Schleswig-Holstein sowie die Bundespolizei). Gegenstand der Gespräche waren beide Einsatzbereiche der Verkehrsdatenabfrage – Strafverfolgung und Gefahrenabwehr. Dort, wo die Landespolizeigesetze einen präventiven Einsatz der Maßnahme nicht erlauben, beschränkten sich die Gespräche selbstredend auf die repressive Variante (Berlin, Bremen, Nordrhein-Westfalen, Sachsen, Sachsen-Anhalt). Insgesamt nahmen 77 Personen an den Interviews teil. Eine Übersicht über die jeweiligen Funktionen bzw. Ar-

beitsbereiche der Interviewpersonen ist diesem Bericht in Anhang C beigefügt. Siehe zu den Ergebnissen ausführlich Teil F, Pkt. 1.

Um die aktuelle Praxis der Verkehrsdatenspeicherung und -auskunft auch aus der Perspektive der beteiligten Unternehmen zu erfassen, wurden ergänzend einige Interviews mit Vertretern aus der Telekommunikationsbranche geführt.

- Befragt werden konnten Repräsentanten der großen Universalanbieter (Deutsche Telekom/T-mobile, E-Plus, Vodafone, O2), von einem Unternehmen, das ausschließlich Online-Dienste anbietet (QSC) sowie stellvertretend für kleinere, regional tätige Anbieter ein Vertreter des Verbandes Eco. Zwei weitere Unternehmen, eines mit dem Schwerpunkt Internetdienste sowie ein regionaler Anbieter, hatten ihre Teilnahme zugesagt, aber bis zuletzt keine Stellungsnahme abgegeben. Insgesamt wurden 6 Personen befragt. Siehe zu den Ergebnissen Teil F, Pkt. 4.

Tabelle A-1: Übersicht über die durchgeführten Interviews

	Polizei	Justiz	Richter
Baden-Württemberg	4	3	5
Bayern	4	2	-
Berlin	5	1	-
Brandenburg	4	1	-
Bremen	1	1	-
Hamburg	5	1	-
Hessen	3	1	-
Meckl.-Vorpommern	3	1	-
Niedersachsen	4	5	-
NRW	5	4	-
Rheinland-Pfalz	5	1	-
Saarland	4	1	-
Sachsen	5	1	-
Sachsen-Anhalt	5	0	-
Schleswig-Holstein	4	1	-
Thüringen	6	1	-
Gesamt	67	25	5
Bundesanwaltschaft	1		
BKA	5		
Bundespolizei	5		
TK-Unternehmen	6		

Die unterschiedlichen Interviewsettings werfen die Frage nach möglichen Methodeneffekten auf.[23] Solche Effekte sind bei der Bewertung der Ergebnisse stets zu beachten. Sie werden vorliegend jedoch durch mehrere Aspekte abgemildert. Die Befragten selbst waren durchweg keine Laien, sondern durchweg Experten, die ausschließlich zu berufsbezogenen Fragen Stellung genommen haben. Darüber hinaus handelte es sich nicht um Spontaninterviews. Sämtliche Befragten hatten den Interviewleitfaden vorab erhalten und waren auf den Gesprächsinhalt vorbereitet. Die Interviews waren zudem terminlich vorher abgesprochen und fanden im Arbeitsumfeld statt (am Arbeitsplatz bzw. in den bekannten Behördengebäuden des BKA). Deutliche Unterschiede traten lediglich in der Dauer der Gespräche zu Tage: während die Gruppengespräche in der Regel eineinhalb Stunden in Anspruch nahmen, dauerten die telefonischen Einzelinterviews im Durchschnitt etwa 20 Minuten. Dieser Unterschied relativiert sich freilich dadurch, dass bei den Gruppengesprächen regelmäßig vier oder fünf Gesprächspartner zugegen waren; damit gleicht sich die individuelle Redezeit weitgehend an.

Soweit befragungsspezifische Effekte dennoch aufgetreten sein können, sind sie im Kontext der vorliegenden Untersuchung als weitgehend unbedenklich zu bewerten. Denn es sollten keine personen- oder gruppenspezifischen Merkmale oder Auffassungsunterschiede ermittelt werden. Ziel der explorativen Interviews war vielmehr das kumulative Zusammentragen möglichst vieler relevanter Fakten. In der Darstellung der Gesprächsinhalte wird auf eine quantitative Gewichtung einzelner Aspekte denn auch weitgehend[24] verzichtet (siehe Teil F).

3.2.3. Kontrastgruppen – Länder ohne Vorratsspeicherung

Zur Abrundung des Bildes wurde ferner die Situation in einigen Ländern analysiert, die derzeit (noch) keine expliziten Bestimmungen zur Vorratsdatenspeicherung haben. Aus Zeitgründen war auch insoweit eine Beschränkung auf einige ausgewählte Jurisdiktionen erforderlich.

Ausgewählt wurden als erste Gruppe Belgien, Österreich und Schweden. Belgien hat die EU-Richtlinie 2006/24/EG bislang noch nicht umgesetzt, in Österreich und Schweden galt dies zum Zeitpunkt der Interviews ebenfalls. Für beide Länder werden auch die aktuellen gesetzgeberischen Entwicklungen dargestellt. Siehe für weitere Einzelheiten unten Teil G, Pkt. 4.1., 4.3. und 4.5. Die zweite Gruppe setzt sich sodann aus Bulgarien und Rumänien zusammen. Die Situation in diesen Ländern ist derjenigen in Deutschland insofern vergleichbar, als auch dort die (ersten) Gesetze zur Einführung der Vorratsdatenspeicherung durch gerichtliche Intervention teilweise oder ganz verworfen wurden. Im Falle Bulgariens geschah dies durch das Oberste Verwaltungsgericht unter Hinweis auf einige eher technische Details (unten Teil G, Pkt. 4.2.). Viel weitreichender sind die Folgen in Rumänien, wo der dortige Verfassungsgerichtshof, in der Sache wesentlich weitergehend als das BVerfG, einen Verstoß nicht nur ge-

---

23 Vgl. zu der Problematik von Intervieweffekten näher *Diekmann, A.*: Empirische Sozialforschung. Reinbek 2007.

24 Eine Ausnahme hiervon bildet u.a. die Auswertung der Eingangsfrage zu der allgemeinen Situationseinschätzung (siehe unten Tabelle D-1)

gen Grundrechte der rumänischen Verfassung, sondern auch gegen Art. 8 EMRK festgestellt hat (unten Teil G, Pkt. 4.4.).

Teil B: Rechtliche Rahmenbedingungen der Verkehrsdatenabfrage in Deutschland

Ausgangspunkt für die empirischen Untersuchungen muss zunächst eine Analyse der rechtlichen Regelungen vor und nach dem Urteil des Bundesverfassungsgerichts sein. Aus Gründen der Übersichtlichkeit wird sich die nachfolgende Darstellung auf die für das Verständnis des Urteils notwendigen Grundlagen beschränken.[25]

Der Zugriff auf Datenbestände beschränkt sich heute nicht mehr lediglich auf die Ermittlung von Online-Sachverhalten. Vielmehr soll der Zugriff insbesondere auf Verkehrsdaten dazu dienen, um Ermittlungsansätze für eine Vielzahl von Delikten zu generieren, auch wenn diese vollständig offline begangen werden. Es ist daher notwendig, in einem ersten Schritt zwischen den grundsätzlich verfügbaren Datenarten und den zugrundeliegenden Speichermöglichkeiten und -pflichten zu differenzieren (nachfolgend 1.), bevor in der gebotenen Kürze die verschiedenen Möglichkeiten dargestellt werden, auf diese Daten zugreifen zu können (2.). In diesem Zusammenhang wird auch aus rechtlicher Sicht die Situation vor und nach dem Wegfall der Vorratsdatenspeicherung beleuchtet.

1. Definition der Datenarten

Der Umgang mit unterschiedlichen Datenarten ist in vielen verschiedenen Gesetzen differenziert geregelt worden, z.B. in der StPO, dem TKG oder dem TMG. Häufig wird grundsätzlich zwischen Bestands-, Verkehrs- und Inhaltsdaten unterschieden. Daneben existieren aber auch Abrechnungs-, Positions- oder Zugangsdaten. Einige dieser Datenkategorien überschneiden sich und lassen sich nicht trennscharf gegeneinander abgrenzen. Auch der Gesetzgeber selbst verwendet die von ihm geschaffenen Datenarten zum Teil in unterschiedlichen Kontexten.

– Als *Bestandsdaten* definiert § 3 Nr. 3 TKG alle Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden. Es geht also um die Daten, die das „Grundverhältnis“[26] zwischen Anbieter und Kunde betreffen, die jedoch grundsätzlich nichts darüber aussagen können, ob im Einzelfall tatsächlich eine Leistung erbracht oder genutzt wurde.

– Der für das Gutachten bestimmende Begriff der *Verkehrsdaten* wird in § 3 Nr. 30 TKG legal definiert. Es handelt sich danach um Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Früher wurde in einigen

---

25 Für ausführlichere Darstellungen vgl. *Gercke/Brunst,* Praxishandbuch Internetstrafrecht, S. 262 ff.

26 Vgl. *Tinnefeld, et al.,* Einführung in das Datenschutzrecht, S. 237.

Gesetzen fast synonym auch der Begriff der „Verbindungsdaten“ verwandt.[27] Dieser Begriff ist inzwischen weitgehend gestrichen und durch die neue Terminologie ersetzt worden.

– Der Begriff der *Vorratsdaten* ist gesetzlich in Deutschland nicht definiert, ist in der Praxis jedoch aus der zugrundeliegenden europäischen Richtlinie übernommen worden.[28]

– Eng mit den Verkehrsdaten verwandt ist der Begriff der *Nutzungsdaten*, der in § 15 Abs. 1 S. 1 TMG definiert wird. Es handelt sich um personenbezogene Daten eines Nutzers, die erhoben oder verwendet werden, um die Inanspruchnahme von Telemedien zu ermöglichen und abzurechnen. Insbesondere bei den gesetzlich genannten Beispielen der Nutzungsdaten, die Aufschluss über Beginn und Ende sowie den Umfang der jeweiligen Nutzung geben, liegt eine weitestgehende Überlagerung mit dem Begriff der Verkehrsdaten vor. Das zentrale Unterscheidungskriterium ist, dass sich Verkehrsdaten auf Telekommunikations- und Nutzungsdaten auf Telemediendienste beziehen. Der Gesetzgeber trennt jedoch die selbst geschaffenen Begriffe nicht scharf und verwischt zunehmend die Grenzen zwischen den einzelnen Diensten.[29]

– Ein Unterfall der Verkehrs- und Nutzungsdaten, der in § 15 Abs. 4 TMG legal definiert, im TKG jedoch nicht selbständig erwähnt wird, sind die *Abrechnungsdaten.* Es handelt sich um Daten, die für Zwecke der Abrechnung mit dem Nutzer erforderlich sind.

– *Standortdaten* sind nach § 3 Nr. 19 TKG die in einem Telekommunikationsnetz erhobenen oder verwendeten Daten, die den Standort eines Endgeräts angeben. Es handelt sich also um geographische Positionsangaben, die Aufschluss über physikalische Bewegungsprofile geben können. Genaugenommen handelt es sich also um einen Unterfall von Verkehrsdaten.

– Der Begriff der *Inhaltsdaten* ist gesetzlich nicht definiert. Er hat sich jedoch allgemein etabliert, um vor allem diejenigen Daten zu bezeichnen, die menschlich wahrnehmbar sind und zwischen Nutzern ausgetauscht werden.[30] Beispiele für Inhaltsdaten sind daher etwa der konkrete Inhalt einer ausgetauschten E-Mail oder die geschriebenen Zeilen einer IRC-

---

27 Vgl. näher *Albrecht et al.,* Rechtswirklichkeit der Auskunftserteilung über TK-Verbindungsdaten.

28 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. EU Nr. L 105 (13.04.2006), S. 54 ff. Der dort genutzte Datenbegriff bezieht sich zwar grundsätzlich auf „Verkehrsdaten und Standortdaten sowie alle damit in Zusammenhang stehende(n) Daten, die zur Feststellung des Teilnehmers oder Benutzers erforderlich sind“, Art. 2 Abs. 2a) der Richtlinie. In Art. 5 der Richtlinie wird eine Speicherpflicht jedoch nur bezüglich bestimmter Datenkategorien verpflichtend angeordnet.

29 Näher zu den Abgrenzungsschwierigkeiten *Gercke/Brunst,* Praxishandbuch Internetstrafrecht, Rn. 639 ff.

30 Vgl. *Gercke/Brunst,* Praxishandbuch Internetstrafrecht, Rn. 636.

Kommunikation.[31] Der Begriff ist jedoch nicht trennscharf. So könnten auch Informationen, die nicht originär als digitale Daten erfasst worden sind, als „Inhaltsdaten“ bezeichnet werden.[32] Schließlich werden zum Teil auch Daten, die noch nicht Bestandteil einer Kommunikation geworden sind, als Inhaltsdaten bezeichnet, z.B. eine Datei, die lokal auf einem Rechner gespeichert worden ist.

Neben diesen allgemeinen Datenarten finden sich zum Teil auch andere, die jedoch lediglich in bestimmten Normenkomplexen Anwendung finden. So erwähnt etwa Art. 34d BayPAG[33] die Kategorie der *Zugangsdaten*.[34] Diese Kategorie sollte ursprünglich ihre Bedeutung im Zusammenhang mit der in der Vorschrift vorgesehenen Befugnis entfalten, Daten online auf fremden Systemen zu verändern oder zu löschen.[35] Mit Wirkung zum 31.07.2009 ist diese Möglichkeit jedoch teilweise wieder gestrichen und die Vorschrift verändert worden, so dass die Kategorie weitgehend bedeutungslos geworden ist.[36] Auf andere als die oben dargestellten Datenkategorien wird daher nachfolgend nur noch in Ausnahmefällen näher einzugehen sein.

2. Zugriff auf Daten zu Ermittlungszwecken

Um die Bedeutung der oben näher dargestellten Datenarten für Ermittlungen besser verstehen zu können, ist es notwendig, den Einsatz der unterschiedlichen Informationen für Ermittlungszwecke überblicksartig zu skizzieren (nachfolgend 1.). Sodann wird kurz auf die Möglichkeiten des Zugriffs auf die wichtigsten Telekommunikationsdaten eingegangen (2.-4.).

2.1. Allgemeiner Datenbedarf

Der Zugriff auf Daten hat in zahlreichen Ländern schon seit geraumer Zeit Eingang in den Ermittlungsalltag gefunden. Die EU-Kommission vertritt sogar der Ansicht, die Auswertung von Telekommunikations-Verkehrsdaten sei inzwischen ein integraler Bestandteil des Ermitt-

---

31 *Graf,* in: Beck´scher Online-Kommentar zur StPO, § 100a StPO Rn. 22 bezeichnet – in diesem Zusammenhang – daher Inhaltsdaten als die „durch das Fernmeldegeheimnis geschützten Inhalt[e] einer Telekommunikation“.

32 Denkbar ist dies etwa bei den im Gesetz lediglich als „Daten“ bezeichneten Aufzeichnungen einer Wohnraumüberwachung, § 100c Abs. 5 S. 4 StPO, denn auch hier sind nicht die äußeren Umstände z.B. eines Gesprächs, sondern die Gesprächsinhalte betroffen.

33 Gesetz über die Aufgaben und Befugnisse der Bayerischen Staatlichen Polizei in der Fassung der Bekanntmachung vom 14.09.1990, zuletzt geändert am 22.04.2010.

34 Auch § 113 Abs. 1 S. 2 TKG enthält eine Vorschrift über Auskünfte zu Daten, „mittels derer der Zugriff auf Endgeräte oder in diesen oder im Netz eingesetzte[n] Speichereinrichtungen geschützt wird“. Dort wird der Begriff der *Zugangsdaten* jedoch nicht genutzt. Gleichwohl ist in diesem Zusammenhang der Begriff durchaus verbreitet, vgl. etwa *Bock,* in: Geppert, et al. (Hrsg.), Beck TKG-Komm., § 113 TKG, Rn. 16 ff.

35 Art. 34d Abs. 1 S. 2 BayPAG i.d.F. vom 01.08.2008.

36 Lediglich im Zusammenhang mit der jährlichen Berichtspflicht gegenüber dem Bayerischen Landtag wird noch auf Zugangsdaten abgestellt, vgl. Art. 34d Abs. 8 S. 1 BayPAG.

lungsalltages in der EU.[37] Tatsächlich haben die Daten – zumindest theoretisch – das Potenzial, sowohl zur Aufklärung bereits begangener Straftaten als auch zur Prävention bevorstehender Taten beitragen zu können. Infolge der immer weiter voranschreitenden Vernetzung wird dieses Potenzial mutmaßlich noch weiter zunehmen. Zu differenzieren ist in diesem Kontext ganz grundsätzlich nach dem potenziellen Nutzen im Rahmen der zwischen der so genannten IuK- oder Online-Kriminalität und im Rahmen von Taten, die konventionell – in den Kategorien des Computerstrafrechts mithin offline – begangen werden.[38]

2.1.1. Online-Kriminalität

Bei Straftaten, die online begangen werden, stehen – anders als bei Offline-Taten, bei denen z.B. Fingerabdrücke, Einbruchsspuren oder ähnliche konventionelle Ermittlungsansätze verfügbar sind – ausschließlich digitale Informationen zu Ermittlungszwecken zur Verfügung. In allererster Linie handelt es sich um die IP-Adresse, die bei jeder Transaktion technisch notwendig übertragen wird. Diese Information führt zwar nicht automatisch zum Täter,[39] sie ist aber ein Ermittlungsansatz, der weiter verfolgt werden kann. Steht keine IP-Adresse (mehr) zur Verfügung, so fehlt – von Ausnahmen einmal abgesehen – regelmäßig jeder technische Ermittlungsansatz.[40]

Die IP-Adresse selbst führt jedoch nicht automatisch zum Täter, sondern lediglich zu der Stelle, die sie dem Nutzer – meist nur für einen beschränkten Zeitraum – zur Verfügung gestellt hat.[41] Diese Stelle wird als sog. *Access-Provider* bezeichnet. Es kann sich dabei um

---

37 Bewertungsbericht zur Richtlinie über die Vorratsdatenspeicherung KOM(2011) 225 endgültig, a.a.O.(Fn. 2), S. 30. Siehe zu diesem Bericht auch die ausführlichen Ausführungen in Teil E.

38 Die Terminologie ist in diesem Bereich nicht trennscharf. Zum Teil wird von Informations- und Kommunikationstechnikkriminalität (IuK-Kriminalität), Cybercrime, Internetkriminalität, Daten(netz)kriminalität oder Computerkriminalität gesprochen, wobei unterschiedlichste Differenzierungen zugrunde gelegt werden, etwa ob eine Straftat mit Hilfe von Computern, Datennetzen oder Kommunikationstechnik begangen wird, ob sie gegen sie gerichtet ist, ob spezielle Risiken der modernen Informationsgesellschaft realisiert werden u.v m. Eine einheitliche Terminologie hat sich noch nicht durchgesetzt. Vgl. hierzu etwa *Sieber,* in: Council of Europe, Organised Crime in Europe, S. 84 ff. Für die nachfolgende Darstellung wird auf diese Differenzierungen nicht näher eingegangen, da vor allem gezeigt werden soll, dass der Rückgriff auf Daten nicht nur für „moderne" Kriminalitätsformen erforderlich ist, sondern *auch bei scheinbar konventionellen Straftaten ohne deutlich ersichtlichen Bezug zu Kommunikationsmitteln* eine große Rolle spielt.

39 Zum einen kann der Täter aktive Verschleierungsmaßnahmen eingesetzt haben, um die Rückverfolgung seiner Spuren zu erschweren. Vgl. hierzu näher *Brunst,* Anonymität im Internet. Zum anderen bedarf es weiterer Schritte, um von der IP-Adresse auf eine konkrete Person schließen zu können. Vgl. hierzu sogleich.

40 Denkbar ist es, dass außerhalb der technischen Ansätze, die durch die IP-Adresse gegeben sind, andere Ermittlungsmöglichkeiten verbleiben. Bei einem Betrug über eine Auktionsplattform kann z.B. eine Lieferadresse angegeben worden sein, bei der konventionelle Ermittlungsmaßnahmen zum Ziel führen können. Bei einer Beleidigung in einem Online-Forum wurde möglicherweise ein Nutzername oder sogar eine E-Mail-Adresse angegeben, der – ggf. zusammen mit weiteren Informationen – für die Ermittlung des Täters ausschlaggebend sein können. Diese Ansätze hängen jedoch stark von der individuellen Fallgestaltung ab, während die IP-Adresse aus technischen Gründen stets übertragen wird und zumindest grundsätzlich für Ermittlungen herangezogen werden kann.

41 Zum Personenbezug von IP-Adressen sowie der Funktionsweise von dynamischen und statischen IP-Adressen vgl. *Gercke/Brunst,* Praxishandbuch Internetstrafrecht, Rn. 704 ff.

einen kommerziellen Anbieter handeln, der Nutzern einen leitungsgebundenen Zugang zum Internet anbietet, z.B. über DSL, um einen WLAN-Accesspoint oder auch um ein Internet Café. Ob der Access-Provider in der Lage ist, den gesuchten Nutzer zu identifizieren, hängt davon ab, ob er die Vergabe der IP-Adressen protokolliert.[42] Nur beim Vorliegen eines solchen Zuordnungsprotokolls kann der Anschluss – aber nicht automatisch der Nutzer –, von dem aus die fraglichen Aktionen durchgeführt wurden, identifiziert werden.

An den genannten Beispielen werden bereits die Erfolgschancen einer rein technisch auf die IP-Adresse ausgerichteten Ermittlung deutlich: Ein DSL-Anschluss, der zu einer privat genutzten Wohnung gehört, kann im Idealfall die Anzahl der Tatverdächtigen auf eine Person einschränken, nämlich den (in diesem Fall einzigen) Wohnungsbesitzer. Bei einem Internetcafé hingegen wird die Identität der Nutzer meist nicht protokolliert. Selbst eine Zuordnung der vergebenen IP-Adressen zu den einzelnen Rechnern wird daher meist nicht dazu führen, dass ein konkreter Tatverdächtiger ermittelt werden kann. Dies gilt jedenfalls für Fälle, in denen ausschließlich diese technischen Ermittlungsansätze zur Verfügung stehen. Bei der rechtswidrigen Nutzung von fremden WLAN schließlich werden regelmäßig überhaupt keine Protokolle geführt, die sich für die Ermittlung der illegalen Nutzer eignen würden.

Zusammenfassend lässt sich daher für den Bereich der online durchgeführten Delikte festhalten, dass – aus technischer Sicht – die IP-Adressen sowie (in einem zweiten Ermittlungsschritt) die Zuordnung einer genutzten Adresse zu einem konkreten Anschluss und damit (in einem dritten Schritt) auch zu einem konkreten Täter der erfolgversprechendste Weg für eine Ermittlung ist. Fehlt es an einem dieser drei Komponenten, d.h. der IP-Adresse, der Möglichkeit, diese einem konkreten Anschluss zuzuordnen, oder der Möglichkeit, einen Anschluss einer natürlichen Person (Nutzer) zuzuordnen, so wird – wiederum aus technischer Sicht – die Ermittlungsarbeit massiv erschwert, da weitere Ermittlungsansätze häufig nicht zur Verfügung stehen.

Der hier benutzte Begriff der Online-Kriminalität ist Teil der IuK-Kriminalität. Hierunter versteht das Bundeskriminalamt alle Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik oder gegen diese begangen werden.[43]

2.1.2. Offline-Kriminalität

Auch bei der reinen Offline-Kriminalität[44] hat der Zugriff auf Daten inzwischen große Bedeutung erlangt. Im Vordergrund stehen hier vor allem zwei Aspekte. Zum einen kommuni-

---

42 Selbst bei einer Protokollierung der IP-Zuteilung können jedoch Situationen eintreten, bei denen eine Rückverfolgung dennoch nicht möglich ist, etwa beim Einsatz von network address translation (NAT), bei dem mehrere Nutzer nach außen unter der gleichen IP-Adresse auftreten, oder wenn aus anderen Gründen zusätzliche Informationen zur Zuordnung des Anschlusses zu einer Kommunikation erforderlich sind.

43 Siehe BKA, Lagebild IuK-Kriminalität 2009, S. 4. Die Terminologie erscheint freilich noch immer unsicher; so hat das Bundekriminalamt das Lagebild 2010 jüngst erstmals unter der Überschrift Cybercrime veröffentlicht: www.bka.de/lageberichte/iuk/bundeslagebild_cybercrime_2010.pdf [Juni 2011].

44 Zu der Terminologie vgl. oben Anm. 38.

zieren auch Offline-Straftäter miteinander. Besondere Bedeutung hat hier nach wie vor die Sprachkommunikation, insbesondere über Mobil-, aber auch über Festnetztelefone und VoIP.[45] Zum anderen werden viele klassische Offline-Delikte aufgrund des geänderten Kommunikationsverhaltens in der Bevölkerung mit digitalen Medien vorbereitet oder durchgeführt. Klassische Betrugsdelikte werden z.B. mit Hilfe von Online-Auktionsplattformen vorbereitet, während der anschließende konventionelle Warenaustausch mit herkömmlichen Mitteln durchgeführt wird.

Die zur Ermittlung dieser Delikte benötigten Daten hängen daher in stärkerem Maße vom jeweiligen Einzelfall ab als bei Ermittlungen von reinen Online-Delikten. Denkbar sind unter anderem die folgenden Szenarien:

– Eine Tätergruppe bedient sich des so genannten *Enkeltricks.*[46] Dabei gibt sich ein Tatbeteiligter gegenüber dem Opfer telefonisch als naher Verwandter aus. Um an dessen Namen zu kommen, wird das Gespräch zum Beispiel mit der Frage „Rate mal, wer gerade anruft?“ eröffnet. Im folgenden Gespräch gibt der Täter – im Namen des Verwandten – vor, sich zum Beispiel im Ausland zu befinden, gerade Opfer eines Überfalls geworden zu sein und daher dringend eine größere Summe Geld zu benötigen, um schnell nach Hause kommen zu können. Geht das angerufene, meist ältere, Opfer auf die Forderung ein, wird telefonisch angekündigt, einen Freund zu schicken, der das Geld abholt (und ggf. auch bei der Abhebung bei der Bank „behilflich“ sein kann). In der Sache geht es also um einen telefonisch durchgeführten Trickbetrug, bei dem vom Opfer durch einen vermeintlichen Verwandten Geld erbettelt wird.[47]

  In diesen Fällen ist der Zugriff auf die Verkehrsdaten des (aufgrund des Alters der Opfer meist Festnetz-) Telefonanschlusses von entscheidender Bedeutung. Kann ermittelt werden, von welcher Telefonnummer aus dieser Anschluss zur fraglichen Uhrzeit angerufen wurde, so ist dies bereits eine erste Spur zur Ermittlung der Täter. Weiterhin kann von Bedeutung sein, Informationen zu den Mobiltelefonen zu ermitteln, die im fraglichen Zeitraum in der unmittelbaren Nähe der Opferwohnung eingeschaltet waren, denn es ist davon auszugehen, dass der Bote unmittelbar vor seinem Einsatz vom Komplizen über den bevor-

---

45 Voice-over-IP-Telefonie (VoIP) bezeichnet die Sprachkommunikation mit Hilfe des TCP/IP-Netzwerks, insbesondere über das Internet. Ein prominentes Beispiel für VoIP ist die Nutzung der Software *Skype*.

46 Vgl. hierzu die Fallbeschreibungen der Bayerischen Polizei; dort konnten 19.000 EUR erbeutet werden, http://www.polizei.bayern.de/news/presse/aktuell/index html/
33548, der Polizei Göttingen, bei der 4.000 EUR übergeben wurden,
http://www.presseportal.de/polizeipresse/p_story htx?nr=672499&firmaid=7452 sowie der Polizei Köln, bei der ein „fünfstelliger Betrag“ abhanden kam, www.presseportal.de/polizeipresse/pm/12415/1575649/polizei_koeln [alle Abrufe Juli 2010].

47 Eine andere Variante wird von der Schweizer Polizei berichtet. Danach erhält das Opfer – falls die vorherigen telefonischen Versuche erfolglos waren – einen Anruf eines vermeintlichen Polizisten, der das Opfer überredet „zum Schein“ auf den Betrug einzugehen, um so den Betrüger zu fassen und Dritte vor Schaden zu bewahren. Vgl. http://www.den-trick-kenne-ich.ch/10/de/2betrug/1praevention_betrugsmethoden/40301enkeltrick.php [Juni 2011].

stehenden Besuch beim Opfer informiert worden ist. Auf diese Weise können mit Hilfe von Verkehrsdaten bereits erste Ansatzpunkte für die weiteren Ermittlungen gewonnen werden.

– Während die Ermittlungen beim Enkeltrick auf einen eng begrenzten Zeitraum beschränkt sind, wird bei *Strukturermittlungen,* z.B. der Organisierten Kriminalität, eher ein langfristiger Zeitraum im Mittelpunkt der Untersuchung stehen. Es geht dabei um die Aufdeckung von übergreifenden Zusammenhängen und Deliktsketten, die den Weg in eine kriminelle Organisation zeigen und den Ansatzpunkt zu ihrer wirksamen Zerschlagung darstellen kann.[48] Mit Hilfe der Verkehrsdaten zunächst eines Beteiligten können Kommunikationsstrukturen aufgedeckt und mögliche Bandenstrukturen erkannt werden. Dieser größere Blickwinkel erlaubt es später, eingriffsintensivere Maßnahmen, wie z.B. Telekommunikationsüberwachungen (TKÜ), bei denen auch Inhaltsdaten erfasst werden, auf die Teilnehmer zu beschränken, die aufgrund der Kommunikationsstrukturen eine größere oder bedeutendere Rolle zu spielen scheinen. Mit Hilfe der Standortdaten können Treffpunkte, die bei mehreren Beteiligten eine Rolle zu spielen scheinen, in die weitere Arbeit, z.B. für Vor-Ort-Überwachungen, einbezogen werden.

– Die insbesondere bei der Mobilfunknutzung anfallenden Verkehrsdaten können nicht nur zu Ermittlungszwecken im engeren Sinne, d.h. zur Überführung eines Täters, sondern auch zu *Entlastungszwecken* eingesetzt werden. Denkbar ist es beispielsweise, dass durch die Standortdaten des Mobilfunktelefons[49] eines Verdächtigen ein Alibi gestützt wird, wonach der Verdächtige sich zum fraglichen Zeitpunkt an einem ganz anderen Ort aufgehalten hat. Weitere Überwachungs- und Ermittlungsmaßnahmen können in diesem Fall entfallen.

Die drei Beispiele machen deutlich, dass auch bei der so genannten Offline-Kriminalität der Zugriff auf Verkehrsdaten eine besondere Rolle spielen kann. Wie nachfolgend gezeigt werden wird, stehen große Bereiche gegenwärtig allerdings nicht mehr zur Verfügung, so dass die Ermittlungsmöglichkeiten stark eingeschränkt und – bei Ermittlungen der Online-Kriminalität – zum Teil fast unmöglich gemacht werden.

2.2. Zugriff auf Bestandsdaten

2.2.1. Speicherung

Telekommunikationsbestandsdaten dürfen grundsätzlich nach § 95 TKG erhoben und verwendet werden. Diese Vorschrift ist durch das Urteil des Bundesverfassungsgerichts nicht tangiert worden. Sie lautet gegenwärtig:

---

48 Vgl. *Hebrok,* Strukturermittlungen, S. 3.

49 Vgl. näher *Hebrok,* Strukturermittlungen, S. 75 ff.

§ 95 Vertragsverhältnisse

(1) Der Diensteanbieter darf Bestandsdaten erheben und verwenden, soweit dieses zur Erreichung des in § 3 Nr. 3 genannten Zweckes erforderlich ist. Im Rahmen eines Vertragsverhältnisses mit einem anderen Diensteanbieter darf der Diensteanbieter Bestandsdaten seiner Teilnehmer und der Teilnehmer des anderen Diensteanbieters erheben und verwenden, soweit dies zur Erfüllung des Vertrages zwischen den Diensteanbietern erforderlich ist. Eine Übermittlung der Bestandsdaten an Dritte erfolgt, soweit nicht dieser Teil oder ein anderes Gesetz sie zulässt, nur mit Einwilligung des Teilnehmers.

(2) Der Diensteanbieter darf die Bestandsdaten der in Absatz 1 Satz 2 genannten Teilnehmer zur Beratung der Teilnehmer, zur Versendung von Informationen nach § 98 Abs. 1 Satz 3, zur Werbung für eigene Angebote, zur Marktforschung und zur Unterrichtung über einen individuellen Gesprächswunsch eines anderen Nutzers nur verwenden, soweit dies für diese Zwecke erforderlich ist und der Teilnehmer eingewilligt hat. Ein Diensteanbieter, der im Rahmen einer bestehenden Kundenbeziehung rechtmäßig Kenntnis von der Rufnummer oder der Postadresse, auch der elektronischen, eines Teilnehmers erhalten hat, darf diese für die Versendung von Text- oder Bildmitteilungen an ein Telefon oder an eine Postadresse zu den in Satz 1 genannten Zwecken verwenden, es sei denn, dass der Teilnehmer einer solchen Verwendung widersprochen hat. Die Verwendung der Rufnummer oder Adresse nach Satz 2 ist nur zulässig, wenn der Teilnehmer bei der Erhebung oder der erstmaligen Speicherung der Rufnummer oder Adresse und bei jeder Versendung einer Nachricht an diese Rufnummer oder Adresse zu einem der in Satz 1 genannten Zwecke deutlich sichtbar und gut lesbar darauf hingewiesen wird, dass er der Versendung weiterer Nachrichten jederzeit schriftlich oder elektronisch widersprechen kann.

(3) Endet das Vertragsverhältnis, sind die Bestandsdaten vom Diensteanbieter mit Ablauf des auf die Beendigung folgenden Kalenderjahres zu löschen. § 35 Abs. 3 des Bundesdatenschutzgesetzes gilt entsprechend.

(4) Der Diensteanbieter kann im Zusammenhang mit dem Begründen und dem Ändern des Vertragsverhältnisses sowie dem Erbringen von Telekommunikationsdiensten die Vorlage eines amtlichen Ausweises verlangen, wenn dies zur Überprüfung der Angaben des Teilnehmers erforderlich ist. Er kann von dem Ausweis eine Kopie erstellen. Die Kopie ist vom Diensteanbieter unverzüglich nach Feststellung der für den Vertragsabschluss erforderlichen Angaben des Teilnehmers zu vernichten. Andere als die nach Absatz 1 zulässigen Daten darf der Diensteanbieter dabei nicht verwenden.

(5) Die Erbringung von Telekommunikationsdiensten darf nicht von einer Einwilligung des Teilnehmers in eine Verwendung seiner Daten für andere Zwecke abhängig gemacht werden, wenn dem Teilnehmer ein anderer Zugang zu diesen Telekommunikationsdiensten ohne die Einwilligung nicht oder in nicht zumutbarer Weise möglich ist. Eine unter solchen Umständen erteilte Einwilligung ist unwirksam.

Im Wesentlichen können danach Bestandsdaten erhoben und verwendet werden, soweit dies zur Vertragserfüllung erforderlich ist.[50] Im Umkehrschluss ergibt sich, dass Bestandsdaten nicht erhoben werden dürfen, wenn dies nicht für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses erforderlich ist. Aus diesem Grund müssen Bestandsdaten z.B. nicht angegeben werden, wenn ein bar zahlender Nutzer ein Internetcafé aufsucht, um von dort aus E-Mails zu verschicken oder andere Handlungen im Internet vorzunehmen.

Eine bedeutende Ausnahme von diesem Grundsatz gilt für die Anbieter von Telefondiensten und insbesondere Mobilfunktelefonen. Nach § 111 Abs. 1 TKG müssen Anbieter, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken und dabei Rufnummern oder andere Anschlusskennungen vergeben für das automatisierte Auskunftsverfahren nach § 112 TKG bestimmte Informationen erheben. Hierzu gehört die Rufnummer, Name und Anschrift des Anschlussinhabers, das Geburtsdatum, die Anschrift des Anschlusses bei Festnetzanschlüssen bzw. die Gerätenummer des überlassenen Mobilfunktelefons sowie das Datum des Vertragsbeginns. Diese Daten sind auch dann zu erheben und zu speichern, wenn sie für betriebliche Zwecke nicht erforderlich sind.[51] Diese Form der „kleinen Vorratsdatenspeicherung“[52] war nicht Gegenstand des Urteils des Bundesverfassungsgerichts und ist demgemäß vom Richterspruch nicht betroffen.

In § 111 Abs. 1 S. 3 TKG ist eine Bestandsdatenspeicherpflicht für Anbieter von E-Mail-Diensten[53] normiert. Bei den dort genannten Informationen handelt es sich um Telemedienbestandsdaten nach § 14 TMG und nicht um Telekommunikationsbestandsdaten, so dass die Vorschrift eigentlich im falschen Gesetz enthalten ist und zudem durch die Verweisungstechnik auch nicht besonders normenklar ist.[54] Die Vorschrift enthält keine originäre Speicherverpflichtung für E-Mail-Anbieter[55] sondern greift nur, wenn ein E-Mail-Anbieter Daten ohnehin erfasst.

---

50 Ausführlicher zur Erhebung und Verwendung von Bestandsdaten *Brunst,* Anonymität im Internet, S. 332 ff.

51 Gegenwärtig besteht allerdings kein Zwang, diese Informationen auch zu überprüfen, was sich u.a. der AK Vorratsdatenspeicherung bei einer Aktion im Jahr 2008 zunutze gemacht hat, als er Prepaidkarten weitergab, die auf nicht existierende Personen registriert waren. Vgl. http://www.golem.de/0805/59954 html [Juni 2011].

52 Der Begriff der „kleinen Vorratsdatenspeicherung“ bietet sich an, da auch hier Daten auf Vorrat gespeichert werden, die für die eigentlichen Zwecke der Anbieter nicht erforderlich sind, die aber die Verfolgung von Ordnungswidrigkeiten nach dem TKG oder dem UWG ermöglichen sollen oder die für die Erledigung der Auskunftsersuchen der in § 112 Abs. 2 TKG genannten Stellen benötigt werden.

53 Kritisch zu dem im Gesetz genutzten Begriff der „elektronischen Post“ *Brunst,* Anonymität im Internet, S. 398 f. und 402.

54 Vgl. ausführlicher zu dieser Frage *Brunst,* Anonymität im Internet, S. 396 m.w.N.

55 Vgl. BT-Drs. 16/5846, S. 68.

2.2.2. Zugriff

Auf gespeicherte Bestandsdaten darf im automatisierten Verfahren nach §§ 111, 112 TKG (dann beschränkt auf die in § 111 Abs. 1 TKG genannten Daten) oder im Rahmen eines manuellen Auskunftsverfahrens nach § 113 TKG zugegriffen werden.

Das Urteil befasst sich unter anderem mit diesen Möglichkeiten.[56] Danach haben auch die zur Beantwortung von behördlichen Auskunftsersuchen herangezogenen Vorratsdaten „erhebliches Gewicht", denn der Gesetzgeber begrenzt auch hierdurch den Umfang der Anonymität von Bürgern im Internet, jedoch bleibt die Aussagekraft dieser Daten für den Staat eng begrenzt und der durch sie geschaffene Erkenntniswert punktuell.[57] Der bislang in der Literatur teilweise vertretenen Ansicht, wonach auch die Nutzung von Verkehrsdaten mit dem Zweck der Ermittlung von Bestandsdaten eines Beschlusses nach § 100g StPO – und damit einer richterlichen Entscheidung – bedürfe,[58] erteilt das Gericht indirekt eine Absage.[59] Bei der Umsetzung der vom Gericht in diesem Zusammenhang vorgesehenen Anforderungen würde es sich anbieten, die immer noch bestehenden Rechtsunsicherheiten[60] dieses Regelungsbereichs durch eine klare Normengestaltung endgültig zu beenden.

Neben der rechtlichen Einschätzung führt der Wegfall der Vorratsdaten auch zu einer mittelbaren praktischen Auswirkung mit großer Bedeutung: Da in vielen Fällen von Anbietern nicht mehr die Zuordnung von IP-Adressen zu einzelnen Nutzern protokolliert wird (vgl. hierzu unten), können Anfragen, die sich auf diesen Vorgang beziehen, bei derartigen Anbietern nicht mehr beantwortet werden. Konkret bedeutet dies, dass diese Anbieter nicht mehr in der Lage sind, darüber Auskunft zu geben, welcher Kunde eine bestimmte IP-Adresse in der Vergangenheit genutzt hat. Ermittlungen, die sich ausschließlich auf IP-Adressen richten, sind daher gegenwärtig in vielen Fällen zum Scheitern verurteilt.

Darüber hinaus können Probleme in den Fällen entstehen, in denen Informationen bei einem Anbieter zwar vorhanden sind, aber nicht aufgrund der allgemeinen Norm des § 96 TKG gespeichert wurden. So erlaubt zwar § 100 TKG ebenfalls die Erhebung und Verwendung von Verkehrsdaten. Allerdings dürfen nach dieser Vorschrift Daten nur erhoben und verwendet werden, soweit dies „zum Erkennen, Eingrenzen oder Beseitigen von Störungen oder Fehlern an Telekommunikationsanlagen" erforderlich ist. Wenn bei einem Anbieter Daten nicht

---

56 Vgl. BVerfG, a.a.O. (Fn. 1), Rz. 254 ff.

57 BVerfG, a.a.O. (Fn. 1), Rz. 258, 256.

58 Vgl. hierzu etwa *Bär,* Handbuch zur EDV-Beweissicherung, Rn. 205 ff.; *Eckhardt,* in: Spindler/Schuster, Recht der elektronischen Medien, § 113 TKG Rn. 9 sowie *Gercke/Brunst,* Praxishandbuch Internetstrafrecht, Rn. 660 ff.

59 BVerfG, a.a.O. (Fn. 1), Rz. 261 a.E. Die wohl überwiegende Auffassung (vgl. Rz. 45 m.w.N.) war bereits vor Einführung der Vorratsdatenspeicherung, dass ein Auskunftsersuchen nach § 113 TKG ausreichend war. Die „Klarstellung" durch den Gesetzgeber bleibt aufgrund der lückenhaften Verweisungskette dennoch unbefriedigend, vgl. *Gercke/Brunst,* Praxishandbuch Internetstrafrecht, Rn. 667.

60 Vgl. *Gercke/Brunst,* Praxishandbuch Internetstrafrecht, Rn. 667 m.w.N.

(mehr) nach § 96 TKG gespeichert vorliegen, aber möglicherweise nach § 100 TKG, so stellt sich die Frage, ob auch diese Informationen für eine Anfrage nach § 113 TKG herangezogen werden dürfen.[61]

In der Praxis wird dies zum Teil so gehandhabt.[62] Bedenken könnten sich im Hinblick darauf ergeben, dass § 113 TKG ausdrücklich nur auf die „nach den §§ 95 und 111 erhobenen Daten" verweist. Die Auskunft nach § 95 TKG ist im vorliegenden Fall jedoch nur mit Hilfe von Verkehrsdaten möglich. § 96 TKG erlaubt einerseits die Erhebung bestimmter Verkehrsdaten nur für „die in diesem Abschnitt […] genannten Zwecke" (§ 96 Abs. 1 S. 1), andererseits ihre Verwendung auch für „durch andere gesetzliche Vorschriften begründete Zwecke" (§ 96 Abs. 1 S. 2). Obwohl die Auskunftsvorschrift des § 113 TKG in einem anderen Abschnitt (Abschnitt 3 – Öffentliche Sicherheit) als die allgemeine Verkehrsdatenvorschrift des § 96 TKG (Abschnitt 2 – Datenschutz) enthalten ist,[63] erlaubt die ganz h.M. den Zugriff auf diese Daten, um die Auskunft nach § 95 TKG erteilen zu können. Während § 96 TKG jedoch ersichtlich als „Generalnorm" für eine ganze Reihe von Auskünften ausgelegt ist[64] und daher einen abschließenden[65] Katalog von Verkehrsdaten enthält, wurde § 100 TKG auf ganz bestimmte Zwecke hin ausgerichtet, nämlich insbesondere die – anbieterinterne – Erkennung, Eingrenzung und Beseitigung von Störungen. Nach § 100 Abs. 3 TKG dürfen in bestimmten Fällen auch Daten zur Aufdeckung und Unterbindung von Missbräuchen erhoben und verwendet werden. Um dies umfassend zu ermöglichen, enthält § 100 TKG auch keine Beschränkung auf bestimmte Daten wie dies bei § 96 TKG der Fall ist,[66] sondern erlaubt – im Rahmen der Erforderlichkeit – grundsätzlich den Zugriff auf beliebige für die Zweckerreichung notwendige Verkehrsdaten. Ein Rückgriff auf diese zweckgebundenen Daten für allgemeine Auskunftszwecke kann daher ungeachtet der Verwendungserweiterung in § 96 Abs. 1 S. 2 TKG

---

61 Bei Anordnungen nach § 100g StPO stellt sich diese Frage strenggenommen nicht, denn § 100g Abs. 1 S. 1 StPO verweist ausdrücklich auf Verkehrsdaten nach § 96 Abs. 1 TKG und § 113a TKG. Hätte der Gesetzgeber den Zugriff auf alle Verkehrsdaten ermöglichen wollen, so hätte sich ein Verweis auf § 3 Nr. 30 TKG angeboten, der Verkehrsdaten allgemein als Daten definiert, „die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden" und die daher auch solche nach § 100 TKG eingeschlossen hätten. Siehe ergänzend auch die Ausführungen in Fn. 75.

62 So stellt das OLG Zweibrücken ZUM 2009, 77 fest, es käme für den Erfolg eines staatsanwaltschaftlichen Auskunftsersuchens darauf an, „ob der betreffende Diensteanbieter von der Möglichkeit des § 100 TKG Gebrauch [gemacht habe] und dadurch überhaupt die Möglichkeit [bestünde], im Nachhinein den Inhaber einer dynamischen IP-Adresse zu individualisieren".

63 Die Zuordnung von IP-Adressen zu Bestandsdaten dient weder der „Erhebung" noch der „Verwendung", da beides auf den in § 3 Nr. 3 genannten Zweck beschränkt ist, sondern ausschließlich der Beantwortung einer Auskunft nach § 113 TKG.

64 Die Vorschrift verweist auf die „in diesem Abschnitt" (gemeint ist der 2. Abschnitt des 7. Teils des TKG) genannten Zwecke sowie auf bestimmte Vorschriften des Zugangserschwerungsgesetzes. Weiterhin verweist auch § 100g StPO ausdrücklich auf Verkehrsdaten nach § 96 Abs. 1 TKG.

65 Vgl. *Robert,* in: BeckTKG-Komm., § 96 TKG Rn. 2.

66 § 100 TKG erlaubt – anders als etwa § 97 TKG, der sich explizit auf „die in § 96 Abs. 1 aufgeführten Verkehrsdaten" bezieht – die Erhebung und Verwendung von *den Verkehrsdaten* der Teilnehmer und Nutzer, enthält also keine über die Erforderlichkeit hinausgehenden Einschränkungen. Vgl. *Wittern,* in: BeckTKG-Komm., § 100 TKG Rn. 2 f.

bedenklich erscheinen. Denn weder § 113 TKG noch § 100g StPO nehmen generell Bezug auf „Verkehrsdaten im Sinne von § 3 Nr. 30 TKG“, was einen allgemeinen Zugriff auf jegliche Verkehrsdaten ermöglicht hätte, sondern explizit auf § 96 Abs. 1 TKG (im Fall von § 100g StPO) bzw. § 95 TKG (im Fall von § 113 TKG). Einen allgemeinen Durchgriff sieht auch das Bundesverfassungsgericht zumindest für Nicht-Katalogtaten durchaus kritisch und formuliert für den Fall der möglichen Wiedereinführung einer Vorratsdatenspeicherung auch für den Rückgriff auf Verkehrsdaten zu Zwecken der IP-Zuordnung bestimmte Anforderungen.[67]

2.3. Zugriff auf Verkehrsdaten

2.3.1. Speicherung

2.3.1.1. Allgemeine Daten

Allgemeine Telekommunikationsverkehrsdaten dürfen grundsätzlich nach § 96 TKG erhoben werden. Danach ist die Erhebung zulässig, wenn dies für Zwecke des 2. Abschnitts des TKG (Datenschutz) oder für die in §§ 2, 4 ZugErschwG genannten Zwecke erforderlich ist. Aufgrund des gegenwärtigen Zustands im Hinblick auf das Zugangserschwerungsgesetz werden hierzu nachfolgend keine weiteren Ausführungen gemacht. Nach § 96 TKG dürfen die folgenden Verkehrsdaten erhoben werden (vorausgesetzt, dies ist zur Erreichung eines der nachfolgenden Zwecke erforderlich):

– die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten,

– der Beginn und das Ende der jeweiligen Verbindung,

– die übermittelten Datenmengen, soweit die Entgelte davon abhängen,

– der vom Nutzer in Anspruch genommene Telekommunikationsdienst,

– die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende und – soweit Entgelte davon abhängen – die übermittelten Datenmengen

– sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.

Nach § 96 Abs. 2 TKG ist eine über Abs. 1 hinausgehende Erhebung oder Verwendung von Verkehrsdaten ausdrücklich unzulässig. Der primäre Zweck der allgemeinen Verkehrsdaten liegt nach den §§ 96, 97 TKG zum einen in der Ermöglichung eines technisch korrekten Verbindungsaufbaus und – vor allem – in der Schaffung der notwendigen Grundlagen für eine

---

67 Vgl. BVerfG, a.a.O. (Fn. 1), Rz. 279 sowie Rz. 254 ff. zu den genauen Anforderungen.

korrekte Entgeltermittlung und -abrechnung. Dem Anbieter wird in diesem Zusammenhang aufgegeben, nach der Beendigung einer Verbindung unverzüglich die für die Berechnung des Entgelts erforderlichen Daten zu ermitteln. Nur diese Abrechnungsdaten dürfen bis zu sechs Monate nach Versendung der Rechnung gespeichert werden. Alle nicht erforderlichen Daten sind hingegen unverzüglich zu löschen.

Gegenwärtig lauten die beiden zentralen für allgemeine Verkehrsdaten einschlägigen Vorschriften:

§ 96 Verkehrsdaten

(1) Der Diensteanbieter darf folgende Verkehrsdaten erheben, soweit dies für die in diesem Abschnitt oder in § 2 oder § 4 des Zugangserschwerungsgesetzes genannten Zwecke erforderlich ist:

1. die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten,

2. den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,

3. den vom Nutzer in Anspruch genommenen Telekommunikationsdienst,

4. die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende nach Datum und Uhrzeit und, soweit die Entgelte davon abhängen, die übermittelten Datenmengen,

5. sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.

Diese Verkehrsdaten dürfen nur verwendet werden, soweit dies für die in Satz 1 genannten oder durch andere gesetzliche Vorschriften begründeten Zwecke oder zum Aufbau weiterer Verbindungen erforderlich ist. Im Übrigen sind Verkehrsdaten vom Diensteanbieter nach Beendigung der Verbindung unverzüglich zu löschen.

(2) Eine über Absatz 1 hinausgehende Erhebung oder Verwendung der Verkehrsdaten ist unzulässig.

(3) Der Diensteanbieter darf teilnehmerbezogene Verkehrsdaten, die vom Anbieter eines Telekommunikationsdienstes für die Öffentlichkeit verwendet werden, zum Zwecke der Vermarktung von Telekommunikationsdiensten, zur bedarfsgerechten Gestaltung von Telekommunikationsdiensten oder zur Bereitstellung von Diensten mit Zusatznutzen im dazu erforderlichen Zeitraum nur verwenden, sofern der Betroffene in diese Verwendung eingewilligt hat. Die Daten der Angerufenen sind unverzüglich zu anonymisieren. Eine zielnum-

mernbezogene Verwendung der Verkehrsdaten durch den Diensteanbieter zu den in Satz 1 genannten Zwecken ist nur mit Einwilligung der Angerufenen zulässig. Hierbei sind die Daten der Anrufenden unverzüglich zu anonymisieren.

(4) Bei der Einholung der Einwilligung ist dem Teilnehmer mitzuteilen, welche Datenarten für die in Absatz 3 Satz 1 genannten Zwecke verarbeitet werden sollen und wie lange sie gespeichert werden sollen. Außerdem ist der Teilnehmer darauf hinzuweisen, dass er die Einwilligung jederzeit widerrufen kann.

§ 97 Entgeltermittlung und Entgeltabrechnung

(1) Diensteanbieter dürfen die in § 96 Abs. 1 aufgeführten Verkehrsdaten verwenden, soweit die Daten zur Ermittlung des Entgelts und zur Abrechnung mit ihren Teilnehmern benötigt werden. Erbringt ein Diensteanbieter seine Dienste über ein öffentliches Telefonnetz eines fremden Betreibers, darf der Betreiber des öffentlichen Telefonnetzes dem Diensteanbieter die für die Erbringung von dessen Diensten erhobenen Verkehrsdaten übermitteln. Hat der Diensteanbieter mit einem Dritten einen Vertrag über den Einzug des Entgelts geschlossen, so darf er dem Dritten die in Absatz 2 genannten Daten übermitteln, soweit es zum Einzug des Entgelts und der Erstellung einer detaillierten Rechnung erforderlich ist. Der Dritte ist vertraglich zur Wahrung des Fernmeldegeheimnisses nach § 88 und des Datenschutzes nach den §§ 93 und 95 bis 97, 99 und 100 zu verpflichten. § 11 des Bundesdatenschutzgesetzes bleibt unberührt.

(2) Der Diensteanbieter darf zur ordnungsgemäßen Ermittlung und Abrechnung der Entgelte für Telekommunikationsdienste und zum Nachweis der Richtigkeit derselben folgende personenbezogene Daten nach Maßgabe der Absätze 3 bis 6 erheben und verwenden:

1. die Verkehrsdaten nach § 96 Abs. 1,

2. die Anschrift des Teilnehmers oder Rechnungsempfängers, die Art des Anschlusses, die Zahl der im Abrechnungszeitraum einer planmäßigen Entgeltabrechnung insgesamt aufgekommenen Entgelteinheiten, die übermittelten Datenmengen, das insgesamt zu entrichtende Entgelt,

3. sonstige für die Entgeltabrechnung erhebliche Umstände wie Vorschusszahlungen, Zahlungen mit Buchungsdatum, Zahlungsrückstände, Mahnungen, durchgeführte und aufgehobene Anschlusssperren, eingereichte und bearbeitete Reklamationen, beantragte und genehmigte Stundungen, Ratenzahlungen und Sicherheitsleistungen.

(3) Der Diensteanbieter hat nach Beendigung der Verbindung aus den Verkehrsdaten nach § 96 Abs. 1 Nr. 1 bis 3 und 5 unverzüglich die für die Berechnung des Entgelts erforderlichen Daten zu ermitteln. Diese Daten dürfen bis zu sechs Monate nach Versendung der Rechnung gespeichert werden. Für die Abrechnung nicht erforderliche Daten sind unverzüglich zu lö-

schen, soweit sie nicht nach § 113a zu speichern sind. Hat der Teilnehmer gegen die Höhe der in Rechnung gestellten Verbindungsentgelte vor Ablauf der Frist nach Satz 2 Einwendungen erhoben, dürfen die Daten gespeichert werden, bis die Einwendungen abschließend geklärt sind.

(4) Soweit es für die Abrechnung des Diensteanbieters mit anderen Diensteanbietern oder mit deren Teilnehmern sowie anderer Diensteanbieter mit ihren Teilnehmern erforderlich ist, darf der Diensteanbieter Verkehrsdaten verwenden.

(5) Zieht der Diensteanbieter mit der Rechnung Entgelte für Leistungen eines Dritten ein, die dieser im Zusammenhang mit der Erbringung von Telekommunikationsdiensten erbracht hat, so darf er dem Dritten Bestands- und Verkehrsdaten übermitteln, soweit diese im Einzelfall für die Durchsetzung der Forderungen des Dritten gegenüber seinem Teilnehmer erforderlich sind.

Mit Ausnahme von § 97 Abs. 3 S. 2 TKG, der pauschal auf § 113a TKG verweist und klarstellt, dass Vorratsdaten auch dann für die vorgesehene Dauer zu speichern sind, wenn sie sich inhaltlich mit Abrechnungs- oder sonstigen Verkehrsdaten überschneiden, hat das Urteil keine unmittelbaren Auswirkungen auf die Erhebungs- und Verwendungsmöglichkeiten allgemeiner Verkehrsdaten. Vielmehr bleibt es bei dem auch schon vorher bestehenden Grundsatz, dass allgemeine Verkehrsdaten nur dann erhoben und verarbeitet werden dürfen, wenn dies für Zwecke der Entgeltermittlung und -abrechnung, Störungsbehebung, Missbrauchsbekämpfung und für die Erstellung von Einzelverbindungsnachweisen notwendig ist.

2.3.1.2. Standortdaten

Für Standortdaten war und ist § 98 TKG einschlägig. Danach dürfen Standortdaten entweder anonymisiert verwendet werden oder, wenn ein Teilnehmer seine Einwilligung erteilt hat, insbesondere für die darauf aufbauenden Dienste. Die Vorschrift lautet gegenwärtig:

§ 98 Standortdaten

(1) Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder Telekommunikationsdiensten für die Öffentlichkeit verwendet werden, dürfen nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Maß und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer seine Einwilligung erteilt hat. Werden die Standortdaten für einen Dienst mit Zusatznutzen verarbeitet, der die Übermittlung von Standortdaten eines Mobilfunkendgerätes an einen anderen Teilnehmer oder Dritte, die nicht Anbieter des Dienstes mit Zusatznutzen sind, zum Gegenstand hat, muss der Teilnehmer abweichend von § 94 seine Einwilligung ausdrücklich, gesondert und schriftlich erteilen. In diesen Fällen hat der Diensteanbieter den Teilnehmer nach höchstens fünfmaliger Feststellung des Standortes des Mobilfunkendgerätes über die Anzahl der erfolgten Standortfeststellungen mit einer Textmitteilung zu informieren, es sei denn, der Teilnehmer hat gemäß § 95 Abs. 2 Satz 2 widersprochen. Der Teilnehmer

muss Mitbenutzer über eine erteilte Einwilligung unterrichten. Eine Einwilligung kann jederzeit widerrufen werden.

(2) Haben die Teilnehmer ihre Einwilligung zur Verarbeitung von Standortdaten gegeben, müssen sie auch weiterhin die Möglichkeit haben, die Verarbeitung solcher Daten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und unentgeltlich zeitweise zu untersagen.

(3) Bei Verbindungen zu Anschlüssen mit der Rufnummer 112, den in der Rechtsverordnung nach § 108 Abs. 2 festgelegten Rufnummern oder der Rufnummer 124 124, hat der Diensteanbieter sicherzustellen, dass nicht im Einzelfall oder dauernd die Übermittlung von Standortdaten ausgeschlossen wird.

(4) Die Verarbeitung von Standortdaten nach den Absätzen 1 und 2 muss auf das für die Bereitstellung des Dienstes mit Zusatznutzen erforderliche Maß sowie auf Personen beschränkt werden, die im Auftrag des Betreibers des öffentlichen Telekommunikationsnetzes oder öffentlich zugänglichen Telekommunikationsdienstes oder des Dritten, der den Dienst mit Zusatznutzen anbietet, handeln.

Durch das Urteil des Bundesverfassungsgerichts ist diese Vorschrift nicht tangiert worden. Allerdings waren in § 113a TKG verschiedene standortbezogene Daten enthalten, die nach dem Urteil nicht mehr zur Verfügung stehen. Im Einzelnen handelt es sich um

– die Funkzellen des anrufenden Anschlusses sowie des angerufenen Anschlusses, die bei Beginn der Verbindung genutzt wurden (§ 113a Abs. 2 Nr. 4 lit. c) TKG),

– die Funkzelle, in der ein anonymes Prepaid-Telefon das erste Mal aktiviert wurde (§ 113a Abs. 2 Nr. 4 lit. d) TKG).

Nach § 113a Abs. 7 TKG war der Anbieter in diesen Fällen verpflichtet, auch Daten vorzuhalten, aus denen sich die geografische Lage der die jeweilige Funkzelle versorgenden Funkantennen sowie deren Hauptstrahlrichtungen ergeben.

2.3.1.3. Vorratsdaten

Die zentrale Norm zur Regelung der Vorratsdatenspeicherung war § 113a TKG. Diese Vorschrift sah vor, dass bestimmte Verkehrsdaten von Anbietern öffentlich zugänglicher Telefondienste, von Anbietern „von Diensten der elektronischen Post“ sowie von Anbietern von Internetzugangsdiensten zu speichern waren. Nicht ausdrücklich genannt, aber im Blickpunkt des Gesetzgebers waren auch die Anbieter von Anonymisierungs- und ähnlichen Diensten.

Tabelle B-1: Synopse der grundsätzlich abfragbaren Datenarten gem. §§ 113a und 96 TKG

§ 113a TKG	**§ 96 TKG**
Abs. 2 S.1 Nr. 1: die Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses Abs. 2 S. 1 Nr. 5: im Falle von Internet-Telefondiensten auch die Internetprotokoll-Adresse des anrufenden und des angerufenen Anschlusses Abs. 3: Die Anbieter von Diensten der elektronischen Post speichern: 1. bei Versendung einer Nachricht die Kennung des elektronischen Postfachs und die Internetprotokoll-Adresse des Absenders sowie die Kennung des elektronischen Postfachs jedes Empfängers der Nachricht, 2. bei Eingang einer Nachricht in einem elektronischen Postfach die Kennung des elektronischen Postfachs des Absenders und des Empfängers der Nachricht sowie die Internetprotokoll-Adresse der absendenden Telekommunikationsanlage, 3. bei Zugriff auf das elektronische Postfach dessen Kennung und die Internetprotokoll-Adresse des Abrufenden, Abs. 4: Die Anbieter von Internetzugangsdiensten speichern: 1. die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse, 2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, Abs. 2 S. 1 Nr. 4: im Fall mobiler Telefondienste ferner a) die internationale Kennung für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss,	Abs. 1 S. 1 Nr. 1: - die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung - personenbezogene Berechtigungskennungen - bei Verwendung von Kundenkarten auch die Kartennummer

b) die internationale Kennung des anrufenden und des angerufenen Endgerätes, c) die Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzten Funkzellen, d) im Falle im Voraus bezahlter anonymer Dienste auch die erste Aktivierung des Dienstes nach Datum, Uhrzeit und Bezeichnung der Funkzelle,	- bei mobilen Anschlüssen auch die Standortdaten
Abs. 2 S. 1 Nr. 2: den Beginn und das Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone Abs. 3 Nr. 4 die Zeitpunkte der in den Nummern 1 bis 3 genannten Nutzungen des Dienstes nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone. Abs. 4 Nr. 3: den Beginn und das Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.	Abs. 1 S. 1 Nr. 2: - den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit Abs. 1 S. 1 Nr. 4: - die Endpunkte von festgeschalteten Verbindungen - ihren Beginn und ihr Ende nach Datum und Uhrzeit
Abs. 2 S. 1 Nr. 3: in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, Angaben zu dem genutzten Dienst	Abs. 1 S. 1 Nr. 3: den vom Nutzer in Anspruch genommenen Telekommunikationsdienst
Abs.2 S. 2: Satz 1 gilt entsprechend bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei sind anstelle der Angaben nach Satz 1 Nr. 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht zu speichern.	Abs. 1 S. 1 Nr. 5: sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwenige Verkehrsdaten
	Abs. 1 S. 1 Nr.2: soweit die Entgelte davon abhängen: die übermittelten Datenmengen Abs. 1 S. 1 Nr.4: soweit die Entgelte davon abhängen: die übermittelten Datenmengen

Durch § 113a Abs. 6 TKG waren auch die Daten dieser Anbieter von der Vorschrift betroffen. Die Vorschrift in der vor dem Urteil gültigen Fassung lautete:

§ 113a Speicherungspflichten für Daten

(1) Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ist verpflichtet, von ihm bei der Nutzung seines Dienstes erzeugte oder verarbeitete Verkehrsdaten nach Maßgabe der Absätze 2 bis 5 sechs Monate im Inland oder in einem anderen Mitgliedstaat der Europäischen Union zu speichern. Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, ohne selbst Verkehrsdaten zu erzeugen oder zu verarbeiten, hat sicherzustellen, dass die Daten gemäß Satz 1 gespeichert werden, und der Bundesnetzagentur auf deren Verlangen mitzuteilen, wer diese Daten speichert.

(2) Die Anbieter von öffentlich zugänglichen Telefondiensten speichern:

1. die Rufnummer oder andere Kennung des anrufenden und des angerufenen Anschlusses sowie im Falle von Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,

2. den Beginn und das Ende der Verbindung nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone,

3. in Fällen, in denen im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können, Angaben zu dem genutzten Dienst,

4. im Fall mobiler Telefondienste ferner:

a) die internationale Kennung für mobile Teilnehmer für den anrufenden und den angerufenen Anschluss,

b) die internationale Kennung des anrufenden und des angerufenen Endgerätes,

c) die Bezeichnung der durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzten Funkzellen,

d) im Fall im Voraus bezahlter anonymer Dienste auch die erste Aktivierung des Dienstes nach Datum, Uhrzeit und Bezeichnung der Funkzelle,

5. im Fall von Internet-Telefondiensten auch die Internetprotokoll-Adresse des anrufenden und des angerufenen Anschlusses.

Satz 1 gilt entsprechend bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht; hierbei sind anstelle der Angaben nach Satz 1 Nr. 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht zu speichern.

(3) Die Anbieter von Diensten der elektronischen Post speichern:

1. bei Versendung einer Nachricht die Kennung des elektronischen Postfachs und die Internetprotokoll-Adresse des Absenders sowie die Kennung des elektronischen Postfachs jedes Empfängers der Nachricht,

2. bei Eingang einer Nachricht in einem elektronischen Postfach die Kennung des elektronischen Postfachs des Absenders und des Empfängers der Nachricht sowie die Internetprotokoll-Adresse der absendenden Telekommunikationsanlage,

3. bei Zugriff auf das elektronische Postfach dessen Kennung und die Internetprotokoll-Adresse des Abrufenden,

4. die Zeitpunkte der in den Nummern 1 bis 3 genannten Nutzungen des Dienstes nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

(4) Die Anbieter von Internetzugangsdiensten speichern:

1. die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,

2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt,

3. den Beginn und das Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone.

(5) Soweit Anbieter von Telefondiensten die in dieser Vorschrift genannten Verkehrsdaten für die in § 96 Abs. 2 genannten Zwecke auch dann speichern oder protokollieren, wenn der Anruf unbeantwortet bleibt oder wegen eines Eingriffs des Netzwerkmanagements erfolglos ist, sind die Verkehrsdaten auch nach Maßgabe dieser Vorschrift zu speichern.

(6) Wer Telekommunikationsdienste erbringt und hierbei die nach Maßgabe dieser Vorschrift zu speichernden Angaben verändert, ist zur Speicherung der ursprünglichen und der neuen Angabe sowie des Zeitpunktes der Umschreibung dieser Angaben nach Datum und Uhrzeit unter Angabe der zugrunde liegenden Zeitzone verpflichtet.

(7) Wer ein Mobilfunknetz für die Öffentlichkeit betreibt, ist verpflichtet, zu den nach Maßgabe dieser Vorschrift gespeicherten Bezeichnungen der Funkzellen auch Daten vorzuhalten, aus denen sich die geografischen Lagen der die jeweilige Funkzelle versorgenden Funkantennen sowie deren Hauptstrahlrichtungen ergeben.

(8) Der Inhalt der Kommunikation und Daten über aufgerufene Internetseiten dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

(9) Die Speicherung der Daten nach den Absätzen 1 bis 7 hat so zu erfolgen, dass Auskunftsersuchen der berechtigten Stellen unverzüglich beantwortet werden können.

(10) Der nach dieser Vorschrift Verpflichtete hat betreffend die Qualität und den Schutz der gespeicherten Verkehrsdaten die im Bereich der Telekommunikation erforderliche Sorgfalt zu beachten. Im Rahmen dessen hat er durch technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den gespeicherten Daten ausschließlich hierzu von ihm besonders ermächtigten Personen möglich ist.

(11) Der nach dieser Vorschrift Verpflichtete hat die allein auf Grund dieser Vorschrift gespeicherten Daten innerhalb eines Monats nach Ablauf der in Absatz 1 genannten Frist zu löschen oder die Löschung sicherzustellen.

Im Wesentlichen sollten durch die Vorschrift alle wesentlichen Verkehrsdaten zentraler Kommunikationsmittel erfasst werden. Nach dem Wegfall der Vorschrift bleiben kaum Speicherpflichten und lediglich einige Speichermöglichkeiten bestehen.

– Anbieter von *öffentlich zugänglichen Telefondiensten* hatten im Rahmen der Vorratsdatenspeicherung Informationen darüber zu speichern, welche Kommunikationsbeziehungen zwischen ihren Teilnehmern bestanden. Dies betrifft z.B. Beginn und Ende einer Verbindung sowie damit in Zusammenhang stehende Informationen, etwa IP-Adressen bei der Nutzung von VoIP-Verbindungen. Nach § 113a Abs. 5 TKG galt diese Speicherpflicht in bestimmten Fällen selbst dann, wenn eine Verbindung nicht zustande gekommen war.[68] Auch Kurznachrichten (SMS) sowie Multimedia- und ähnliche Nachrichten (MMS) waren im Hinblick auf die durch sie erzeugten Verkehrsdaten zu speichern. Bei der Nutzung von Mobiltelefonen war ferner die internationale Kennung des Anschlusses (IMSI) sowie des Endgerätes (IMEI) zu erfassen. Schließlich waren, wie oben bereits dargelegt, bestimmte standortbezogene Informationen zu speichern.

  Diese Informationen werden nach der aktuellen Rechtslage im Wesentlichen nicht mehr erfasst, es sei denn, sie werden zu Zwecken der Entgeltermittlung und -abrechnung benötigt. Aufgrund der zunehmenden Anzahl von Flatrate-Tarifen dürfte die Anzahl der darüber zu gewinnenden Daten kontinuierlich abnehmen. Da nicht zustande gekommene Anrufe sich im Hinblick auf das Entgelt nicht auswirken, dürften derartige Daten ganz entfallen.

---

68 Die Speicherpflicht gilt nach § 113a Abs. 5 TKG nur, wenn diese Verkehrsdaten für eigene Zwecke gespeichert oder protokolliert wurden. Der Gesetzgeber hatte dabei Fälle vor Augen, bei denen der Anbieter den Nutzer z.B. per SMS über einen vergeblichen Anrufversuch unterrichtet. In diesem Fall sollte diese Information nicht im Rahmen der regulären Löschungsfristen vernichtet werden, sondern zusammen mit anderen Vorratsdaten für diesen Zeitraum aufbewahrt werden.

– Anbieter von *Diensten der elektronischen Post*[69] hatten nicht nur die Kommunikationsbeziehungen zu speichern, d.h. Versendung und Eingang von E-Mail-Nachrichten, sondern auch jegliche Zugriffe auf E-Mail-Postfächer.

  Sofern – wie offenbar bei der Mehrzahl der gegenwärtig angebotenen E-Mail-Anbieter üblich – der Dienst kostenlos erbracht wird, ist weder die Erfassung von Telekommunikationsverkehrs- noch die Aufzeichnung von Telemediennutzungsdaten zulässig.[70] Nach dem Urteil werden diese Daten daher regelmäßig nicht zur Verfügung stehen.

– Anbieter von *Internetzugangsdiensten* hatten insbesondere die Zuordnung dynamisch zugewiesener IP-Adressen zu den Anschlüssen der Kunden zu erfassen. Wie oben dargelegt, ermöglicht erst die Speicherung dieser Zuordnung die spätere Identifizierung des unter der IP-Adresse agierenden Rechners und damit des spezifischen Nutzers.

  Da die reine Zuteilung einer IP-Adresse nichts darüber aussagt, ob die Leistung des Internetzugangsdienstes richtig erbracht wurde, ist diese Protokollierung zu Abrechnungszwecken regelmäßig unzulässig. Während dies bei Einzelabrechnungstarifen noch umstritten ist, besteht weitgehende Einigkeit bei Flatrate-Tarifen.[71] Nach den allgemeinen datenschutzrechtlichen Grundsätzen bei solchen Tarifen darf die Zuordnung dynamischer IP-Adressen daher nur für den eigentlichen Verbindungsvorgang erhoben werden. Unmittelbar nach der Beendigung der Verbindung müssen die Daten wieder gelöscht werden.[72] Eine Ausnahme ist lediglich für Fälle denkbar, in denen der Nutzer ausdrücklich einen Einzelverbindungsnachweis gefordert hat, § 99 Abs. 1 S. 1, 2. HS TKG.

  Abgesehen von der – in der Praxis vermutlich wenig Bedeutung aufweisenden – Ausnahme nach § 99 TKG besteht die Möglichkeit (nicht jedoch die Verpflichtung) eines Providers derartige Daten für einige Tage vorzuhalten, um Störungen und Missbräuche seiner Telekommunikationsanlagen und -dienste zu verfolgen und zu beseitigen, § 100 TKG. Eine aktuelle Entscheidung des OLG Frankfurt hat die von der wohl herrschenden Auffassung vertretene Frist von bis zu sieben Tagen inzwischen bestätigt.[73] Streitig ist die Reichweite des staatlichen Zugriffs auf die nach dieser Vorschrift gespeicherten Daten. § 100g StPO bezieht sich ausweislich des Klammerzusatzes ausdrücklich auf Verkehrsdaten nach

---

69 Zur Kritik an diesem Begriff siehe oben Anm. 53.

70 Sofern mit der Kennung des elektronischen Postfachs die darüber abgerufene E-Mail-Adresse bezeichnet oder der Zeitpunkt des Zugriffs erfasst wird, handelt es sich dabei um Telemediennutzungsdaten. Bei IP-Adressen sowie den damit im Zusammenhang stehenden Informationen handelt es sich um Telekommunikationverkehrsdaten. Vgl. hierzu näher *Brunst,* Anonymität im Internet, S. 397 f.

71 Vgl. *Ditscheid/Rudloff,* in: Spindler/Schütz (Hrsg.), Recht der elektronischen Medien, § 45i TKG, Rn. 37; *Wüstenberg,* RDV 2006, 102 ff.

72 Zu der diesbezüglichen Rechtsprechung und dem (in diesem Fall verunglückten) Verhältnis der Telemedien- und Telekommunikationsdatenschutznormen vgl. ausführlich *Brunst,* Anonymität im Internet, S. 347 ff.

73 Vgl. OLG Frankfurt, Urt. vom 16.06.2010, Az. 13 U 105/07. Gegenwärtig abrufbar über die Hessische Landesrechtsprechungsdatenbank, http://www.lareda.hessenrecht hessen.de [Juni 2011].

§ 96 Abs. 1 und § 113a TKG.[74] Die ehemals in § 96 Abs. 2 normierte Weiterverweisung auf die „durch andere gesetzliche Vorschriften begründeten Zwecke“ war nach der wohl h.M. gesperrt.[75] Unter Berufung auf diese Ansicht hätten Provider die Herausgabe vorhandener Daten an die Strafverfolgungsbehörden verweigern dürfen, wenn diese lediglich zu internen Zwecken der Störungs- und Missbrauchsbekämpfung erhoben wurden. Mit der Überführung der erwähnten Verweiskette in den § 96 Abs. 1 S. 2[76] dürfte dieser Streitpunkt obsolet geworden sein.

– Anbieter von *Anonymisierungs- und Proxydiensten* waren nach § 113a Abs. 6 TKG verpflichtet, die Rückverfolgung aller veränderten Daten zu protokollieren. Anonymisierungsdienste leiten – ebenso wie einige Arten von Proxyservern – Informationen Dritter „im eigenen Namen“, d.h. mit der eigenen IP-Adresse, weiter.[77] Beim Empfänger einer Kommu-Kommunikation ist daher lediglich die IP-Adresse dieses Anbieters sichtbar, nicht jedoch die des eigentlichen Absenders. Wird die Umschreibung nicht protokolliert, so ist die Verbindung nicht mehr bis zum eigentlichen Absender zurückverfolgbar, was bei Anonymisierungsdiensten sowie einigen Proxydiensten regelmäßig zum Geschäftsmodell gehört, bei anderen Anbietern jedoch eher unbeabsichtigte Nebenfolge sein kann. § 113a Abs. 6 TKG schreibt Anbietern, die „nach Maßgabe dieser Vorschrift zu speichernde Angaben verändern“ vor, sowohl die ursprünglichen als auch die neuen Angaben als auch den Zeitpunkt der Umschreibung zu protokollieren. Der wichtigste Anwendungsfall dürfte sich, wie im obigen Beispiel geschildert, auf die Umschreibung von IP-Adressen beziehen, die nach § 113a Abs. 4 Nr. 1 TKG bei der Vergabe zu protokollieren sind. Durch die Speicherpflicht soll verhindert werden, dass Verbindungen mit Hilfe von Anonymisierungs- und ähnlichen Diensten verschleiert werden können.[78]

---

74 Insoweit weist der in Anm. 73 zitierte Fall eine Besonderheit auf, denn im entschiedenen Fall hatte der Kunde die Möglichkeit, sich mit Hilfe seiner Zugangsdaten auch über andere Wege einzuwählen, z.B. über Hotspots oder GSM-Verbindungen. In diesem Fall wären besondere Nutzungsentgelte fällig geworden, so dass zumindest bis zu dem Zeitpunkt, an dem feststeht, ob die IP-Adresse zur Abrechnung dieser Leistungen benötigt wird, die Zuordnung auch nach § 96 TKG gespeichert werden durfte. Das Gesetz verlange, so das Gericht, lediglich eine unverzügliche und nicht etwa eine sofortige Löschung. Ob diesbezüglich ebenfalls die Sieben-Tage-Frist noch ausreichend gewesen wäre (was angesichts der für die Rechnungserstellung regelmäßig zur Verfügung stehenden Rechnerkapazitäten zu bezweifeln ist) musste nicht entschieden werden, da jedenfalls nach § 100 TKG eine Speicherung in diesem Zeitraum zulässig war.

75 Im Gegensatz zu der Ansicht von *Bär,* MMR 2008, 307, der den Zugriff auf Daten nach § 100 TKG im Rahmen des § 100g StPO stets für zulässig erachtete, stand dem nach der wohl h.M. der Wortlaut des § 100g StPO entgegen, welcher explizit nur auf die Verkehrsdaten nach §§ 96 Abs. 1, 113a TKG verweist. Ungeachtet der gesetzgeberischen Absicht (vgl. die Erläuterungen in BT-Drucks. 16/5846, S. 51) wurde ein unbegrenzter Zugriff auf sämtliche anbieterseits verfügbaren Daten mit Hinweis auf die unterschiedlichen Zweckbestimmungen des TKG für unzulässig erachtet. Vgl. *Hegmann,* in: Graf (Hrsg.), Beck'scher Online-Kommentar, § 100g StPO Rn. 1 sowie *Nack,* KK-StPO, § 100g StPO Rn. 1.

76 Art. 2 des Gesetzes zur Bekämpfung der Kinderpornographie in Kommunikationsnetzen vom 17.2.2010, BGBl. I, S. 78.

77 Vgl. zu den technischen Grundlagen und rechtlichen Bewertungen ausführlich *Brunst,* Anonymität im Internet.

78 Zu den Erfolgsaussichten dieses Vorhabens vgl. wiederum *Brunst,* Anonymität im Internet.

> Nach dem Wegfall der Vorschrift verbleibt es bei der alten Rechtslage. Dies bedeutet, dass Anonymisierungsdienste keine Zuordnungen speichern müssen. Sie wären allenfalls dazu berechtigt, falls sie diese Informationen zu Zwecken der Entgeltermittlung und -abrechnung benötigen würden. Da die Wahrung der Anonymität aber gerade zum Geschäftsmodell der Anbieter gehört, ist davon auszugehen, dass derartige Daten nicht erhoben werden.[79]

Zusammenfassend lässt sich daher festhalten, dass ein Großteil der durch die Vorratsdatenspeicherung verpflichtend angeordneten Datenspeicherungen nach dem Urteil nicht mehr zur Verfügung steht. Ausnahmen dürften sich vor allem in den Fällen ergeben, in denen Daten zu Abrechnungszwecken vom Anbieter benötigt werden und – mangels Pauschaltarif oder aufgrund Einzelverbindungsnachweiswunsch des Nutzers – auch nach einigen Tagen dort noch existieren.

2.3.2. Zugriff

Der Zugriff auf Verkehrsdaten für Zwecke der Strafverfolgung ist in Deutschland in § 100g StPO geregelt. Bislang gewährte die Vorschrift den Zugriff auf bestimmte Verkehrsdaten. Aufgrund des Wegfalls der Speicherpflicht von Vorratsdaten verbleibt es gegenwärtig bei den Zugriffsmöglichkeiten auf die oben näher dargelegten Datenbestände. Hinsichtlich der Verwertung der erhobenen Daten soll eine enge Ausnahme für Alt-Fälle bestehen, in denen Daten während des Zeitraums der einstweiligen Anordnung gesichert und bereits übermittelt wurden.[80] Zunächst hatte das OLG Hamm in drei Fällen, dass sich in diesen Fällen die legitimierende Wirkung der einstweiligen Anordnungen hinsichtlich der Beweisgewinnung bei der Beurteilung der Datenverwertung fortsetzt.[81] Diese Linie hat inzwischen auch der BGH eingeschlagen.[82]

Abseits des Zugriffs auf Verkehrsdaten über § 100g StPO verbleiben vor allem zwei Problembereiche, die nicht unmittelbar mit den Auswirkungen des Urteils zu tun haben, zum Teil darin jedoch erwähnt werden. Zum einen geht es um den Zugriff auf Telemediennutzungsdaten, zum anderen um den Zugriff auf Verkehrsdaten im weiteren Sinne mit Hilfe der meist als „Quick Freeze“ bezeichneten Technik.

---

79 Der Anbieter JonDonym bietet beispielsweise verschiedene Vorkasse-Verfahren zur Bezahlung seiner Dienste an, z.B. Paysafecard, Barzahlungen per Brief, Überweisungen oder Paypal. Insbesondere die ersten beiden Varianten generieren keine Daten, die zur Identifikation des Nutzers herangezogen werden könnten.

80 Zu dem vom Bundesverfassungsgericht während dieser Zeit vorgegebenen Verfahren vgl. näher *Gercke/Brunst,* Praxishandbuch Internetstrafrecht, Rn. 742 ff.

81 Vgl. die Entscheidungen des OLG Hamm, Beschlüsse vom 13.04.2010, Az. 3 Ws 140/10, 3 Ws 156/10 und 3 WS 166/10. Die Entscheidungen sind online über Rechtsprechungsdatenbank der Gerichte in Nordrhein-Westfalen abrufbar, http://www.justiz.nrw.de/ [Juni 2011].

82 BGH vom 4.11.2010 (4 StR 404/10), NJW 2011, S. 476, und vom 18.1.2011 (1 StR 663/10), NJW 2011, S. 1377.

2.3.2.1. Telemediennutzungsdaten

Während im internationalen Bereich meist ausschließlich von „traffic data“ gesprochen wird und damit alle im Zusammenhang mit Telekommunikation im weitesten Sinne anfallenden Begleitumstände gemeint sind, differenziert das deutsche Recht zwischen Verkehrsdaten auf der einen und Nutzungsdaten auf der anderen Seite. Verkehrsdaten sind nach § 3 Nr. 30 TKG Daten, die bei der Erbringung eines „Telekommunikationsdienstes“ anfallen. Telekommunikationsdienste sind nach § 3 Nr. 24 TKG die in der Regel gegen Entgelt erbrachten Dienste, die „ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen.“ Nutzungsdaten fallen hingegen bei der „Inanspruchnahme von Telemedien“ an, § 15 TMG. Der Begriff der Telemediendienste wird nicht näher definiert, lediglich § 1 Abs. 1 TMG erstreckt den Anwendungsbereich des Gesetzes auf Telemedien, d.h. „alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste […], die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste […] oder Rundfunk […] sind.“ Aufgrund der Überschneidungen zwischen TKG und TMG besteht gerade für viele Internetdienste Rechtsunsicherheit, ob sie als Telekommunikations-, als Telemediendienst oder sogar als beides gleichzeitig einzustufen sind.[83] Ohne auf diese Fragen an dieser Stelle im Einzelnen näher einzugehen, lässt sich verallgemeinernd sagen, dass Telekommunikationsdienste im Grundsatz eher den Transport von Informationen betreffen, während Telemediendienste eher die inhaltlichen Komponenten berühren.[84]

Ein Problem besteht in der Frage, ob – und wenn ja, wie – Ermittlungsbehörden auf Telemediennutzungsdaten zugreifen können. Während in § 113a TKG zumindest einige Telemediennutzungsdaten aufgeführt waren (z.B. E-Mail-Adressen oder der Zeitpunkt des Zugriffs auf ein E-Mail-Postfach), gibt es für andere Telemediennutzungsdaten, z.B. Abrufe von Webseiten oder Zeitpunkte von Anmeldungen in sozialen Netzwerken, keine korrespondierende Norm. § 15 Abs. 4 S. 3 TMG stellt lediglich die datenschutzrechtliche Erlaubnisnorm dar, gewährt selbst jedoch keinen Zugriff auf die Daten.[85] Schwierigkeiten gibt es mit der Kehrseite zu dieser Erlaubnisnorm, nämlich der strafprozessualen Zugriffsnorm. Nach einer bislang vertretenen Auffassung gibt es gegenwärtig keine Möglichkeit, diese Daten anzufordern, da § 100g StPO ausdrücklich Verkehrsdaten (nicht aber Nutzungsdaten) in Bezug nimmt und hierfür im Klammerzusatz ausschließlich auf die §§ 96, 113a TKG verweist.[86] Bei anderen Vorschriften, insb. den §§ 94 ff. StPO, wurde zum Teil angezweifelt, ob durch sie Eingriffe in das Fernmeldegeheimnis bewirkt werden können.[87] Aufgrund einer neueren Entscheidung des Bundesverfassungsgerichts stellt sich jedoch die Frage, ob diese Auffassung auch zukünf-

---

83 Vgl. hierzu näher *Brunst,* Anonymität im Internet, S. 379 ff. m.w.N.

84 Zum technisch (weitgehend) korrespondierenden ISO/OSI-Schichtenmodell vgl. *Brunst,* Anonymität im Internet, S. 48 ff.

85 Vgl. *Gercke/Brunst,* Praxishandbuch Internetstrafrecht, Rn. 771.

86 Vgl. *Gercke/Brunst,* Praxishandbuch Internetstrafrecht, Rn. 712 ff. m.w.N.

87 Vgl. zu diesem Problemkomplex *Gercke/Brunst,* Praxishandbuch Internetstrafrecht, S. 712 f. m.w.N.

tig Bestand haben kann.[88] In der Rechtsprechung anderer Gerichte ist diese Frage jedoch – soweit ersichtlich – bislang noch nicht unter diesem Gesichtspunkt diskutiert worden.

2.3.2.2. Quick Freeze

Der zweite Problemkomplex im Zusammenhang mit Verkehrsdaten betrifft das meist als „Quick Freeze" bezeichnete Instrument, das ebenfalls einen Zugriff auf relevante Daten ermöglichen soll und häufig als Alternative zur Vorratsdatenspeicherung propagiert wird.[89]

2.3.2.2.1. Funktionsweise

Für den Bereich der Bekämpfung der Computerkriminalität ist das Quick-Freeze-Verfahren insbesondere vom Europarat propagiert worden. Es hat Einzug gefunden in Art. 16 des Übereinkommens über Computerkriminalität (sog. Cybercrime Konvention).[90] Die Vorschrift lautet auszugsweise:

Artikel 16 – Umgehende Sicherung gespeicherter Computerdaten

(1) Jede Vertragspartei trifft die erforderlichen gesetzgeberischen und anderen Maßnahmen, damit ihre zuständigen Behörden die umgehende Sicherung bestimmter Computerdaten einschließlich Verkehrsdaten, die mittels eines Computersystems gespeichert wurden, anordnen oder in ähnlicher Weise bewirken können, insbesondere wenn Gründe zu der Annahme bestehen, dass bei diesen Computerdaten eine besondere Gefahr des Verlusts oder der Veränderung besteht.

(2) Führt eine Vertragspartei Absatz 1 so durch, dass eine Person im Wege einer Anordnung aufgefordert wird, bestimmte gespeicherte Computerdaten, die sich in ihrem Besitz oder unter ihrer Kontrolle befinden, sicherzustellen, so trifft diese Vertragspartei die erforderlichen gesetzgeberischen und anderen Maßnahmen, um diese Person zu verpflichten, die Unversehrtheit dieser Computerdaten so lange wie notwendig, längstens aber neunzig Tage, zu sichern und zu erhalten, um den zuständigen Behörden zu ermöglichen, deren Weitergabe zu erwirken. Eine Vertragspartei kann vorsehen, dass diese Anordnung anschließend verlängert werden kann.

---

88 In der Entscheidung zum Zugriff auf die beim Provider gespeicherten E-Mails, BVerfG CR 2009, 591 ff. führt das Gericht aus, dass die „Aneinanderreihung unterschiedlicher Maßnahmen [im achten Abschnitt der StPO] nicht den Schluss nahe[legen], der Gesetzgeber habe Eingriffe in Art. 10 GG nur aufgrund von § 99, § 100a und § 100g StPO zulassen wollen", wie dies bis dahin die wohl ganz h.M. annahm. Auch ein Zugriff über § 94 StPO ermögliche daher Eingriffe in das Grundrecht aus Art. 10 GG. In der Konsequenz würde dies bedeuten, dass – unter den im Urteil genannten Voraussetzungen – ein Zugriff auch auf Telemediennutzungsdaten im Wege der Beschlagnahme oder – als milderes Mittel – durch die Anfertigung einer Kopie möglich wäre.

89 Vgl. http://de.wikipedia.org/wiki/Quick_Freeze [Juni 2011].

90 Übereinkommen des Europarates über Computerkriminalität, CETS 185, unterzeichnet am 23.11.2001 in Budapest. Die bereinigte deutsche Übersetzung zwischen Deutschland, Österreich und der Schweiz ist online abrufbar unter http://conventions.coe.int/Treaty/GER/Treaties/Html/185 htm [Juni 2011].

Sinn und Zweck des Quick-Freeze-Verfahrens ist es, vorhandene Verkehrsdaten[91] vor ihrer regulären Löschung zu bewahren, so dass ein Zugriff darauf auch zu einem späteren Zeitpunkt noch möglich ist. Im gegenwärtigen Zustand ohne Vorratsdatenspeicherung könnte ein Quick-Freeze-Verfahren Bedeutung erlangen, da bestimmte Daten zwar bei den Anbietern anfallen, z.B. im Rahmen eines Verbindungsaufbaus, unmittelbar im Anschluss aber wieder gelöscht werden, da sie für Zwecke der Entgeltermittlung und -abrechnung nicht mehr gebraucht werden. Das Quick-Freeze-Verfahren sieht in diesem Fall ein mehrstufiges Verfahren vor.

– Als ersten Schritt kann jede „zuständige Behörde“[92] bei einem Anbieter die umgehende Sicherung bestimmter dort gespeicherter Computerdaten anordnen. In welcher Form die Anordnung erfolgen muss, ist in der Konvention nicht vorgegeben. Im einfachsten Falle kann ein telefonischer Anruf ausreichen.[93] An dieser Stelle zeigen sich bereits die größten Unterschiede zur Vorratsdatenspeicherung:

  – Während die Vorratsdatenspeicherung unterschiedslos Daten aller Bürger betrifft, richtet sich das Quick-Freeze-Verfahren ausschließlich auf Daten eines bestimmten Verdachtsfalles, z.B. einer konkreten IP-Adresse oder eines bestimmten Anschlusses.

  – Die Vorratsdatenspeicherung ist ausschließlich retrograd angelegt, betrifft also das Vorrätighalten bestimmter Daten. Das Quick-Freeze-Verfahren hingegen betrifft aktuelle Daten, bei denen sichergestellt werden soll, dass sie zu einem späteren Zeitpunkt noch unbeschadet verfügbar sind.

  – Die Vorratsdatenspeicherung ist auf einen bestimmten Katalog von Daten beschränkt. Das Quick-Freeze-Verfahren hingegen kann sich – zumindest grundsätzlich – auf beliebige Verkehrs- und Nutzungsdaten oder sogar auf Bestands- und Inhaltsdaten[94] richten. Es ist damit wesentlich flexibler einsetzbar als die Vorratsdatenspeicherung.

---

91 Da die Unterscheidung von Verkehrs- und Nutzungsdaten eine deutsche Besonderheit ist, bezieht sich das Quick Freeze Verfahren grundsätzlich auf beide Datenarten. Dies kommt auch im Konventionstext „bestimmter Computerdaten *einschließlich* Verkehrsdaten“ (Hervorhebung durch d. Verf.) zum Ausdruck.

92 Da es sich bei der Cybercrime Konvention um ein internationales Instrument handelt, werden zuständige Behörden erst auf nationaler Ebene festgelegt.

93 Da durch die Anordnung alleine noch keine Daten herausgegeben werden, besteht keine Notwendigkeit, bereits zu diesem Zeitpunkt größere Anforderungen an die Form der Anordnung zu stellen. Denkbar ist daher, dass eine Anordnung telefonisch erteilt wird und, z.B. zu Beweissicherungszwecken, eine schriftliche Bestätigung einige Stunden oder wenige Tage später auf dem Post- oder Faxweg übermittelt wird.

94 Convention on Cybercrime, Explanatory Report, Abs. 159 spricht allgemein von “data, which already exists in a stored form.” Diese Daten sollen durch die Quick Freeze Anordnung davor bewahrt werden, dass sie modifiziert, verschlechtert oder gelöscht werden, so dass Ermittlungsbehörden zu einem späteren Zeitpunkt noch darauf zugreifen können. Vgl. auch Abs. 161, der sogar auf Geschäfts-, Gesundheits und sonstige personenbezogene Daten verweist.

– Das Quick-Freeze-Verfahren ist, über Art. 29 der Konvention, (mit geringen Abweichungen)[95] auch in internationalen Fällen einsetzbar. Auf diese Weise sollen die üblicherweise langwierigen formalen Verfahren im Rahmen eines Rechtshilfeverfahrens abgesichert werden, so dass trotz möglicherweise längerer Wartezeit die benötigten Daten weiterhin verfügbar bleiben.

Die wichtigste Einschränkung des Quick-Freeze-Verfahrens an dieser Stelle betrifft das Vorhandensein der Daten. Das bedeutet, dass nur diejenigen Daten, die bei einem Anbieter auch tatsächlich anfallen und üblicherweise gespeichert werden – und im Zeitpunkt des Eingangs der Anordnung beim Provider noch vorhanden sind –, eingefroren werden können. Ein Anbieter ist nicht verpflichtet, Daten speziell für das Quick-Freeze-Verfahren zu erfassen.[96] Auch Daten, die üblicherweise nur wenige Minuten (z.B. zum Aufbau einer Verbindung) bei einem Anbieter gespeichert und sonst anschließend wieder gelöscht werden, können mit Hilfe des Quick-Freeze-Verfahrens – zumindest theoretisch[97] – eingefroren werden.[98]

– Im zweiten Schritt wird der Anbieter die in der Anordnung genannten Daten „einfrieren". Dies bedeutet, dass sie aus dem regulären Löschrhythmus herausgenommen werden. Die anordnende Behörde hat anschließend Zeit, alle notwendigen Dokumente zu sammeln und Beschlüsse einzuholen, ohne befürchten zu müssen, dass im Anschluss daran Daten nicht mehr vorhanden sind.

  Die Konvention sieht einen maximalen Speicherzeitraum von 90 Tagen im Anschluss an die Anordnung vor, der jedoch verlängert werden kann, wenn diese Möglichkeit in einem Land vorgesehen ist.

– Im dritten Schritt wendet sich die anordnende Behörde an die im jeweiligen Land zuständige Stelle, z.B. einen Richter. Dieser kann die eigentliche Herausgabe der Daten vom An-

---

95 Beim Verfahren nach Art. 29 kann sich die ersuchende Behörde, insb. aus Gründen der nationalen Souveränität, nicht unmittelbar an das speichernde Unternehmen wenden, sondern muss Kontakt mit der anderen Vertragspartei aufnehmen. Diese bewirkt dann nach innerstaatlichem Recht die umgehende Sicherung der Daten, die dann bis zur erfolgreichen Durchführung des Rechtshilfeabkommens zur Verfügung stehen.

96 Vgl. Convention on Cybercrime, Explanatory Report, Abs. 150: "The measures described in the articles [16 & 17] operate *only where computer data already exists and is currently being stored*." (Hervorhebungen durch d. Verf.).

97 Eine entscheidende Einschränkung in diesem Zusammenhang betrifft das Eintreffen der Anordnung beim Provider. Erst ab diesem Zeitpunkt müssen – bereits (und noch) existierende – Daten eingefroren werden. In Fällen, in denen Daten nur wenige Minuten verfügbar sind, kommt eine „preservation order" nur in Betracht, wenn die genauen Rahmenbedingungen bereits vorher feststehen. Grundsätzlich wäre in diesem Fall auch an eine zukunftsbezogene Verkehrsdatenerhebung nach § 100g StPO zu denken. Diese ist jedoch auf die in §§ 96, 113a TKG genannten Daten beschränkt, während sich eine „preservation order" – zumindest grundsätzlich – auch auf davon abweichende Daten beziehen kann.

98 Convention on Cybercrime, Explanatory Report, Abs. 153 weist in diesem Zusammenhang allerdings darauf hin, dass die Vorschrift nicht so verstanden werden könne, dass ein Anbieter verpflichtet sei, neue technische Verfahren zu implementieren, um etwa auf eine Anfrage so schnell reagieren zu können, dass auch flüchtige Daten sofort eingefroren werden können.

bieter an die Behörde bewirken. Erst in diesem Zeitpunkt erhält die staatliche Behörde daher Kenntnis vom Inhalt der eingefrorenen Daten.

Zwar wird das Quick-Freeze-Verfahren häufig als Alternative zur Vorratsdatenspeicherung oder sogar als davon abgedeckt angesehen. Tatsächlich handelt es sich jedoch um eine eigenständige Maßnahme mit selbständigem Anwendungsbereich. Zweck der Vorratsdatenspeicherung ist es, dass bestimmte *retrograde* Daten zur Verfügung stehen, wenn eine Straftat verfolgt werden soll. Zweck des Quick-Freeze-Verfahrens ist es hingegen *zukunftsgerichtet* dafür zu sorgen, dass bestimmte Daten, die zwar gegenwärtig (noch) zur Verfügung stehen, von denen aber zu befürchten ist, dass sie in naher Zukunft verändert oder gelöscht werden, auch in einiger Zeit noch in der gegenwärtigen Form zur Verfügung stehen. Wie oben dargestellt wurde, können sich beide Instrumente auch im Hinblick auf die von ihnen betroffenen Datenarten unterscheiden.

2.3.2.2.2. Umsetzung in Deutschland

In Deutschland enthält § 16b WpHG eine Vorschrift, welche das Quick-Freeze-Verfahren mit Blick auf Insidergeschäfte und Marktmanipulationen umsetzt. Die Vorschrift lautet:

§ 16b WpHG – Aufbewahrung von Verbindungsdaten

(1) Die Bundesanstalt kann von einem Wertpapierdienstleistungsunternehmen sowie von einem Unternehmen mit Sitz im Inland, die an einer inländischen Börse zur Teilnahme am Handel zugelassen sind, und von einem Emittenten von Insiderpapieren sowie mit diesem verbundenen Unternehmen, die ihren Sitz im Inland haben oder deren Wertpapiere an einer inländischen Börse zum Handel zugelassen oder in den regulierten Markt oder Freiverkehr einbezogen sind, für einen bestimmten Personenkreis schriftlich die Aufbewahrung von bereits existierenden Verbindungsdaten über den Fernmeldeverkehr verlangen, sofern bezüglich dieser Personen des konkreten Unternehmens Anhaltspunkte für einen Verstoß gegen § 14 oder § 20a bestehen. Das Grundrecht des Artikels 10 des Grundgesetzes wird insoweit eingeschränkt. Die Betroffenen sind entsprechend § 101 Abs. 4 und 5 der Strafprozessordnung zu benachrichtigen. Die Bundesanstalt kann auf der Grundlage von Satz 1 nicht die Aufbewahrung von erst zukünftig zu erhebenden Verbindungsdaten verlangen.

(2) Die Frist zur Aufbewahrung der bereits existierenden Daten beträgt vom Tage des Zugangs der Aufforderung an höchstens sechs Monate. Ist die Aufbewahrung der Verbindungsdaten über den Fernmeldeverkehr zur Prüfung des Verdachts eines Verstoßes gegen ein Verbot nach § 14 oder § 20a nicht mehr erforderlich, hat die Bundesanstalt den Aufbewahrungspflichtigen hiervon unverzüglich in Kenntnis zu setzen und die dazu vorhandenen Unterlagen unverzüglich zu vernichten. Die Pflicht zur unverzüglichen Vernichtung der vorhandenen Daten gilt auch für den Aufbewahrungspflichtigen.

Für den strafprozessualen Zugriff auf Verkehrsdaten enthält lediglich §§ 100g Abs. 1, 2 i.V.m. 100b Abs. 1 S. 2 StPO einen Ansatz, wonach die Staatsanwaltschaft bei Gefahr im

Verzug eine eigene Anordnung zur Erhebung von Verkehrsdaten treffen kann, die dann aber innerhalb von drei Werktagen von einem Gericht bestätigt werden muss. Diese Vorschrift ist aber in mehrfacher Hinsicht nicht mit dem oben skizzierten Quick-Freeze-Verfahren vergleichbar. So ist sie auf Fälle von Gefahr im Verzug beschränkt, während das Quick-Freeze-Verfahren auch in sonstigen Fällen Anwendung finden soll. Vor allem aber ist das Verfahren nach § 100g StPO gegenwärtig (in Folge des Urteils des Bundesverfassungsgerichts) auf bestimmte Verkehrsdaten (häufig auf Abrechnungsdaten) beschränkt, was das Verfahren in Zeiten zunehmender Flatrate-Tarife in vielen Fällen wertlos erscheinen lassen dürfte. Nach der allgemeinen Konzeption des Quick-Freeze-Verfahrens ist letzteres flexibler und allgemeiner einsetzbar.

Bei der Neuregelung der verdeckten Ermittlungsmaßnahmen in der StPO war der Gesetzgeber der Auffassung, dass die Einführung eines Quick-Freeze-Verfahrens „vor allem aufgrund der zugleich umzusetzenden Richtlinie zur ‚Vorratsdatenspeicherung„ entbehrlich geworden“ sei, denn die relevanten Daten wären aufgrund der Vorratsdatenspeicherung ohnehin bereits vorhanden.[99] Dieses Argument ist, wie oben bereits erwähnt, kritisch zu sehen, denn selbst bei (Wiederinkrafttreten der) Vorratsdatenspeicherung steht lediglich ein (wenn auch weiträumiger) Katalog von Daten zur Verfügung, nicht aber das in im Quick Freeze Verfahren vorgesehene flexible Modell, mit dem unter Umständen sogar Inhaltsdaten eingefroren werden könnten.[100]

2.4. Zugriff auf Inhaltsdaten

2.4.1. Speicherung

Der Umgang mit Inhaltsdaten ist restriktiv geregelt. Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet. Auch nach Ende der die Geheimhaltungspflicht begründenden Tätigkeit wirkt es weiter fort. Es erstreckt sich nicht nur auf den Inhalt der Telekommunikation, sondern auch auf die näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Die näheren Umstände der Kommunikation werden durch die Vorratsdatenspeicherung in weiten Teilen protokolliert und bei einem staatlichen Zugriff darauf sichtbar gemacht. Für den Inhalt gilt jedoch nach wie vor der Schutz aus Art. 10 GG sowie § 88 TKG. Dies wurde auch in (der gegenwärtig für nichtig erklärten Vorschrift des) § 113a Abs. 8 TKG noch einmal ausdrücklich klargestellt.

Nach § 88 Abs. 3 TKG ist es den Verpflichteten untersagt, „sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste […] hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen.“ Dieses Verbot gilt auch nach dem Urteil weiter. Das Verbot einer Speicherungspflicht für Inhaltsdaten ist nicht betroffen.

---

99 Vgl. BT-Drs. 16/5846, S. 53.

100 Siehe hierzu auch *Brunst/Sieber,* German Cybercrime Legislation, in: Basedow, et al. (Hrsg.), German National Reports to the 18th International Congress of Comparative Law, S. 765

2.4.2. Zugriff

Möchten Ermittlungsbehörden Zugriff auf nicht öffentliche Inhaltsdaten nehmen, so bedürfen Sie nach der bisherigen ganz einhelligen Meinung regelmäßig eines Beschlusses nach §§ 100a, 100b StPO, wenn es sich um Telekommunikationsinhalte handelt;[101] für sonstige Inhalte ist regelmäßig eine Sicherstellung oder Beschlagnahme gem. §§ 94 ff. StPO ausreichend. Für den Bereich der neuen Medien war über lange Zeit streitig, wie auf E-Mails (also Telekommunikationsinhalte) zugegriffen werden darf, die sich auf den Rechnern eines Anbieters befinden.[102] Das Bundesverfassungsgericht hat sich keiner der bis dahin bestehenden Auffassungen angeschlossen, sondern eine eigene Möglichkeit aus der Verfassung abgeleitet.[103] Danach sind derartige Mails zwar vom Fernmeldegeheimnis geschützt, unabhängig von der Frage, ob sie bereits abgerufen worden sind oder gerade erst eingeliefert wurden. Ein Zugriff soll aber durch beliebige Vorschriften des achten Abschnitts der StPO möglich sein, insbesondere durch die §§ 94 ff. StPO, sofern bestimmte Voraussetzungen eingehalten werden.[104] Das Urteil zur Vorratsdatenspeicherung hatte hingegen keine unmittelbaren Auswirkungen für die Speicherung von oder den Zugriff auf Inhaltsdaten.

---

101 Näher hierzu *Gercke/Brunst,* Praxishandbuch Internetstrafrecht, Rn. 789 ff.

102 Zu den bisherigen Ansichten vgl. die Ausführungen bei *Gercke/Brunst,* Praxishandbuch Internetstrafrecht, Rn. 810 ff.

103 Vgl. BVerfG CR 2009, 591 ff. m. krit. Anm. *Brunst.*

104 Näher *Gercke/Brunst,* Praxishandbuch Internetstrafrecht, Rn. 818 ff.

Teil C: Quantitative Entwicklung der Verkehrsdatenabfrage

1. Amtliche Statistik

Statistisch erfasst werden Daten zu der Praxis der Verkehrsdatenabfrage in Deutschland nur in begrenztem Umfang. Sie beschränken sich auf die Abfragen im Kontext der Strafverfolgung; Informationen über den präventiven Einsatz der Maßnahme sind nicht verfügbar. Die Erhebung der veröffentlichten Zahlen zum repressiven Einsatz erfolgt auf der Grundlage des § 100g Abs. 4 StPO nach den dort genannten Parametern. Dies umfasst namentlich die Anzahl der Verfahren, in denen im jeweiligen Kalenderjahr Maßnahmen gem. § 100g durchgeführt worden sind, die Anzahl der Anordnungen, unterteilt nach Erst- und Verlängerungsanordnungen, die zugrunde liegende Anlassstraftat, unterschieden nach solchen gem. Abs. 1 Nr. 1 bzw. Nr. 2, das ‚Alter' der angeforderten Daten nach Monaten sowie die Zahl der ergebnislosen Anfragen infolge von Nichtverfügbarkeit der Daten. Nicht näher aufgeschlüsselt sind die Zahlen nach den konkret betroffenen Sektoren (Festnetz, Mobilfunk, Internet).[105]

Aktuell verfügbar sind die entsprechenden Daten erstmalig für die Jahre 2008 und 2009.[106] Die nachfolgenden Berechnungen wurden auf der Grundlage der Statistiken für 2008 erstellt.[107] Danach wurden in 8.316 Verfahren eine oder mehrere Verkehrsdatenabfragen durchgeführt. Bezogen auf die Gesamtzahl der in 2008 erledigten Ermittlungsverfahren (4.605.291 Js- und 3.539.237 UJs-Sachen[108]) betrifft dies mithin nur einen Bruchteil aller Verfahren[109]. Bezogen auf die einschlägigen Verfahren wurden pro Verfahren im Durchschnitt 1,7 Anordnungen getroffen. Absolut wurden dabei 13.904 Anordnungen registriert, davon 13.426 Erst- und 478 Verlängerungsanordnungen (Schaubild 1).

Im direkten Vergleich mit den Inhaltsüberwachungen gem. § 100a StPO (siehe ebenfalls Schaubild 1) ergibt sich, dass die Verkehrsdatenüberwachung als – jedenfalls in ihrer systematischen Anwendung – noch recht junge Ermittlungsmaßnahme das klassische Abhören der

---

105 Eine vergleichbare Veröffentlichungspflicht besteht gem. § 100b Abs. 5 u. 6 StPO für die TKÜ-Maßnahmen. In beiden Bereichen (TKÜ und VDÜ) weichen die vom Bundesamt für Justiz ausgewiesenen Zahlen im Vergleich zu den vormals von der Bundesnetzagentur bzw. der früheren Regulierungsbehörde veröffentlichten deutlich nach unten ab; dies wird u.a. mit der Bereinigung von Mehrfachzählungen begründet. Auch die im Rahmen der MPI-Studie 2008 durchgeführte Schätzung zu der Häufigkeit der Verkehrsdatenabfrage hatte höher gelegen. Vgl. *Albrecht/Kilchling/Grafe* 2008, S. 65 u. 69. Für den vorliegenden Bericht werden ausschließlich die vom Bundesamt vorgelegten Zahlen zugrunde gelegt.

106 Die detaillierten Angaben, aufgeschlüsselt nach den Anwendungen in den Bundesländern und beim Generalbundesanwalt, sind auf der Website des Bundesamtes für Justiz veröffentlicht; siehe auch Tabellen 1a und b in Anhang A.

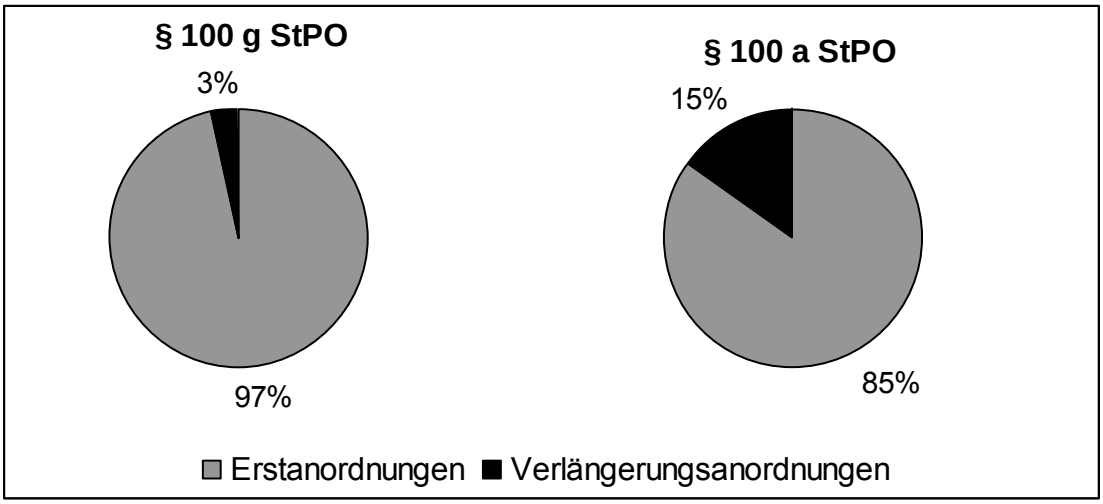
107 Für 2009 ergibt sich eine Zunahme der Anordnungen von 13.904 auf 16.626.

108 Stat. Bundesamt, Staatsanwaltschaften 2008, Tab. 1.1.

109 Etwa 0,1 Prozent.

Telekommunikation verfahrensbezogen in der Bedeutung inzwischen deutlich überholt hat; letztere kam lediglich in 5.348 Verfahren[110] zum Einsatz. Das ist in Anbetracht des breiteren deliktischen Anwendungsbereiches und der geringeren Eingriffsschwere der Maßnahme auch plausibel. Etwas höher ist im Rahmen der Telekommunikationsüberwachung derzeit allerdings (noch) die Zahl der einzelnen Anordnungen, was aber fast ausschließlich auf den deutlich höheren Anteil von Wiederholungsanordnungen zurückzuführen ist; dieser macht hier einen Anteil von etwas mehr als 15 % aus gegenüber weniger als einem Prozent bei den Verkehrsdatenabfragen. Nach den Erkenntnissen aus der Evaluationsstudie des MPI zur Telekommunikationsüberwachung sind hier selbst zwei-, drei- und viermalige Verlängerungen mehr als nur Einzelfälle.[111] Auch dieser Unterschied ist plausibel, ist doch die Verkehrsdatenabfrage in den meisten Fällen auf retrograde Daten ausgerichtet[112], während die Verlängerung bei der TKÜ regelmäßig zukunftsgerichtet angelegt ist.

*Schaubild C-1: Anordnungen zur Verkehrsdatenabfrage sowie zur Inhaltsüberwachung in 2008**



*) Quelle: Bundesamt für Justiz. Prozentuierungen nach eigener Berechnung.

Ausgewiesen ist in der Jahresstatistik ferner das Alter der jeweils abgefragten Daten in Monaten (Schaubild C-2). Zunächst fällt auf, dass nur ein sehr geringer Teil der Abfragen ausschließlich auf zukünftig anfallende Daten ausgerichtet ist. 2008 machten diese Daten nur knapp 5 % aller Anfragen aus. Nicht erfasst sind insoweit freilich diejenigen Abfragen, die sowohl retrograde als auch zukunftsgerichtete Daten erfassen. Nach den im Rahmen der MPI-Studie 2008 analysierten Verfahren lag diese Konstellation etwa 12 % aller Beschlüsse

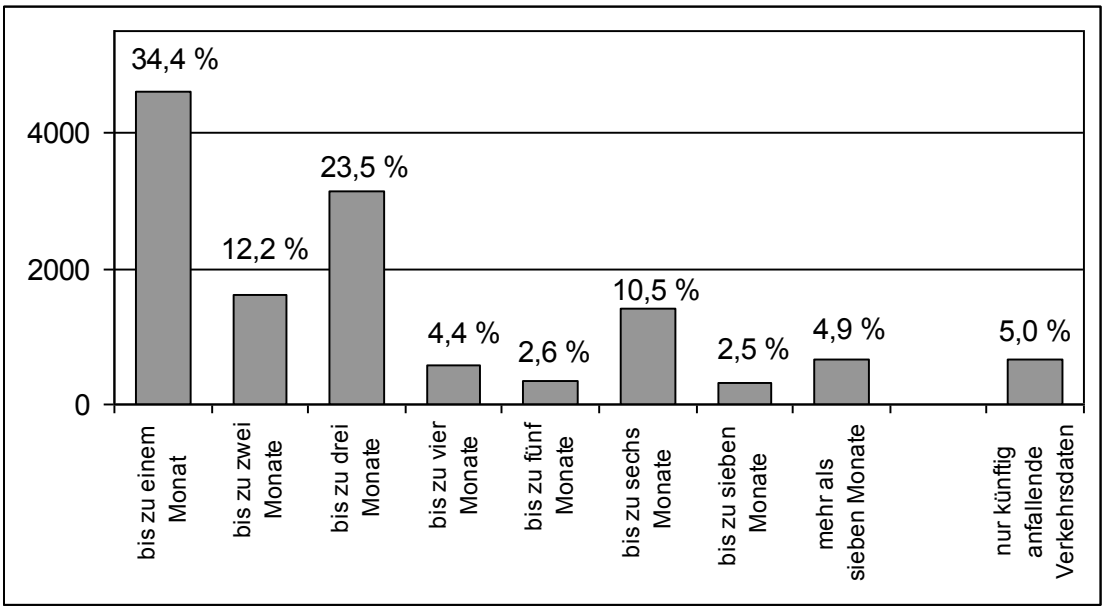
110 Die Übersichten zu den Maßnahmen gem. § 100a StPO sind ebenfalls auf der Website des Bundesamtes für Justiz publiziert.

111 *Albrecht/Dorsch/Krüpe* 2003, S. 174ff.

112 Dazu auch gleich unten Schaubild C-2.

zugrunde.[113] Der Schwerpunkt der anderen Anfragen bezieht sich mit einem Anteil von zusammen ca. 70 % in der Hauptsache auf Daten aus den letzten drei Monaten, wobei ein Monat mit mehr als einem Drittel nach wie vor der am häufigsten abgefragte Zeitraum ist. An zweiter Stelle folgt mit knapp unter einem Viertel der Dreimonatszeitraum. Ähnliche Schwerpunkte haben sich auch in der MPI-Studie 2008 herauskristallisiert, wenn auch in noch deutlicherem Ausmaß. Insoweit wird im Hinblick auf die Abfragepraxis unter den Bedingungen der – im Vergleich zu damals längeren – Vorratsdatenspeicherung eine leichte Verschiebung hin zu älteren Daten erkennbar, die vor Inkrafttreten des Telekommunikationsüberwachungsneuregelungsgesetzes 2007[114] bei den TK-Unternehmen nicht erreichbar gewesen wären. So betrafen 2008 immerhin 17,5 % der Abfragen Daten im Alter von mehr als drei bis zu sechs Monaten, 7,4 % sogar noch ältere. Dabei kann im Hinblick auf die älteren Daten ein Schwerpunkt bei solchen Abfragen identifiziert werden, die das nach den (damaligen) rechtlichen Rahmenbedingungen der Vorratsdatenspeicherung erreichbare Maximum von sechs Monaten auch tatsächlich ausschöpfen wollten (10,5 %).

*Schaubild C-2: Alter der abgefragten Daten in 2008**



*) Quelle: Bundesamt für Justiz. Prozentuierungen nach eigener Berechnung.

Die Verteilung der Abfragezeiträume zeigt auch starke regionale Unterschiede. Diese werden aus Tabelle C-1 ersichtlich. Dort wird auch der Mittelwert der Abfragezeiträume ausgewiesen. Danach fragten die Behörden in Schleswig-Holstein deutlich häufiger länger zurückliegende Daten ab (Durchschnittswert 4,2 Monate) als insbesondere in Berlin und Sachsen-Anhalt (jeweils 2,1 Monate). Über dem Durchschnittswert von 2,8 liegen auch Baden- Würt-

113 *Albrecht/Grafe/Kilchling* 2008, S. 190ff.

114 Siehe dazu oben Teil B.

temberg, Bayern, Hessen, Niedersachsen, Nordrhein-Westfalen, Sachsen und Thüringen. Besonders augenfällig werden die unterschiedlichen Werte bei den Abfragezeiträumen bis zu einem und bis zu drei Monaten.[115]

*Tabelle C-1: Anteile der Abfragen nach der zurückliegenden Zeit**

Bundesland	1 Monat	2 Monate	3 Monate	4 Monate	5 Monate	6 Monate	7 Monate	> 7 Monate	Durchschnitt Monate
BB	0,44	0,12	0,2	0,06	0,02	0,09	0,03	0	2,5
BE	0,19	0,17	0,42	0,05	0,01	0,03	0,01	0,01	2,7
BW	0,35	0,1	0,23	0,06	0,02	0,09	0,04	0,05	3,0
BY	0,41	0,12	0,12	0,04	0,03	0,14	0,02	0,07	3,0
HB	0,54	0,16	0,16	0,04	0,02	0,02	0,01	0,04	2,1
HE	0,24	0,06	0,3	0,02	0,01	0,06	0,01	0,05	3,0
HH	0,33	0,31	0,12	0,04	0,04	0,11	0,01	0,02	2,6
MV	0,44	0,1	0,11	0,06	0,02	0,01	0,05	0,01	2,3
NI	0,23	0,1	0,33	0,04	0,02	0,06	0,01	0,09	3,2
NW	0,31	0,09	0,33	0,03	0,02	0,12	0,03	0,03	3,0
RP	0,49	0,1	0,17	0,02	0,02	0,15	0	0,01	2,5
SH	0,24	0,04	0,24	0,02	0,02	0,16	0,02	0,2	4,2
SL	0,32	0,14	0,38	0,08	0	0,07	0	0	2,5
SN	0,35	0,14	0,13	0,05	0,04	0,17	0,04	0,04	3,2
ST	0,48	0,21	0,19	0,02	0,02	0,05	0,01	0	2,1
TH	0,3	0,12	0,15	0,04	0,1	0,18	0,02	0,02	3,3

*) Quelle: Bundesamt für Justiz. Prozentuierungen nach eigener Berechnung. Anteile x 100 = Prozent. Differenz zu 100 % durch fehlende Anteile für ausschließlich zukunftsgerichtete Abfragen. Durchschnittswert aller Bundesländer: 2,8 Monate.

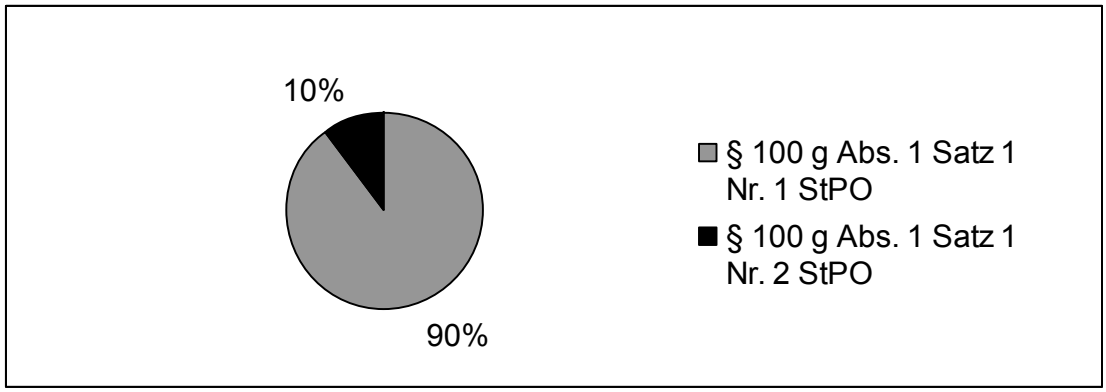
Bei der Bewertung der veröffentlichten Zahlen für 2008 ist allerdings zu berücksichtigen, dass in das erste Viertel des Erhebungszeitraumes dieser ersten justiziellen Jahresstatistik zur Verkehrsdatenerhebung bereits die erste einstweilige Anordnung des BVerfG zur eingeschränkten Nutzbarkeit von Vorratsdaten[116] fällt, sodass die Zahlen einer generalisierenden Interpretation nur sehr eingeschränkt zugänglich sind. Zu beachten ist ferner, dass gesonderte Zahlen für die Zeiträume vor bzw. nach dem Stichtag der Anordnung ebenfalls nicht vorliegen, sodass sich unmittelbare Effekte auf die Zugriffshäufigkeit nach dem 11.3.08 nicht nachzeichnen lassen.

---

115 Für weitere Detailauswertungen zu den Abfragezeiträumen basierend auf den Daten der MPI-Studie 2008 siehe auch unten 4.

116 Beschluss vom 11.3.2008 – 1 BvR 256/08. Siehe dazu oben Teile A und B.

*Schaubild C-3: Anlassstraftaten in 2008**



*) Quelle: Bundesamt für Justiz. Prozentuierungen nach eigener Berechnung.

Die erwähnte Unsicherheit in der Aussagefähigkeit der 2008er-Statistik (Schaubild C-3) betrifft insbesondere die Klassifizierung der Anlassdelikte. Ausweislich der veröffentlichten Zahlen liegt der eindeutige Schwerpunkt bei den Delikten gem. § 100g Abs. 1 Nr. 1 StPO (TKÜ-Katalogdelikte gem. § 100a Abs. 2 StPO und andere Straftaten von auch im Einzelfall erheblicher Bedeutung). Annähernd neun von zehn Abfragen hatten ein solches Delikt zum Gegenstand (89,8 %); nur eine von zehn bezog sich hingegen auf Delikte gem. § 100g Abs. 1 Nr. 2 (mittels Telekommunikation begangene Straftaten; 10,2 %). Insoweit ist allerdings zu beachten, dass die Abfragemöglichkeit bei Anlassstraften gem. Nr. 2 mit Inkrafttreten der einstweiligen Anordnung faktisch suspendiert war, sodass die 1.414 Abfragen mutmaßlich fast vollständig auf das erste Quartal 2008 entfallen dürften. Darüber, ob die Häufigkeit ohne die gerichtliche Einschränkung tatsächlich bis zu dreimal höher gelegen hätte, kann allenfalls spekuliert werden. Bei den im Rahmen der MPI-Studie 2008 analysierten Fällen machten die Beschlüsse betreffend die damals sog. mittels Endeinrichtung begangenen Straftaten gem. § 100g Abs. 1 S. 1 StPO a.F. jedenfalls ca. 28 % aller Fälle aus.[117] Unter Berücksichtigung der deutlichen Zunahme von Straftaten aus dem Bereich der sog. IuK-Kriminalität im engeren[118] und weiteren Sinne (Online-Kriminalität) dürfte deren Anteil inzwischen tatsächlich weit höher liegen als die statistisch für § 100g Abs. 1 Nr. 2 StPO ausgewiesenen Fälle; er dürfte auch höher liegen als die damals vom MPI ermittelten 28 %. Nach dem Wegfall der gerichtlichen Suspendierung des Zugriffs in Fällen gemäß Nr. 2 dürfte sich die Verteilung aktuell sicherlich deutlich von der im Jahr 2008 erfassten unterscheiden. Dies legen auch die Interviewergebnisse nahe (siehe dazu ausführlich unten Teil F). Die Anzahl der auf die entsprechenden Delikte gem. § 100g Abs. 1 Nr. 2 ausgerichteten Abfragen für 2008 macht jedenfalls gerade einmal 3,7 % der in 2008 gezählten IuK-Fälle im engeren Sinne[119] aus.

---

117 *Albrecht/Grafe/Kilchling* 2008, S. 133.

118 So hat die Zahl der vom BKA registrierten IuK-Delikte im engeren Sinne von 2008 auf 2009 um 32,6 % auf 50.254 Fälle zugenommen; vgl. Bundeskriminalamt, Bundeslagebild IuK-Kriminalität 2009, S. 5.

119 N = 37.900; Quelle wie Fn. 118.

Die Statistiken zur Abfragepraxis im Jahr 2008 erlauben ferner eine begrenzte Sekundäranalyse, in die weitere Daten zum Kriminalitätsaufkommen sowie zu den erledigten Strafverfahren des Jahres 2008 einbezogen werden können. Tabelle C-2 zeigt, dass die Anordnungspraxis zusammenhängt mit den Ausprägungen verschiedener Formen der Schwerkriminalität sowie der in den Bundesländern insgesamt erledigten Strafverfahren und der im Bezugsjahr angefallenen Verfahren mit Organisierter Kriminalität. Je mehr sich der Korrelationskoeffizient (R) dem möglichen Maximalwert 1.0 nähert, desto größer ist der Zusammenhang zwischen der jeweiligen Variablen (z.B. Gewaltkriminalität) und der Häufigkeit der Verkehrsdatenabfrage. Lediglich beim schweren Diebstahl fällt der Zusammenhang geringer aus.

*Tabelle C-2: Zusammenhänge zwischen Kriminalitäts- und Verfahrensdaten sowie der Anzahl der Abfragen in den Bundesländern 2008*****

Variable	Koeffizient (R)	Signifikanz	N
Kriminalität insgesamt	.647***	.007	16
Gewaltkriminalität	.608**	.013	16
Schwerer Diebstahl	.440*	.088	16
Betäubungsmittelhandel	.608**	.012	16
Anzahl der erledigten Verfahren	.672***	.004	16
Anzahl der OK-Verfahren	.648***	.007	16

* nicht signifikant, ** signifikant auf dem 5% Niveau, *** signifikant auf dem 1% Niveau

****) Quellen: Kriminalstatistiken der Bundesländer 2008; Stat. Bundesamt, Staatsanwaltschaftsstatistik 2008; BKA, Lagebericht Organisierte Kriminalität 2008.

Insgesamt ergibt sich somit auf der Grundlage der Struktur der (schweren) Kriminalität eine im Wesentlichen nachvollziehbare Abfragepraxis bei Telekommunikationsverkehrsdaten.

Im Einzelnen zeigen sich allerdings Differenzen, die insbesondere in der Anzahl der Abfragen pro Verfahren und der Zahl der Abfragen pro 100.000 der Wohnbevölkerung sichtbar werden. Insbesondere fallen die pro 100.000 der Wohnbevölkerung ermittelten Abfragen weit auseinander. Die entsprechenden Werte sind in Tabelle C-3 ausgewiesen. Dabei werden erhebliche regionale Unterschiede, etwa bei der Zahl der Abfragen pro Verfahren, sichtbar. Während für Berlin hier eine Verteilung von exakt 1:1 angegeben wird[120], finden im Saarland im Durchschnitt mehr als drei Abfragen pro Verfahren statt. Nahe am allgemeinen Durchschnittswert (1,68) liegen hingegen Baden-Württemberg, Bremen und Nordrhein-Westfalen. Berechnet auf 100.000 der Wohnbevölkerung wurden 2008 deutschlandweit etwa 20 Abfragen initiiert. Hier zeigt sich für Hamburg und das Saarland ein mehr als doppelt so hoher Wert.

---

120 Diese Relation erscheint allerdings wenig plausibel; demnach hätte es dort kein einziges Verfahren mit mehr als einem Beschluss gegeben. Am nächsten kommen dem Berliner Wert Sachsen-Anhalt und Brandenburg; obwohl diese nominal auf eine geringe Anzahl kommen, gab es auch dort zumindest einige Verfahren mit mehrfachen Anträgen.

Tabelle C-3: Absolute und relative Kennziffern zur Abfragepraxis in den Bundesländern

		Anzahl Verfahren mit Abfrage	Anzahl Abfragen pro Verfahren	Anzahl erledigte Verfahren pro Abfrage	Abfragen pro 100.000 der Bevölkerung
Brandenburg	1	168,00	1,20	884,13	8,04
Berlin	1	408,00	1,00	749,71	12,00
Bremen	1	150,00	1,66	230,48	35,57
Baden-Württemberg	1	1711,00	1,63	175,58	26,06
Bayern	1	1405,00	1,44	280,53	16,19
Hessen	1	550,00	1,40	488,68	12,64
Hamburg	1	405,00	1,95	200,49	43,83
Mecklenburg-Vorpommern	1	330,00	1,49	239,00	29,00
Niedersachsen	1	766,00	1,59	390,74	15,19
Nordrhein-Westfalen	1	942,00	1,72	729,41	9,02
Rheinland-Pfalz	1	311,00	2,01	439,01	15,60
Saarland	1	147,00	3,19	140,38	46,90
Sachsen-Anhalt	1	306,00	1,17	401,02	14,96
Schleswig-Holstein	1	190,00	2,32	379,49	15,75
Sachsen	1	373,00	1,79	322,36	15,90
Thüringen	1	127,00	1,27	786,99	7,00
Mittelwert			1,68	427,38	20,23
Median			1,61	385,12	15,68
Standardabweichung			0,53	237,40	12,43

*) Quelle: Bundesamt für Justiz (Spalte 1) und eigene Berechnungen.

Abfragen und Verfahren pro 100.000 sind sodann in Schaubild C-4 insgesamt und in Schaubild C-5 für Drogenkriminalität im Bezug auf die Bundesländer sichtbar gemacht. Dabei werden die erwähnten regionalen Unterschiede und Schwerpunkte noch deutlicher erkennbar. Auch normiert auf die Wohnbevölkerung hängt die Anzahl der Abfragen tendenziell von der Anzahl der Verfahren ab. Es sind aber starke länderspezifische Abweichungen festzustellen (Schaubild C-4). Deutlicher ist der Zusammenhang zwischen dem registrierten BtM-Handel und der normierten Anzahl der Abfragen (Schaubild C-5). Gleichwohl dominieren auch hier länderspezifische Besonderheiten.

Schaubild C-4: Bundesländer, Abfragen und erledigte Verfahren pro 100.000 der Wohnbevölkerung

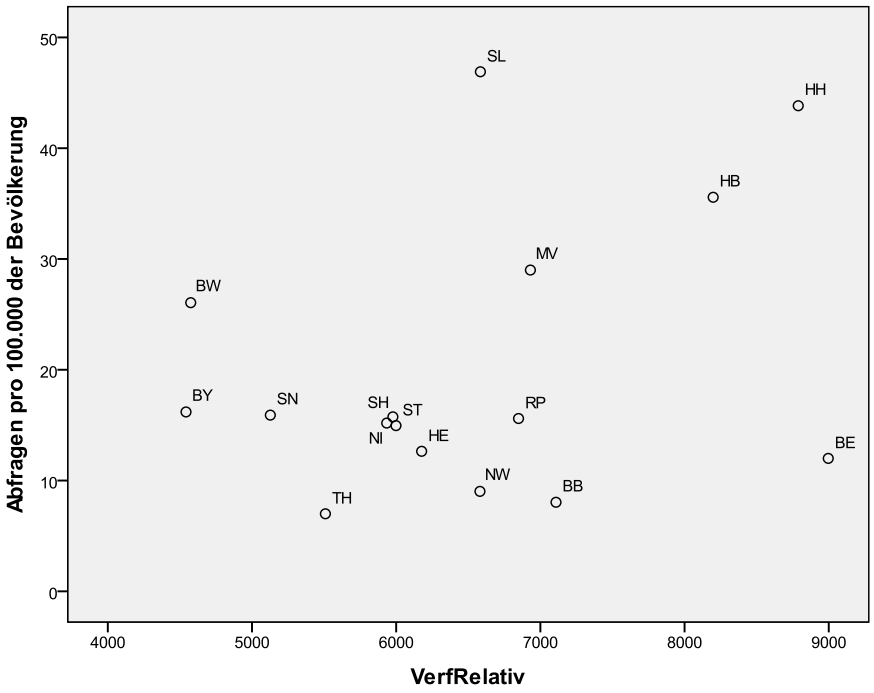


Schaubild C-5: Bundesländer, Abfragen und BtM-Handel pro 100.000 der Wohnbevölkerung

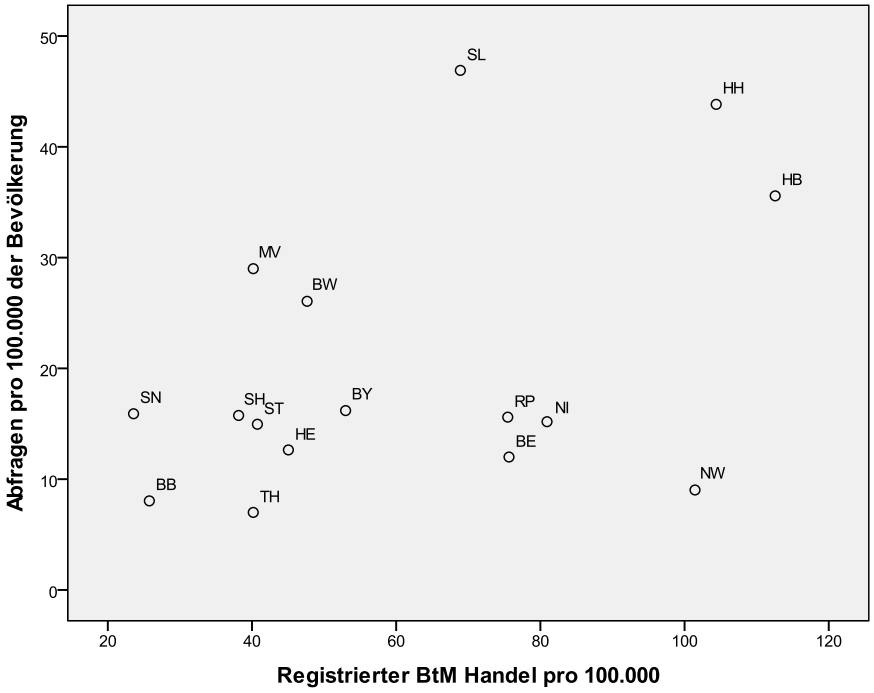


Schaubild C-6: Bundesländer, Abfragen und TKÜ-Maßnahmen (absolute Zahlen)

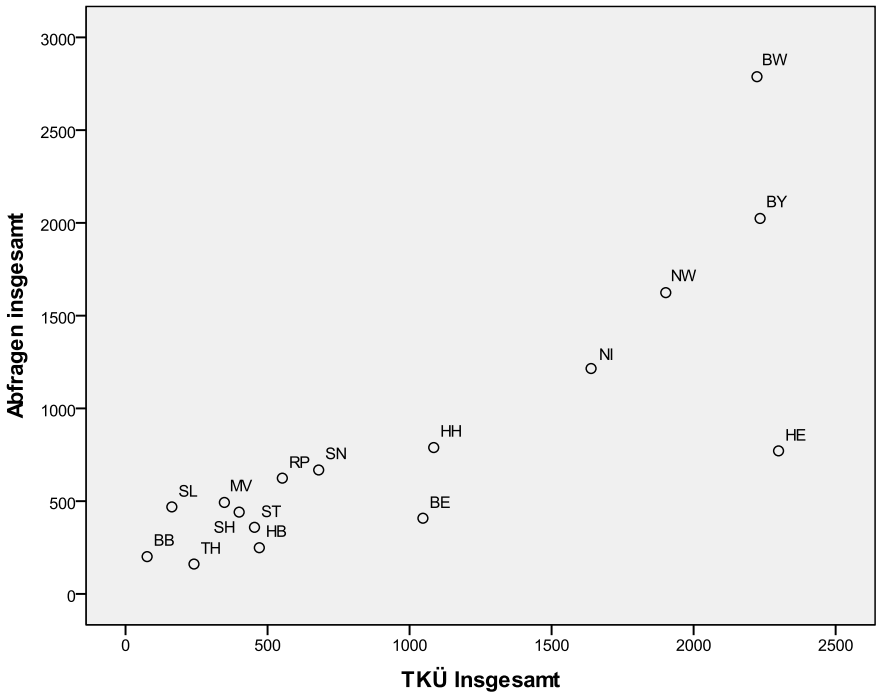
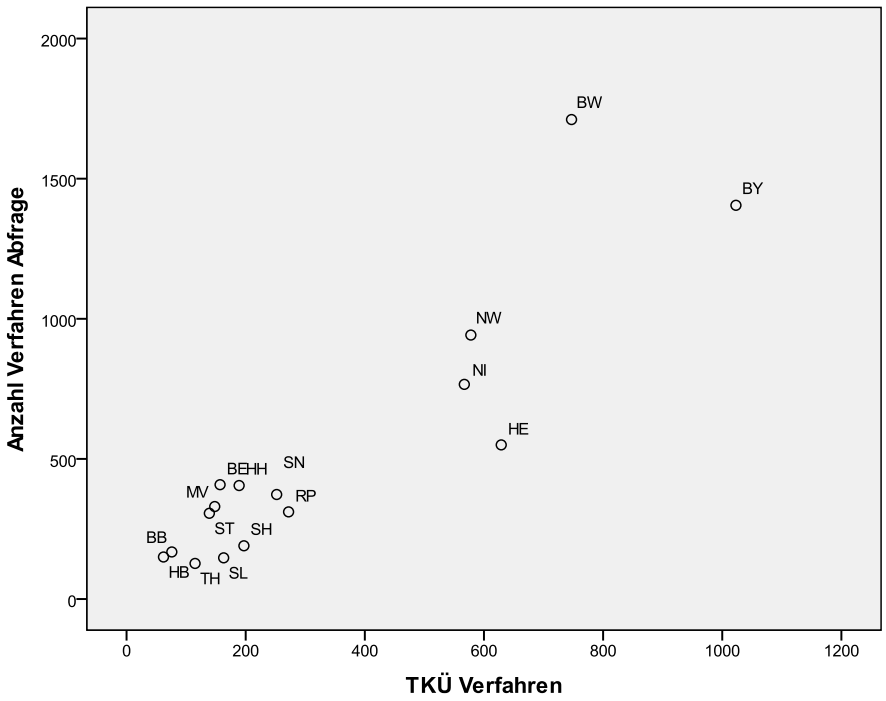


Schaubild C-7: Bundesländer, Abfragen und TKÜ-Verfahren (absolute Zahlen)



Schließlich wurde der Zusammenhang zwischen der Abfragepraxis und der Praxis der Inhaltsüberwachung der Telekommunikation analysiert. Dabei ergibt sich ein statistisch starker linearer Zusammenhang, der durch die enge Gruppierung entlang der gedachten Diagonale sehr schön sichtbar wird (r = .82). Lediglich Hessen und Baden-Württemberg fallen etwas heraus, wobei in Hessen im Verhältnis zu den Anordnungen nach §100a StPO relativ wenige Abfragen von Verkehrsdaten registriert werden (vgl. Schaubild C-6 bezogen auf Maßnahmen insgesamt sowie Schaubild C-7 im Verfahrensbezug).

2. Sondererhebung 2008/09

Etwas detailliertere Daten, die einige vorsichtige Aussagen zu möglichen Effekten erlauben, liegen jedoch zumindest für einen Teil des Zeitraumes vor, in dem die einstweilige Verfügung in Kraft war. Sie basieren auf einer Sonderhebung, die vom Bundesamt für Justiz im Zuge des Verfahrens beim BVerfG in drei Wellen erhoben wurden und zusammen den 16-Monatszeitraum vom 1.5.2008 bis zum 31.8.2009 abdecken; erfasst werden alle bei den Landesjustizbehörden sowie beim Generalbundesanwalt geführten Ermittlungsverfahren.[121]

Da sich der Referenzzeitraum teilweise mit dem der 2008er-Statistik überschneidet, sind vergleichende Aussagen zu der Entwicklung in den absoluten Zahlen betreffend die Zahl der einschlägigen Verfahren sowie der Maßnahmen insgesamt nicht möglich. Ein interner Vergleich der drei Wellen erscheint ebenfalls nur bedingt sinnvoll, da sie jeweils unterschiedlich lange Zeiträume abdecken. Eine gewisse Vergleichsbasis bietet zunächst die dritte Welle, die den Sechsmonatszeitraum vom 1.3. bis zum 31.8.2009 und damit exakt ein halbes Jahr abdeckt. Vergleicht man das Fallaufkommen in diesem halben Jahr mit dem vorausgegangenen Gesamtjahr 2008, deutet sich freilich ein dramatischer Einbruch an. Hier stehen der für 2008 registrierten Anzahl von 8.316 Verfahren mit Verkehrsdatenabfrage ganze 607 für den erfassten Halbjahreszeitraum 2009 gegenüber. Ebenso verhält es sich bei den Anordnungen mit nur noch 1.090 gegenüber mehr als 13.900 in 2008. Hochgerechnet auf das ganze Jahr 2009 ergäbe sich hieraus ein geschätzter Anteil von nur etwa einem Siebtel des Aufkommens aus dem Jahr davor.

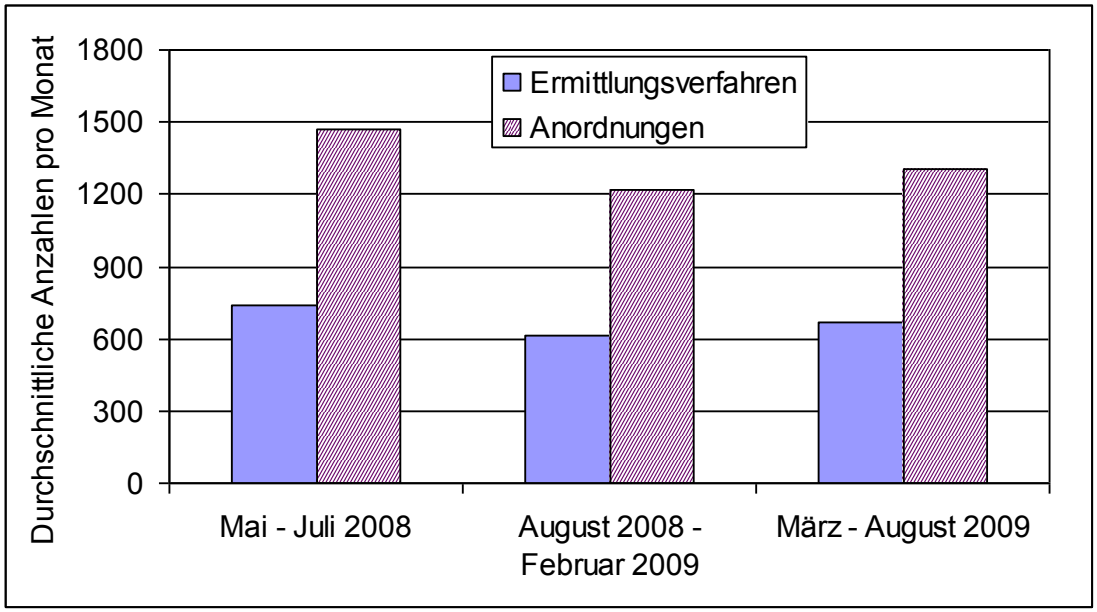
Basierend auf den Gesamtwerten für die drei Wellen wurde ergänzend der statistische Durchschnittswert für die Anzahl einschlägiger Verfahren bzw. Anordnungen insgesamt errechnet. Dieser kann als fiktiver monatlicher Wert für den jeweiligen Zeitraum interpretiert werden. Aus dem Vergleich der einzelnen Werte ergibt sich, dass der Rückgang sich offenbar in Stufen vollzogen hat (Schaubild C-8). Zunächst ist die Anzahl der Anordnungen im Frühjahr 2008 auf durchschnittlich ca. 1.468 pro Monat zurückgegangen, ab dem Spätsommer dann nochmals deutlich auf 1.218. Dieser niedrigere Wert für den zweiten Erhebungszeitraum

---

121 Siehe für die ausführlichen Werte, aufgeschlüsselt nach dem Fallaufkommen in den Bundesländern sowie beim Generalbundesanwalt, Tabellen 2 bis 4 in Anhang A. Einige Basiszahlen finden sich auch in der Antwort der Bundesregierung, BT-Drucks. 17/1482 vom 23.4.2010.

(August 2008 bis Februar 2009) dürfte mutmaßlich mit dem ersten Verlängerungsbeschluss vom 1.9.2008 erklärbar sein. Ab dem Frühjahr 2009 erhöhte sich die Zahl wieder leicht auf dann ca. 1.304. Dies könnte zum einen mit einem ein Jahr nach der ersten Anordnung besser eingespielten, routinierteren Umgang mit der Situation erklärbar sein, könnte zum anderen aber auch die Rückkehr zu dem allgemeinen Zunahmetrend anzeigen, wie er im Bereich der Telekommunikations- und Verkehrsdatenüberwachung seit längerer Zeit zu beobachten ist. Danach dürfte die Zahl unter gleichen Rahmenbedingungen ohne sonstige Effekte per se zunehmen. Das moderate Ausmaß der Zunahme wäre im Hinblick auf die damalige durchaus plausibel. Möglicherweise ergänzen sich diese beiden Faktoren sogar. Bezogen auf die Verfahrensebene fallen die Bewegungen moderater aus. Hier ging die Zahl zunächst auf monatlich etwa 737 zurück, dann weiter auf 609; zuletzt waren es dann 665.

*Schaubild C-8: Durchschnittliche Anzahl von Verfahren bzw. Anordnungen pro Monat für die drei (Sonder-) Erhebungszeiträume 2008/09**



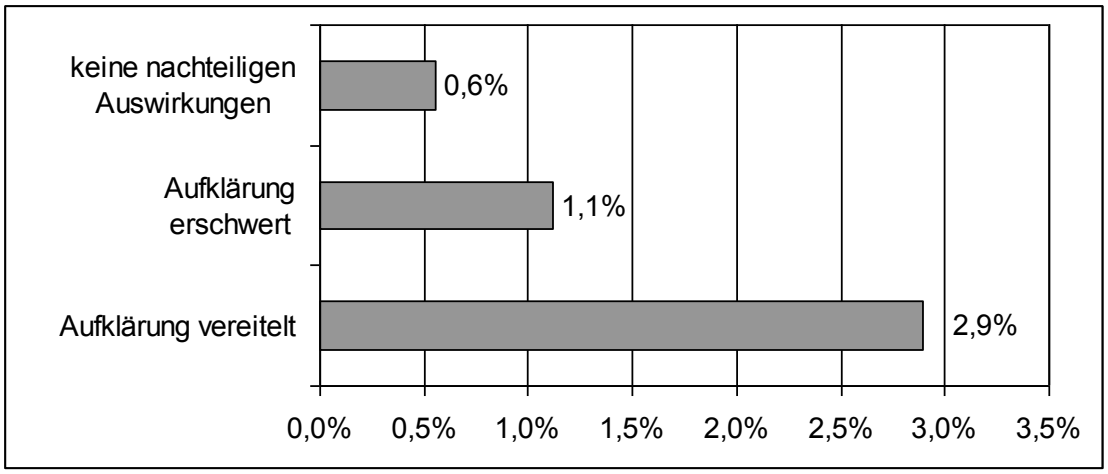
*) 1.5.2008 bis 31.8.2009. Datenquelle: Bundesamt für Justiz; Durchschnittswerte nach eigenen Berechnungen.

Bezogen auf den gesamten Erhebungszeitraum entfielen auf 10.359 einschlägige Verfahren insgesamt 20.543 Einzelanordnungen (darunter 19.877 Erst- und 666 Verlängerungsanordnungen). In 449 dieser Verfahren blieb das Auskunftsersuchen der Strafverfolgungsbehörden ganz oder teilweise erfolglos, weil kein Katalogdelikt i.S.v. § 100a StPO zugrunde lag und die Abfrage daher nicht beauskunftet wurde; das ist ein Anteil von weniger als 5 %. Hinzu kommen 423 erfolglose bzw. teilweise erfolglose Ersuchen aufgrund der Übergangsfrist des § 150 Abs. 12b TKG.[122] In 300 dieser Verfahren ist nach der Klassifizierung der erhebenden Stellen die Tataufklärung aufgrund der nicht erreichbaren Verkehrsdaten gescheitert (2,9 % aller Verfahren), in 116 war sie erschwert (1,1 %), in 57 hatte das Fehlen der Daten im Er-

122 Angaben im Verfahrensbezug fehlen insoweit.

gebnis keine negativen Auswirkungen auf das weitere Verfahren (0,6 %; siehe zum Ganzen Schaubild C-9). Auch hinsichtlich dieser Zahlen ist zu berücksichtigen, dass sie sich explizit auf die Sondersituation während der Erhebung beziehen. Viele Ermittlungsverfahren aus dem Bereich der IuK-Kriminalität waren zum Zeitpunkt der Sondererhebungen mutmaßlich ruhend gestellt oder vorübergehend eingestellt, sodass ihr konkreter Ausgang nicht erfasst worden sein dürfte.

*Schaubild C-9: Auswirkungen erfolgloser Verkehrsdatenabfragen auf das weitere Verfahren in 2008/09**

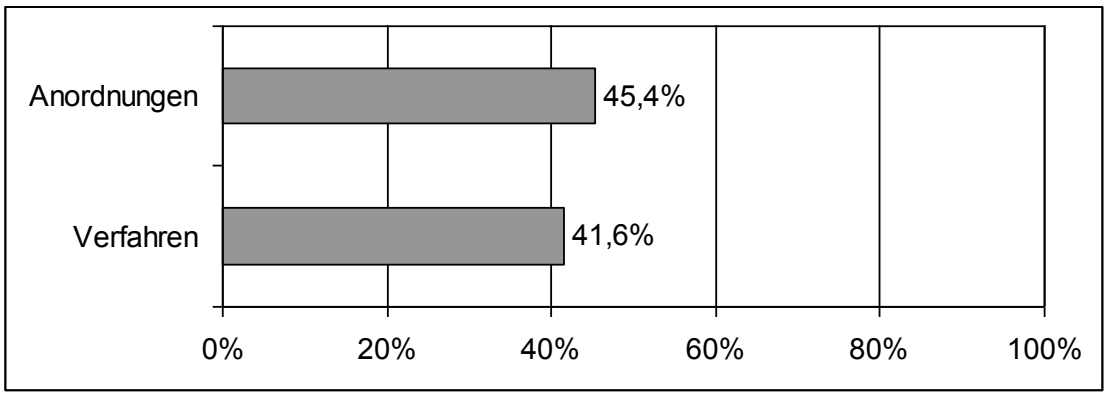


*) 1.5.2008 bis 31.8.2009. Quelle: Bundesamt für Justiz. Prozentuierungen nach eigener Berechnung.

Bemerkenswert erscheint, über den konkreten Anlass der Sondererhebung hinaus, der Anteil der Verkehrsdatenabfragen, bei denen auch oder ausschließlich auf Vorratsdaten gem. § 113a TKG zugegriffen werden musste. Dies war mit 45,4 % nämlich nur in weniger als der Hälfte der Verfahren mit Verkehrsdatenabfrage bzw. bei 41.6 % der einzelnen Anordnungen der Fall (Schaubild C-10). Das müsste im Umkehrschluss bedeuten, dass in den anderen Fällen auf der Grundlage des §§ 96 sowie gegebenenfalls auch der §§ 97, 99, 100 u. 101 TKG gespeicherte Daten abgefragt worden sein dürften. Eine weitere Unsicherheit ergibt sich daraus, dass der exakte Anteil nicht zweifelsfrei bestimmbar ist, da die konkrete Datenart in 21,7 % der Fälle nicht exakt ermittelbar war.[123] Ungeachtet dieser Unsicherheiten wird aber deutlich, dass zu einem Zeitpunkt, zu dem die Vorratsdaten grundsätzlich, wenn auch für ein beschränktes Fallspektrum, weiterhin noch zur Verfügung standen, trotz des normtechnischen Vorrangs des § 113a TKG für Verkehrsdatenabfragen zu Zwecken der Strafverfolgung offensichtlich in so vielen Fällen auf anderweitig gespeicherte Daten zugegriffen wurde. Über eine Erklärung kann nur spekuliert werden. Zum einen ist an die verzögerte Umsetzungsfrist für Internetprovider im Allgemeinen und kleine Anbieter im Besonderen zu denken. Zum anderen hatten mehrere Unternehmen auf dem Verwaltungsrechtsweg einstweilige Anordnungen zur vorläugfigen Suspendierung von der Verpflichtung gem. § 113a TKG erwirkt.

123 N = 2.247.

*Schaubild C-10: Anteil der Vorratsdaten (§ 113a TKG) an den abgefragten Verkehrsdaten in 2008/09**



*) 1.5.2008 bis 31.8.2009. Quelle: Bundesamt für Justiz. Prozentuierungen nach eigener Berechnung (45,4 %: n = 4.707; 41,6 %: n = 8.551).

3. Situation 2010

Für den Zeitraum seit dem 2.3.2010 liegen bislang keine belastbaren statistischen Zahlen vor. Auf der Grundlage des engen zeitlichen Rahmens für die vorliegende Ausarbeitung sahen sich die Landesjustizverwaltungen leider nicht in der Lage, die Erhebung exakter Zahlen zu veranlassen. Auch die befragten Experten erachteten den Zeitraum seit dem 2.3.2010 in aller Regel für zu kurz, um mögliche Veränderungen in der Häufigkeit der Abfragen gem. § 100g StPO verlässlich quantifizieren oder auch nur abschätzen zu können. Dasselbe gilt für die TKÜ-Maßnahmen gem. § 100a StPO, die nicht nur in begrenztem Rahmen als Substitut in Frage kommen, sondern häufig auch hinsichtlich Vorbereitung, Auswahl und Durchführung von der Verkehrsdatenabfrage abhängig sein können. Siehe dazu auch unten die Experteneinschätzungen in Teil F.

Eine dezidierte Aussage zu möglichen quantitativen Auswirkungen des Urteils seit dem 2.3.2010 muss daher in dem vorliegenden Rahmen unterbleiben.

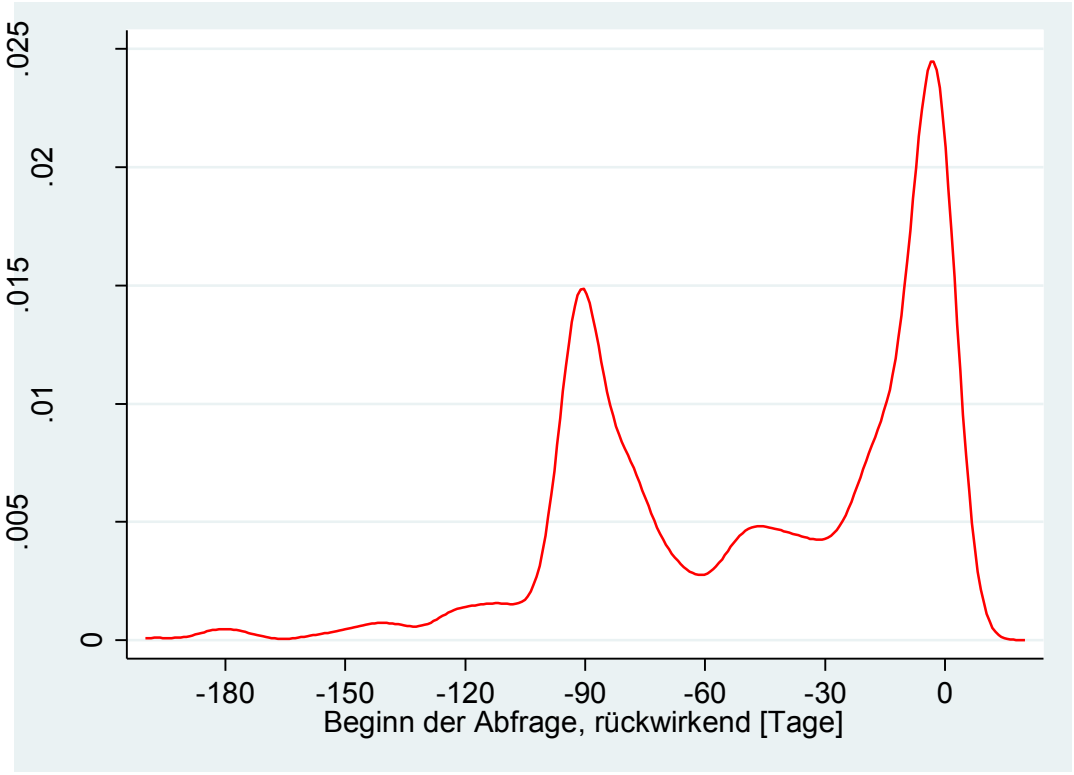
4. Ergänzende Befunde aus der ersten MPI-Verkehrsdatenuntersuchung (2008)

In Ergänzung zu den quantitativen Befunden, soweit sie aus den offiziellen Statistiken gezogen werden konnten, wurde eine Reanalyse ausgewählter Datensätze aus der MPI-Studie 2008 zur Verkehrsdatenabfrage durchgeführt. Damals wurden die Beschlüsse gem. § 100g/h StPO a.F. aus der Aktenstichprobe der Jahre 2003 und 2004 untersucht.[124] Sie bezogen sich

124 N = 1.257 Beschlüsse aus 467 Verfahren; für nähere Einzelheiten vgl. *Albrecht/Grafe/Kilchling* 2008, S. 111ff.

in 66% der Fälle auf den Mobilfunk und zu 28% auf Anschlüsse im Festnetz. In 86% der Fälle wurden Verbindungsdaten im engeren Sinne abgefragt. Weiterhin wurden IMEI Kennungen (10%) und andere Angaben ermittelt. Bei der Bewertung der folgenden Ergebnisse ist zu berücksichtigen, dass diese Untersuchung Fälle aus der Zeit vor Einführung der Vorratsdatenspeicherung Ende des Jahres 2007 betrifft. Damals stellten sich sowohl die gesetzlichen Grundlagen betreffend die Datenspeicherung als auch die Marktsituation im Bereich der Flatrate- und Prepaid-Tarife anders dar als heute. Die folgenden Ergebnisse spiegeln mithin die Abfragepraxis in den Jahren 2003 und 2004 wider, die sich – damals wie auch gegenwärtig wieder – ganz wesentlich an den Speicherpraktiken der TK-Unternehmen orientierte. Insbesondere im Hinblick auf die Abhängigkeit der abfragenden Ermittlungsbehörden von den unternehmerischen Interessen der TK-Industrie erscheint die damalige Situation grundsätzlich (wieder) mit der heutigen vergleichbar, sofern berücksichtigt wird, dass sich sowohl der unternehmensinterne Speicherbedarf für Abrechnungszwecke als auch die Speicherfristen mittlerweile anders darstellen dürften. Diese für die Praxis wesentlichen Veränderungen sind Gegenstand des Interviewteils und werden dort im Einzelnen erläutert (siehe unten Teil F).

*Schaubild C-11: Alter der abgefragten Verkehrsdaten**

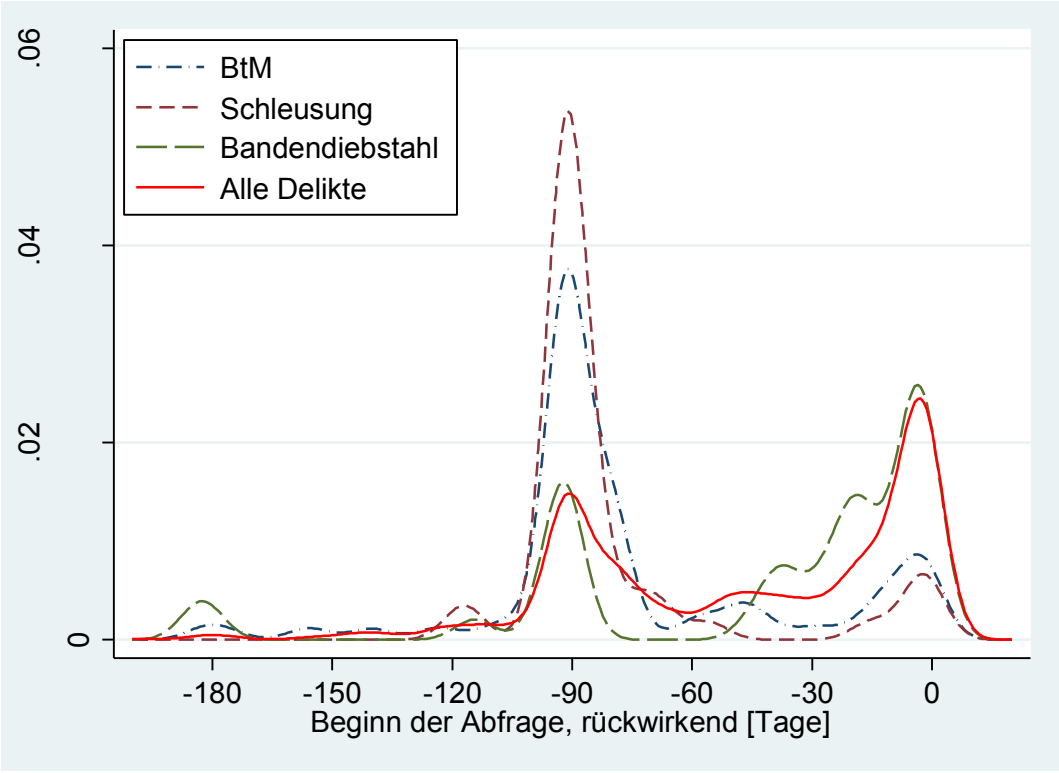


*) Quelle: Erste MPI-Studie.

Schaubild C-11 zeigt zunächst die erwähnte Orientierung der Abfragepraxis an der Erreichbarkeit der Daten. Bei minus 90 Tagen brechen die Anfragen mehr oder weniger vollständig

ab. Dies deckt sich mit den Befunden zur damaligen Speicher- bzw. Löschpraxis.[125] Innerhalb dieser faktischen Speicher-(höchst-)dauer lassen sich zwei ermittlerische Schwerpunkte erkennen, nämlich bei sehr kurzfristig orientierten Abfragen sowie bei längerfristigen. Von eher nachgeordneter Bedeutung sind im Vergleich dazu die 'mittelalten' Verkehrsdaten zwischen 30 und 60 Tagen. Bezogen auf einige Hauptdeliktsarten (Schaubild C-12) ergibt sich dann weiter, dass der Bedarf an längerfristigen Daten bei Strukturermittlungen in den Bereichen Drogen- und Schleusungskriminalität besonders hoch ausfällt. Ein ganz anderes Muster wird bei den Ermittlungen beim Bandendiebstahl erkennbar. Diese Fälle scheinen sehr verschieden gelagert zu sein und führen zu ganz unterschiedlichen Abfragen. Je nach Fall können hier Daten jeden Alters von Bedeutung sein; hier gibt es sowohl den größten Anteil an Abfragen bezogen auf 'mittelalte' Daten, mit zwei Schwerpunkten bei etwa 20 und etwa 40 Tagen, als auch die einzig auffallende Nachfrage nach Daten im Alter von 180 Tagen, was vor Inkrafttreten der Vorratsdatenspeicherung ein Ausnahmefall war.

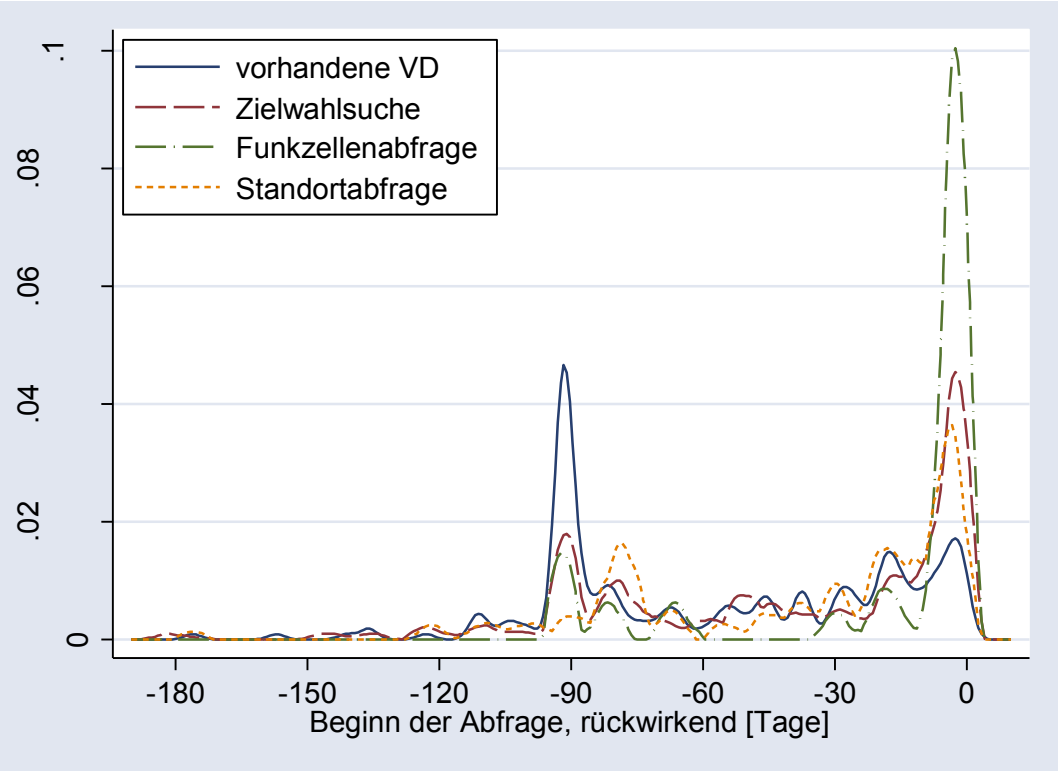
*Schaubild C-12: Alter der abgefragten Verkehrsdaten nach Deliktsgruppen**



*) Quelle: Erste MPI-Studie.

125 Diese betrug zwischen 80 und 90 Tagen. Vgl. *Albrecht/Grafe/Kilchling* 2008, S. 101ff.

*Schaubild C-13: Alter der abgefragten Verkehrsdaten nach verschiedenen Abfragearten**

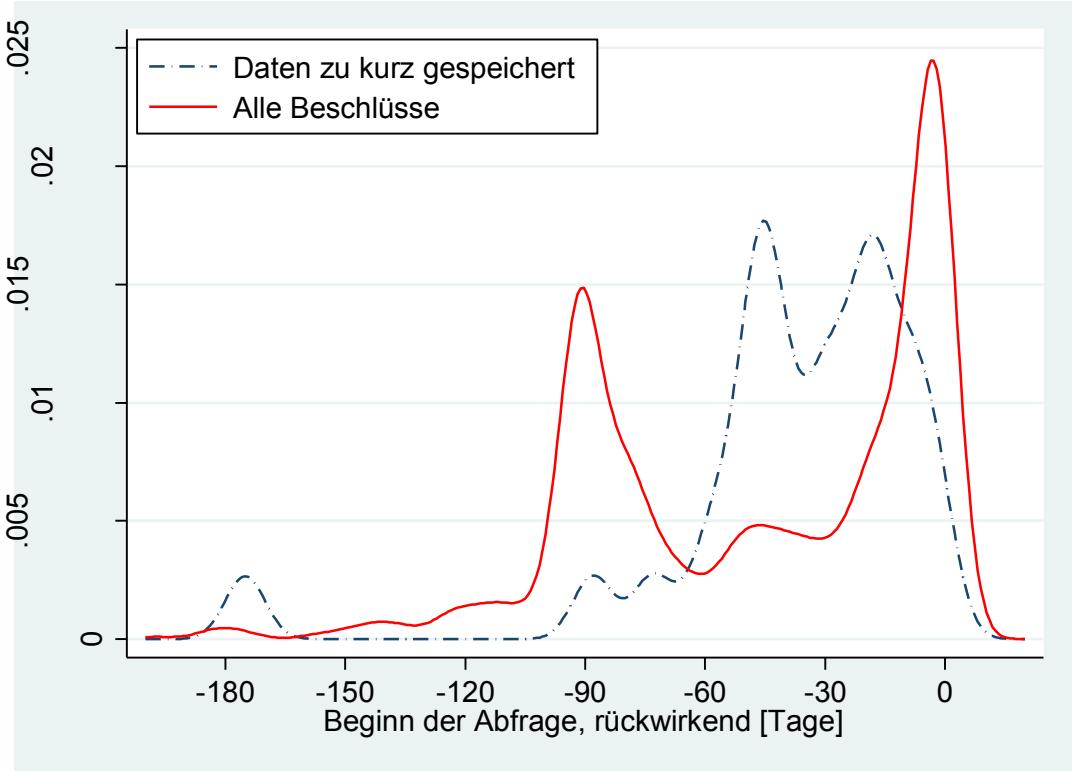


*) Quelle: Erste MPI-Studie.

Erwartungsgemäß differenziert sich das Bild noch weiter, wenn man die verschiedenen Abfragearten zugrundelegt (siehe Schaubild C-13). Danach sind es vor allem die kommunikationsbezogenen Verbindungsdaten im 'klassischen' Sinne, die den maximalen Speicherzeitraum ausschöpfen oder auszuschöpfen versuchen (nach damaliger Kategorisierung „vorhandene Verkehrsdaten“). Ein ganz anderes Muster ergibt sich für die Funkzellenabfrage, die extrem kurzfristig angelegt ist. Meist werden nur wenige Tage, oft sogar nur wenige Stunden abgefragt.[126] In einigen wenigen Fällen werden Funkzellenabfragen auch für einen schon länger zurückliegenden Zeitraum eingesetzt. Dies bedeutet allerdings nicht zwingend, dass tatsächlich der gesamte Zeitraum (70, 80, 90 Tage) abgefragt wird; wahrscheinlicher sind Situationen, in denen, dem allgemeinen Muster der Funkzellenabfrage entsprechend, ein länger zurückliegender kurzer Zeitraum (ein Tag, mehrere Tage) ausgewertet wird. Etwas gleichmäßiger verteilt ist die Abfragedauer schließlich bei der Standortabfrage und der Zielwahlsuche. Freilich gibt es auch dort einen gewissen Schwerpunkt bei den kurzfristigen Daten.

126 Bei der detaillierten Analyse der Funkzellenabfragen bei einem größeren bundesweiten Anbieter bezog sich etwa ein Viertel auf einen Zeitraum von unter einer Stunde, das Maximum lag bei drei Tagen. Vgl. *Albrecht/Kilchling/Grafe* 2008, S. 104.

*Schaubild C-14: Alter der abgefragten Verkehrsdaten insgesamt und bei erfolglosen Abfragen infolge zu kurzer Speicherdauer**



*) Quelle: Erste MPI-Studie.

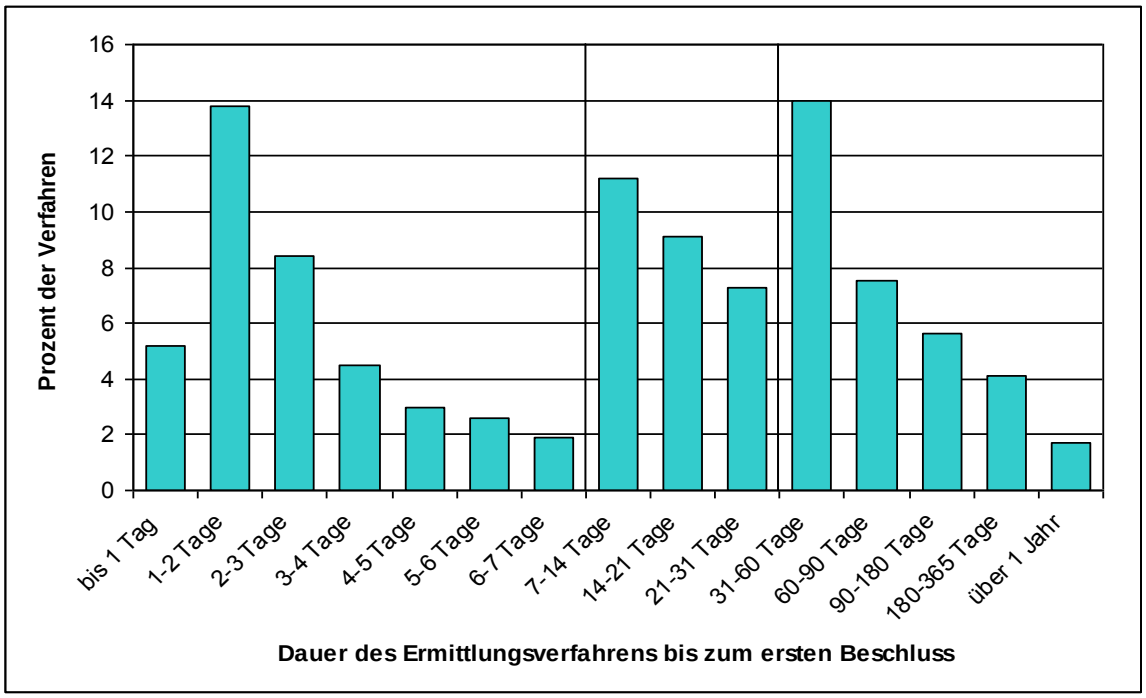
Im nächsten Schritt geht es um mögliche Zusammenhänge zwischen dem 'Alter' der abgefragten Daten und zwischenzeitlich eingetretenen Löschungen. Schaubild C-14 zeigt zunächst noch einmal das 'Alter' der abgefragten retrograden Daten nach der relativen Häufigkeit sowie, nach demselben Maß, die 'Alters-Verteilung' für diejenigen Fälle an, in denen die Abfrage erfolglos bleib, weil die angeforderten Daten nicht mehr gespeichert waren. Insgesamt kam diese letztere Konstellation überhaupt nur in 2,9 % der analysierten Akten vor.[127] Sie betraf vermehrt Abfragen mit Zielwahlsuchen, Funkzellenabfragen oder Geodaten, bei denen in jeweils ca. 3,5 % der Fälle eine zu kurze Speicherung angegeben war. Bei anderen Abfragearten, meist ausgehende Verbindungsdaten betreffend, war dies bei 1,5 % der Fall.

Der Verlauf der unterbrochenen Linie zeigt zunächst an, dass es bei dem Zugriff auf kurzfristig zurückliegende Daten nur wenige Verluste gab. Im Ausmaß gering sind diese auch bei den älteren Datenanforderungen zwischen 60 und 90 Tagen und selbst bei den damals noch seltenen rückwirkenden Abfragen bis zu 6 Monaten. Bei den Ermittlern scheint es damals eine recht gute Kenntnis über die längerfristig gespeicherten Datenarten gegeben zu haben. In Relation zu der Anzahl der entsprechenden Abfragen (durchgezogene Linie) ist die Wahr-

127 N = 37.

scheinlichkeit des Ausfalls allerdings höher als bei den drei Monate alten Daten (dort bleibt die unterbrochene Linie sehr deutlich unter der durchgehenden), hingegen traten speicherfristbedingte Datenverluste am häufigsten bei Daten mit einer Speicherzeit zwischen etwa 15 und 60 Tagen auf. Dabei lassen die beiden Peaks die Zeitpunkte erkennen, bei denen das Risiko des Datenverlusts unter den damaligen Bedingungen am höchsten war: nach etwa 15 bis 20 Tagen sowie nach 45-50 Tagen.

Schaubild C-15: Dauer der Ermittlungsverfahren bis zum ersten Beschluss/***

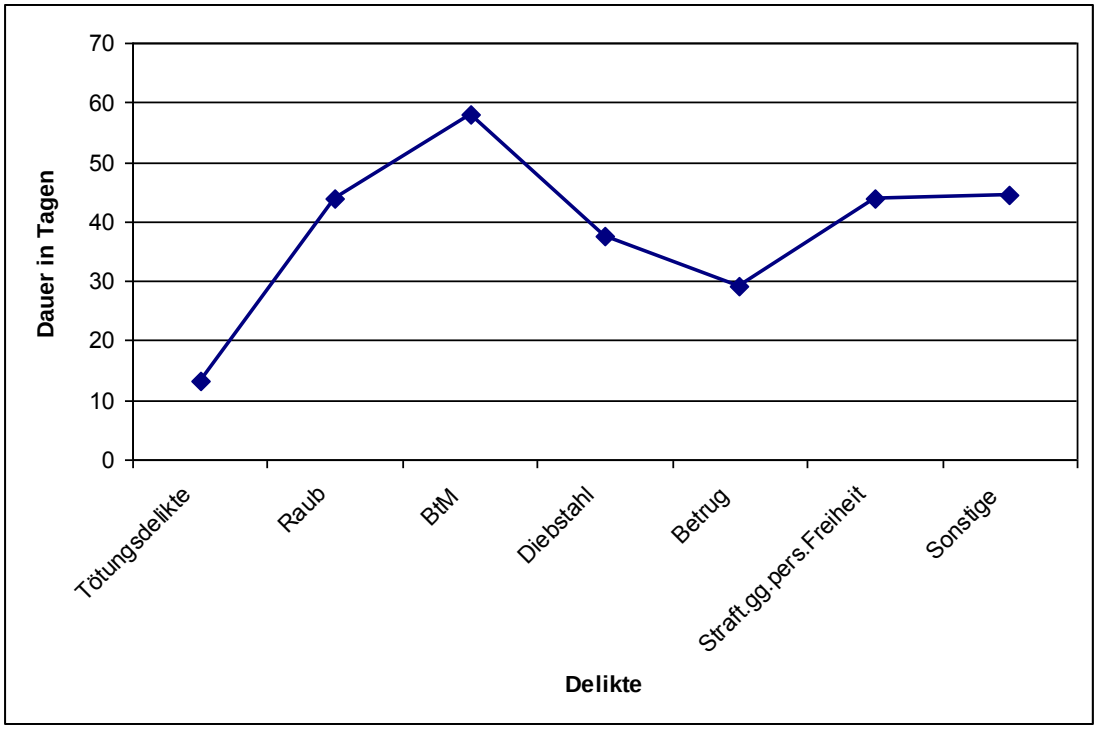


*) Quelle: Erste MPI-Studie.
**) §§ 100g/h StPO a.F.

Mit entscheidend für die Frage, ob und wie lange Verkehrsdaten für die Strafverfolgungsbehörden erreichbar sind, ist neben der Speicherdauer der Zeitpunkt der bzw. die Zeitdauer bis zur Abfrage. Es ist zugleich dasjenige Zeitintervall, das die Ermittlungsbehörden selbst steuern können. Daher wurde ergänzend die Dauer der Ermittlungsverfahren bis zum ersten Abfragebeschluss ermittelt (Schaubild C-15). Einen ersten Schwerpunkt machen dabei die sehr kurzfristig veranlassten Abfragen aus, die in den ersten beiden bzw. ersten drei Tagen veranlasst werden. Diese Fälle machen ca. 27 % der Verfahren aus. Die beiden weiteren Häufungen in der zweiten Woche bzw. im zweiten Monat entstehen durch das Zusammenfassen größerer Zeiträume. Tatsächlich werden erste Verbindungsdatenabfragen mit der Dauer des Ermittlungsverfahrens langsam immer seltener. Insgesamt werden 50 % der ersten Beschlüsse innerhalb von 14 Tagen erlassen. In 13 % der Verfahren erfolgte die erste Abfrage aber erst nach drei Monaten oder noch später, darunter in immerhin 1,5 % erst nach mehr als einem Jahr.

Übertrüge man die damalige Ermittlungspraxis auf die gegenwärtige Situation, in welcher Verkehrsdaten tatsächlich maximal 7 Tage mit recht hoher Wahrscheinlichkeit erreichbar sind, würde dies bedeuten, dass in mehr als 60 % aller Verfahren (repräsentiert durch die Säulen in den beiden rechten Sektoren des Schaubildes) Verkehrsdatenabfragen nunmehr geringeren oder gar keinen Erfolg versprechen. Um dies zu vermeiden hat die Praxis inzwischen Konsequenzen gezogen und versucht jetzt, Beschlüsse nach § 100g StPO möglichst frühzeitig zu erwirken (siehe hierzu ausführlich den Interviewteil F). Zu berücksichtigen ist freilich auch, dass sich unter den länger dauernden Verfahren viele Ermittlungen einschließlich Strukturermittlungen im Bereich schwerer und Drogenkriminalität finden, in denen regelmäßig auch zukunftsgerichtete Verkehrsdatenüberwachungen stattfinden. Diese letztere Konstellation ist vom Wegfall der Vorratsdatenspeicherung nicht betroffen, sodass eine längere Verfahrensdauer nicht zwangsläufig einen endgültigen Datenverlust indiziert.

*Schaubild C-16: Dauer bis zum ersten Beschluss nach Deliktsgruppen**



*) Quelle: Erste MPI-Studie.

Schaubild C-16 schlüsselt die Verfahrensdauer gesondert nach einigen Hauptdeliktsgruppen auf. Hier bestätigt sich der eben erwähnte Schwerpunkt von langer Ermittlungsdauer und später Verkehrsdatenabfrage bei Drogenermittlungen noch einmal. Das Gegenstück bilden die Ermittlungen in Tötungsfällen, wo die Ermittlungsbehörden sehr viel schneller einen Beschluss erwirken. Dies sind oft Fälle, in denen die Verkehrsdaten zunächst einen der ersten, wenn nicht sogar den ersten Ermittlungsansatz überhaupt darstellen.

Weitere punktuelle Detailanalysen konzentrierten sich schließlich auf die Frage, ob die betriebsinterne Speicherdauer der Daten und damit einhergehend die Wahrscheinlichkeit, dass Daten vorhanden sind, einen systematischen Einfluss auf den Ermittlungserfolg haben könnte. Hierfür wurde in einem ersten Schritt bestimmt, wie weit der Abfragezeitraum der einzelnen Beschlüssen in die Vergangenheit zurück reichte. Diese Angabe kann den Kategorien in Tabelle C-4 (Spalte N) entnommen werden. Mit einbezogen sind hier, im Gegensatz zu den vorangegangenen Analysen zu den retrograden Abfragen, auch die zukunftsgerichteten Zeiträume. Denn speziell für die Erfolgsanalyse ist neben der Erfassung des retrograden Zeitraumes der Abfrage zu berücksichtigen, welchen Gesamtzeitraum die Abfrage insgesamt abdecken soll. So kann z.B. eine Abfrage, die den zurückliegenden Dreimonatszeitraum abdecken soll, auch dann erfolgreich sein, wenn nur noch Daten aus dem letzten Monat gespeichert sind. Hier ist festzustellen, dass sich die Beschlüsse, unabhängig davon wie weit sie in die Vergangenheit zurückreichen, meist auf einen sehr großen Abfragezeitraum beziehen. So umfassen etwa ein Drittel der Beschlüsse, deren Abfragezeitraum über drei Monate in die Vergangenheit reicht (Zeile „vor mehr als 90 Tage“), zugleich auch Daten in der Zukunft. Eine Konzentration auf einen kürzeren Abfragezeitraum ist bei Beschlüssen festzustellen, deren Abfragen nur wenige Tage in die Vergangenheit reichen (Zeilen „1-7 Tage zurückliegend“ und „1 Tag zurückliegend“).

*Tabelle C-4: Abfragezeiträume bei Beschlüssen die sich nur auf die Vergangenheit bezogen**

	N	<-90	-60 - -90	-30 - -60	-7 - -30	-1 - -7	-1	>0
Beginn der Abfrage in der Vergangenheit								
vor mehr als 90 Tagen	182	9	2	5	11	10	78	65
60-90 Tage zurückliegend	148		10	4	10	6	68	46
30-60 Tage zurückliegend	101			37	10	6	17	26
7-30 Tage zurückliegend	134				49	18	14	52
1-7 Tage zurückliegend	186					146	19	18
1 Tag zurückliegend	65						57	7
Beginn in der Zukunft	441							441

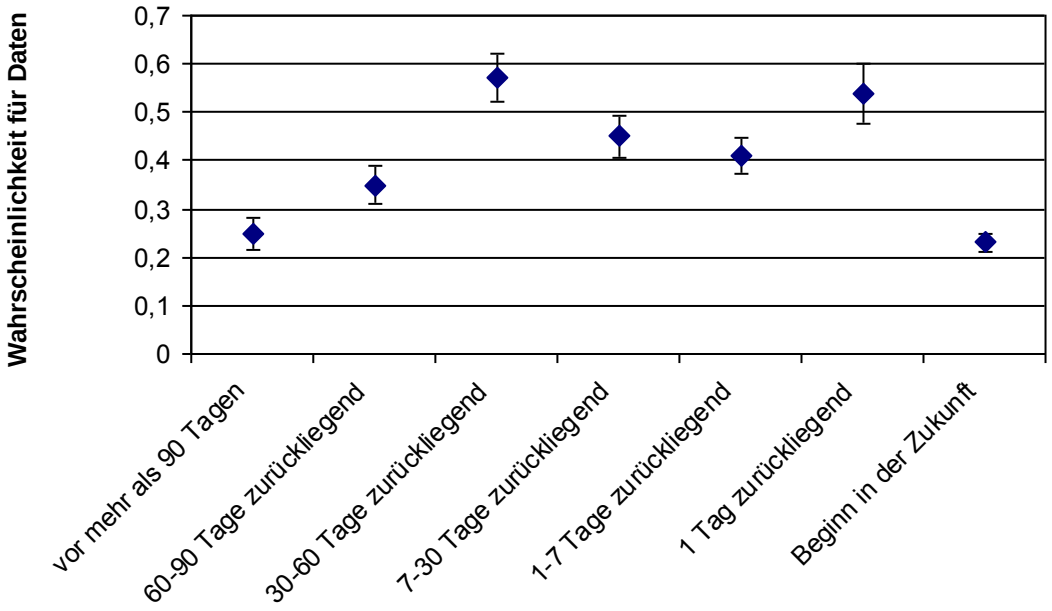
*) Quelle: Erste MPI-Studie.

Da keine Angaben darüber vorlagen, auf welchen konkreten Zeitraum innerhalb einer Abfrage ggf. die Erfolge zurückzuführen waren, wurde im Folgenden der Beginn des Abfragezeitraums als Kriterium genommen.

Zur Abschätzung des Erfolges von Verbindungsdatenabfragen wurde zunächst die Grundvariable erhoben: Wurden überhaupt Verbindungsdaten durch TK-Anbieter geliefert (Ja/Nein)? Sodann wurde erfasst, ob in der Akte zu den jeweiligen Beschlüsse mindestens ein spezifischer Erfolg, wie z.B. die Ermittlung weiterer Täter, die Lokalisierung eines Täters, etc. verzeichnet war. Ein weiteres Kriterium war die Erfolgseinschätzung des Auswerters, bzw. die Erwähnung einer solchen allgemeinen Einschätzung in der Akte (dreistufige Skala: 0 = kein Erfolg; 1 teilweise erfolgreich; 2 erfolgreich).

Diese drei Angaben wurden differenziert nach dem zeitlichen Anfang des Abfragezeitraums ausgewertet. Dabei wurde die Abfragedauer, wie auch die spezifische Art der Abfrage (z.B. Funkzellenabfrage) nicht weiter berücksichtigt.[128] Die Wahrscheinlichkeit, dass tatsächlich Daten geliefert wurden (Schaubild C-17) ist, soweit es den Beginn des Abfragezeitraums betrifft, von 2 Monaten in die Vergangenheit bis zur Gegenwart mit ca. 50% gleichbleibend. Geht der Abfragezeitraum weiter in die Vergangenheit zurück, sinkt die Wahrscheinlichkeit, dass Daten geliefert wurden bis auf 25% (mehr als 3 Monate zurück) ab. Gleichfalls ist die Wahrscheinlichkeit, dass Verbindungsdaten geliefert werden, für zukünftige Daten mit ca. 23% relativ gering.[129] Dieses Ergebnis ist nicht einfach durch die Löschung von weiter zurück liegenden Daten zu erklären, reichen doch gerade die Abfragezeiträume dieser Beschlüsse meist bis in die Gegenwart, und es sollten dann wenigstens für diese erst kurz zurückliegenden Zeiträume Daten vorhanden sein. Möglicherweise könnte der Wunsch nach weit zurück liegenden Daten gerade in Fällen aufkommen, die wegen ihres gegebenenfalls schon vorhandenen zeitlichen Abstandes zur Tat prinzipiell schwerer aufzuklären sind.

*Schaubild C-17: Wahrscheinlichkeit für Verkehrsdaten in Abhängigkeit vom Beginn des Abfragezeitraums**



*) Beschlussbezogen (Daten_ja/nein: ja). Quelle: Erste MPI-Studie.

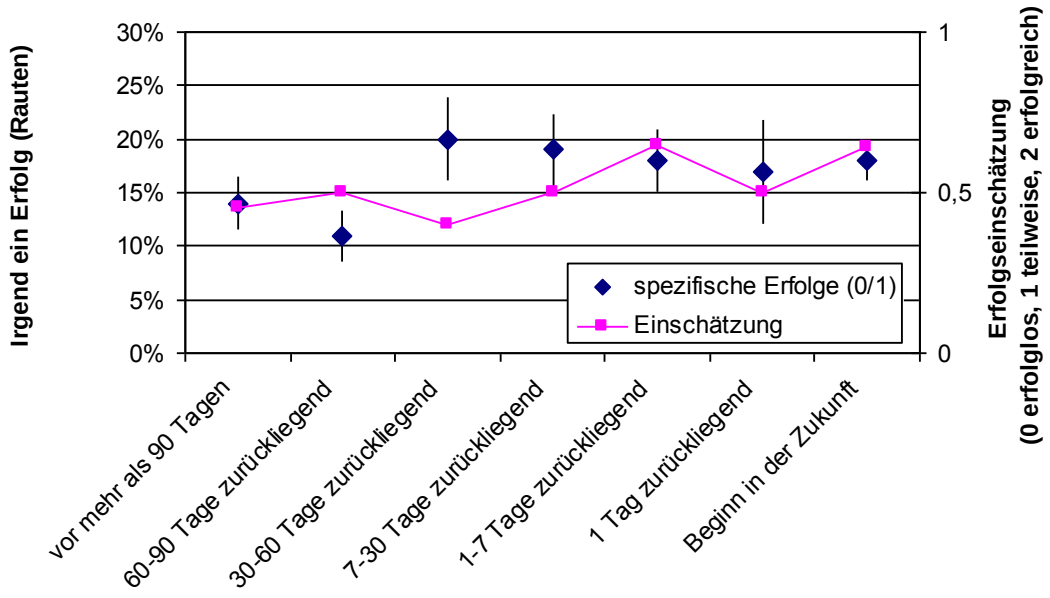
---

128 Zwar verbessert sich z.B. bei einer logistischen Analyse der spezifischen Erfolge (0/1) die erreichte Varianzaufklärung von knapp 1 % bei Berücksichtigung des Anfangs (kategorisiert) auf fast 4%, wenn zusätzlich das Ende der Abfrage (in den verschieden Kombinationen mit dem Anfang) mit berücksichtigt wird. Allerdings ist keiner der dann zu bestimmenden 25 Parameter signifikant und es ist keine sinnvolle Struktur zu erkennen; vielmehr streuen die einzelnen Parameterwerte in eher zufälliger Weise.

129 Insgesamt werden durch diese Differenzierung ca. 5 % der Varianz erklärt. Nimmt man noch das Ende der Abfrage als weitere kategoriale Variable hinzu, so steigert sich diese Varianzaufklärung nur unwesentlich, und fast alle zusätzlichen Parameter sind nicht signifikant.

Direkter als die Angabe, dass überhaupt Daten geliefert wurden, sollte der Erfolg der Abfragen durch spezifische Erfolge und die allgemeine Erfolgseinschätzung zu fassen sein. In Schaubild C-18 sind diese beiden Kriterien in Abhängigkeit vom Beginn des Abfragezeitraums dargestellt. Die Existenz spezieller Erfolge betreffend ist kein signifikantes Ergebnis festzustellen. Allenfalls kann von einer Tendenz zu weniger Erfolgen in den ersten beiden Kategorien, also bei den ältesten Daten, gesprochen werden. Auch die allgemeine Erfolgseinschätzung, die im Mittel zwischen erfolglos (0) und teilweise erfolgreich (1) schwankt, differiert nicht signifikant entlang dieser Kategorien. Allenfalls kann von einem Trend gesprochen werden, dass Abfragen, die nicht zu weit in die Vergangenheit reichen, etwas erfolgreicher sind.

Schaubild C-18: Wahrscheinlichkeit eines spezifischen Erfolges sowie die Mittelwerte der allgemeinen Erfolgseinschätzung in Abhängigkeit vom Beginn des Abfragezeitraums***



*) Mittelwerte dreistufig skaliert (0 = kein Erfolg; 1 = teilweise erfolgreich; 2 = erfolgreich);
**) Beschlussbezogen. Quelle: Erste MPI-Studie.

Die Ergebnisse sind aus verschiedenen Gründen nur bedingt aussagekräftig: Da die Angaben in den Akten anderen Prioritätensetzungen als der differenzierten Darstellung der Abfragen folgen, sind sie oft hinsichtlich der hier untersuchten Fragestellung unvollständig. So waren z.B. Beschlüsse zu Verbindungsdatenabfragen in einigen Fällen in den Akten nicht enthalten, die Sonderhefte aber nicht zugänglich. Dies zeigt sich in den Daten daran, dass z.B. wesentliche Angaben wie das Beschlussdatum bei ca. 5% der Beschlüsse nicht erfasst werden konnte und Angaben zu dem zeitlichen Ablauf der Abfragen (Beginn und Ende der Abfrage) bei ca. 20% der Beschlüsse fehlten. Gleichfalls problematisch sind aus diesem Grund auch die Angaben zu Erfolg/Misserfolg eines Auskunftsersuchens. Sie dürften gleichfalls, insbesondere im Falle eines Misserfolgs, nicht immer erwähnt sein. Zu beachten ist ferner, dass im Einzel-

fall auch ein negativer Bescheid (dass keine Daten vorlagen) die Ermittlungen vorantreiben kann.

Zusammenfassend ist festzuhalten, dass der Beginn des Abfragezeitraums hinsichtlich des Erfolgs der Abfrage kaum differenziert. Diese mangelnde Differenzierung weist darauf hin, dass der Abfragezeitraum selbst keinen wesentlichen Einfluss – zumindest keinen systematischen – auf den Erfolg der Abfragen hat. *Alleine* aus dem Abfragezeitraum und, daran angelehnt, der Wahrscheinlichkeit des Datenverlustes, können mithin auch keine Schutzlücken hergeleitet werden. Entscheidender dürften vielmehr spezifische Merkmale der jeweils konkreten Ermittlungssituation sein, etwa die Frage, ob es andere Ermittlungsansätze gibt oder nicht.

5. Aktuelle Bewertung

Zunächst ist feststellen, dass die aktuelle Situation nicht mit derjenigen während der Geltungsdauer der einstweiligen Verfügungen vergleichbar erscheint. Denn zum einen ist der rechtliche Anwendungsbereich der Verkehrsdatenabfrage jetzt wieder breiter, da das gesamte gesetzlich vorgesehene Tatspektrum, also insbesondere Anlasstaten gem. § 100g Abs.1 Nr. 2 StPO, für die der Zugriff auf Vorratsdaten zwischenzeitlich faktisch suspendiert war, wieder in Frage kommt; dasselbe gilt für die auch im Einzelfall erheblichen Nicht-Katalogtaten gem. § 100g Abs.1 Nr. 1 StPO. Zum anderen ist freilich zu berücksichtigen, dass auf der Basis des § 100g StPO nunmehr nur noch die Verkehrsdaten gem. § 96 TKG abgefragt werden können; gerade im Bereich der Straftaten gem. § 100g Abs. 1 Nr. 2 StPO wird die Abfrage mangels ausreichender Verfügbarkeit längerfristig zurückliegender retrograder Daten hier in vielen Fällen leerlaufen. Während somit für den Zeitraum der einstweiligen Anordnung objektiv Daten gespeichert waren, auf die die Ermittlungsbehörden in vielen Fällen nicht zugreifen durften, ist der Zugriff in diesen Fällen rechtlich nunmehr wieder möglich, scheitert aber häufig daran, dass faktisch keine oder keine vollständigen Daten mehr verfügbar sind. Daher können insbesondere die niedrigen Anteile erfolgsloser Abfragen während der Sondererhebung keinen Aussagewert für die gegenwärtige Situation beanspruchen. Siehe hierzu auch unten die Experteneinschätzungen in Teil F.

Die gegenwärtige Situation kann auch nicht eins zu eins mit dem Status quo ante aus der Zeit vor Inkrafttreten des Telekommunikationsüberwachungsneuregelungsgesetzes 2007 verglichen werden. Zwar decken sich – abgesehen von zahlreichen technischen Präzisierungen im Rahmen von § 113a TKG – die beiden Rechtsgrundlagen, was die erfassten Datenarten anbetrifft, im Wesentlichen (siehe oben Tabelle B-1). Zu beachten ist allerdings, dass die Speicherbefugnis bei § 96 TKG unter dem Vorbehalt der Abrechnungsrelevanz steht. Dies betrifft zum ersten die eingehenden Gespräche, deren Daten, abgesehen von einigen Roaming-Konstellationen, faktisch in Gänze wegfallen. Zum anderen sind auch Kundenbeziehungen mit Flatrates und Verbindungen mit Prepaid-Karten betroffen. Deren Verbreitung hat sich seit

der Zeit vor 2007 stark verändert. Dies lässt sich aus Informationen der Bundesnetzagentur ableiten, die im Wege einer Anfrage bei der Behörde eingeholt wurden. Danach ergibt sich, bezogen auf die wichtigsten Kommunikationsformen, das folgende Bild:

Die Nutzung von Flatrates unterscheidet sich entlang der verschiedenen Nutzungsformen. Am weitesten verbreitet sind sie bei der Internetnutzung. Dort wurden im Jahr 2009 87 % aller privaten Onlineverbindungen im Festnetz per Flatrate abgerechnet; 2007, also unmittelbar vor Beginn der Vorratsdatenspeicherung, hatte diese Quote noch bei 69 % gelegen.[130] Konkrete Rückschlüsse auf die Anzahl der betroffenen (statischen oder dynamischen) IP-Adressen, dem entscheidenden Anknüpfungspunkt für die Ermittlungsarbeit, können hieraus freilich nicht gewonnen werden. Zwei gegenläufige Effekte sind denkbar: zum einen kann eine IP-Adresse eine Vielzahl von Verbindungen bündeln (z.B. von anderen Familienangehörigen, die den gleichen Anschluss nutzen); zum anderen können im Rahmen einer Verbindung mehrere IP-Adressen einem Anschluss zugewiesen worden sein, insbesondere wenn die Verbindung nach einer gewissen Zeit der Inaktivität ab- und anschließend wieder aufgebaut wird. Annahmen dazu, in welchem Verhältnis beide Effekte zueinander stehen, können von hier aus nicht getroffen werden und wären reine Spekulation. Was freilich festzuhalten bleibt, ist der Umfang der allgemeinen Zunahme der Flatrates von 2007 zu 2009 um 26 %, womit die Wahrscheinlichkeit, dass Verkehrsdaten im Online-Bereich derzeit infolge mangelnder Abrechnungsrelevanz nicht oder nur kurzfristig gespeichert werden, um den entsprechenden Anteil zugenommen haben dürfte.

Etwas geringer ist die Verbreitung von Flatrates dann im Bereich der Festnetztelefonie. Die Bundesnetzagentur schätzt den Anteil der Festnetzkunden, die Flatratetarife nutzen, aktuell (Mai 2011) auf mehr als 80 Prozent.[131] Im ersten Quartal 2009 wurden etwas mehr als 60 % des leitungsvermittelten Gesprächsvolumens über Flatrates abgewickelt, 2007 lag dieser Anteil bei 50 %. Dies beinhaltet (leitungsvermittelte) Inlandsverbindungen, Auslandsverbindungen und Verbindungen in Mobilfunknetze. In absoluten Zahlen betrug das Flatratevolumen im Jahr 2009 vermutlich 99 Mrd. Minuten bzw. 72,2 Mrd. Minuten im Jahr 2007. Die Anzahl von Verbindungen wird nicht gesondert erfasst. Legt man wie die Agentur eine geschätzte durchschnittliche Gesprächsdauer von 4,5 Minuten pro Anruf aus, so dürften 2009 mutmaßlich ca. 22 Mrd. Verbindungen im Jahr 2009 und ca. 15,6 Mrd. Verbindungen im Jahr 2007 auf Flatrates entfallen.[132] Das würde eine Zunahme um 41 % bedeuten mit den entsprechenden Rückwirkungen, was das Risiko des teilweisen oder kompletten Ausfalls von Verkehrsdaten in dem Bereich der Festnetztelefonie betrifft.

---

130 Quelle: ARD/ZDF-Online-Studie 2005-2009, www.ard-zdf-onlinestudie.de/index.php?id=175 [Juni 2011].

131 Bundesnetzagentur, Referat IS16: Ergebnis der Datenerhebung: Speicherpraxis von Telekommunikationsverkehrsdaten (internes Papier vom 4.5.2011, am 6.04.2011 den Ministerien BMI, BMJ und BMWi präsentiert).

132 Persönlich übermittelte Zahlen; diese wurden im Hinblick auf die schätzungsbedingte Unsicherheit nicht in den Tätigkeitsbericht 2009 der Bundesnetzagentur aufgenommen. Der Tätigkeitsbericht 2010 enthält hierzu ebenfalls keine näheren Angaben.

Am niedrigsten ist die Nutzung von Flatrates im Mobilfunkbereich. Nach Berechnungen der Bundesnetzagentur wurden 2009 schätzungsweise zwei Drittel der in Mobilfunknetzen abgehenden Gespräche über eine Flatrate abgerechnet[133]; 2007 waren es erst ein Drittel. In absoluten Zahlen betrug das Volumen des Flatrateverkehrs im Jahr 2009 mehr als 45 Mrd. Minuten bzw. 22,6 Mrd. Minuten in 2007. Die Anzahl der Verbindungen wird auch hier nicht gesondert erfasst. Bei Zugrundelegung der von der Agentur geschätzten durchschnittlichen Gesprächsdauer von 2 Minuten pro Anruf gab es 2009 etwa 22,5 Mrd. Flatrateverbindungen, verglichen mit 11,3 Mrd. Verbindungen in 2007.[134] Das Aufkommen – und damit das Risiko des Datenausfalls – hätte sich damit im Hinblick auf Mobilfunkverbindungen in etwa verdoppelt.

Auf den Mobilfunkbereich konzentriert sich ferner die Problematik des Einsatzes von Prepaid-Karten. Auch insoweit können sich Fragen der Rechnungsrelevanz stellen, die an dieser Stelle nicht vertiefend behandelt werden können. Nach den von der Bundesnetzagentur veröffentlichen Zahlen nutzten Ende 2010 ca. 55 % der Teilnehmer eine vorausbezahlte SIM-Karte.[135] Der Anteil der Prepaid-Karten ist damit im Vergleich zu dem Jahr 2007 nur unwesentlich gestiegen; damals hatte der Anteil 55 % ausgemacht.[136] Im Einzelfall können auch hier Daten zu Dokumentationszwecken im Rahmen der meist automatisierten Billing-Vorgänge zumindest während einer kurzen temporären Speicherzeit vorhanden sein. Siehe hierzu auch die Auskünfte der Experten aus dem Bereich der TK-Anbieter (unten Teil F unter Pkt. 4.).

*Tabelle C-5: Spannweiten der Speicherzeiten in den Bereichen Mobilfunk, Festnetz, Internet, VoIP und E-Mail**

Tabelle 1	Speicherzeiten [Tage] (t-Spannweite bei NB&SP)			Speicherzeiten [Tage] (t-Spannweite bei NB&SP)				
		MobFu	Festnetz (analog/ISDN/VoIP)			Internet (DSL/Breitband)	VoIP	E-Mail
A1: Speicherung der Rufnummer des anrufenden Anschlusses	nicht pauschal abgerechnete Verbindungen	7 - 180	7 - 180	A2: zugewiesene Benutzerkennung	nicht pauschal abgerechnete Verbindungen	7 - 90	7 - 180	1 - 60
	Flatrate	7 - 120	7 - 180		Flatrate	7 - 90	7 - 90	
B1: Speicherung der Rufnummer des angerufenen Anschlusses	nicht pauschal abgerechnete Verbindungen	7 - 180	90 - 210	A2´: zugewiesene Internet-Protokoll-Adresse	nicht pauschal abgerechnete Verbindungen	2 - 90	7 - 30	1 - 60
	Flatrate	7 - 210	7 - 210		Flatrate	2 - 10	7 - 30	

*) Januar 2011. Quelle: Bundesnetzagentur (vgl. Fn. 131).

Die Bundesnetzagentur hat im Januar 2011 eine Erhebung zu der aktuellen Speicherpraxis ausgewählter TK-Anbieter durchgeführt, aus der sich Erkenntnisse zu den unterschiedlichen

133 Vgl. Bundesnetzagentur, Jahresbericht 2010, S. 87.

134 Vgl. Bundesnetzagentur, Tätigkeitsbericht Telekommunikation 2008/2009, S. 53.

135 Vgl. Bundesnetzagentur, Jahresbericht 2010, S. 83.

136 Vgl. Bundesnetzagentur, Jahresbericht 2009, S. 89.

Speicherzeiträumen sowie zu der durchschnittlichen Speicherdauer ergeben.[137]. Tabelle C-5 zeigt die Speicherdauer getrennt nach anrufenden und angerufenen Nummern. Die dargestellten Spannweiten ergeben sich aufgrund der unterschiedlichen Praxis der jeweiligen Anbieter.[138] Die Varianz ist in allen Dienstebereichen beträchtlich. Im Bereich der Telefonie liegen die Speicherzeiten hinsichtlich der Rufnummer des anrufenden Anschlusses (A-Teilnehmer) zwischen sieben und 180 Tagen, die Rufnummer des angerufenen Anschlusses (B-Teilnehmer) wird zwischen sieben und 210 Tagen gespeichert. Kürzere Speicherzeiten sind bei den internetorientierten Diensten wie DSL/Breitband, VoIP und E-Mail zu erkennen. Die zugewiesenen IP-Adressen werden in einem Zeitfenster zwischen zwei und 90 Tagen gespeichert; bei Flatrate-Tarifen zwischen zwei bis 30 Tagen. Die Speicherdauer bestimmt sich nach der Abwicklung der Rechnungsstellung zwischen Diensteanbietern und Endkunden sowie zwischen Netzbetreibern und Service Providern. Tabelle C-6 gibt ergänzend die durchschnittlichen Speicherzeiten für die entsprechenden Segmente wieder. Hier fällt eine relativ lange Speicherzeit der B-Teilnehmer im Bereich der Mobil- und Festnetztelefonie auf, selbst bei Flatratekunden. Im Bereich der IP-Adressen beschränkt sich die Verfügbarkeit hingegen auf wenige Tage. Dies sind freilich rechnerische Durchschnittswerte, die allenfalls eine gewisse Wahrscheinlichkeit andeuten, wie lange Ermittler im Bedarfsfalle mit dem Vorhandensein von Verkehrsdaten rechnen können. Bei den ausgewiesenen durchschnittlichen Speicherzeiten handelt es sich nämlich um die arithmetischen Mittelwerte[139], die die tatsächliche Verteilung nur beschränkt abzubilden vermögen. Sie sagen nichts über die Verteilung der realen Speicherzeiträume aus. Aussagekräftiger erscheinen daher die Mindestspeicherfristen, wie sie sich aus Tabelle C-5 ergeben.

*Tabelle C-6: Durchschnittliche Speicherzeiten in den Bereichen Mobilfunk, Festnetz, Internet, VoIP und E-Mail**

Tabelle 2	Durchschnittliche Speicherzeiten [Tage]				Durchschnittliche Speicherzeiten [Tage]				
		MobFu	Festnetz (analog/ISDN/BB)			Internet (DSL/Breitband)	VoIP	E-Mail
A1: Speicherung der Rufnummer des anrufenden Anschlusses	nicht pauschal abgerechnete Verbindungen	28	23	A2: zugewiesene Benutzerkennung	nicht pauschal abgerechnete Verbindungen	48	20	23
	Flatrate	28	22		Flatrate	47	20	
B1: Speicherung der Rufnummer des angerufenen Anschlusses	nicht pauschal abgerechnete Verbindungen	112	132	A2´: zugewiesene Internet-Protokoll-Adresse	nicht pauschal abgerechnete Verbindungen	4	7	22
	Flatrate	96	55		Flatrate	4	7	

*) Januar 2011. Quelle: Bundesnetzagentur (vgl. Fn. 131).

137 Siehe oben Fn. 131. Die Daten wurden vom 13.1.2011 bis zum 21.3.2011 bei insgesamt 16 Unternehmen erhoben, die in den Bereichen Festnetztelefonie, Mobiltelefondienst, Internet und E-Mail tätig sind; sie decken Marktanteile zwischen 85 und 100 Prozent ab.

138 Ähnliche Varianzen ergeben sich aus einer Aufstellung des LKA Niedersachsen; siehe unten Tabelle D-2.

139 Telefonische Auskunft des zuständigen Sachbearbeiters.

Was das quantitative Bild der Verkehrsdatenabfragen anbetrifft, so ist zu berücksichtigen, dass die justizielle Statistik stets nur solche Verfahren erfasst, in denen tatsächlich (mindestens) eine Verkehrsdatenabfrage erfolgte. Nicht enthalten sind diejenigen Fälle, in denen eine Abfrage wegen vermuteter Aussichtslosigkeit von vornherein unterbleibt. Wie hoch dieser Anteil gegenwärtig in der Praxis ist, kann nicht verlässlich abgeschätzt werden. Einerseits gibt es Dienststellen, die in aussichtslosen Fällen von vornherein von der Beantragung eines Beschlusses absehen, beispielsweise dann, wenn wegen Ablaufs der faktisch nur noch sehr kurzen mutmaßlichen Speicherfrist der Verlust der benötigten Daten erwartet wird. Ein gegenteiliger Effekt kann sich andererseits auf der Grundlage der ebenfalls in manchen Dienststellen vorzufindenden Praxis ergeben, jedenfalls in geeignet erscheinenden Fällen vermehrt bereits unmittelbar bei Aufnahme der Ermittlungen einen Beschluss zur Verkehrsdatenabfrage zu erwirken, um einem möglicherweise drohenden Datenverlust vorzubeugen. Siehe hierzu im Einzelnen unten die Experteneinschätzungen in Teil F. Die amtlichen Zahlen gem. § 100g Abs. 4 StPO für das Jahr 2010 sind noch nicht veröffentlicht.

Nicht erfasst sind ferner, weder in der amtlichen Statistik noch in der Sondererhebung, die Fälle mit ‚klassischen' Abhörmaßnahmen. Bekanntlich fallen bei der Inhaltsüberwachung auf der Grundlage von § 100a StPO die Verkehrsdaten mit an. Die hier analysierten statistischen Informationen zur Verkehrsdatenabfrage bilden mithin nur einen Teilbereich ab. In vielen Fällen kommen freilich beide Maßnahmen zum Einsatz. Nach den Ergebnissen der MPI-Studie 2008 war dies in 24 % der untersuchten Verfahren der Fall.[140] Dieser Anteil betrifft allerdings nur diejenigen Fälle, in denen – zumeist zur Vorbereitung einer nachfolgenden Inhaltsüberwachung (TKÜ)[141] – ein eigener Beschluss erwirkt wurde.[142] All diejenigen Fälle, in denen die Ermittlungsbehörden Verkehrsdaten auf der Grundlage einer Maßnahme nach § 100a StPO mit erheben und auswerten, werden nirgendwo gesondert erfasst. Diese Konstellation ist im Übrigen von der Problematik der Vorratsdatenspeicherung nicht berührt, da die Daten in diesen Fällen von den Behörden selbst erhoben werden. Dies ist allerdings nur im Hinblick auf Echtzeit- und zukünftig anfallende Daten möglich; retrograde Daten, die den größten Anteil der Abfragen ausmachen (siehe oben Schaubild C-2), können auf diese Weise nicht erfasst werden.

---

140 *Albrecht/Grafe/Kilchling* 2008, S. 285.

141 Vgl. *Albrecht/Grafe/Kilchling* 2008, S. 277ff., 292f., 336f.

142 Methodischer Ausgangspunkt der Untersuchung waren Beschlüsse gem. § 100g/h a.F. StPO.

Teil D: Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten, Ermittlungseffizienz und Aufklärungsquoten

1. Einleitung: Der Stellenwert von Verkehrsdaten (Vorratsdaten) für Aufklärungsquote und Aufklärungseffizienz

In der Begründung der Vorratsdatenspeicherung von Telekommunikationsdaten wird vor allem auf ihre Bedeutung für die Aufklärung und Aufklärbarkeit von schweren Straftaten Bezug genommen. Die Aufklärung eines Falles gilt als besonders relevanter Indikator für die Effizienz der Strafverfolgungsbehörden und das Ausmaß des Schutzes von zentralen Rechtsgütern durch das Strafrecht, wie eben die fehlende Aufklärung (und niedrige Aufklärungsquoten) als Sicherheitsprobleme indizierend gelten. Dabei wird in den Diskursen um die Relevanz von auf Vorrat gespeicherten Daten der Telekommunikation auch darauf hingewiesen, dass die Aufklärungsquote und ihre Interpretation sehr stark von dem jeweiligen Deliktstypus abhängig seien [143]. Ladendiebstähle oder die Beförderungserschleichung führen zum Beispiel deshalb zu hohen Aufklärungsquoten, weil hier mit der Registrierung eines Delikts nach einer Anzeige durch die Verletzten (oder Kontrollpersonal) in aller Regel gleichzeitig eine tatverdächtige Person sichtbar wird. Auch in verschiedenen Fallgruppen der Transaktionskriminalität, in denen direkte Opfer nicht vorhanden sind (beispielsweise Betäubungsmitteldelikte) wird die Registrierung von Straftaten häufig mit der Ermittlung eines Tatverdächtigen zusammenfallen. Die Aufklärungsquote ist in solchen Deliktsbereichen davon abhängig, in welchen Formen die Polizei ermittelt und ermitteln darf (reaktiv/proaktiv) und welche Ressourcen für polizeiliche Ermittlungen zur Verfügung gestellt werden. Hier geht es – wie bei Vorfelddelikten oder abstrakten Gefährdungsdelikten – um Sachverhalte, die bei einer nur reaktiven Strategie den Strafverfolgungsbehörden gar nicht bekannt würden. Die Aufklärungsquote als Indikator der Ermittlungseffizienz ist deshalb vor allem für solche Delikte von Bedeutung, bei denen die Anzeige eines Verletzten oder die Kenntnisnahme durch die Strafverfolgungsbehörden die Ermittlungen auslöst, nicht jedoch gleichzeitig zu der Benennung eines Tatverdächtigen führt.

Verkehrsdaten und Bestandsdaten hinter dynamisch vergebenen IP-Adressen erlauben verschiedene Einsatzstrategien in der Aufklärung von Straftaten. Dabei geht es bei auf Vorrat gespeicherten Verkehrsdaten um retrospektive Abfragen, die in Form von Suchläufen zur Identifizierung der Anschlüsse bzw. Anschlussinhaber, von denen aus ein bestimmtes Kommunikationsgerät kontaktiert worden ist oder die von einem bestimmten Gerät (Anschluss kontaktiert wurden, führen können. Funkzellenabfragen sollen bestimmte oder alle (aktiven) Geräte/Anschlüsse in einem definierten Raum und für eine bestimmte Zeit ermitteln, um da-

---

143 Vgl. bspw.: Aus einem Schriftwechsel des MDB Wolfgang Bosbach: http://wiki.vorratsdatenspeicherung.de/Position_von_Wolfgang_Bosbach [Juni 2011].

mit jedenfalls Ansätze für weitere Ermittlungen identifizieren zu können [144]. Die Abfrage von Bestandsdaten hinter einer dynamischen IP-Adresse zielt auf die Ermittlung von Personen, für die der der Verdacht vor allem von Urheberrechtsverletzungen oder des Herunter- oder Hochladens (Sich verschaffen, Besitz bzw. Verbreitung) von Kinderpornografie besteht. Grundsätzlich kommt für den Ansatz der Verkehrsdatenabfrage die gesamte Bandbreite der „Internetkriminalität" in Betracht.

Die Verkehrsdatenabfrage in Gestalt von Suchläufen nach Kontakten (bzw. mit den Kontakten zusammenhängenden Informationen wie Zeit, Ort oder Dauer) hat vor allem für Ermittlungen bei der Transaktionskriminalität Bedeutung. In Fällen des Betäubungsmittelhandels kann es um Ansatzpunkte für die Ermittlung von Abnehmern oder Verkäufern gehen; bei der Schleusung von Immigranten können Verkehrsdaten wie bei allen Bandendelikten über Gruppenstrukturen oder Transport- und Schmuggelwege Aufschluss geben. Allerdings wird auch bei Tötungsdelikten, Raub- oder Erpressungsdelikten ein Suchlauf nach Kontakten und dahinter stehenden Personen manchmal in Frage kommen. Für die Abfrage von Funkzellendaten wird darauf hingewiesen, dass hierdurch Ermittlungsansätze sowohl im Falle von Serientaten als auch Einzeltaten gewonnen werden können. Bei Serientaten geht es um die Verknüpfung verschiedener Tatorte über Verkehrsdaten[145], bei Einzeltaten können Funkzellenabfragen Ansatzpunkte für weitere Ermittlungen bieten, in denen Hinweise auf in der Nähe des Tatorts zur Tatzeit sich befindende Personen/Mobiltelefone für die Überprüfung der Personen im Hinblick auf einen möglichen Tatverdacht entstehen können. Spektakuläre Mord- und Mordversuchsfälle, wie beispielsweise die Fälle Mannichl[146], Moshammer[147], Holzklotzwurf[148] zeigen allerdings an, dass die Orientierung an Verkehrsdaten nicht nur zur Aufklärung nichts beitragen kann, sondern teilweise wohl auch dazu geeignet ist, die Ermittlungsressourcen in eine wenig ertragreiche Richtung zu lenken. Das Aufklärungspotenzial von Funkzellendaten wird ferner noch von weiteren Merkmalen abhängig gemacht (beispielsweise geographische Distanz der Tatorte)[149].

---

144 *Henrichs, A.*: Funkzellenauswertung. Rechtliche und taktische Aspekte der telekommunikativen Spurensuche. Die Kriminalpolizei 2010, www.kriminalpolizei.de/articles,funkzellenauswertung,1,275.htm [Juni 2011].

145 Instruktiv LG Rostock, 8. Große Strafkammer, Beschluss vom 16.10.2007, 19 Qs 97/07, Richterliche Anordnung des Eingriffs in das Fernmeldegeheimnis; Prüfung der Geeignetheit und Erforderlichkeit von Funkzellenabfragen.

146 Funkzellendaten ergaben hier keine Ermittlungsansätze (abgesehen davon, dass sie für Personen aus dem nahen Umfeld als Alibi interpretiert wurden).

147 Der Fall wurde über einen Abgleich der DNA und einen entsprechenden Treffer gelöst.

148 Im Fall des Holzklotzwurfs von einer Autobahnbrücke am 23. März 2008 in der Nähe von Oldenburg mit tödlichen Folgen wurden alle Gespräche und SMS, die an diesem Tag zwischen 17 und 22 Uhr geführt worden sind, abgefragt. Nach Medienberichten wurden etwa 12.000 Kontakte in die Analyse einbezogen. Der Fall wurde allerdings durch andere Ermittlungsansätze aufgeklärt.

149 Europolice vom 9.3.2010: www.euro-police noblogs.org/ 2010/03/ Funkzellenauswertung [Juni 2011].

2. Rechtspolitische Diskurse zu Zusammenhängen zwischen Vorratsdatenspeicherung, Aufklärung und Sicherheit

Die Debatten über den Zusammenhang zwischen Ermittlungseffizienz und auf Vorrat gespeicherten Telekommunikationsdaten sind derzeit durch die nachdrückliche Betonung der Bedeutung von Vorratsdaten für die Aufklärung spezifischer Delikte einerseits sowie ebenso deutliche Hinweise auf eine fehlende Datengrundlage für die Behauptung von Aufklärungsrelevanz andererseits gekennzeichnet. Hieraus resultieren Missverständnisse, vor allem aber Misstrauen. Als Beispiel (und stellvertretend für die laufenden rechtspolitischen Auseinandersetzungen) kann die Antwort auf eine Kleine Anfrage im Niedersächsischen Landtag aus dem Jahr 2010 herangezogen werden. Die Kleine Anfrage befasste sich mit der Notwendigkeit der Vorratsdatenspeicherung und suchte vor allem Auskunft zum Einfluss des Wegfalls der Vorratsdatenspeicherung nach der Entscheidung des Bundesverfassungsgerichts vom März 2010 auf Ermittlungseffizienz und die Aufklärungsquoten. In der Antwort wird zunächst und als Einleitung ausgeführt, dass die Vorhaltung von Telekommunikationsverkehrsdaten über einen gewissen Mindestzeitraum insbesondere für die Strafverfolgung und für die Abwehr erheblicher Gefahren im Bereich des Terrorismus und der organisierten Kriminalität sowie in Deliktsfeldern wie der Kinderpornografie von essenzieller Bedeutung sei. Dies ist nichts anderes als die allgemeine Begründung der europäischen Richtlinie 2006/24/EG und der Einführung der Vorratsdatenspeicherung in das deutsche Recht Ende 2007. Betont wird in den im Wesentlichen gleich lautenden Begründungen, dass konspirativ vorgehende Tätergruppen sich zunehmend der neuen Informations-/Kommunikationstechnologien bedienten, ein Argument, das seit Ende der 1980er Jahre die Debatten um die mit Organisierter Kriminalität zusammenhängenden Risiken und Ermittlungsprobleme kennzeichnet[150], jedoch im Kern nichts anderes besagt, als dass Personen, die in kriminellen Netzwerken und illegalen Märkten operieren, das Mobiltelefon, das Internet, Verschlüsselungstechniken in der Übertragung von Daten, eben die moderne Infrastruktur der Kommunikation nutzen. Etwas Anderes wäre auch völlig überraschend. Dass der Drogenhandel im Kilobereich detailliert via E-Mail-Verkehr abgestimmt und Kinderpornografie über Chatrooms im Internet weiter gegeben werde, besagt deshalb nur, dass heute gerade im Zusammenhang mit auf wirtschaftlichen (und anders motivierten) Transaktionen beruhender Kriminalität zusätzliche Informationen entstehen, die für die Aufklärung genutzt werden können. Dass deshalb aber der Zugriff auf Verkehrsdaten der Telekommunikation oder auf die IP-Adressen für die Aufklärung von Straftaten unabdingbar sei, ist damit nicht gesagt.

In der Antwort auf die Kleine Anfrage im niedersächsischen Parlament werden dann spezifische Delikte aufgegriffen, für die ein besonderer Bedarf an auf Vorrat gespeicherten Verkehrsdaten geltend gemacht wird. Besondere Bedeutung wird selbstverständlich der Vorrats-

---

150 *Albrecht, H.-J.*: Organisierte Kriminalität - Theoretische Erklärungen und empirische Befunde. In: Albrecht, H.-J., Dencker, F. u. a. (Hrsg.): Organisierte Kriminalität und Verfassungsstaat. Deutsche Sektion der Internationalen Juristen-Kommission. Rechtsstaat in der Bewährung. Bd. 33, Heidelberg 1998, S. 1-40.

datenspeicherung bei Ermittlungen in solchen Fällen zugesprochen, in denen elektronische Kommunikationsmittel bei Vorbereitung oder Durchführung einer Straftat eine Rolle gespielt haben. Dabei werden auch der sexuelle Missbrauch von Kindern und Straftaten gegen das Leben genannt. Des Weiteren werden Delikte wie Erpressungen, Bedrohungen, insbesondere die Nachstellung (Stalking), bandenmäßig begangene Delikte und/oder Taten, bei denen aufgrund kriminalistischer Erfahrungen im Zusammenhang mit den bisherigen Ermittlungen anzunehmen sei, dass mindestens zwei Täter im Rahmen der Tatvorbereitung und/oder Tatnachphase miteinander kommuniziert hätten, angegeben. Auch in Fällen von Brandstiftungen, Raubdelikten sowie der Ausspähung von Daten seien in der Vergangenheit entscheidende Ermittlungsansätze durch die Erhebung von Telekommunikationsdaten gewonnen worden. Gravierende Auswirkungen werden für den Wegfall der Vorratsdatenspeicherung im Bereich solcher Straftaten festgestellt, die mittels Telekommunikation und insbesondere über das Internet begangen werden, also bei der so genannten IuK-Kriminalität (wobei sich der Begriff im Wesentlichen decken wird mit den Begriffen der Cyber- und Computerkriminalität). Hervorgehoben wird, dass bei der Verfolgung von Internetkriminalität die IP-Adresse des Täters regelmäßig den einzigen Ermittlungsansatz darstelle. Zur Ermittlung der einer dynamischen IP zuzuordnenden Bestandsdaten müssten die Netzbetreiber auf Verkehrsdaten, die sogenannten Log-Files, zurückgreifen. Nach dem Wegfall der Vorratsdatenspeicherung würden diese Daten – mangels betrieblicher Speichererfordernisse – nicht mehr oder nur noch wenige Tage gespeichert. Eine retrograde Ermittlung des Nutzers einer bestimmten IP sei daher regelmäßig nicht mehr möglich. Der Wegfall der Vorratsdatenspeicherung betreffe daher insbesondere Verfahren wegen Verbreitung, Erwerb und Besitz kinder- und jugendpornographischer Schriften gemäß §§ 184b und 184c StGB. Erheblich beeinträchtigt würden auch Ermittlungen hinsichtlich mittels Telekommunikation begangener Bedrohungen oder Beleidigungen. Der jeweilige Anrufer könne durch Verkehrsdatenabfragen oft nicht ermittelt werden, weil die Kennung eines eingehenden Anrufs von dem Netzbetreiber entweder überhaupt nicht oder nur für wenige Tage gemäß § 96 Abs. 1 TKG gespeichert werde. Vergleichbare Probleme ergäben sich bei Ermittlungen wegen des Verdachts der Nachstellung (Stalking) mittels Telefonanrufen oder SMS gemäß § 238 Abs. 1 Nr. 2 StGB. Die Angaben des Opfers zu den bisherigen Kontaktversuchen des Täters würden zum Nachweis der „Beharrlichkeit“ der Nachstellung in der Regel nicht genügen. Aufgrund der entweder nur sehr kurzen Speicherzeiträume hinsichtlich Kennungen eingehender Anrufe und Anrufversuche bzw. der gänzlich unterbleibenden Speicherung dieser Daten werde ein belastbarer objektiver Nachweis der in der Vergangenheit erfolgten beharrlichen Nachstellung oftmals nicht mehr möglich. Im Bereich der Verfolgung der organisierten Kriminalität habe der Wegfall der Vorratsdatenspeicherung insgesamt massive Auswirkungen; denn diese Art der Kriminalität lebe von der schnellen Kommunikation zur gemeinsamen Planung und arbeitsteiligen Begehung schwerer Straftaten. Durch die zum Teil nur kurzen Speicherfristen bestünde insbesondere die Gefahr, dass aus der Auswertung retrograder Verkehrsdaten sich erschließende Zusammenhänge zwischen Einzeltaten, z. B. bei Serieneinbrüchen „reisender“ Tätergruppierungen,

nicht erkannt und damit auch die hinter den Einzeltätern agierenden hauptverantwortlichen (OK-)Täter nicht mehr identifiziert und verfolgt werden könnten[151].

Die in der Antwort angegebenen Gefahren und die darin enthaltenen Annahmen über Auswirkungen auf die Ermittlungsarbeit sowie die Aufklärungsmöglichkeiten sollten durch empirische Daten belegbar sein. Jedenfalls bedürfte es nachvollziehbarer Informationen, die über die Erfassung der zentralen Kennzeichen der Ermittlungen in den genannten Bereichen entstehen. Eine solche Erfassung ist allerdings weder implementiert, noch ist eine solche Erfassung angedacht. Insoweit ist auch verständlich, dass auf die Frage 2 der Anfrage: „Welche und wie viele Straftaten konnten dadurch (Rückgriff auf Vorratsdaten) aufgeklärt oder verhindert werden?“ geantwortet wird: „Für den Bereich der niedersächsischen Polizei sowie der Staatsanwaltschaften gilt Folgendes: Aufgrund einer fehlenden Erfassung kann hierzu keine Aussage getroffen werden“. Die dritte Frage („Hat sich durch die Vorratsdatenspeicherung bzw. den Rückgriff auf die Daten bei Verdacht einer Straftat die Aufklärungsquote in Niedersachsen signifikant verändert?“) wird mit einem Verweis auf die Antwort zu Frage 2 beschieden. Dies bedeutet auch, dass die eingangs getroffenen Feststellungen jedenfalls an Hand von systematischer Datenanalyse nicht substantiiert werden können.

Im Kern enthalten die Antworten auf die Fragen 2 und 3 der Kleinen Anfrage also zwei Aussagen:

(1) Auf Vorrat gespeicherte Telekommunikationsdaten sind unabdingbar für die Aufklärung vor allem schwerer Kriminalität, allerdings auch solcher Straftaten, die mittels Internet oder Telekommunikation begangen werden.

(2) Über die Auswirkungen der Vorratsdatenspeicherung und den Wegfall der Vorratsdatenspeicherung auf die Aufklärung von Straftaten (wie immer die Frage der Aufklärung auch gestellt wird) ist nichts bekannt, da entsprechende Daten nicht erhoben werden.

Die Aussage, es sei nichts bekannt, ist jedoch zu relativieren. Denn aus der Antwort ergibt sich immerhin, dass die niedersächsische Polizei für den Zeitraum vom 1. Juli 2010 bis zum 10. November 2010 eine interne Erhebung durchgeführt habe. Diese Datensammlung habe ergeben, dass bei den – für diesen Zeitraum – 454 gemeldeten Straftaten, in denen es aus Ermittlungsgründen erforderlich gewesen wäre, die Verbindungsdaten zu erheben, 409 Taten gar nicht mehr bzw. nur noch unzureichend aufgeklärt werden konnten. Dieser Umstand belege, dass für eine Vielzahl von Straftaten Verkehrsdaten den einzigen Ermittlungsansatz darstellten und nach Wegfall der Vorratsdatenspeicherung nicht mehr bzw. nur wesentlich erschwert aufgeklärt werden könnten[152]. Für die niedersächsische Verfassungsschutzbehörde

---

151 Niedersächsischer Landtag − 16. Wahlperiode Drucksache 16/3056, Kleine Anfrage mit Antwort. Wie weiter mit der Vorratsdatenspeicherung?, S. 4f.

152 Niedersächsischer Landtag − 16. Wahlperiode Drucksache 16/3056, Kleine Anfrage mit Antwort Wie weiter mit der Vorratsdatenspeicherung?, S. 6.

wird mitgeteilt, dass diese zwischen dem 24. Januar 2009 und dem 2. März 2010 vier Mal Daten, die nach § 113 a des Telekommunikationsgesetzes gespeichert wurden, abgefragt habe. Die Antwort ergibt im Übrigen auch, dass von den Staatsanwaltschaften des Landes Niedersachsens im Jahr 2008 in insgesamt 766 Verfahren (1208 Anordnungen) und im Jahr 2009 in 679 Verfahren (1.441 Anordnungen) Verkehrsdaten nach §100g StPO abgefragt worden sind. Mitgeteilt wird hierzu: „Eine Erfassung der Fälle, in denen in der Zeit vom 1. Januar 2008 bis zum 2. März 2010 im Rahmen von Verkehrsdatenerhebungen gemäß § 100g Abs. 1 StPO auf nach § 113a TKG vorsorglich gespeicherte Daten (sogenannte Vorratsdaten) zurückgegriffen wurde, ist nicht erfolgt. Entsprechende Zahlen können daher nicht mitgeteilt werden“ [153]. Dies bedeutet auch, dass an die Europäische Kommission für Zwecke der Evaluation der Richtlinie 2006/24/EG aus Deutschland keine Daten mitgeteilt werden konnten, die sich spezifisch auf die Nutzung auf Vorrat gespeicherter Verkehrsdaten beziehen.

Auch die im Zusammenhang mit einer Anfrage im Bundestag von 2010 bekannt gewordenen Informationen aus Erhebungen des Bundeskriminalamts, die sich auf den Zeitraum zwischen März und September 2010 beziehen, sind für die Abschätzung der Auswirkungen des Wegfalls der Vorratsdatenspeicherung auf die Aufklärungsquoten nicht geeignet[154]. Denn Bezugszahlen zu den in der Antwort genannten Abfragen, die erfolglos geblieben seien, sind nicht enthalten. Ferner ergeben sich keine Hinweise darauf, warum in einem Ermittlungsverfahren der einzige Schlüssel zur Aufklärung (bzw. zur Anklagefähigkeit) Verkehrsdaten gewesen sein sollen. Schließlich zeigt die Informationsaufbereitung, dass sich die Abfragen im Wesentlichen auf Bestandsdaten (hinter einer dynamischen IP-Adresse) und ganz überwiegend auf Verbreitung oder Besitz von Kinderpornografie beziehen, und dass der Zeitraum zwischen Nutzung einer dynamischen IP-Adresse und der Abfrage nicht bekannt sei.

Die Debatte um die Evaluation der Richtlinie 2006/24/EG durch die Europäische Kommission dokumentiert ebenfalls die Probleme, die sich bei einer nachvollziehbaren und überzeugenden Evaluation stellen. Die Debatten verweisen 2009 und 2010 immer wieder darauf, dass die Kommission zum Herbst 2010 – wie durch die Richtlinie vorgesehen – eine Evaluation habe vorlegen wollen. Tatsächlich gab es bis dahin lediglich Hinweise darauf, dass eine solche Evaluation noch nicht stattgefunden hat. Vorläufige Berichte deuteten bereits darauf hin, dass eine nachvollziehbare und überzeugende Evaluation auch nicht stattfinden konnte. Dies ergibt sich nicht zuletzt aus den vorstehend dokumentierten Informationen aus der Beantwortung der Kleinen Anfrage in Niedersachsen. Denn wenn Deutschland bis Ende 2010 die In-

---

153 So auch die Antwort auf eine Anfrage im Hamburger Senat, Bürgerschaft der Freien und Hansestadt Hamburg Drucksache 19/7389, 19, Wahlperiode 01. 10. 2010.

154 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Jan Korte, Ulla Jelpke, Petra Pau, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 17/3721 – Verfügbarkeit von Telekommunikationsverbindungsdaten seitens des Bundeskriminalamts und Rückschlüsse auf eine „Schutzlücke“ bei der Verbrechensbekämpfung. Deutscher Bundestag Drucksache 17/3974, 17. Wahlperiode 29. 11. 2010; vgl. im Übrigen Bundeskriminalamt: Stand der statistischen Datenerhebung im BKA sowie der Rechtstatsachensammlung für Bund (BKA, BPOL, ZKA) und Länder zu den Auswirkungen des Urteils des Bundesverfassungsgerichts zu Mindestspeicherungsfristen, Wiesbaden, Stand: 17.09.10.

formationen nicht besaß, die Auskunft geben könnten über den Einfluss der Vorratsdatenspeicherung auf die Aufklärungseffizienz oder die Effizienz der Gefahrenabwehr, wie sollte dann eine solche Aussage für die Europäische Union insgesamt möglich sein. Denn tatsächlich verfügt Deutschland, verglichen mit anderen Mitgliedsstaaten der Europäischen Union um eines der besten statistischen Erfassungssysteme im Bereich des Strafrechts und des Strafverfahrens. Allerdings ergibt sich aus der Informationsgrundlage ganz klar, dass in Deutschland Daten, die zur Beschreibung und zur Analyse der Vorratsdatenspeicherung dienen könnten, gar nicht erhoben worden sind.

Bereits das im Sommer 2010 durch Indiskretionen der Öffentlichkeit bekanntgewordene Dokument, das auch die bis dahin vorliegenden Datengrundlagen für eine Evaluation der Richtlinie 2006/24/EG beschreibt[155], unterstreicht lediglich, wie auch das nunmehr offizielle Evaluationsdokument[156], dass die europaweite Situation sich von der deutschen Datengrundlage nicht unterscheidet. Die im Europäischen Parlament zur Evaluation gestellten Anfragen und die Antworten belegen dies nachdrücklich. In einer Antwort auf eine Anfrage im Europäischen Parlament vom 9. September 2010 wies die Kommission darauf hin, dass die Evaluation fortgesetzt werde, und dass es zu früh sei, über mögliche Ergebnisse und Schlussfolgerungen hieraus zu spekulieren. In einer Antwort auf eine Anfrage vom 11. November 2010 (E-7009/2010) sagte die Kommission, dass die Mitgliedstaaten am 27. Juli (2010) angeschrieben worden seien, um zusätzliche Informationen zu erlangen, wie die gespeicherten Daten in der Praxis genutzt werden und welche konkreten Auswirkungen sie auf Strafverfolgungsmaßnahmen haben. Aus den Statistiken, die die Mitgliedstaaten vor dieser Anfrage zur Datenermittlung zur Verfügung gestellt hätten, ginge aber bereits hervor, dass die gespeicherten Daten in der ganzen EU jährlich millionenfach angefordert würden. Es sei aber nicht ersichtlich, ob und wie diese Daten zu Strafverfolgungsergebnissen geführt hätten. In der Beantwortung einer Anfrage vom 14. September 2010 sagte die Kommission am 18. November 2010 (E-5059/2010) wiederum, dass ihr bewusst sei, dass die Vorratsdatenspeicherung für die Behörden ein wichtiges Instrument darstelle und ihr Nutzen in einem angemessenen Verhältnis zu den Kosten für den Privatsektor und den Folgen, insbesondere im Hinblick auf Bürgerrechte und Datenschutz, stehen müsse. Auch hier wurde darauf verwiesen, dass eine Bewertung noch nicht abgeschlossen sei und deshalb auf Ergebnisse nicht eingegangen werden könne. Jedoch wird, ohne dass sich die Evaluationsgrundlagen bis dahin verändert hätten, am 3. Dezember anlässlich einer Konferenz zu der Richtlinie 2006/24/EG vorgetragen, dass sich die Vorratsdatenspeicherung bewährt habe und dass die Vorratsdatenspeicherung zur Bekämpfung der Kriminalität nützlich sei. Denn, so die simple Analyse und Schlussfolgerung: Die Strafverfolgungsbehörden hätten nicht millionenfach Verkehrsdaten abgefragt (durchschnittlich 148.000 Fälle der Abfrage pro Mitgliedsland für 2008/2009), wenn sie davon keinen

---

155 Room Document: Evaluation of Directive 2006/24/EC and of National Measures to Combat Misuse and Anonymous Use of Electronic Communications, Brüssel, Juni 2010.

156 Report From the Commission to the Council and the European Parliament: Evaluation Report on the Data Retention Directive (Directive 2006/24/EC), Brüssel, 18. 4. 2011, COM (2011) 225 final.

Nutzen gehabt hätten. Mitgliedsländer hätten mitgeteilt, dass Verkehrsdaten in bis zu 86% aller Verfahren, die zur Anklage geführt hätten, abgefragt worden seien. Die Vorratsdatenspeicherung habe deshalb einen substanziellen Beitrag zur Sicherheit in Europa geleistet[157].

Tatsächlich sind die der Kommission vorliegenden und die Grundlage des Evaluationsberichts bildenden Informationen aus den Mitgliedsländern nicht für eine systematische Evaluation geeignet (obwohl der Zeitraum zwischen 2006 und 2010 durchaus ausreichend gewesen wäre, eine Datenerhebung vorzubereiten, die jedenfalls einfache Beschreibungen der Nutzung auf Vorrat gespeicherter Verkehrsdaten zugelassen hätte). Der Hinweis darauf, dass auf Vorrat gespeicherte Verkehrsdaten in der Europäischen Union jährlich millionenfach abgefragt und genutzt werden, zeigt, dass in den Datensätzen nicht zwischen dem Zugriff auf Verkehrsdaten, dem Zugriff auf eine Kombination zwischen Verkehrs- und Bestandsdaten (im Falle dynamischer IP-Adressen) und dem einfachen Zugriff auf Bestandsdaten unterschieden wird. Denn ein millionenfacher Zugriff kann sich nur dann ergeben, wenn die (einfache) Bestandsdatenabfrage eingeschlossen wird. Ferner zeigt dies auch, dass nicht unterschieden wird zwischen einer regulären Verkehrsdatenabfrage und dem Zugriff von auf Vorrat gespeicherten Verkehrsdaten. Der Hinweis auf die Nachforderung von Daten aus den Mitgliedsstaaten, die den Einfluss des Zugriffs auf gespeicherte Verkehrsdaten auf die Aufklärung von Straftaten belegen sollen, lässt erkennen, dass bis zu diesem Zeitpunkt (etwa 3 Monate vor der geplanten Fertigstellung der Evaluation) gar nicht an diese Kernfrage gedacht worden war.

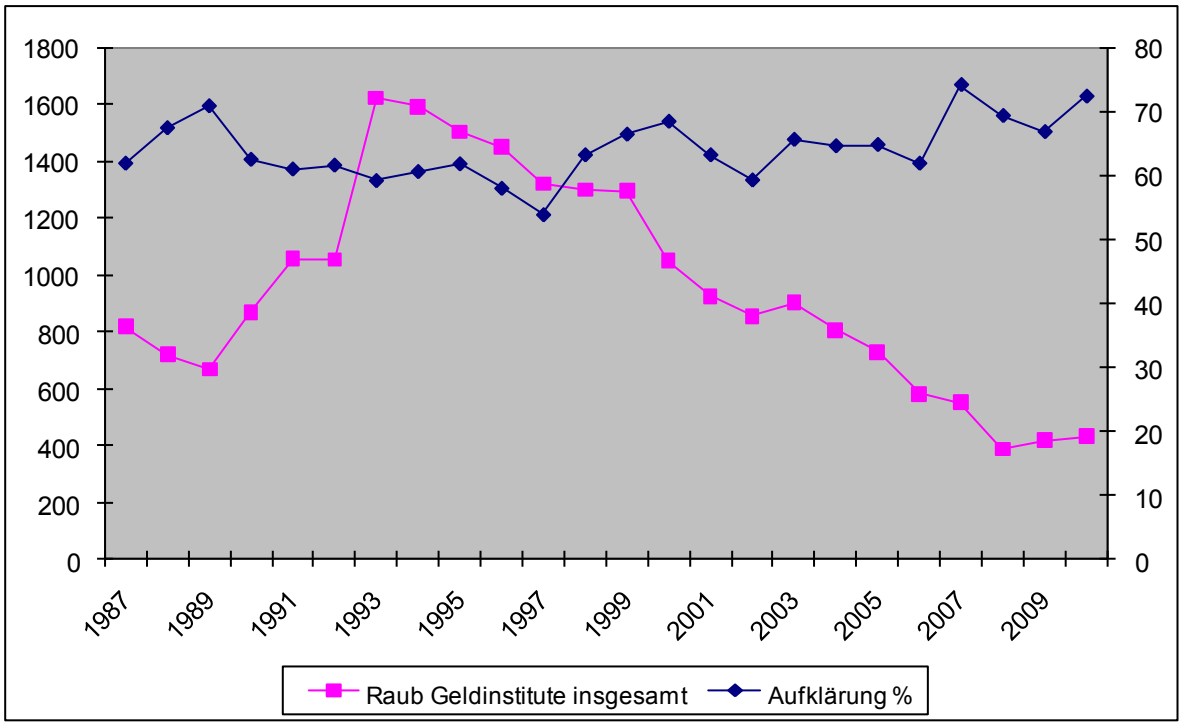
3. Quantitative Analysen und Einzelfallbetrachtungen

In den Auseinandersetzungen um die Vorratsdatenspeicherung treffen zwei Diskurse aufeinander, die einerseits auf die quantitativ bedeutsamen Folgen der Vorratsdatenspeicherung in Form der Entwicklung der Aufklärungsquoten sowie in diesem Zusammenhang den Gebrauch von Vorratsdaten abheben, zum andern um eine Perspektive, die an Einzelfällen orientiert (und den gesunden Menschenverstand bemühend) die Bedeutung von Verkehrsdatenabfragen für Ermittlungen hervorhebt und die Einzelfälle mit Begriffen wie „oft“ und „typisch“ zusammenführt, wobei offengelegt wird, dass quantitativ nutzbare Daten, die das „Typische“ oder „Häufige“ belegen könnten, nicht vorhanden sind (weil sie eben nicht erfasst werden oder nicht erfasst werden können).

---

157 *Cecilia Malmström*, Member of the European Commission responsible for Home Affairs: Taking on the Data Retention Directive European Commission conference in Brussels, 3. Dezember 2010.

*Schaubild D-1: Raubüberfälle auf Geldinstitute insgesamt und Aufklärung (%)**



*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

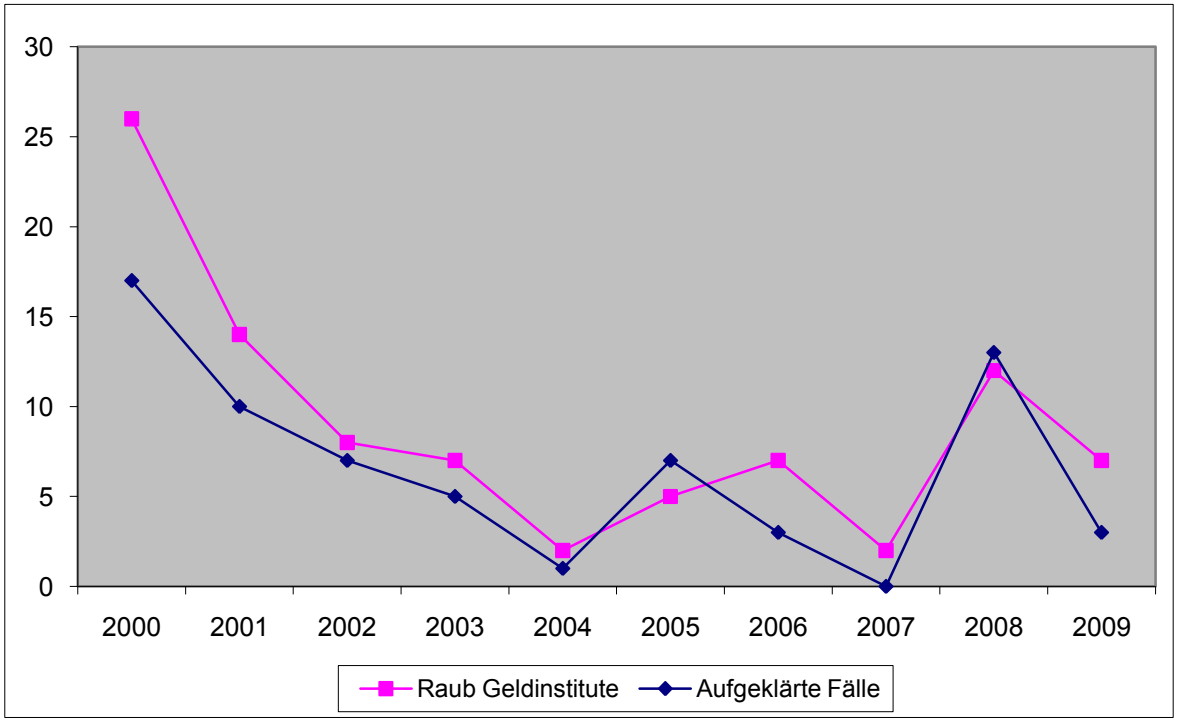
Die Einzelfallbezogenheit der Argumentation zeigt sich beispielsweise in einem Bericht des Innenministers des Landes Thüringen vom 29.7.2010. Der Minister erklärte, dass er der EU-Kommission für Zwecke der Evaluation zwei Fallberichte zugeleitet habe, die belegten, dass die Vorratsdatenspeicherung unverzichtbar sei. Dabei handelt es sich um eine Raubserie, die mehrere Täter einschloss, die bei Begehung der Taten miteinander Kontakt über Mobiltelefone hielten, und die an Hand von über Verkehrsdaten ermittelten Kontaktmustern, Standortdaten, Bewegungsprofilen und einer darauf gestützten Inhaltsüberwachung der Telekommunikation hätten identifiziert werden können. Dies wird als eine typische Fallkonstellation (wohl des Bankraubs) bezeichnet, angesichts der geringen Zahl der Banküberfälle in Thüringen eine mehr als kühne Behauptung (vgl. Schaubild D-2). Zum anderen geht es um einen Fall des Drogenhandels und damit verbunden um einen Auftragsmord. Über Verkehrsdaten des Tatverdächtigen des Auftragsmords sei versucht worden, die Täter zu identifizieren, was nicht gelungen sei, weil der Zugriff auf für sechs Monate gespeicherte Daten für eine „umfassende Analyse“ nicht ausgereicht habe (warum länger als 6 Monate zurückreichende Verkehrsdaten (die ja auch gar nicht gespeichert worden wären) die Ermittlungen hätten befördern können,

wird aber nicht mitgeteilt). Allerdings habe die Polizei in diesem Verfahren schwere Drogenhandelsfälle aufklären können[158].

Blickt man nun auf die Entwicklung der Aufklärungsquoten bei Raubüberfällen auf Geldinstitute (einschließlich Postfilialen), dann zeigt sich ein gleich bleibender Verlauf, wobei die Schwankungen gerade in den 1990er Jahren wohl eher durch Besonderheiten in den Neuen Bundesländern bedingt gewesen sein dürften. Im Jahr 2007, als Vorratsdaten noch nicht zur Verfügung standen, wird die bislang höchste Aufklärungsquote dokumentiert. Im Jahr danach, in dem auf Vorratsdaten zurückgegriffen werden konnte, geht die Aufklärungsquote zurück, ebenso wie im Jahr 2009, während im Jahr 2010 wiederum ein Zuwachs in der Aufklärung festzustellen ist.

Geht man auf die Ebene des Landes Thüringen, so ergibt sich für den Raub bei Geldinstituten das folgende Bild (Schaubild D-2).

*Schaubild D-2: Raubüberfälle auf Geldinstitute in Thüringen und aufgeklärte Fälle (N)**



*) Quelle: Landeskriminalamt Thüringen: Polizeiliche Kriminalstatistik. Jena 2010.

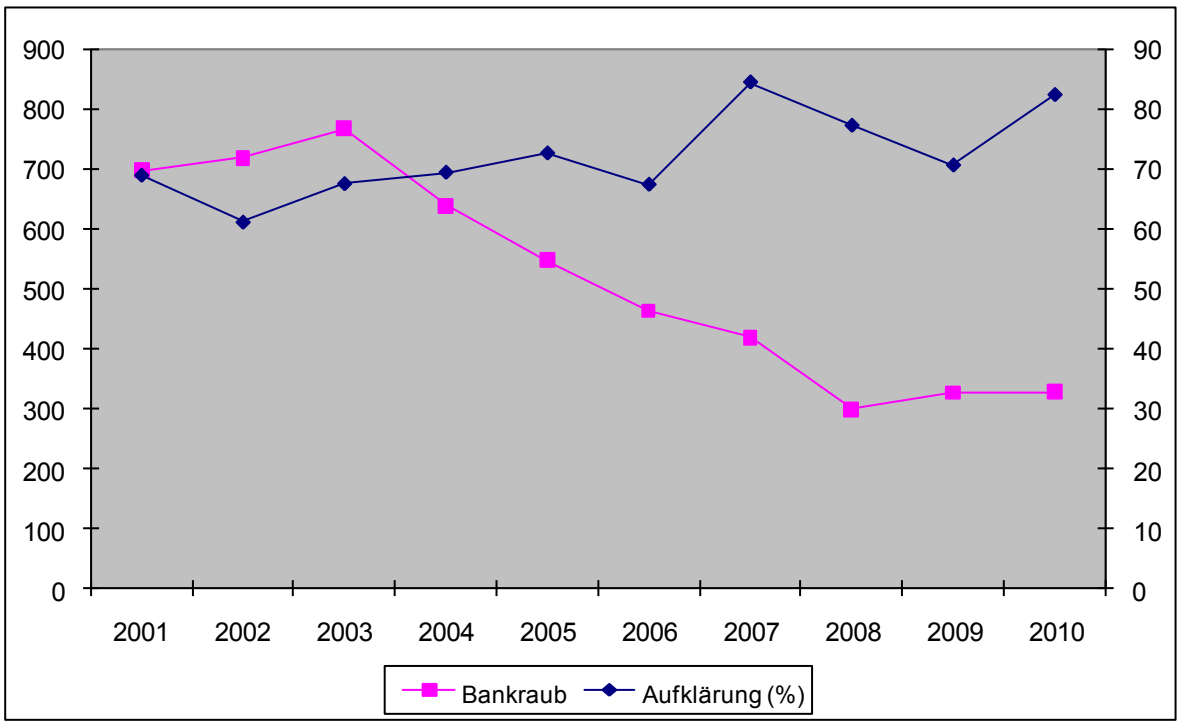
Die absoluten Zahlen des Raubs bei Geldinstituten und die absolute Zahl aufgeklärter Fälle liegen im Zeitraum 2000 bis 2009 sehr eng beieinander. Auch hier deutet nichts darauf hin, dass durch die Vorratsdatenspeicherung und den Rückgriff auf die Vorratsdatenspeicherung eine grundsätzliche Veränderung der Aufklärung in Gang gekommen wäre. Es handelt sich

158 www.jenapolis.de/71302/vorratsdatenspeicherung-bei-schweren-straftaten-oft-unverzichtbar-um-taeter-ermitteln-zu-koennen/ [Juni 2011].

dabei um eine insgesamt recht hohe Aufklärungsquote (durchschnittlich über 2000 – 2009 68% bei einer Standardabweichung von knapp 40), die tatsächlich durch Einzelfälle (wegen der geringen Gesamtzahl an Fällen) beeinflussbar ist. Dies ergibt sich allerdings nicht nur für den Zeitraum 2008-2009, sondern für das gesamte Jahrzehnt. Denn auch in den Vorjahren kam es zu Einzeljahren in denen nahezu alle oder alle Überfälle auf Geldinstitute hatten aufgeklärt werden können.

Auch wenn nur der Banküberfall im engeren Sinne für Deutschland insgesamt betrachtet wird, ergibt sich ein Bild der Entwicklung der Aufklärungsquoten, das mit den bisherigen Ausführungen stimmig ist.

*Schaubild D-3: Banküberfälle (nur Banken und Sparkassen) und Aufklärung (%)**

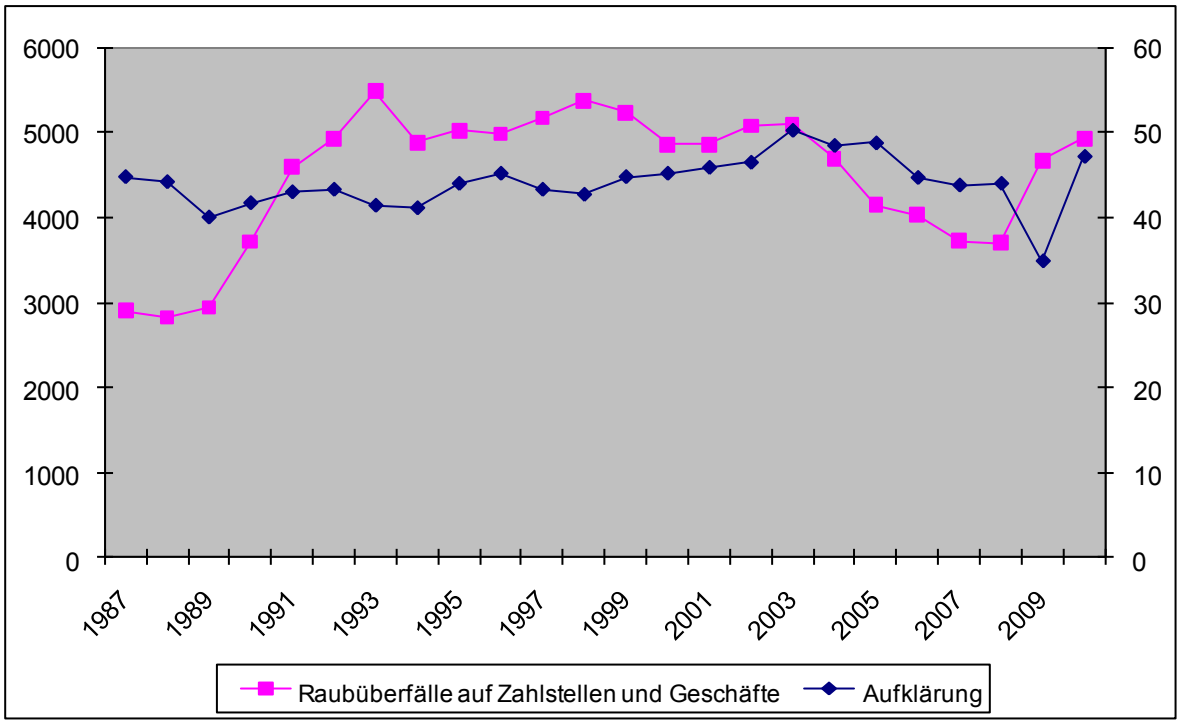


*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

Die Zahl der Banküberfälle geht deutlich zurück. Die Aufklärungsquote nimmt tendenziell bis zum Jahr 2007 zu, um dann (mit dem Beginn der Vorratsdatenspeicherung) zurückzugehen und im Jahr 2010 wieder anzusteigen. Die Zeitreihen geben keinen Hinweis auf durch Vorratsdaten der Telekommunikation bedingte Veränderungen.

Die Entwicklungen bei Raubüberfällen auf „sonstige Zahlstellen und Geschäfte“ verweisen auf vergleichbare Verläufe.

*Schaubild D-4: Raubüberfälle auf sonstige Zahlstellen und Geschäfte sowie Aufklärung (%)**



*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

Die Aufklärungsquote nimmt in dieser Fallgruppe seit Anfang des neuen Jahrtausends ab, nach einem tendenziellen Anstieg bis etwa 2001. Die Erklärung der starken Abnahme der Aufklärungsquote zwischen 2008 und 2009 dürfte wohl in dem ebenso starken Anstieg der Raubüberfälle auf sonstige Zahlstellen und Geschäfte und damit unter Umständen zusammenhängenden veränderten Begehungsformen zu suchen sein. Im Jahr 2010 erreicht die Aufklärungsquote wiederum das Niveau der Zeit vor 2009.

Nun schließt eine solche quantitative Betrachtung selbstverständlich nicht aus, dass Einzelfälle, wie die vom Innenminister Thüringens mitgeteilten Fälle, beobachtet werden können, in denen Verkehrsdaten (und speziell auf Vorrat gespeicherte Verkehrsdaten) zur Aufklärung eines einzelnen Falls beigetragen haben (oder hätten beitragen können). So wird auch in einer Untersuchung der (repressiven) Rasterfahndung ein Fall mitgeteilt, in dem eine Kombination von verschiedenen Datenquellen (Telekommunikationsinhaltsüberwachung, Funkzellendaten und Spielcasinobesucherdaten) zur Aufklärung des Tatgeschehens geführt hat[159]. Allerdings wirken sich solche Einzelfälle nicht auf die Gesamttendenz in der Entwicklung der Aufklärungsquoten aus.

---

159 *Pehl, D.*: Die Implementation der Rasterfahndung. Berlin 2008, S. 162 ff.

4. Die Entwicklung der Aufklärungsquoten bei einzelnen Delikten in Deutschland

4.1. Einführung

Nur wenige Untersuchungen befassen sich in systematischer Art und Weise mit der Beschreibung und Erklärung der Aufklärung von Straftaten bzw. mit der Frage, was einzelne Ermittlungsmaßnahmen zur Aufklärung beitragen[160]. Dabei ist klar, dass die Aufklärungsquoten seit den 1960er Jahren deutlich gesunken sind[161]. Erst in neuerer Zeit werden in empirischen Untersuchungen einzelne Ermittlungsansätze (verdeckte Ermittlungen) auch im Zusammenhang mit ihren Auswirkungen auf Aufklärungsquoten und Anklage- bzw. Verurteilungsraten aufgegriffen[162]. Im Zusammenhang mit den gerade für die Vorratsdatenspeicherung besonders herausgehobenen Phänomenen des Terrorismus und der organisierten Kriminalität ist die Aufklärungseffizienz ebenfalls kaum in der empirischen Forschung thematisiert worden. Eine Ausnahme stellt insoweit die Untersuchung von Kinzig zur Bewältigung von Strafverfahren wegen organisierter Kriminalität dar, wo auch zur Effizienz verdeckter Ermittlungsmaßnahmen für die Aufklärung und zur Einordnung der Verkehrsdatenabfrage im Kontext verschiedener Ermittlungsmaßnahmen Stellung genommen wird[163]. Die Untersuchung zeigt, dass bei Ermittlungen in Fällen organisierter Kriminalität in aller Regel verschiedene verdeckte Ermittlungsmaßnahmen kombiniert genutzt werden, wobei der Inhaltsüberwachung der Telekommunikation in Verfahren wegen organisierter Kriminalität die größte Bedeutung zukommt. Dies folgt auch daraus, dass Betäubungsmitteldelikte in der Zusammensetzung organisierter Kriminalität die größte Rolle spielen. Hieraus ergibt sich nicht, dass der Verkehrsdatenabfrage eine entscheidende Rolle zukommt oder gar in einzelnen Verfahren den einzigen Ermittlungsansatz repräsentiert.

---

160 Vgl. aber *Greenwood, P. W., Chaiken, J., Petersilia, J.*: The criminal investigation process. Lexington 1977, wo eine umfassende empirische Untersuchung zur Frage der Bedingungen erfolgreicher Aufklärung durchgeführt worden ist. Allerdings blieb diese Untersuchung eine Ausnahme und bietet auch heute noch international den Bezugspunkt für Analysen der Aufklärungseffizienz, vgl. hierzu beispw. *Liederbach, J., Fritsch, E. J., Womack, C. L.*: Detective workload and opportunities for increased productivity in criminal investigations. Police Practice and Research 12 (2011), S. 50-65, S. 50. Für den Bereich der konventionellen Kriminalität folgt aus der Untersuchung, dass die Aufklärung maßgeblich von den Informationen abhängig ist, die ein Opfer/Anzeigeerstatter in einer ersten Vernehmung den Ermittlern zur Verfügung stellen kann. Anschließende Ermittlungen erbringen demgegenüber kaum zusätzliche Beträge für die Aufklärung; vergleichbare Ergebnisse in *Dölling, D.*: Die Dauer von Strafverfahren vor den Landgerichten. Köln 2000.

161 Vgl. *nur Blinkert, B.*: Kriminalität als Modernisierungsrisiko? Das „Hermes-Syndrom" der entwickelten Industriegesellschaften. Soziale Welt 39(1988), S. 397-412; *Ahlberg, J.*: Crime clearance and efficiency. An analysis of the factors affecting trends in the clear-up rate. Stockholm 2002.

162 *Albrecht, H.-J., Dorsch, C., Krüpe, C.*: Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen. Freiburg 2003; *Meyer-Wieck, H.*: Der Große Lauschangriff – eine empirische Untersuchung zu Anwendung und Folgen § 100c Abs. 1 Nr. 3 StPO. Berlin 2005; *Pehl, D.*: Die Implementation der Rasterfahndung – Eine empirische Untersuchung der gesetzlichen Regelungen zur operativen Informationserhebung durch Rasterfahndung. Freiburg 2008; *Albrecht, H.-J., Grafe, A., Kilchling, M.*: Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO. Berlin 2008.

163 *Kinzig, J.*: Die rechtliche Bewältigung von Erscheinungsformen organisierter Kriminalität. Berlin 2004, insb. S. 443 ff.

Die in der Polizeilichen Kriminalstatistik mitgeteilten Informationen erlauben es, die Entwicklung der Aufklärung langfristig zu betrachten. Im Folgenden sollen diese Entwicklungen deliktsspezifisch vorgestellt und, soweit möglich, in den Zusammenhang mit verfügbaren Erkenntnissen zu Aufklärungsquoten (und der in ihnen enthaltenen Informationen) gestellt werden. Einbezogen werden auch die Sachverhalte, die vom Bundeskriminalamt für den Zeitraum nach der Entscheidung des Bundesverfassungsgerichts als Hinweis für den Bedarf an Vorratsdaten registriert worden sind[164].

Bei der Auswahl der Delikte handelt es sich einerseits um solche Straftatbestände, die sehr stark mit der Nutzung des Internets bzw. der Informationstechnologie korrelieren, zum anderen um Kapitaldelikte, die wegen ihrer Schwere besondere Relevanz besitzen.

4.2. Softwarepiraterie

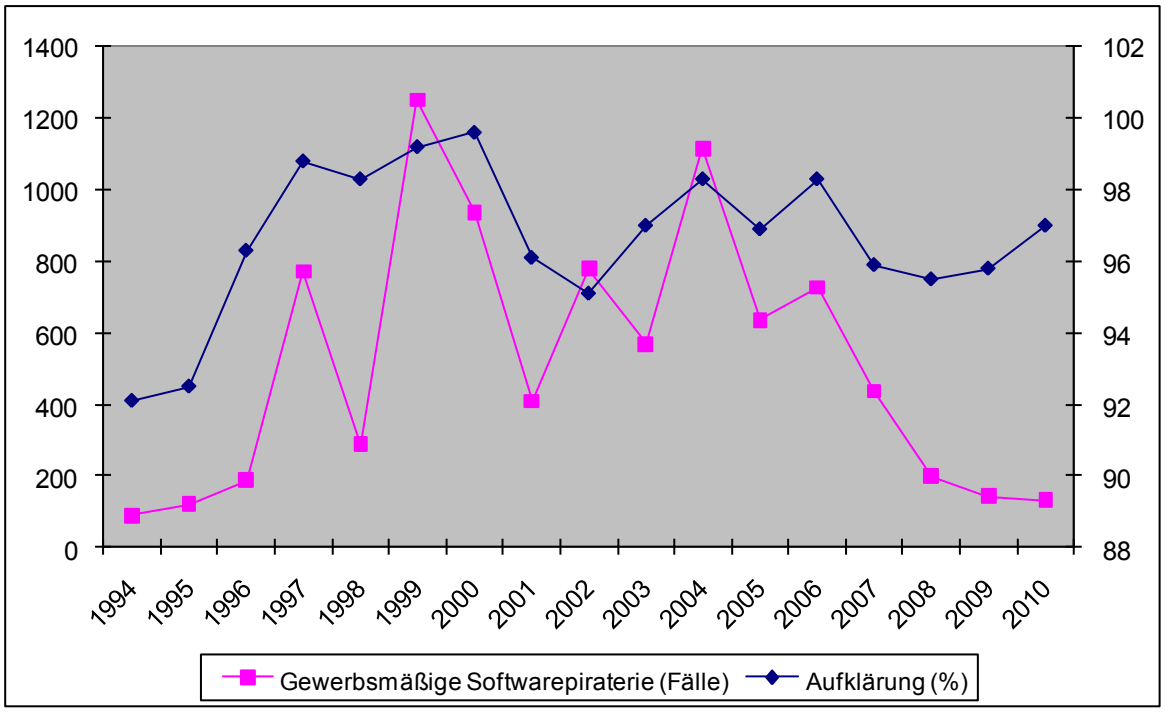
Die Entwicklungen bei Fallzahlen und Aufklärungsquoten für die gewerbsmäßige und private Softwarepiraterie verweisen auf erhebliche Schwankungen, die keinen Hinweis dafür hergeben, dass durch die Einführung der Vorratsdatenspeicherung 2008 Veränderungen eingetreten sind. Die Entwicklungen sind einerseits von Verfolgungsstrategien und Anzeigemustern privater Rechteinhaber abhängig, zum anderen auch von der Reaktion der Strafverfolgungsbehörden auf eine vor allem im neuen Jahrtausend zunehmende Anzeigebereitschaft der Rechteinhaber (die mit der Anzeige insbesondere die hinter der dynamischen IP stehende Person identifizieren wollten)[165]. Nach den Erkenntnissen des Landeskriminalamts Nordrhein-Westfalen resultieren die meisten im Bereich Softwarepiraterie erfassten Delikte aus Ermittlungsverfahren wegen Verstößen gegen das Urheberrechtsgesetz (UrHG) und gegen Nutzer so genannter „Filesharing-Börsen“. Die Schwankungen der Zahl polizeilich registrierter Taten in diesem Deliktsfeld resultieren demnach regelmäßig aus gezielten Schwerpunktaktionen der privaten Rechteinhaber.

---

164 Bundeskriminalamt: Stand der statistischen Datenerhebung im BKA sowie der Rechtstatsachensammlung für Bund (BKA, BPOL, ZKA) und Länder zu den Auswirkungen des Urteils des Bundesverfassungsgerichts zu Mindestspeicherungsfristen, Wiesbaden, Stand: 17.09.10.

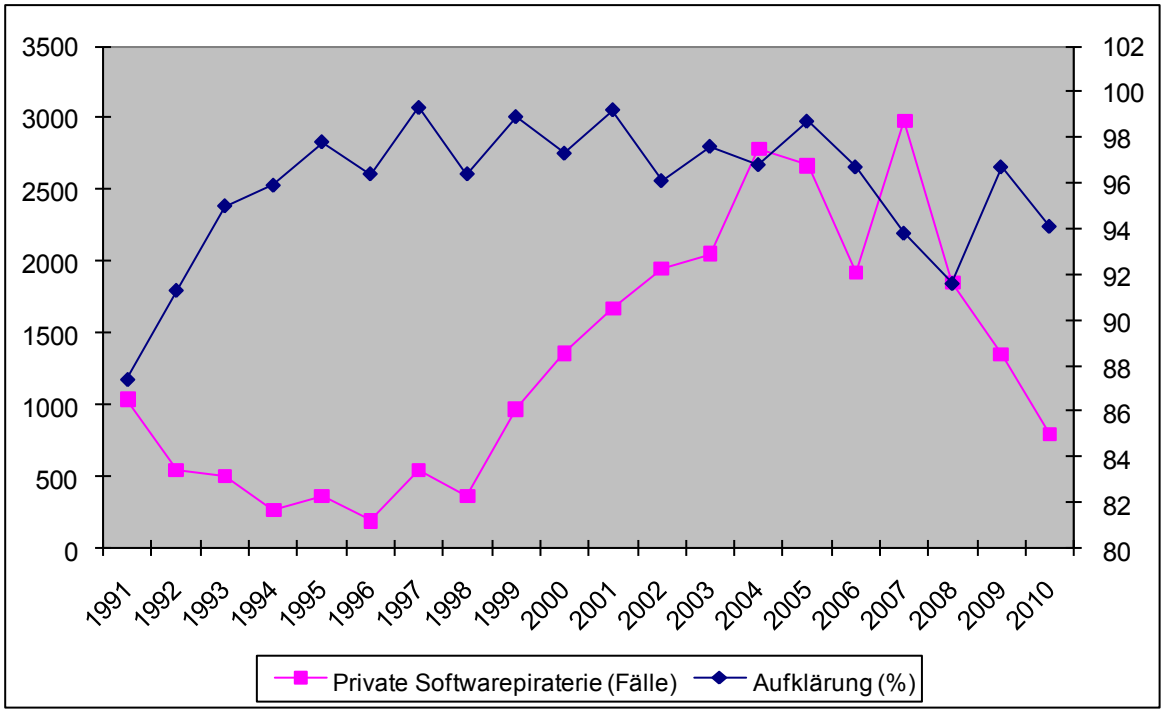
165 Hierzu auch *Rau, L.*: Phänomenologie und Bekämpfung von „Cyberpiraterie“. Göttingen 2004.

*Schaubild D-5: Aufklärungsquoten bei gewerbsmäßiger Softwarepiraterie**



*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

*Schaubild D-6: Aufklärungsquoten bei privater Softwarepiraterie**



*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

Nach den Erkenntnissen aus Nordrhein-Westfalen erstatteten geschädigte Firmen der Musikindustrie bis Ende 2007 zur Identifizierung von Tätern und anschließender Geltendmachung zivilrechtlicher Ansprüche Strafanzeigen bei den Staatsanwaltschaften. Die Ermittlungsvorgänge wurden dann nach Feststellung der IP-Adressen-Benutzer an die zuständigen Polizeibehörden zu weiteren Ermittlungen übersandt. Die Strafverfahren wurden i. d. R. mit Hinweis auf ein Privatklagedelikt durch die Staatsanwaltschaften eingestellt. Auf die bis 2007 festgestellte starke Zunahme der Anzeigen reagierten die Generalstaatsanwaltschaften mit Änderungen in der Verfahrensweise, die dann in einer starken Reduzierung der Fallzahlen ab dem Jahr 2008 führte. Die Anzeigen werden ab 2008 nicht mehr an die Polizeibehörden weitergeleitet. Damit entfällt eine Erfassung in der Statistik. Die Novellierung des Urheberrechtsgesetzes im Jahr 2008 führte dann zu einem eigenen Auskunftsanspruch gemäß §101 UrHG sowie zur Einführung einer Grenzziehung, die durch den „gewerblichen Umfang" markiert wird. Diese ist in Nordrhein-Westfalen an ca. 3.000 Musik- oder 200 Filmdateien orientiert. Diese Grenzwerte werden offensichtlich nur in Ausnahmefällen erreicht bzw. überschritten[166]. Im Übrigen werden die hohen Aufklärungsquoten bei der Softwarepiraterie so erklärt, dass hier Straftaten in der Regel nur bei bekanntem Tatverdächtigen zur Anzeige gelangen, da Straftaten erst bei Feststellung der Tatverdächtigen erkannt werden[167].

4.3. Kriminalität unter Ausnutzung der Informations- und Kommunikationstechnik (IuK-Kriminalität/Computerkriminalität)

Die so genannte IuK-Kriminalität wird in polizeilichen Lageberichten erst seit kurzem gesondert erfasst[168]. Es geht um Straftaten, die unter Ausnutzung der Informations- und Kommunikationstechnik oder gegen diese durchgeführt werden. Eine langfristige Betrachtung der Aufklärungsquoten lässt die in der Polizeilichen Kriminalstatistik gesondert ausgewiesene Computerkriminalität zu. Hier zeigt sich eine seit dem Jahr 2000 fallende Aufklärungsquote, wobei der Trend auch durch die Einführung der Vorratsdatenspeicherung 2008 nicht unterbrochen wird.

Der in Nordrhein-Westfalen für den IuK Bereich festgestellte Rückgang der Aufklärungsquote im Jahr 2009 von 32,1 % gegenüber 2008 (34,7 %) wird durch den Anstieg des Phänomens Phishing erklärt. Dies wird auch vom Bundeskriminalamt im Lagebericht IuK Kriminalität 2009 dokumentiert. Für das Jahr 2009 wurden dem BKA 2.923 Sachverhalte im Phänomenbereich des Phishings gemeldet. Im Vergleich zum Jahr 2008 (1.778 Fälle) bedeutet dies einen Anstieg der Fallzahlen um etwa zwei Drittel. Die Aufklärungsprobleme resultieren in diesem Deliktsbereich ausweislich der Angaben des LKA Nordrhein-Westfalen vor allem daraus, dass der Großteil der Tatverdächtigen über im Ausland liegende Server vorgeht[169].

---

166 Landeskriminalamt Nordrhein-Westfalen: Computerkriminalität. Lagebild 2009, Düsseldorf 2010, S. 3.

167 Landeskriminalamt Nordrhein-Westfalen: Computerkriminalität. Lagebild 2009, Düsseldorf 2010, S. 4.

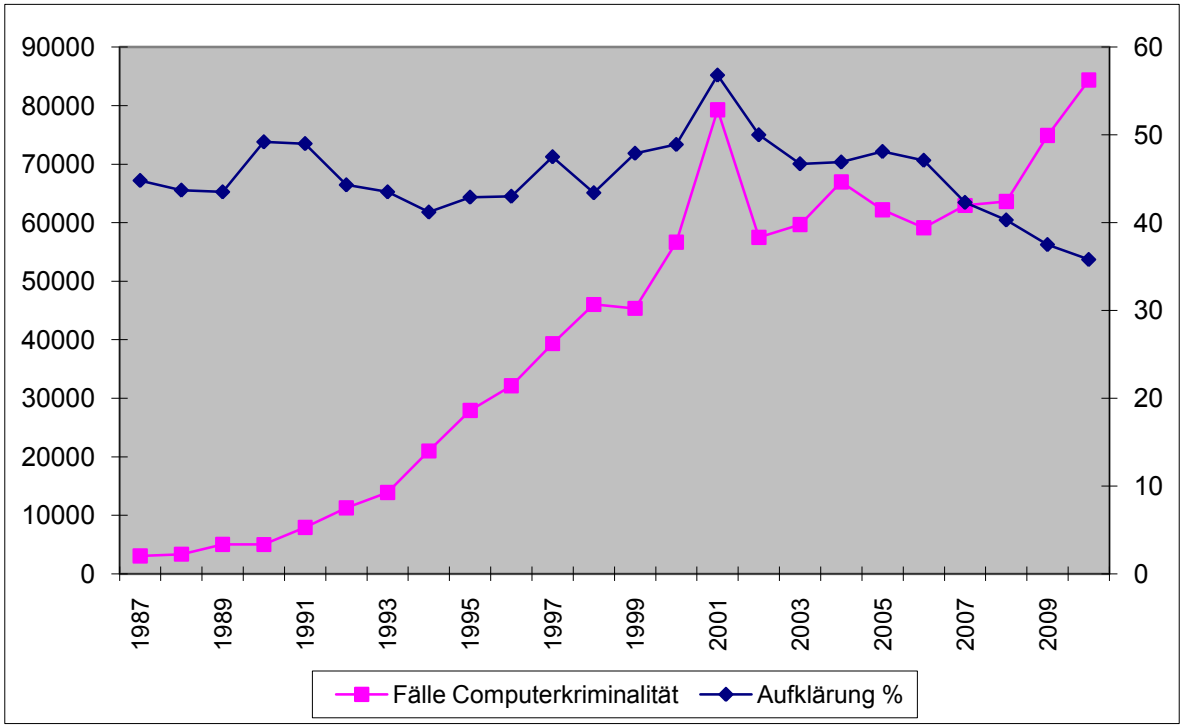
168 Vgl. hierzu Bundeskriminalamt: IuK-Kriminalität. Lagebericht 2009, Wiesbaden 2010, wo (teilweise) ein Bezug auf den Zeitraum 2006-2009 vorgenommen wird.

169 Landeskriminalamt Nordrhein-Westfalen: Computerkriminalität. Lagebild 2009, Düsseldorf 2010, S. 4.

Hinzu treten Verschleierungspraktiken, die die Rückverfolgung von Datentransfers erschweren. Im Falle des Einsatzes entwendeter Daten wird als häufig auftretendes Problem genannt, dass Online-Händler keine IP-Adresse protokollieren. Im IuK Bericht des LKA Baden-Württemberg für das Jahr 2010 wird die Vorratsdatenspeicherung als unbedingt erforderlich bezeichnet[170]. Allerdings gibt der Bericht nicht einmal im Ansatz einen Hinweis dafür, wo und in welchem Umfang eine Vorratsdatenspeicherung die Aufklärungsmöglichkeiten verbessern könnte[171].

Im Fallmaterial des Bundeskriminalamts, das den Zeitraum zwischen der Entscheidung des Bundesverfassungsgerichts und September 2010 abdeckt, befinden sich zwei Phishing-Fälle, die offensichtlich nicht weiter ermittelt werden konnten, weil Verkehrsdaten bzw. Bestandsdaten nicht abgefragt werden konnten. Hieraus ergibt sich allerdings nicht, dass bei einer Zugriffsmöglichkeit angesichts der oben mitgeteilten weiteren Probleme eine Aufklärung der Fälle hätte erfolgen können.

*Schaubild D-7: Fallentwicklung der Computerkriminalität (insgesamt) und Aufklärung (%)**



*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

---

170 Landeskriminalamt Baden-Württemberg: IuK-Kriminalität 2010, Stuttgart 2011, S. 11.

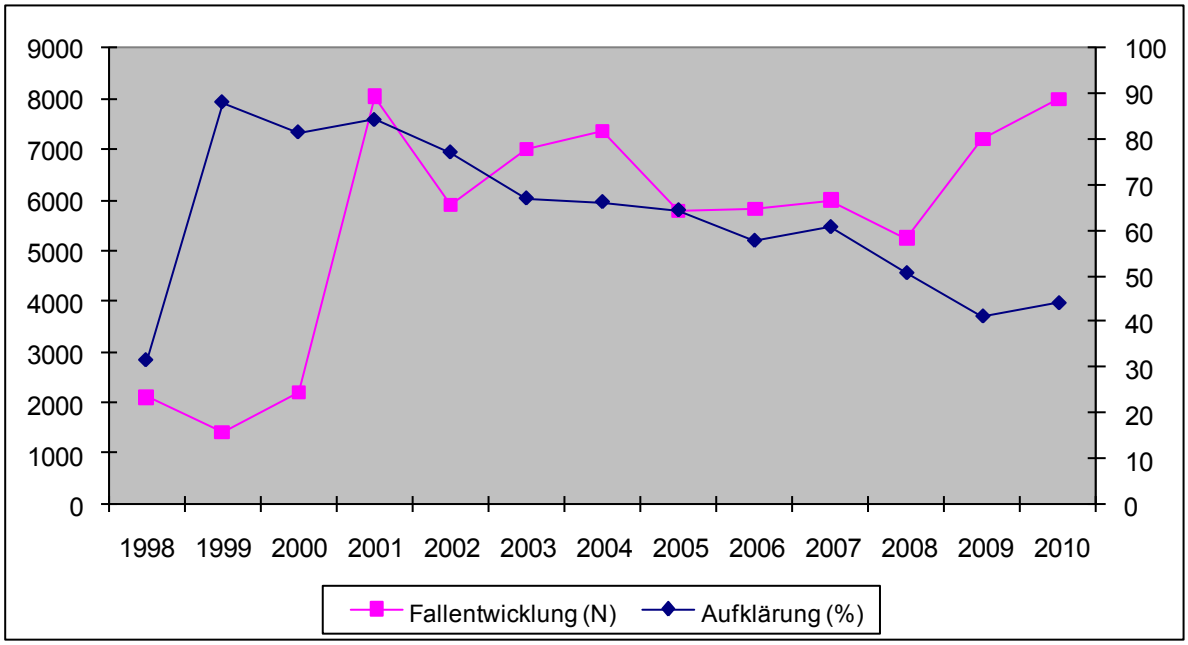
171 Landeskriminalamt Baden-Württemberg: IuK-Kriminalität 2010. Stuttgart 2011, S. 11, als Indiz wird der Rückgang „erfolgreicher Bestandsdatenanfragen“ genannt, ohne dass freilich belegt oder auch nur angedeutet worden wäre, dass erfolgreiche Bestandsdatenabfragen für die Aufklärung von Straftaten Bedeutung gehabt hätten.

Besondere Bedeutung wird im Zusammenhang mit Internetkriminalität dem Betrug bei Onlineauktionen (Anbieten eines Artikels, Kassieren des Höchstgebotbetrages, Nichtliefern der Ware) zugeordnet. Dieser habe sich zum Massendelikt entwickelt. Als besonderes Ermittlungsproblem wird für Frankfurt in diesem Deliktsfeld der mobile Internetzugang über freie WLAN-Netze genannt, die Ortung und Identifizierung der Nutzer ausschließen würden[172]. Die seit 2007 im Bereich der Internetkriminalität stark gestiegenen Fallzahlen resultieren auch aus dem Einsatz neuer bzw. fortentwickelter Software, mit der die technische Sicherung von strafrechtlich relevanten Handlungen im Internet systematisch betrieben werden kann[173].

Die Zeitreihe der als Computerkriminalität registrierten Straftaten zeigt seit etwa 2000 eine andauernde Abnahme der Aufklärungsquote. Der Zeitraum, in dem Vorratsdaten zur Verfügung standen, lässt keine Veränderung im langfristigen Trend erkennen.

4.3.1. Betrug bei Zugang zu Kommunikationsmitteln

*Schaubild D-8: Betrug bei Zugang zu Kommunikationsmitteln und Aufklärungsquote**



*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

Der als IuK-Kriminalität erfasste Betrug bei Zugang zu Kommunikationsmitteln zeigt ab 2000 einen kurzfristigen starken Anstieg in den Fallzahlen, einen tendenziellen Rückgang ab 2001 bis zum Jahr 2008 und für 2009 und 2010 wiederum einen starken Anstieg. Die Aufklärungsquote geht seit Ende der 1990er Jahre stark zurück. Dieser Trend wird auch durch die

172 Polizeipräsidium Frankfurt: Polizeiliche Kriminalstatistik 2008. Teil 2, Frankfurt 2009, S. 145.

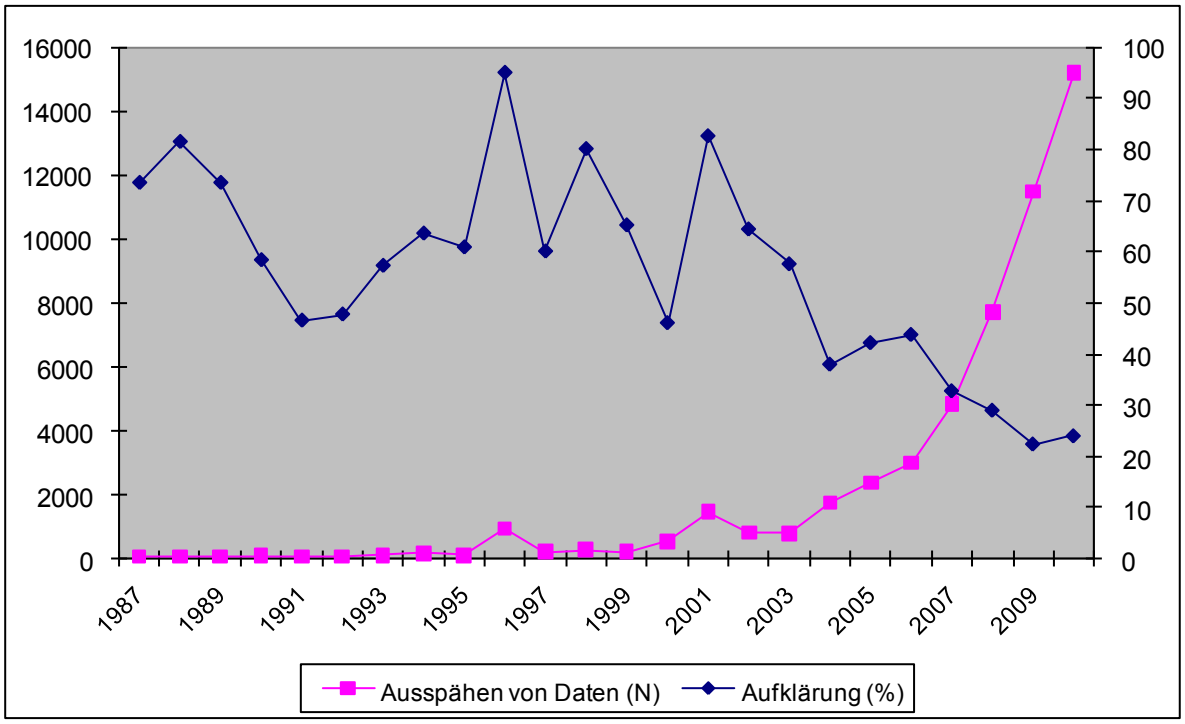
173 Kleine Anfrage des Abg. Dr. Hans-Peter Wetzel FDP/DVP und Antwort des Innenministeriums, Internetkriminalität Landtag von Baden-Württemberg 14. Wahlperiode, Drucksache 14 / 5006, 18. 08. 2009, S. 3.

Einführung der Vorratsdatenspeicherung nicht unterbrochen, vielmehr kommt es im Jahr der vollständigen Suspendierung der Vorratsdatenspeicherung (2010) zu einem Anstieg in der Aufklärung.

4.3.2. Ausspähen von Daten

Das Delikt des Ausspähens von Daten zeigt zwischen 1987 und etwa 2002 nur geringe Fallzahlen, bei einer extremen Schwankungen unterliegenden Aufklärungsquote. Die Aufklärungsquote geht dann von etwa 60% Anfang des neuen Jahrtausends auf etwas über 20% im Jahr 2009 zurück. Im gleichen Zeitraum steigt die Registrierung von Vorfällen des Ausspähens auf knapp 12.000 [174]. Hinter den Fällen des Ausspähens von Daten stehen fast ausnahmslos das rechtswidrige Erlangen von Zahlungskartendaten (Skimming) sowie das so genannte Phishing (durch Einführung von Schadprogrammen in fremde Computer)[175]. Der Anstieg mag auch bedingt sein durch eine Erweiterung der Strafbarkeit auf die Vorbereitung des Ausspähens und Abfangens durch das 41. Strafrechtsänderungsgesetz im Jahr 2007 und eine entsprechende Veränderung der Anzeigebereitschaft. Jedenfalls wird hier ebenfalls deutlich, dass das Jahr 2008 keine Änderung im Trend der Aufklärung bewirkte.

*Schaubild D-9: Aufklärungsquoten beim Ausspähen von Daten**



*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

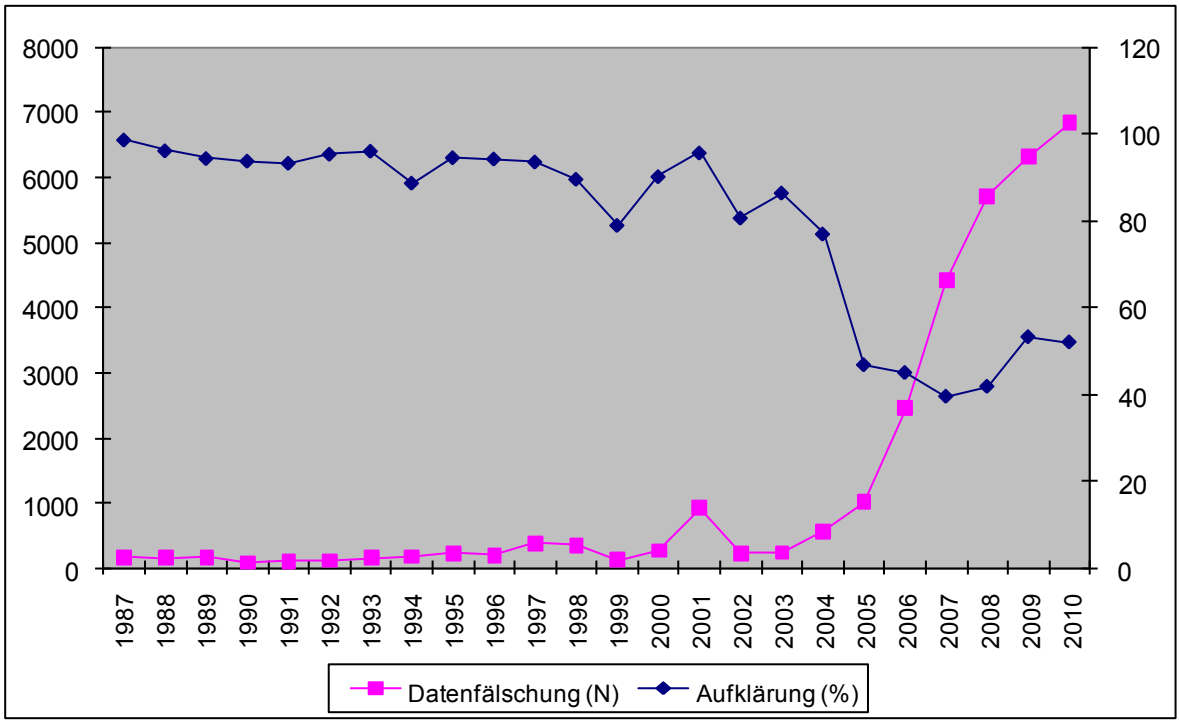
174 Vgl. zum Anstieg auch Landeskriminalamt Baden-Württemberg: IuK-Kriminalität Lagebericht 2008, Stuttgart 2009, S. 7.

175 Landeskriminalamt Hessen: Kriminalstatistik 2009. Pressepapier, Wiesbaden 2010, S. 10.

4.3.3. Datenfälschung

Für das Delikt der Datenfälschung kann seit etwa 2005 ein sehr starker Anstieg festgestellt werden. Mit dem starken Anstieg korrespondiert eine ebenso starke Abnahme der Aufklärungsquote. Allerdings scheint sich die starke Abnahmetendenz ab 2007 wieder umzukehren. Sowohl 2008 als auch 2009 liegen Zuwächse in der Aufklärungsquote vor.

*Schaubild D-10: Aufklärungsquoten bei Datenfälschung**

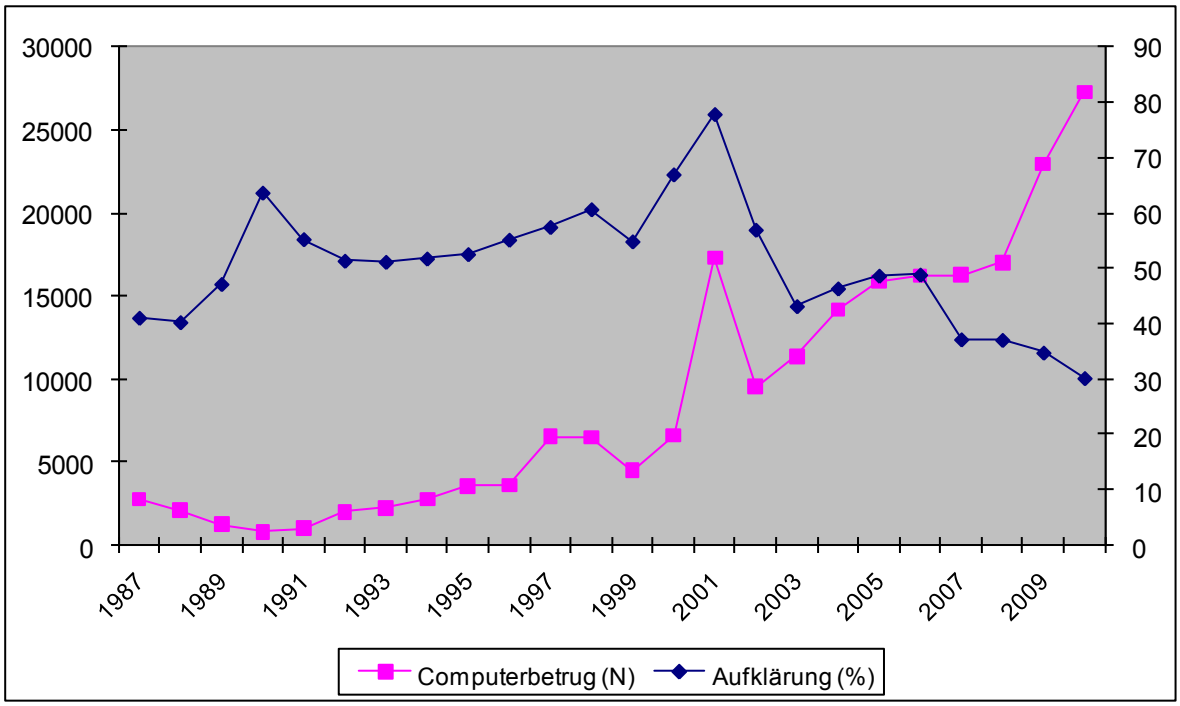


*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

4.3.4. Computerbetrug

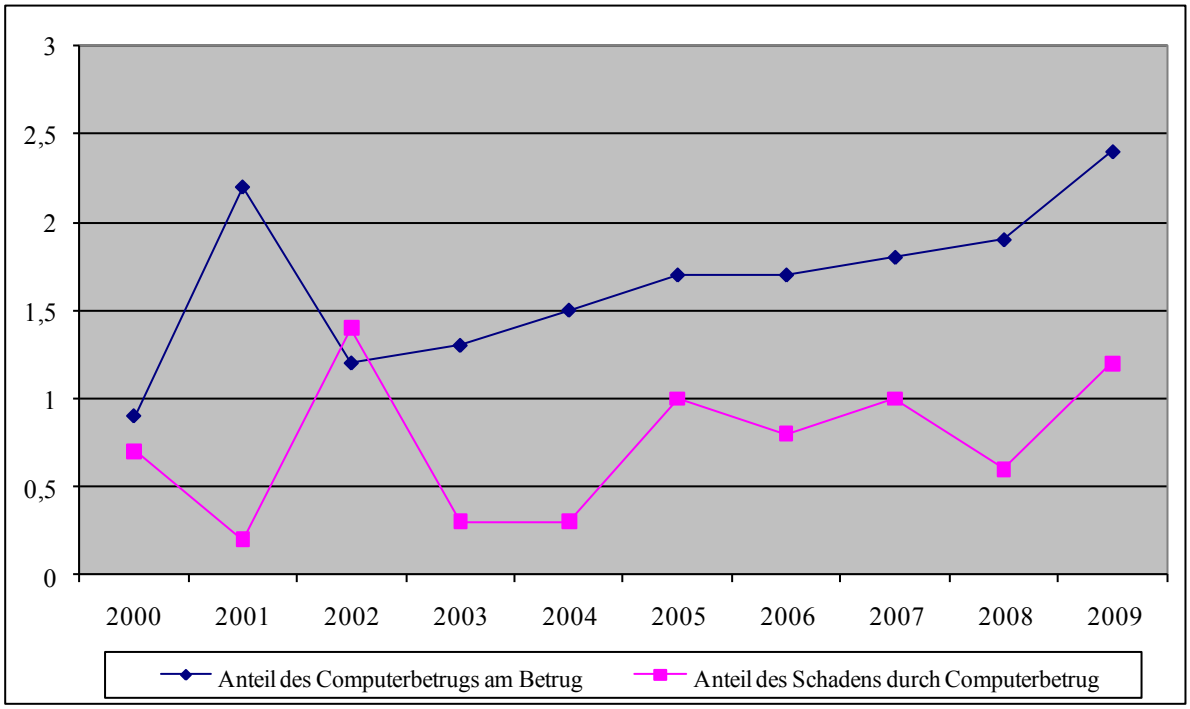
Die Fallzahlen des Computerbetrugs bewegen sich ab Ende der 1990er Jahre steil nach oben. Dem entspricht eine deutliche Abnahme der Aufklärungsrate, die ebenfalls Ende der 1990er Jahre einsetzt. Der Einbruch der Aufklärungsquote lässt sich im Zeitraum 2000-2003 lokalisieren. In dieser Periode halbiert sich die Aufklärungsquote. In der Folge kommt es zu einem sehr viel schwächeren Abgleiten, das durch die Vorratsdatenspeicherung im Jahr 2008 nicht unterbrochen wurde. Da etwa zwei Drittel der knapp 25.000 Computerbetrugsfälle nicht aufgeklärt werden, ist allerdings auch zu fragen, wie bei der bis 2008/2009 etablierten Praxis der Verkehrsdatenabfrage die Aufklärungsquote hätte verbessert werden können.

*Schaubild D-11: Aufklärungsquoten beim Computerbetrug**



*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

*Schaubild D-12: Schadensentwicklung bei Computerbetrug im Verhältnis zum Betrugsschaden insgesamt**

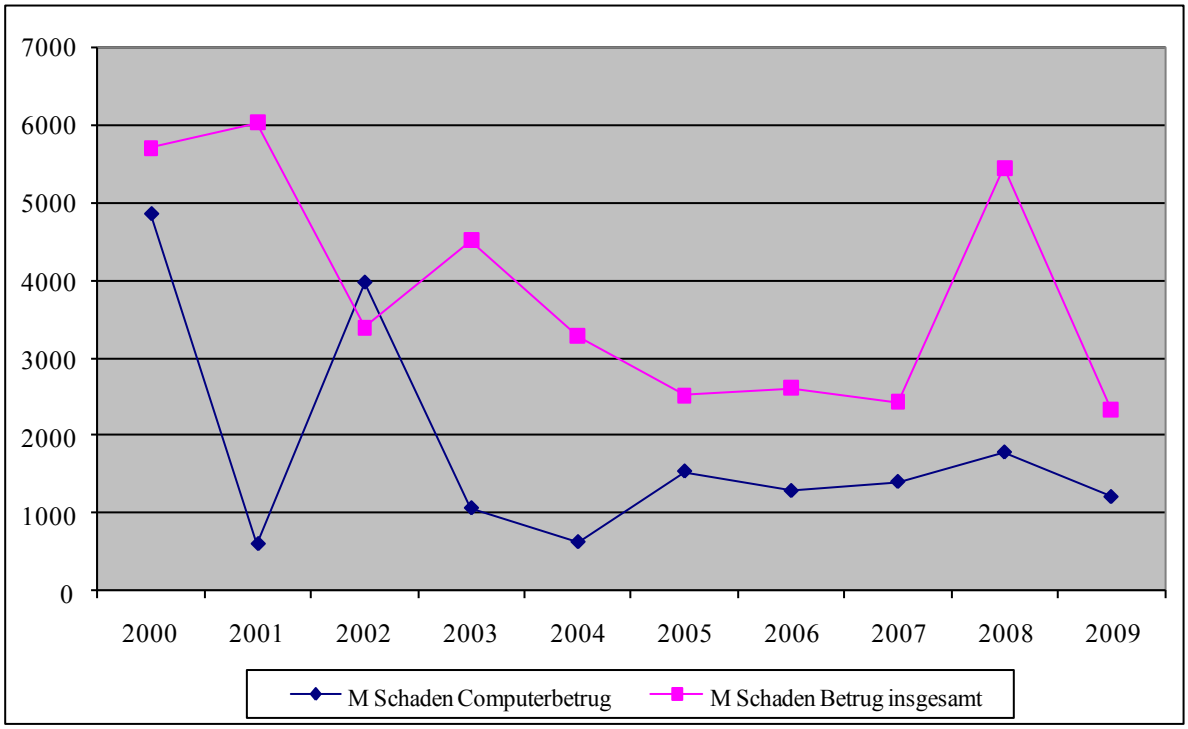


*) Quellen: Polizeiliche Kriminalstatistiken 2000 bis 2009, jeweils Tabelle 7.

Die polizeilichen Daten zum Computerbetrug lassen auch eine Einschätzung im Hinblick auf Schaden, Schadensentwicklung und deren Verhältnis zum Betrug insgesamt zu. Der Computerbetrug nimmt einen kleinen Anteil an den Betrugsfällen insgesamt ein. Dieser Anteil erhöht sich bis zum Jahr 2010 auf etwa 2,5%. Deutlich darunter liegt der Anteil der durch Computerbetrugsfälle bedingten Schadenssumme an dem durch Betrug insgesamt verursachten Schaden (etwas mehr als 1%, Schaubild D-12).

Für den Zeitraum 2000 bis 2009 zeigen die Daten der Polizeilichen Kriminalstatistik auch, dass der durchschnittliche Schaden bei Computerbetrug bis auf das Jahr 2002 deutlich unter dem durchschnittlichen Schadensbetrag bei Betrugsfällen insgesamt liegt. Dies verweist, ebenso wie vorstehenden Ausführungen, darauf, dass der Computerbetrug im Zusammenhang mit dem durch die Betrugstatbestände strafrechtlich gewährleisteten Vermögensschutz keine herausgehobene Stellung einnimmt. Ferner kann aus den Entwicklungen nicht entnommen werden, dass über das letzte Jahrzehnt Veränderungen eingetreten sind, die auf eine zunehmende Bedeutung des Computerbetrugs für die Vermögenssicherheit schließen lassen könnten.

*Schaubild D-13: Durchschnittliche Schadensbeträge bei Computerbetrug und Betrug insgesamt**

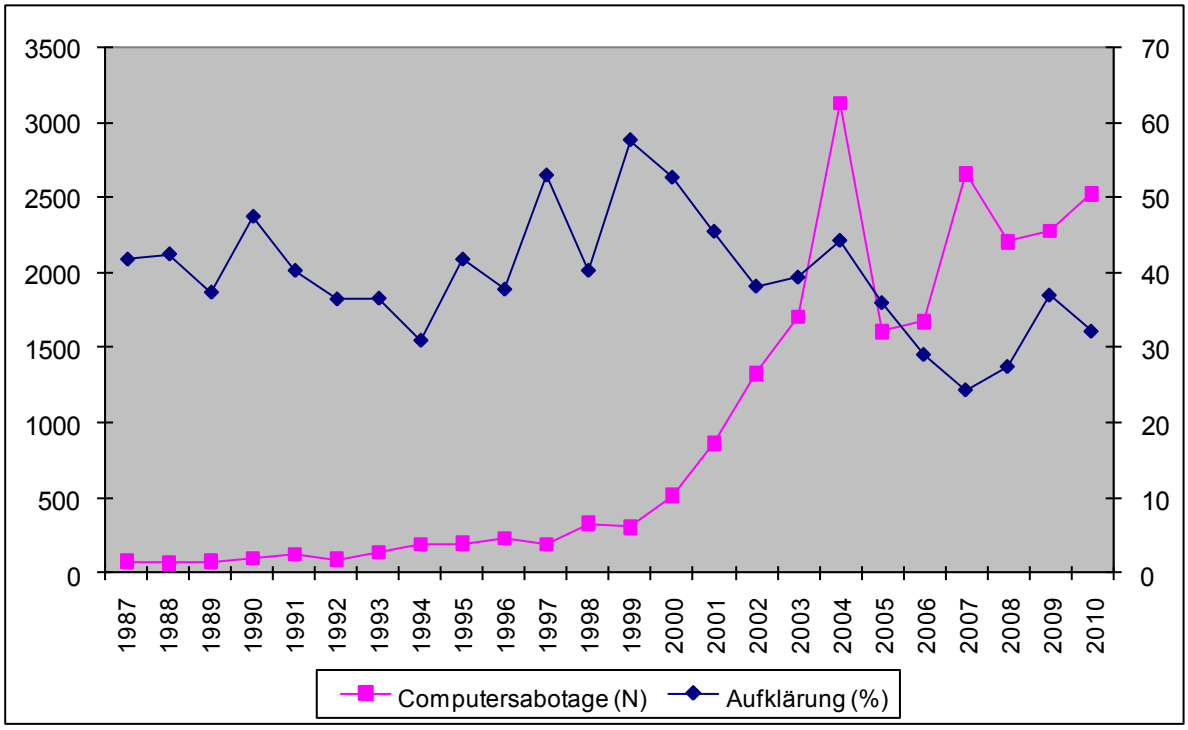


*) Quellen: Polizeiliche Kriminalstatistiken 2000 bis 2009, jeweils Tabelle 7.

4.3.5. Computersabotage

Das Delikt der Computersabotage nimmt seit Anfang 2000 stark zu. Dies wird begleitet von einem ebenso starken Rückgang in der Aufklärungsquote. Die rückläufige Entwicklung der Aufklärungsquote endet im Jahr 2007. 2008 und 2009 sind Zuwächse zu beobachten, deren Bedingungen mit den verfügbaren Informationen ebenso wenig nachgewiesen werden können wie der Rückgang im Jahr 2010.

*Schaubild D-14: Aufklärungsquoten bei Computersabotage**



*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

4.4. Verbreitung und Besitz von Kinderpornografie

In den Diskursen zur Vorratsdatenspeicherung wird insbesondere die Strafverfolgung der Verbreitung und des Besitzes der Kinderpornografie betont. Hier sei der Rückgriff auf IP-Adressen unabdingbar, wenn nicht dem Handel mit kinderpornografischen Schriften Tür und Tor geöffnet werden solle[176]. In diesem Zusammenhang wird vor allem auch darauf hingewiesen, dass hinter jedem kinderpornografischen Bild ein realer Missbrauch stehe, und dass demnach Beschränkungen im Zugriff auf IP-Adressen unmittelbar auf den sexuellen Miss-

176 Niedersächsischer Landtag − 16. Wahlperiode Drucksache 16/3056, Kleine Anfrage mit Antwort, Wie weiter mit der Vorratsdatenspeicherung?, S. 3.

brauch von Kindern zurückwirkten. So erklärte der Innenminister Schleswig-Holsteins, dass derjenige, der jetzt noch mit der notwendigen Gesetzgebung (Vorratsdatenspeicherung) warte, „unendliches, irreparables und lebenslanges Leid traumatisierter Kinder und Jugendlicher“ ignoriere[177]. Die Annahme eines (kausalen) Zusammenhangs zwischen dem Aufkommen an sexuellem Missbrauch von Kindern, Herstellung von Kinderpornografie und Verbreitung sowie Besitz von Kinderpornografie ist aber nicht begründet. Nachvollziehbare Untersuchungen, dass ein solcher Zusammenhang bestehen könnte, gibt es nicht. Vereinzelt wird in Lageberichten zur IuK Kriminalität bzw. in Auswertungen von Kinderpornografieverfahren darauf hingewiesen, dass ein laufender Missbrauch von Kindern habe beendet werden können. Für 2008 teilt das LKA Baden-Württemberg einen solchen Fall für Niedersachsen mit, bei einer Zahl von etwas mehr als 1000 initiierten Verfahren wegen der Verbreitung von Kinderpornografie[178]. Dies heißt, dass sexueller Missbrauch in Verfahren wegen der Verbreitung von Kinderpornografie als Zufallsfund gelten kann, keineswegs geht es um eine quantitativ erhebliche oder Schutzlücken indizierende Zahl von Fällen (angesichts von knapp 11.000 registrierten Fällen des sexuellen Missbrauchs pro Jahr im Bundesgebiet). Ferner geben die wenigen systematischen Untersuchungen zum Stellenwert des Internets und einzelner Teilbereiche des Netzes wenig für die Annahme her, dass kommerziell ausgerichtete Webseiten für die Verbreitung von Kinderpornografie eine signifikante Rolle spielen würden. Aus einer noch nicht abgeschlossenen Untersuchung, die sich auf das Bundesland Niedersachsen und das Jahr 2008 erstreckt, sind hierzu einige vorläufige Daten zu entnehmen. Danach spielen kommerzielle Transaktionen für das Verfahrensaufkommen kaum eine Rolle. Im Vordergrund steht der Tausch (in entsprechenden Netzwerken), durch (elektronische) Briefe oder MMS. Das Web und einschlägige (kommerzielle und andere) Webseiten sind von untergeordneter Bedeutung. Etwa die Hälfte der Verfahren kommt durch Zufallsfunde zustande (Untersuchungen in anderen Verfahren beschlagnahmter Computer oder Datenträger). Große und/oder international angelegte Operationen tragen zum Fallaufkommen wenig bei. Die Vorratsdatenspeicherung wird offensichtlich von vornherein nur begrenzt nützlich, da die Auswertung von Computern und Datenträgern häufig weitaus länger als 6 Monate dauert[179]. Entsprechende Hinweise ergeben sich aus dem Sicherheitsbericht für die Schweiz und das Jahr 2009[180]. Das Problem wird in einem Bericht für Sachsen-Anhalt unterstrichen, wo derzeit beim Landeskriminalamt noch 48 Terabyte an Speicher (etwa 364 Millionen Bilder) auf eine Auswertung warten[181]. In diesem Zusammenhang ist darauf hinzuweisen, dass in Landtagen verschiedentlich die Frage der Belastung der Ermittlungsbehörden durch die Auswertung beschlagnahmter Datenträger thematisiert worden ist. Nach den vorliegenden Auskünften ist die schiere

---

177 Heise online (www heise.de) [02.11.2010].

178 Landeskriminalamt Baden-Württemberg: IuK-Kriminalität. Lagebild 2008, Stuttgart 2009, S. 6.

179 Auf der Suche nach den Verbreitungswegen der Kinderpornografie. Der Kampf gegen Vergewaltigungsbilder im Netz basiert auf falschen Annahmen. Forscher raten der Politik, sich nicht auf das WWW zu beschränken, abrufbar unter www.zeit.de [25. November 2010].

180 Bundesamt für Polizei: Bericht Innere Sicherheit Schweiz 2007, Bern 2008, S. 60.

181 Im Netz der Kinderschänder, abrufbar unter www faz.net [4.1.2011].

Anzahl beschlagnahmter Datenträger (und Daten) enorm. So wurden vom Landeskriminalamt Berlin für das Jahr 2006 77.452 beschlagnahmte Datenträger registriert (2007 51.978, 2008 65.510; 2007/2008 kommen 20.731 Datenträger durch die Operation „Himmel“ hinzu). Die entsprechenden Zahlen an Tatverdächtigen für die Jahre 2006 bis 2008 lauten für Berlin 282, 779, 204[182]. Sowohl Volumenverfahren als auch Verfahren gegen einzelne Tatverdächtige oder kleinere Gruppen äußern sich demnach in einem erheblichen Aufkommen an beschlagnahmten Datenträgern, die offensichtlich zu Engpässen in der Auswertung und teilweise zur Rückgabe der Datenträger ohne Auswertung führen[183]. Kosten- bzw. Kosten-Nutzen-Analysen sind für diesen Bereich bislang nicht durchgeführt worden.

Die vorläufigen Befunde aus der Niedersachsenstudie decken sich mit den Ergebnissen einer neuen Untersuchung zur Rolle des Web und kommerzieller Webseiten für die Verbreitung von Kinderpornografie. Die zentralen Ergebnisse der Studie lauten:

- In den letzten Jahren kam es zu einem signifikanten Rückgang in der Zahl aktiver kommerzieller Webseiten, die (auch) Kinderpornografie anbieten.
- Die Betreiber einschlägiger Webseiten verbreiten Kinderpornografie, sind aber an der Herstellung nicht beteiligt.
- Bildmaterial ist im Allgemeinen historisch und wird immer wieder neu aufgelegt.
- Viele der Anbieter sind (desorganisierte) Einzelpersonen.
- Kommerzielle Webseiten werfen keine großen Profite ab.
- Zu Kinderpornografie existieren zahlreiche Zugangsmöglichkeiten.
- Hersteller von Kinderpornografie nutzen in aller Regel gesicherte Räume im Internet, in denen Bilder und Filme weitgehend kostenfrei getauscht werden[184].

Die Rolle von Großverfahren für Ermittlungen und Aufklärungserfolge in Fällen der Kinderpornografie ist bislang über die vorstehend berichteten vorläufigen Befunde hinaus nicht sys-

---

182 Abgeordnetenhaus Berlin Kleine Anfrage 16. Wahlperiode, Kleine Anfrage des Abgeordneten Peter Trapp (CDU) vom 10. März 2009 (Eingang beim Abgeordnetenhaus am 12. März 2009) und Antwort Auswertung beschlagnahmter Datenträger aufgrund des Verdachts kinderpornografischer Inhalte Drucksache 16 / 13 202.

183 Kinderpornografie im Internet. „Viele Kriminelle werden nicht zur Verantwortung gezogen“, abrufbar unter www.spiegelonline.de [10.09.2010]; dies scheint international als Problem der Ermittlungen bei Computerkriminalität aufzutreten, vgl. *Hinduja, S.*: Computer Crime Investigations in the United States: Leveraging Knowledge from the Past to Address the Future. International Journal of Cyber Criminology 1(2007), S. 1-26, S. 13; so auch U.S. Department of Justice, Office of the Inspector General Audit Division: The Federal Bureau of Investigation´s Efforts to Combat Crimes Against Children, Washington 2009, S. 36 f.

184 European Financial Coalition: 14 months on: A combined report from the European Financial Coalition 2009-2010, An intelligence assessment on the commercial distribution of child sexual abuse images, Brüssel 2010, S. 5.

tematisch ausgeleuchtet. Jedoch ergeben sich einzelne Hinweise darauf, dass bei manchmal zehntausenden Tatverdächtigen der Ermittlungsertrag nicht immer überzeugend ausfällt.

So führte die nach der Operation „Landslide“ in den USA ausgelöste Aktion „Genesis“ in der Schweiz bei 1550 Verdächtigen bei knapp 1100 Hausdurchsuchungen und der Beschlagnahme von 2000 Computern sowie etwa 35000 Datenträgern zu etwas mehr als 400 Verurteilungen, die überwiegend auf Geldstrafen lauteten[185]. Die ebenfalls an „Landslide“ anschließende Aktion „Ore“ wird in England mittlerweile eher kritisch gesehen, da offensichtlich auf der Grundlage von aus den USA gelieferten Informationen zu mutmaßlichen Kunden kinderpornographischer, kommerzieller Webseiten identifizierte Personen heute eher als Opfer von Kreditkartenbetrügern eingestuft werden. Diese Überlappung zwischen Kreditkartenbetrug und dem Abfragen von Kinderpornografie hat in der an Landslide anschließenden Strafverfolgung in den USA wohl bereits dazu geführt, dass sich aus etwa 35.000 Personenhinweisen nur etwa 100 Anklagen (wegen Besitzes von Kinderpornografie) ergaben.[186]

Für Deutschland lassen sich aus den weiter oben berichteten vorläufigen Befunden der Niedersachsen-Studie ebenfalls keine Hinweise dafür ableiten, dass Großoperationen für die effiziente Verfolgung von Kinderpornografie signifikante Bedeutung hätten. Die sich in Deutschland an „Landslide“ anschließende Aktion wurde durch den Hinweis begleitet, dass sich hier neue Dimensionen der kommerziellen Verbreitung von Kinderpornografie ergeben würden. Das Unternehmen Landslide hat zwar Millionenumsätze (ca. 5,5 Millionen US-$) gemacht (über einen kurzen Zeitraum), allerdings auch und wohl vor allem mit durchschnittlicher Pornografie und musste im Übrigen nach heutigem Wissensstand deshalb schließen, weil es Opfer systematischen und organisierten Betrugs wurde[187]. In der Operation „Pecunia“ wurden in Deutschland immerhin Wohnungen von mehr als 1.400 Personen durchsucht und jeweils Computer beschlagnahmt (dazu etwa 47.000 Datenträger und 25.000 Videos). Diese Personen wurden verdächtigt, sich gegen Bezahlung Zugang zu kinderpornografischen Internetseiten (über Landslide) verschafft zu haben[188]. Die Daten, die die Strafverfolgungsstatistik zu Verurteilungen wegen Besitz und Verbreitung zur Verfügung stellt (2002 477 und 2003 753 Verurteilungen, davon (2003) etwa 84% Geldstrafen, hieraus etwa drei Viertel bis zu 90 Tagessätzen) lassen jedenfalls dann, wenn die Verteilungen zur Entstehung von Verfahren aus der Niedersachsenstudie herangezogen werden, keinen signifikanten Beitrag zu den Verurteilungszahlen erkennen.

---

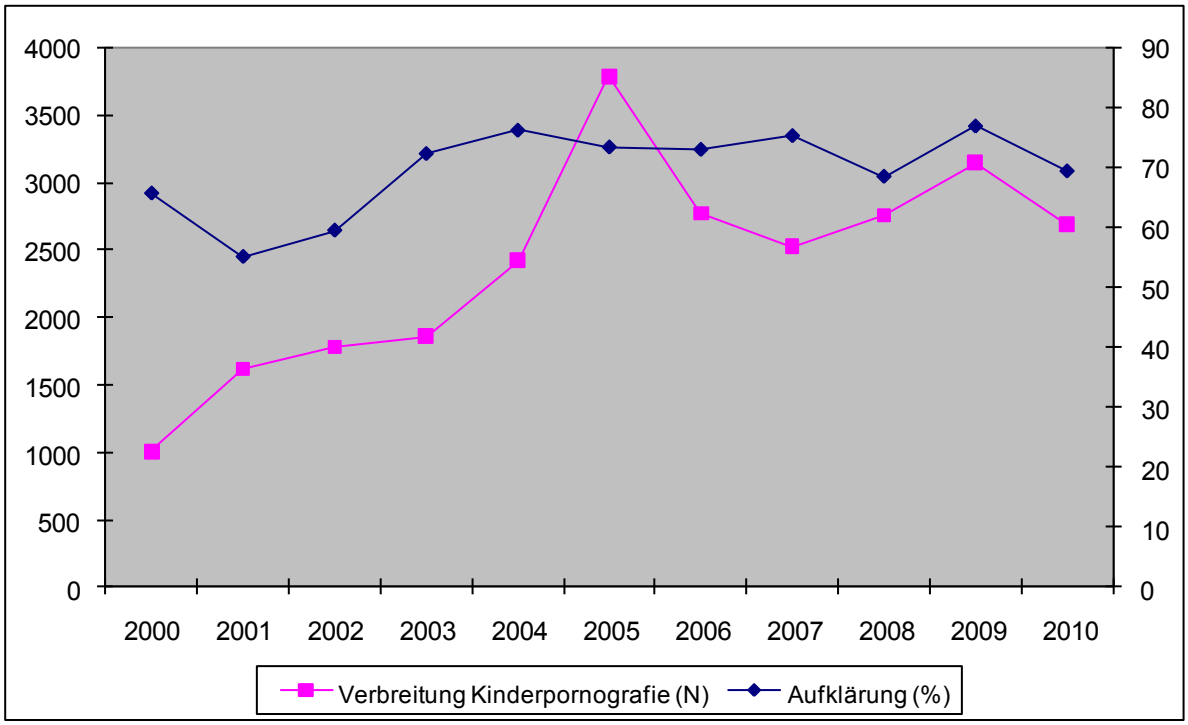
185 www.ejpd.admin.ch/content/ejpd/de/home/dokumentation [Juni 2011].

186 *Duncan Campbell*: Operation Ore exposed, 1. Juli 2005: www.pcpro.co.uk [Juni 2011].

187 Entsprechende Informationen sind auch über Wikileaks verbreitet worden; mirror.wikileaks.info/wiki/An_insight_into_child_porn/index html [Juni 2011].

188 Pressemitteilungen des BKA, 2002.abrufbar unter www.bka.de [Juni2011].

*Schauild D-15: Fallentwicklung und Aufklärungsquote bei der Verbreitung von Kinderpornografie**



*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

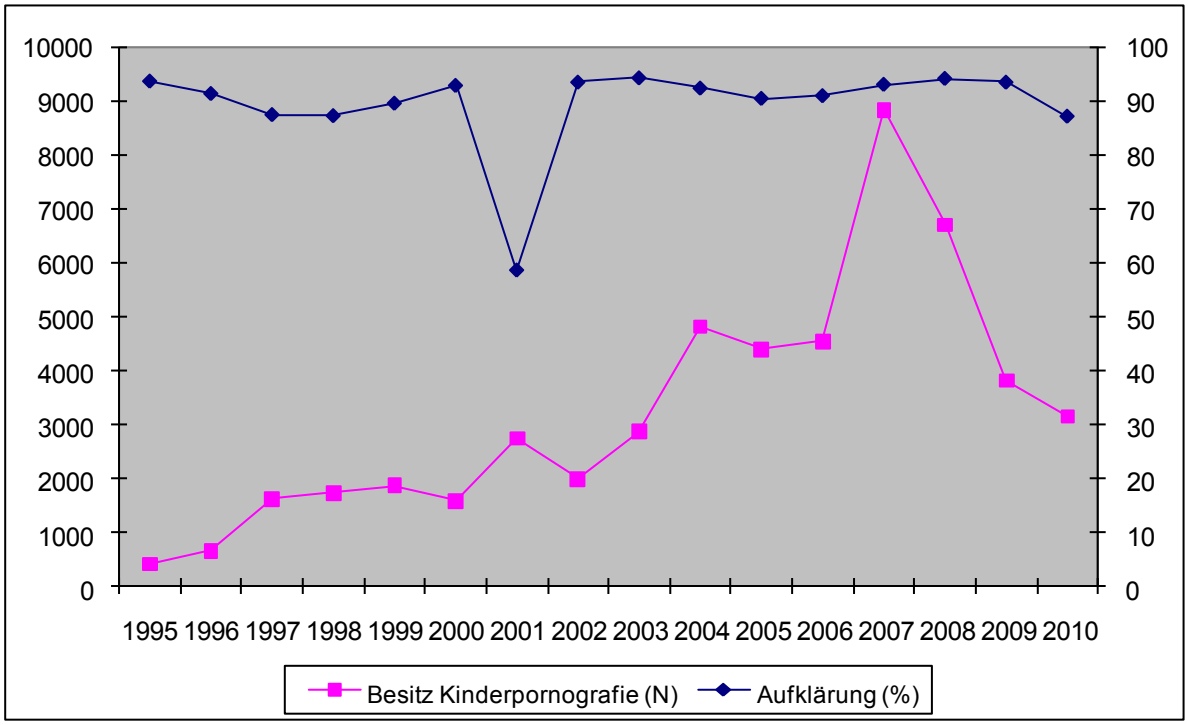
Die Aufklärungsquote bei dem Delikt der Verbreitung von Kinderpornografie verändert sich seit etwa 2003 wenig (Schaubild D-15). Auch die Entwicklung der Fallzahlen zeigt keinen erkennbaren Einfluss der Speicherung von Verkehrsdaten (bzw. die Rückgriffsmöglichkeiten auf Daten, die hinter einer dynamischen IP-Adresse stehen).

Die Aufklärungsquote für den Besitz von Kinderpornografie verändert sich nicht (Schaubild D-16). Der Ausreißer des Jahres 2001 wird wohl durch eine fallspezifische Besonderheit erklärbar sein. Deutlich wird aber, dass das Fallaufkommen nach einem sprunghaften Anstieg von 2006 auf 2007 ab 2007 deutlich sinkt, wobei der Einbruch mit dem ersten Jahr der Geltung der Vorratsdatenspeicherung zusammenfällt. Die Fallzunahme im Jahr 2007 ist auf die Operation „Himmel“ zurückzuführen, in der zunächst von etwa 12.000 Tatverdächtigen ausgegangen worden war[189]. Eine systematische Bestandsaufnahme dieser Operation ist zwar bundesweit nicht erfolgt, jedoch dürften nach vereinzelten Informationen lediglich eine kleine Zahl von Strafverfahren in Gang gekommen und mit strafrechtlichen Sanktionen abgeschlossen worden sein. Für einzelne Regionen wird von der Einstellung fast aller Verfahren

189 Vgl. hierzu auch Landeskriminalamt Hessen: Kriminalstatistik 2009. Pressepapier, Wiesbaden 2010, S. 10; Spiegel online: Operation „Himmel“, Riesiger Kinderporno-Skandal schockiert Deutschland [24. 12. 2007].

berichtet (insbesondere im Raum Nordrhein-Westfalen)[190]. Aus Baden-Württemberg wurde bekannt, dass bei anfänglich 1.696 Verdächtigen 741 Verfahren „im Vorfeld“ eingestellt worden seien. In 942 Fällen wurden Wohnungen durchsucht und dabei 1.697 PC/Notebooks und über 47.000 Datenträger sichergestellt. In 598 Fällen sei schließlich der Tatvorwurf des Besitzes von Kinderpornografie bestätigt worden[191]. Erkenntnisse zur Erledigung der durch die Staatsanwaltschaft eingeleiteten Verfahren liegen nicht vor. Jedoch ist davon auszugehen, dass ein weiterer Schwund auch durch Geringfügigkeitseinstellungen verursacht wurde.

*Schaubild D-16: Aufklärungsquote bei Besitz von Kinderpornografie**



*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

Die allgemeinen Entwicklungen in der Registrierung von Fällen der Kinderpornografie und in den Aufklärungsquoten sprechen jedenfalls dafür, dass sich die Vorratsdatenspeicherung in der Generierung von Fällen der Kinderpornografie nicht ausgewirkt hat. Veränderungen im Fallaufkommen können im Übrigen auch durch Verlagerungen (des Tausches oder des Erwerbs) und damit (erwartbare) Anpassungen, die auch aus anderen illegalen Märkten bekannt sind, bedingt sein.

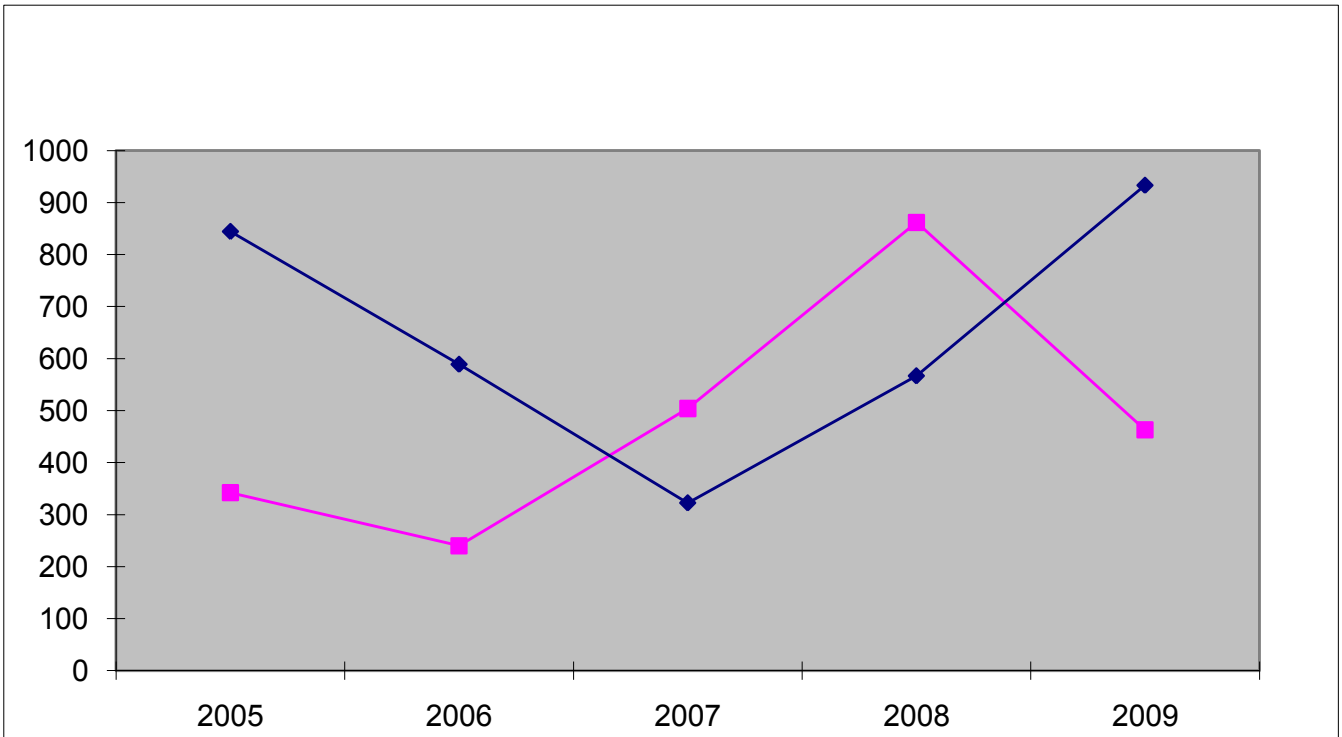
Die Aufklärungsquote entsprechender Fälle in Österreich unterscheidet sich zwischen 2005 und 2009 von der Aufklärungsquote in Deutschland nicht. Eher dürfte die Aufklärungsquote

190 www heise.de/newsticker/meldung/Kinderporno-Wie-erfolgreich-war-die-Operation-Himmel-177176.html [Juni 2011].

191 Landeskriminalamt Baden-Württemberg: IuK-Kriminalität Lagebericht 2008. Stuttgart 2009, S. 6.

in Österreich nach der nachstehenden Grafik (in der Verbreitung und Besitz zusammengefasst sind) etwas höher als die deutsche Quote liegen.

*Schaubild D-17: Kinderpornografiefälle und Aufklärungsquote in Österreich**



*) Quelle: Bundesministerium für Inneres: Sicherheitsberichte 2005 bis 2009. Wien 2006-2010.

Die vom Bundeskriminalamt ermittelten insgesamt 4 Fälle, in denen es wegen fehlender Vorratsdaten nicht zu weiteren Ermittlungen wegen des Besitzes oder der Verbreitung von Kinderpornografie gekommen ist [192], beziehen sich in zwei Fällen auf Einzelpersonen in P2P Plattformen und in zwei Fällen auf Volumenoperationen. Eine von Brasilien ausgehende Information zu 147 IP-Adressen, die in Deutschland lokalisiert wurden, bezieht sich auf den Zeitraum zwischen 29.5. und 11.9.2009 und wurde dem Bundeskriminalamt am 25.5. 2010 übermittelt[193]. In diesem Fall hätte bei sechsmonatiger Speicherungsdauer von vornherein kein Zugriff mehr auf Verkehrsdaten stattfinden können. Wurden auch diese IP-Abfragen bei den negativen Abfragen abgelegt, so erklärt sich nicht, warum die in der Dokumentation des BKA enthaltene Verteilung der negativen Abfragen auf notwendige Speicherungszeiten nicht den Zeitraum 6-12 Monate einführt[194]. Ein zweiter Volumenfall enthält 40 Kontakte (E-Mail- und IP-Adressen) zu einer Webseite, auf der kinderpornographisches Material angeboten worden sein soll. Hier war eine Identifizierung der Bestandsdaten nicht mehr vorzunehmen.

---

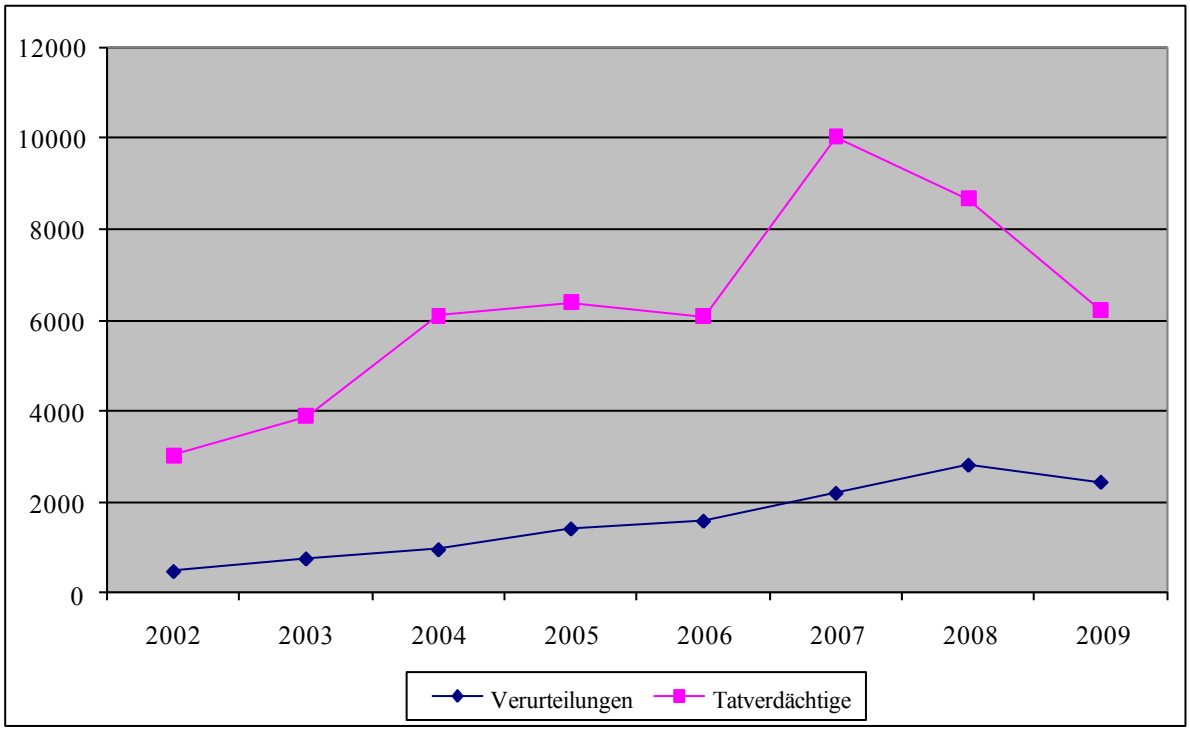
192 Bundeskriminalamt: Stand der statistischen Datenerhebung, a.a.O. (Fn. 164), Anlage 1, S. 24 ff.

193 Bundeskriminalamt: Stand der statistischen Datenerhebung, a.a.O. (Fn. 164), Anhang 2, S. 28 f.

194 Bundeskriminalamt: Stand der statistischen Datenerhebung, a.a.O. (Fn. 164), vgl. die Grafik „erforderliche Speicherungsdauer“ auf S. 12.

Hieraus hätten demnach, geht man (konservativ und damit überzeichnend, angesichts des Verhältnisses zwischen Tatverdächtigen und Verurteilten in diesem Deliktsfeld, vgl. Schaubild D-17) von einer Verurteilungsquote von etwa einem Drittel aus, etwa 14 Verurteilungen wegen des Besitzes von Kinderpornografie resultieren können.

*Schaubild D-18: Tatverdächtige u. Verurteilte bei Verbreitung u. Besitz von Kinderpornografie**



*) Quellen: Statistisches Bundesamt: Strafverfolgungsstatistik 2002-2009. Wiesbaden 2003-2010; Bundeskriminalamt: Polizeiliche Kriminalstatistik 2002-2009. Wiesbaden 2003-2010.

Die Informationen des Bundeskriminalamts zu folgenlos bleibenden Abfragen zu Anschlüssen sprechen dafür, dass der Bereich der Kinderpornografie für die Verkehrsdatenabfrage ganz im Vordergrund stehen wird. Etwa 70% der Abfragen beziehen sich auf Kinderpornografie. Es wird in diesem Zusammenhang wiederum darauf verwiesen, dass hier die Priorität bei der Unterbindung fortgesetzten Missbrauchs liegen müsse[195]. Ob allerdings hinter den erfolglosen Abfragen tatsächlich fortgesetzter Missbrauch steht, oder ob es sich um (bereits seit langem) abgeschlossene Sachverhalte handelt, erschließt sich hieraus nicht. Jedenfalls bezieht sich der brasilianische Volumenfall auf Vorgänge, die in Brasilien schon zu Festnahmen der Täter geführt haben. Die eingangs vorgestellten Befunde lassen die Wahrscheinlichkeit, dass gerade über Volumenverfahren sexueller Missbrauch verhindert werden kann, als eher gering erscheinen. Dabei handelt es sich eher um Zufallsfunde, die auch bei sonstigen Ermittlungen auftreten dürften, wie die vorläufigen Ergebnisse der Niedersachsenstudie ausweisen.

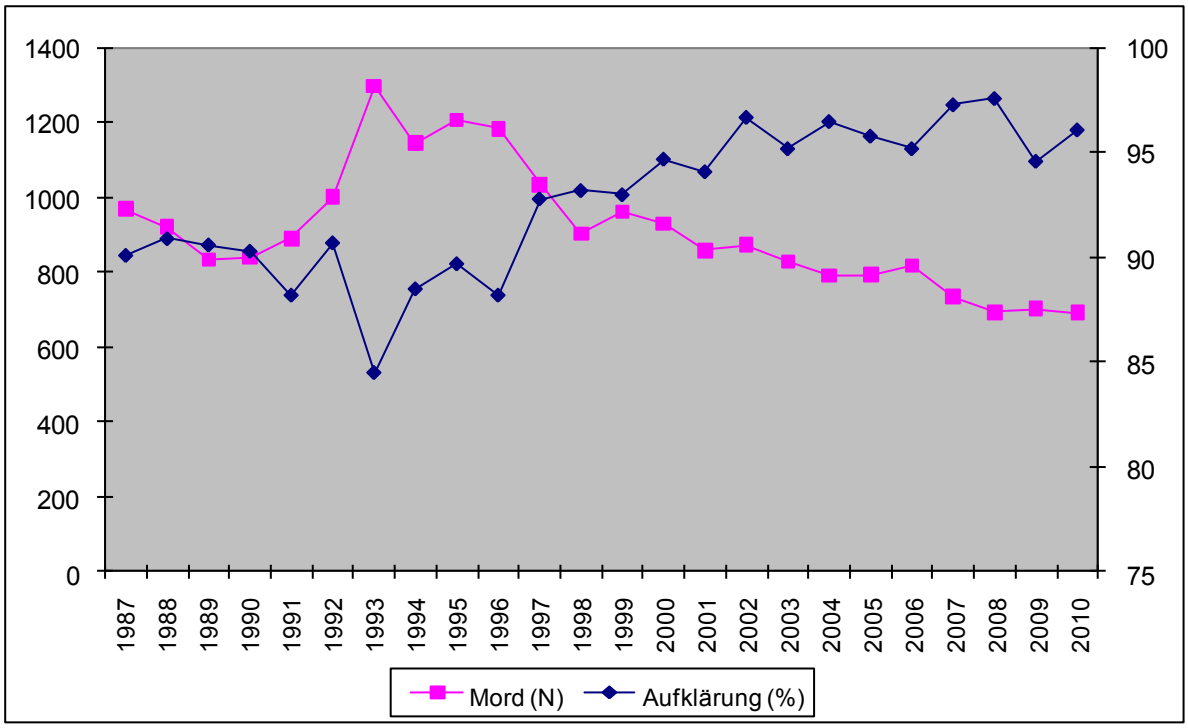
---

195 Bundeskriminalamt: Stand der statistischen Datenerhebung, a.a.O. (Fn. 164), S. 10.

4.5. Vorsätzliche Tötungsdelikte

Die Aufklärungsquote bei Tötungsdelikten ist stark bestimmt durch das Verhältnis zwischen Täter und Opfer. Dies ergibt sich bereits aus der Untersuchung von Sessar, die Verfahren aus den 1970er Jahren erfasst und besondere Probleme der Aufklärung bei Tötungsdelikten feststellt, in denen keine (bekannte) Beziehung zwischen Täter und Opfer vorliegt[196]. Die seit langer Zeit recht hohe Aufklärungsquote bei Tötungsdelikten ist wohl auch auf eine Entwicklung zurückzuführen, die Tötungsdelikte zwischen Fremden schon im 19. Jahrhundert zu relativ seltenen Ereignissen werden lässt[197].

*Schaubild D-19: Fallentwicklung und Aufklärung bei Mord 1987 bis 2010**



*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

Die Entwicklung von Aufklärungsraten und Fällen bei Morddelikten zeigt eine beständige Abnahme der Fallzahlen ab Anfang der 1990er Jahre und eine entsprechende Zunahme der Aufklärungsquote. Auch hier ergibt sich kein Hinweis darauf, dass sich die Vorratsdatenspeicherung in sichtbarer Weise ausgewirkt haben könnte.

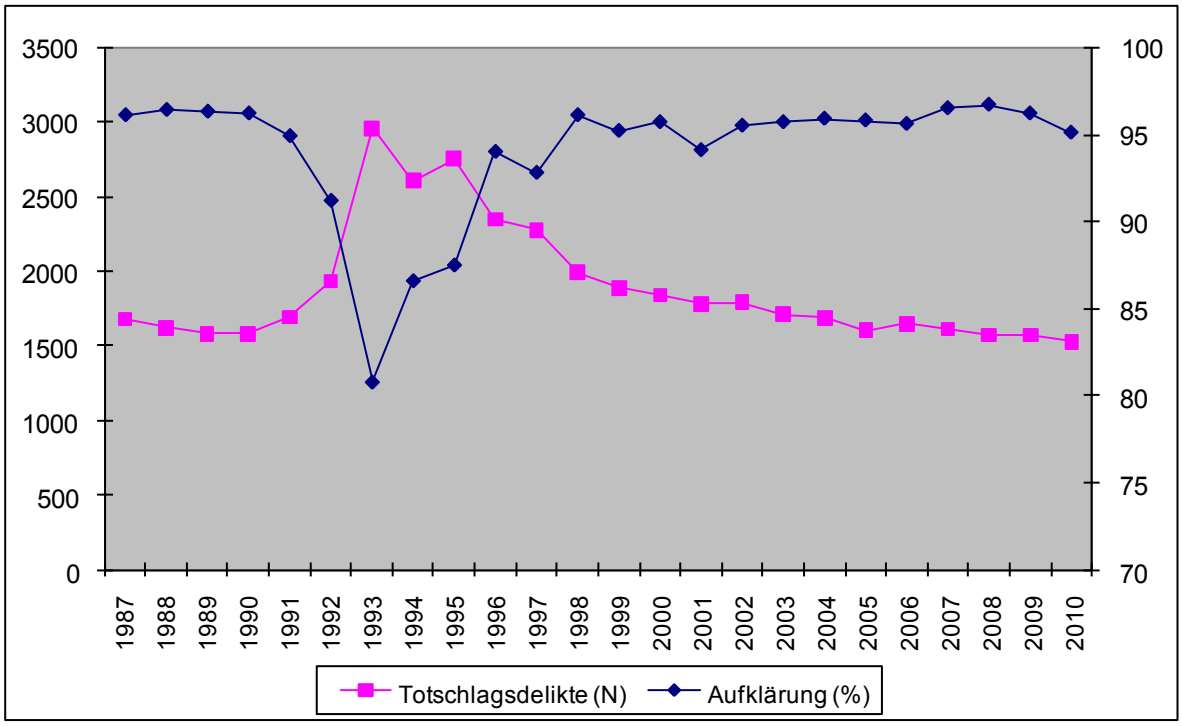
---

196 *Sessar, K.*: Rechtliche und soziale Prozesse einer Definition der Tötungskriminalität, Freiburg 1981, S. 130.

197 *Albrecht, H.-J.*: Gewaltkriminalität – Ursachen und Wirkungen. In: Dölling, D., Meier, B.-D., Verrel, T., Götting, B. (Hrsg.): Verbrechen – Strafe – Resozialisierung. Festschrift für Heinz Schöch zum 70. Geburtstag, Berlin 2010, S. 31-47.

Die Fallentwicklung und die Aufklärungsquote bei Delikten des Totschlags (§§ 212ff. StGB) enthält (wie bei Morddelikten) Besonderheiten, die in der ersten Hälfte der 1990er Jahre liegen und spezifische Phänomene dieser Jahre (Ermittlungen im Zusammenhang mit Schusswaffengebrauch an der ehemaligen innerdeutschen Grenze, Brandanschläge auf Asylbewerberheime) widerspiegeln. Die Jahre 1999-2009 sind durch stabile Aufklärungsquoten (und durch den Rückgang des Fallaufkommens) gekennzeichnet.

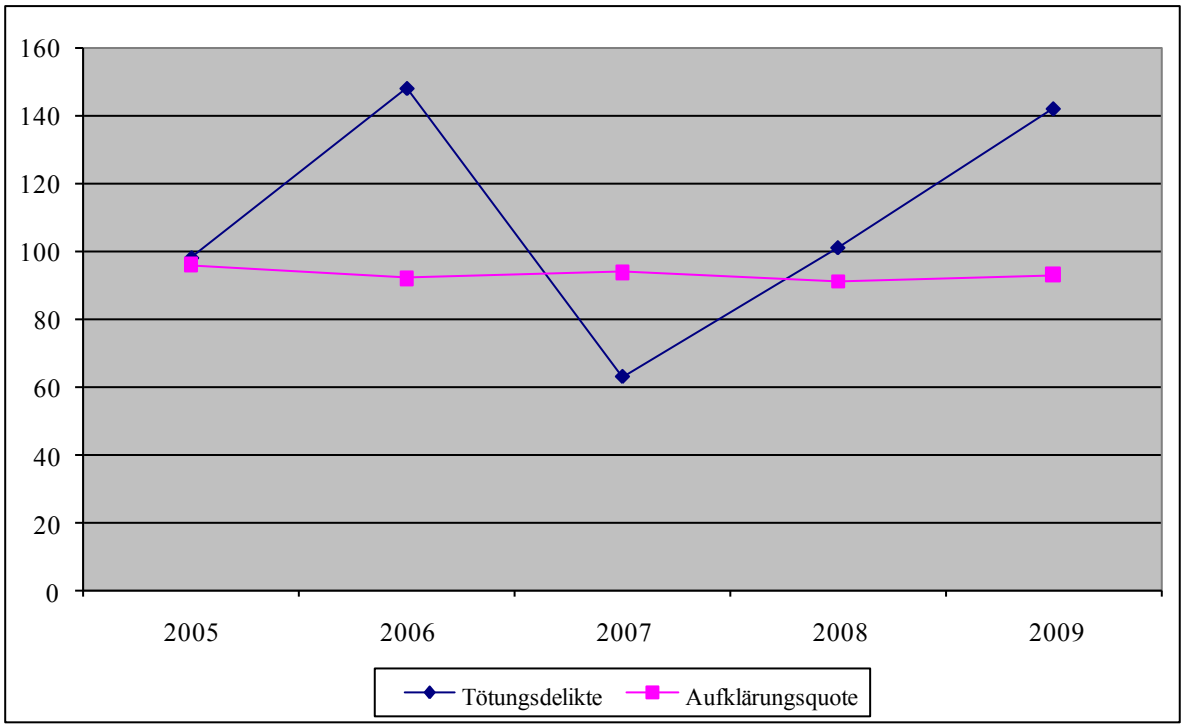
*Schaubild D-20: Fallentwicklung und Aufklärung bei Totschlag (§ 212 StGB)**



*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

In Österreich, wo Vorratsdaten bislang nicht gespeichert werden, ergeben sich für den Zeitraum 2005 bis 2009 keine Veränderungen in den Aufklärungsquoten bei vorsätzlichen Tötungsdelikten. Die Aufklärungsquoten liegen hier ebenso hoch wie in Deutschland (Schaubild D-21).

*Schaubild D-21: Tötungsdelikte und Aufklärungsquote in Österreich**



*) Quelle: Bundesministerium für Inneres: Sicherheitsberichte 2005 bis 2009. Wien 2006-2010.

In der vom Bundeskriminalamt vorgelegten Dokumentation sind verschiedene Tötungsdelikte aufgelistet, hinsichtlich derer Verkehrsdaten zentral für erfolgreiche Ermittlungen gewesen seien, aber wegen unergiebiger Abfragen nicht hätten genutzt werden können. Insgesamt handelt es sich um 7 Fälle aus 2009/2010 (die jedenfalls in einen Zusammenhang mit einem vorsätzlichen Tötungsdelikt gerückt werden (5 Verfahren wegen einer vorsätzlichen Tötung, 1 Verfahren wegen Straftaten im Umfeld eines im Ausland begangenen Tötungsdelikts, 1 Aufenthaltsermittlung eines aus Polen heraus im Ausland gesuchten und wegen Mordes Tatverdächtigen)[198]. Die Auswahl konzentriert sich auf Sachverhalte, die vom Bundeskriminalamt als „herausragende Rechtstatsachen“ und offensichtlich für den Nachweis der Bedeutung von auf Vorrat gespeicherten Verkehrsdaten als besonders aussagekräftig (im Hinblick auf die Entstehung von Sicherheitsdefiziten) bezeichnet werden[199].

> In dem aus Tauberbischofsheim berichteten Ermittlungsverfahren wegen des am 18.6. 2010 begangenen Tötungsdelikts an einer Frau[200] wurde am 25.11.2010 Anklage wegen Mordes erhoben. Die Beweislage ist nach Angaben der Polizei (auch auf Grund von DNA-Spuren) offensichtlich ohne Rückgriff auf Verkehrsdaten völlig ausreichend (nicht zuletzt deshalb, weil sich an der Tatwaffe DNA des Angeklagten

198 Bundeskriminalamt: Stand der statistischen Datenerhebung, a.a.O. (Fn. 164), Anhänge 1 und 2.

199 Bundeskriminalamt: Stand der statistischen Datenerhebung, a.a.O. (Fn. 164), S. 14.

200 Bundeskriminalamt: Stand der statistischen Datenerhebung, a.a.O. (Fn. 164), S. 19.

fand)[201]. Der Angeklagte wurde im Dezember 2010 zu lebenslanger Freiheitsstrafe verurteilt[202].

Der für Schleswig-Holstein eingeführte Fall einer vorsätzlichen Tötung vom 30.1. 2010[203] ist erstinstanzlich abgeschlossen. Der Angeklagte wurde im Dezember 2010 zu lebenslanger Freiheitsstrafe verurteilt[204]. Auch hier waren Verkehrsdaten zur Aufklärung und zum erfolgreichen Abschluss des Strafverfahrens nicht erforderlich.

Im Zusammenhang mit dem Tötungsdelikt an einem italienischen Staatsangehörigen in Leverkusen wurden offensichtlich vier Tatverdächtige und der Tatort innerhalb von 3 Monaten identifiziert. Es handelt sich um ein Tötungsdelikt im „Milieu“ (nach dem Toten war im Übrigen wegen verschiedener Raubdelikte gefahndet worden). Mittlerweile wird allerdings wohl wieder davon ausgegangen, dass Ansatzpunkte für weiterführende Ermittlungen nicht vorhanden sind[205]. Ein Hinweis dafür, dass Verkehrsdaten vorhanden und für die weiteren Ermittlungen hilfreich sein könnten, ergibt sich aus dem zugänglichen Ermittlungsstand allerdings nicht.

Der Fall eines vorsätzlichen Tötungsdelikts an einer jungen Frau in Mittelhessen (Cölbe) vom 24. April 2010[206] war bereits nach zwei Tagen (vor allem nach einem umfassenden Geständnis des Ex-Freundes) aufgeklärt[207]. Verkehrsdaten waren für den erfolgreichen Abschluss der Ermittlungen nicht erforderlich. Das Geständnis wurde in der Strafkammerverhandlung vom 17.11.2010, die zur Verurteilung wegen Totschlags führte[208], wiederholt[209].

Das Tötungsdelikt an einem Polizeibeamten am 23.11.2009 in Lauchhammer ist bislang nicht aufgeklärt. Gegen zwei Tatverdächtige wird weiter ermittelt. Ein Ermittlungsrichter sah jedoch bei einem Antrag der Staatsanwaltschaft auf Haftbefehl keinen dringenden Tatverdacht. DNA-Spuren am Tatort konnten den Tatverdächtigen nicht zweifelsfrei zugeordnet werden. Ein Lichtbild aus einem Blitzgerät, das einen der Tatverdächtigen im PKW des Opfers zeigen soll, wird von Staatsanwaltschaft und

---

201 www.polizei-tauberbischofsheim.de/PDTauberbischofsheim/Presse/Pressemitteilungen/20101125.pdf. [Juni 2011].

202 Südwest Presse, 14.12.2010.

203 Bundeskriminalamt: Stand der statistischen Datenerhebung, a.a.O. (Fn. 164), Anhang 2, S. 25 f.

204 Kieler Nachrichten Online [21.12.2010].

205 www rp-online.de/bergischesland/leverkusen/nachrichten/Mordkommission-Razzia-im-Saunaclub_aid_831031 html [Juni 2011].

206 Bundeskriminalamt: Stand der statistischen Datenerhebung, a.a.O. (Fn. 164), Anhang 2, S. 43.

207 www.hna.de/nachrichten/hessen/ex-freund-gesteht-mord-22-jaehriger-733131.html [Juni 2011].

208 rtl-hessen.de/videos.php?start=1120&video=12224&kategorie=&PHPSESSID=p616tf3g3lgjq7g69um26n0p54 [Juni 2011].

209 www hr-online.de/website/rubriken/nachrichten/indexhessen34938.jsp?rubrik=36090&key=standard_document_40201209 [Juni 2011].

Ermittlungsrichterin unterschiedlich bewertet. Erfolgreiche (beantwortete) Funkzellenabfragen zum unmittelbaren Tatort im Jahr 2009 erbrachten keine Hinweise auf die Tatverdächtigen; eine weitere Funkzellenabfrage für den weiteren Umkreis des Tatorts Monate später blieb wegen nicht mehr gespeicherter Daten weitgehend unbeantwortet. Allerdings wird nicht klar, warum bei der gegebenen Ermittlungslage hieraus Indizien für eine Täterschaft der immer noch Tatverdächtigen gezogen werden sollten. Denn die Tatverdächtigen kommen aus dem Umkreis des Tatorts[210].

Auf ein vorsätzliches Tötungsdelikt wird noch im Zusammenhang mit einem in Dubai lokalisierten und gut dokumentierten Fall Bezug genommen (Mord an einem Hamas-Waffenhändler). Hier geht es aber um eine mittelbare Falschbeurkundung (und ggfs.) nachrichtendienstliche Praktiken (des israelischen Geheimdienstes), da einer der (bekannten und dem israelischen Geheimdienst zugerechneten) Tatverdächtigen sich in Deutschland Ausweispapiere erschlichen hat, die für die Einreise nach Dubai benutzt wurden.

Ein weiterer Sachverhalt ergibt sich aus einer von Polen veranlassten Überprüfung von Einlog-Spuren in Deutschland (E-Mail), die einer in Polen wegen Mordes gesuchten Person zugeordnet werden sollten. Ob sich die gesuchte Person in Deutschland befunden hat und ob Einlog-Nachweise (mutmaßlich in Internetcafes) tatsächlich zur Ergreifung des Tatverdächtigen hätten führen können, ist allerdings wohl fraglich.

Insoweit lässt sich für Ermittlungen bei Tötungsdelikten auch aus dem durch das Bundeskriminalamt vorgelegten Material ein Bild zeichnen, das nicht dafür spricht, dass durch den Wegfall gespeicherter Verkehrsdaten schwerwiegende Sicherheitslücken wegen Unaufklärbarkeit schwerer Gewalt aufgetreten sind. Gerade auf die Feststellungen zu Tötungsdelikten hat sich aber offensichtlich der Beschluss der Innenministerkonferenz vom November 2010 gestützt, in dem es heißt, „Die IMK nimmt den Bericht "Stand der statistischen Datenerhebung im BKA sowie der Rechtstatsachensammlung für Bund (BKA, BPOL, ZKA) und Länder zu den Auswirkungen des Urteils des Bundesverfassungsgerichts zu Mindestspeicherfristen (Stand: 17.09.10) zur Kenntnis“ und wo dann festgestellt wird, dass mehr als ein halbes Jahr nach dem Urteil des Bundesverfassungsgerichts Erhebungen nachdrücklich belegten, dass der Wegfall der Mindestspeicherfrist für Telefon- und Internet-Verkehrsdaten zu einer erheblichen Schutzlücke in der Kriminalitätsbekämpfung geführt habe. Schwerste Verbrechen seien unaufgeklärt geblieben. In diesen Zusammenhang wird dann eine effektive Terrorismusbekämpfung gestellt, die angesichts einer anhaltenden Bedrohungslage auf Verkehrsdaten unbedingt angewiesen sei[211]. Auch in einer Stellungnahme des BDK wird auf die in der

---

210 www morgenpost.de/brandenburg-aktuell/article1474788/DNA-Spuren-ergeben-keinen-dringenden-Tatverdacht html [Juni 2011].

211 Ständige Konferenz der Innenminister und -senatoren der Länder Sammlung der zur Veröffentlichung freigegebenen Beschlüsse der 191. Sitzung der Ständigen Konferenz der Innenminister und -senatoren der Länder. Berlin, den 23.11.2010, S. 11.

Dokumentation des BKA enthaltenen Straftaten gegen das Leben verwiesen, die einen unabweisbaren Bedarf an Verkehrsdaten begründen würden[212]. Angesichts der Ermittlungsstände und Verfahrenserledigungen zu den durch das Bundeskriminalamt mitgeteilten und als Beleg für die Notwendigkeit der Vorratsdatenspeicherung gehandelten Tötungsdelikte handelt es sich hier ganz offensichtlich um ein jedenfalls folgenreiches Narrativ, das empirischen Grundlagen entbehrt, jedoch ein politisches Eigenleben entfalten sollte und konnte. Sichtbar wird dies auch im Evaluationsbericht der Europäischen Kommission, wo der Lauchhammer-Fall (vorsätzliches Tötungsdelikt an einem Polizeibeamten) prominent platziert wurde[213].

4.6. Cyber-Grooming

Der Prävention der Vorbereitung des sexuellen Missbrauchs durch bestimmte Formen der Kontaktaufnahme mit Kindern im Internet wird neuerdings (wieder) erhebliche öffentliche Aufmerksamkeit zuteil[214].

Insgesamt sind bislang nur wenige repräsentative Untersuchungen durchgeführt worden, die sich mit Risiken von Kindern und Jugendlichen, nach der Initiierung von Kontakten über das Internet, Opfer von Sexualstraftaten sei es on- oder offline zu werden, befassen[215]. Risiken für junge Menschen im Zusammenhang mit dem Internet werden in Kontakte mit Pornografie, Bullying sowie Cyber-Stalking und in die eingangs genannten Kontakte mit Erwachsenen, die sexuelle Beziehungen zu Kindern oder Jugendlichen (online oder offline) aufnehmen wollen, unterschieden[216]. Erwartungsgemäß tritt die gewollte und ungewollte Konfrontation mit pornographischen Inhalten nach allen Untersuchungen häufig auf[217]. Aus einer europäischen Studie ergibt sich ein Anteil von 14% in der Altersgruppe der 11-16 Jährigen, der mit sexualbezogenen Bildern konfrontiert war; ein Drittel fand die Betrachtung der Bilder unangenehm[218]. 22% der befragten 11-16 Jährigen sahen sich im Internet potenziell riskanten Inhalten ausgesetzt (darunter Suizid, Drogen, Hasspropaganda etc.). Wie vor dem Hintergrund

---

212 Bund Deutscher Kriminalbeamter Landesverband Hessen: BDK-Verbandszeitschrift Nr. 10, Oktober 2010 – Onlineausgabe, S. 6.

213 European Commission, Fn. 152, 2011, S. 24.

214 *Feil, C.*: Kinder und Internet – Chancen und Gefahren. Recht der Jugend und des Bildunsgwesens 58 (2010), S. 410-415.

215 Zusammenfassend *Roberts, L.*: Cyber-Victimisation in Australia. Extent, Impact on Individuals and Responses. Hobart 2008.

216 Vgl. nunmehr hierzu auch das Schwerpunktheft 4/2010 von Recht der Jugend und des Bildungswesens.

217 *Altstötter, C.*: Pornografie und neue Medien. Eine Studie zum Umgang Jugendlicher mit sexuellen Inhalten im Internet. Mainz 2006; *Wolak, J., Mitchell, K., Finkelhor, D.*: Unwanted and Wanted Exposure to Online Pornography in a National Sample of Youth Internet Users. Pediatrics 119 *(*2007), S. 247-257.

218 *Livingstone, S., Haddon, L., Görzig, A., Ólafsson, K.*: Risks and Safety on the Internet. The perspective of European children. Initial findings from the EU Kids Online survey of 9-16 year olds and their parents. www.eukidsonline.net, 21. Oktober 2010, S. 11.

der Ergebnisse der Dunkelfeldforschung zu erwarten war, überlappen sich Täter- und Opferrollen auch im Falle des Cyber-Bullying[219].

Aus einer amerikanischen Untersuchung zu Fällen sexuellen Missbrauchs, die ihren Ausgangspunkt in der Herstellung von Internetkontakten hatten, ergibt sich, dass die Opfer ganz überwiegend zwischen 13 und 15 Jahre alt waren. Keines der Opfer war jünger als 12 Jahre. Die Täter waren zu etwa drei Viertel älter als 26 Jahre[220]. Täuschungen über das Alter der Täter und Altersunterschiede kommen selten vor; sie unterscheiden sich im Ausmaß wohl nicht von Schönungen des Alters und Anderem, die auch in Online- und Offline Kontaktanbahnungen zwischen Erwachsenen beobachtet werden können. Der Internetkontaktaufnahme folgen häufig Telefonate, die Übersendung von Fotos und Geschenken. In etwa der Hälfte der Fallberichte der Polizei wird festgehalten, dass die Opfer das Gefühl einer engen Freundschaft mit dem Täter entwickelt hätten. Soziale Netzwerke im Internet spielen nach einer amerikanischen Untersuchung von polizeilich registrierten Fällen von Sexualdelikten an Kindern vor allem wegen polizeilicher Praktiken der Tatprovokation eine Rolle. Etwa 73% der aus sozialen Netzwerken resultierenden Fälle gehen auf verdeckte Ermittlungen zurück, in denen sich Polizeibeamte als Kinder oder Jugendliche ausgeben[221]. Kontaktaufnahmen durch Fremde sind stark bestimmt durch das Vorhandensein eines Profils in einem sozialen Netzwerk und durch das Online-Stellen von Fotos[222]. Online-Kontakte resultieren selten in riskanten Situationen. Nach dieser Studie ist die Online Kommunikation fast ausschließlich auf bereits vorher bekannte Personen bezogen[223]. 8% der 9- bis zu 16-Jährigen, die Online-Kontakte mit anderen Personen hatten, haben diese dann auch offline getroffen. Davon geben etwas mehr als 10% der Kinder und Jugendlichen an, dieses Treffen sei „unangenehm“ oder „störend“ gewesen[224]. Unangenehm kann natürlich eine ganze Reihe von Erlebnissen sein. Da sich die Autorinnen über das „Unangenehme“ nicht näher auslassen, können die Resultate wohl so interpretiert werden, dass nichts Schwerwiegendes passiert ist. In absoluten Zahlen zeigt sich, dass bei 23.420 Befragten 240 sich nach Online-Kommunikation auf als „störend“ oder „unangenehm“ empfundene Offline Kontakte mit einer Person einließen, die sie vorher nicht gekannt hatten[225]. Dabei handelt es sich fast ausschließlich um Kontakte mit Gleichaltrigen oder jüngeren Personen. 10 der Befragten gaben an, entsprechende Kontakte mit Er-

---

219 *Pujazon-Zazik, M., Park, M.J.*: To Tweet, or Not to Tweet: Gender Differences and Potential Positive and Negative Health Outcomes of Adolescents' Social Internet Use. American Journal of Mens Health 4 (2010), S. 77-85, S. 81.

220 *Wolak, J., Finkelhor, D., Mitchell, K.*: Internet-initiated Sex Crimes against Minors: Implications for Prevention Based on Findings from a National Study. Journal of Adolescent Health 35 (2004), S. 424.e11–424.e20.

221 *Mitchell, K.J., Finkelhor, D., Jones, L.M., Wolak, J.*: Use of Social Networking Sites in Online Sex Crimes Against Minors: An Examination of National Incidence and Means of Utilization. Journal of Adolescent Health 47 (2010) S. 183–190, S. 185.

222 *Smith, A.*: PEW Internet and American Life Project, abrufbar unter www.pewinternet.org [14.10.2007].

223 *Livingstone, S., Haddon, L., Görzig, A., Ólafsson, K.*: a.a.O. (Fn. 218), S. 46.

224 *Livingstone, S., Haddon, L., Görzig, A., Ólafsson, K.*: a.a.O. (Fn. 218), S. 98f.

225 *Livingstone, S., Haddon, L., Görzig, A., Ólafsson, K.*: a.a.O. (Fn. 218), S. 98.

wachsenen (>20 Jahre) gehabt zu haben (0,04% der Befragten). Letzteres bedeutet, dass das Internet offensichtlich im Hinblick auf Kontakte mit Erwachsenen in der Altersgruppe der 9-16-Jährigen nichts Relevantes hinzufügt. Schließlich zeigt sich in der europäischen Studie wieder einmal das Problem, über die Herstellung von Ranglisten hinaus in eine sinnvolle vergleichende Analyse einzutreten. Denn der Befund, dass knapp ein Viertel der rumänischen Kinder und Jugendlichen sexuell konnotierte Mitteilungen erhielten und lediglich 3% der italienischen jungen Menschen wird sich wohl nicht vollständig aufklären lassen[226].

Die meisten Online-Kontakte von jungen Menschen betreffen ihre eigene Altersgruppe und sind erwartungsgemäß nicht-sexueller Art sowie den Eltern bzw. Erziehungsberechtigten bekannt[227]. Kontaktaufnahmen zu jungen Menschen, die sexuellen Charakter oder sexuelle Anspielungen beinhalten, gehen ganz überwiegend (>90%) von anderen Jugendlichen oder Heranwachsenden aus. Davon wiederum sind die meisten nicht auf Treffen in der realen Welt hin angelegt[228]. Die Fälle sexueller Kontaktanbahnungen sind im Übrigen auf Jugendliche konzentriert. Kinder sind davon kaum betroffen. Ferner wird darauf hingewiesen, dass die meisten Kontaktversuche ignoriert oder jedenfalls angemessen beantwortet werden[229]. Kommt es zu (seltenen) Treffen in der realen Welt, so handelt es sich in der Regel um Jugendliche (und nicht um Kinder), denen die Motive der Anderen bekannt sind; kommt es zu sexuellen Handlungen, dann sind diese freiwillig, jedenfalls nicht durch Gewalt bestimmt [230]. Emotionale Zuwendung, Geld und Geschenke spielen eine Rolle[231], in besonderem Maße lassen sich solche junge Menschen auf im Internet initiierte Annäherungen von Erwachsenen ein, die im familiären Umfeld und darüber hinaus besonderen Problemen ausgesetzt sind[232]. Was in der Verteilung des (polizeilich registrierten sexuellen Missbrauchs insgesamt zum Ausdruck kommt, nämlich ein besonderes Risiko im sozialen Nahraum, in der Familie sowie in Institutionen dürfte sich im Übrigen im Cyberraum wieder finden. Auch Untersuchungen polizeilich registrierter und über das Internet initiierter Sexualdelikte an Kindern und Jugendlichen verweisen darauf, dass im Vordergrund Täter stehen, die dem Opfer bereits bekannt sind.

---

226 *Livingstone, S., Haddon, L., Görzig, A., Ólafsson, K.*: a.a.O. (Fn. 218), S. 80, über den Hinweis hinaus, es sei schwierig diese Muster zu interpretieren, findet sich auch kein ernsthafter Versuch der Auseinandersetzung mit den auch bei anderen Variablen auftretenden offensichtlichen und krassen Differenzen.

227 *Schrock, A., Boyd, D.*: Online Threats to Youth: Solicitation, Harassment, and Problematic Content. Literature Review Prepared for the Internet Safety Technical Task Force http://cyber.law harvard.edu/research/isttf. Berkman Center for Internet & Society Harvard University, S. 17 [31.12.2008].

228 *Schrock, A., Boyd, D.*: a.a.O. (Fn. 227), S. 9.

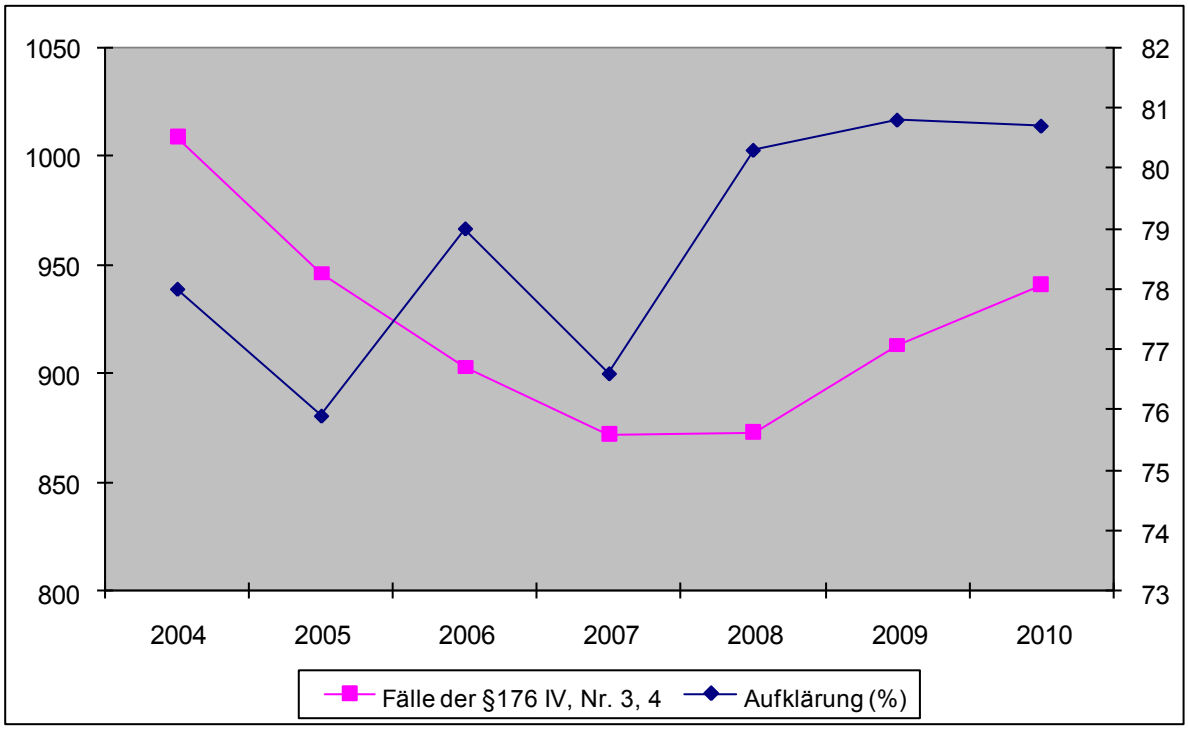
229 *Schrock, A., Boyd, D.*: a.a.O., (Fn. 227), S. 10 f.

230 *Pujazon-Zazik, M., Park, M.J.*: a.a.O., 2010, S. 77-85.

231 *Shannon, D.*: Vuxnas kontakter med barn via Internet. Omfattning, karaktär, åtgärder (The online sexual solicitation of children by adults in Sweden). Report 11, Stockholm 2007.

232 *Shannon, D.*: a.a.O.

*Schaubild D-22: Aufklärungsquote bei § 176 Abs. 4, Nr. 3, 4 StGB**



*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

Allerdings lassen die in der Polizeistatistik enthaltenen Daten keine Differenzierung zwischen den Tatbeständen des § 176Abs. 4 Nr. 3 und 4 StGB zu. Ob überhaupt in nennenswerter Anzahl Fälle des Cybergrooming (Nr. 3) enthalten sind, muss deshalb offen bleiben.

4.7. Nachstellen (Stalking)

Besondere Probleme der Aufklärung und besonderer Bedarf an Vorratsdaten werden bei Ermittlungen wegen des Delikts der Nachstellung (§ 238 StGB) geltend gemacht. Hier habe die Ermittlungsarbeit ausweislich veröffentlichter Stellungnahmen einen erheblichen Rückschlag erlitten, der unmittelbar mit dem Verbot der Vorratsdatenspeicherung durch das Bundesverfassungsgericht zusammenhänge[233]. Dagegen werden in den bislang vorliegenden Untersuchungen der Strafverfolgung bei Stalking, die auf eine systematische Zusammenstellung auch der Beweisprobleme abzielen, fehlende Möglichkeiten des Rückgriffs auf gespeicherte Telekommunikationsdaten nicht genannt[234]. Dies ist auch gar nicht zu erwarten, denn die Forschung zu Stalking belegt, dass Anzeigen in akuten Situationen des Nachstellens gestellt

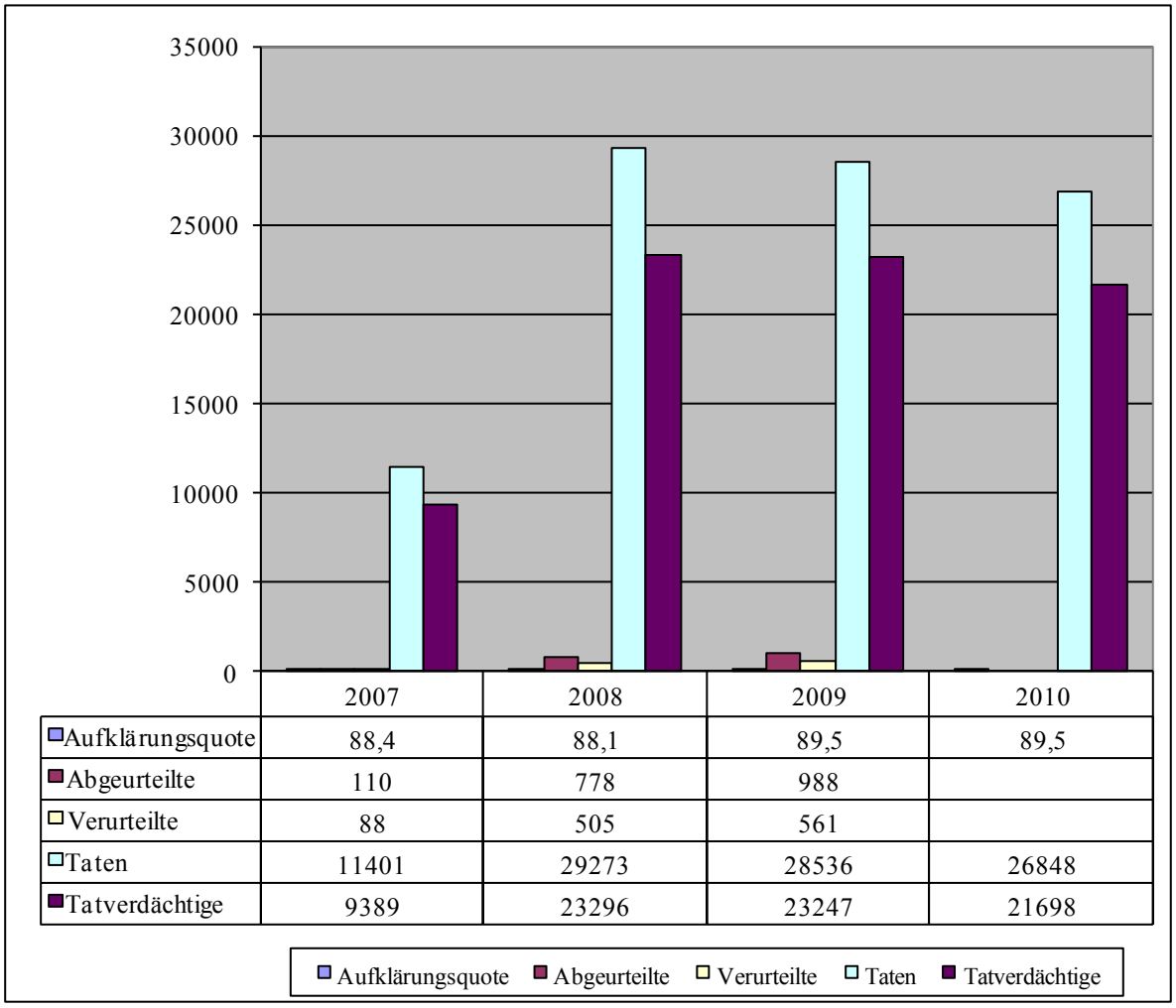
---

233 Süddeutsche Zeitung, 14.10.2010, Stalking – Verfolgt auf Schritt und Tritt.

234 Vgl. hierzu *Fünfsinn, H.*: Erste Erfahrungen mit dem Stalking-Bekämpfungsgesetz. Lawzone 1 (2010), S. 13-16; *Etzel, T.*: §238 StGB (Nachstellen) in der anwaltlichen Praxis. Lawzone 1 (2010), S. 17-22; *Rusch, S.*: Das „Gesetz zur Strafbarkeit beharrlicher Nachstellung" – Allheilmittel polizeilicher Intervention bei Stalking? Lawzone 1 (2010), S. 22-30.

werden, die dann zu auf die Gegenwart und auf die Zukunft angelegte Ermittlungen führen werden (falls Ermittlungsaufwand überhaupt betrieben wird)[235].

*Schaubild D-23: Aufklärungsquote und Fallentwicklung bei Stalking (Nachstellen, § 238 StGB)**



	2007	2008	2009	2010
Aufklärungsquote	88,4	88,1	89,5	89,5
Abgeurteilte	110	778	988	
Verurteilte	88	505	561	
Taten	11401	29273	28536	26848
Tatverdächtige	9389	23296	23247	21698

*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2009, www.bka.de (Berichte und Statistiken); Statistisches Bundesamt: Strafverfolgungsstatistiken 2007-2010. Wiesbaden 2008- 2011.

Die kurze Geltung des Tatbestandes der Nachstellung erlaubt zwar keine Längsschnittbetrachtung, doch bieten die Daten der polizeilichen Kriminalstatistik sowie der Strafverfolgungsstatistik, die die Jahre 2007 bis 2009 (2010) abbilden, einige bedeutsame Hinweise. Das Delikt des Nachstellens ist durch ein hohes Aufkommen an registrierten Taten und Tatverdächtigen gekennzeichnet sowie durch eine hohe Aufklärungsquote. Dem steht eine sehr kleine Zahl von Abgeurteilten und Verurteilten gegenüber. Die außerordentliche Diskrepanz

235 Vgl. zu entsprechenden Klagen über fehlende Bereitschaft zu Ermittlungen von Opfern/Anzeigeerstattern bei *Etzel, T.*: § 238 StGB (Nachstellen) in der anwaltlichen Praxis. Lawzone 1 (2010), S. 17-22; *Burgheim, J.*: Stalking – Erklärungsansätze und neue Forschungsergebnisse. Die Kriminalpolizei 2007, S. 52-58, S. 57.

zwischen der Zahl der Tatverdächtigen und derjenigen der Verurteilten wird sichtbar, wenn auf das Verhältnis zwischen Tatverdächtigen und Verurteilten insgesamt abgestellt wird.

Während in Deutschland insgesamt durchschnittlich etwa 30 Verurteilte auf 100 Tatverdächtige im Jahr 2009 entfallen (656.122 Verurteilte, 2.187.217 Tatverdächtige (wobei darauf hinzuweisen ist, dass Polizeiliche Kriminalstatistik und Strafverfolgungsstatistik nicht unmittelbar aufeinander bezogen werden können, da es sich nicht um Verlaufsstatistiken handelt), liegt die Quote beim Delikt des Nachstellens bei 2 %. Das Problem liegt hier ganz offensichtlich nicht in der Aufklärung und in der Ermittlung von Tatverdächtigen (denn diese sind den Opfern und über deren Anzeige den Strafverfolgungsbehörden regelmäßig bekannt), sondern in Bereichen, die mit dem Zugang zu Verkehrsdaten zur Identifizierung eines Tatverdächtigen nicht zusammenhängen können[236]. Denn die Jahre 2007 bis 2009 zeigen eher einen kleinen Zuwachs in der von vornherein recht hohen Aufklärungsquote. Da die Strafzumessungspraxis bei den Verurteilungen wegen Nachstellens zunächst durch Geldstrafen (70 %) und durch zu Bewährung ausgesetzte Freiheitsstrafen (25 %) charakterisiert ist, ist anzunehmen, dass ein erheblicher Teil der Verfahren über Geringfügigkeitseinstellungen erledigt wird. Dies ergibt sich aus für das Bundesland Hessen für 2008 mitgeteilten Daten, die sich auf 1209 erledigte Verfahren wegen Nachstellens beziehen[237]. Danach wurden nach §§ 170 Abs. 2, 152 Abs. 2 StPO 33,4 % der Verfahren eingestellt, wegen Geringfügigkeit kam es in 18 % der Verfahren zur Einstellung. 21,7 % der Fälle wurden auf den Privatklageweg verwiesen; in 13,7 % der Fälle kam es zu sonstigen Entscheidungen. 4,4 % der Verfahren resultierten in einem Strafbefehl und 9,2% in einer Anklage. Nahezu die Hälfte der Verfahren führen demnach wegen eines fehlenden öffentlichen Interesses nicht zu einer Anklage bzw. zu einem Strafbefehl. Im Übrigen bereiten insbesondere die Tatbestandsmerkmale, die sich auf „Beharrlichkeit“ und „schwerwiegende Konsequenzen für das Opfer“ beziehen, Probleme[238]. Im Zusammenhang mit Hauptverhandlungen wird gerade wegen der Komplexität der sich teilweise über lange Zeiträume hinziehenden Handlungen eine Tendenz zu Absprachen angesprochen[239]. Ferner wird es bei der Verfolgung von Anzeigen wegen Nachstellens auch zu Ermittlungen wegen anderer Straftaten (Körperverletzung, Nötigung, Beleidigung, Hausfriedensbruch etc.) kommen, die dann zur Verurteilung gelangen und teilweise dazu führen, dass jedenfalls in der Strafverfolgungsstatistik (in die das jeweils schwerste Delikt aufgenommen wird) eine Verurteilung nicht mehr auftaucht.

---

236 Hierzu *Fünfsinn, H.*: Erste Erfahrungen mit dem Stalking-Bekämpfungsgesetz. Lawzone 1 (2010), S. 13-16, S. 15, der aus einer hessischen Untersuchung mitteilt, dass nach Angaben der Staatsanwaltschaften die in wegen Stalking gestellten Anzeigen mitgeteilten Sachverhalte überwiegend den Tatbestand des § 238 nicht erfüllten.

237 *Fünfsinn, H.*: Erste Erfahrungen mit dem Stalking-Bekämpfungsgesetz. Lawzone 1 (2010), S. 13-16, S. 15.

238 Zu entsprechenden Erfahrungen und Verteilungen in Schleswig-Holstein vgl. *Stahlmann-Liebelt, U.*: § 238 StGB - Das Wundermittel der Zukunft? Gemeinsam gegen Stalking. Fachtagung am 31. Oktober 2007 im Landeshaus in Kiel.

239 *Etzel, T.*: § 238 StGB (Nachstellen) in der anwaltlichen Praxis. Lawzone 1 (2010), S. 17-22, S. 21.

Die im Kontext der Strafverfolgung des Nachstellens entstandene Diskussion verlangt für Verbesserungen der Strafverfolgung im Übrigen eine Anpassung der Tatbestandsmerkmale (Beharrlichkeit und schwerwiegende Konsequenzen) und strukturierte Vernehmungen[240] bzw. eine der Komplexität der Fälle gerechte Aufbereitung und Substantiierung in der Anklageschrift[241]. Angesichts der weiter oben dargestellten Verteilungen und Entwicklungen ist nicht einmal in Ansätzen nachvollziehbar, warum der Wegfall der Vorratsdatenspeicherung für die Strafverfolgung von Stalking zu Defiziten in Ermittlungen und Schutzlücken resultieren sollte. Das „Nachstellen" stellt sich in der polizeistatistischen Erfassung schon fast als ein Massendelikt dar, dessen Profil auf die Zielsetzungen der Vorratsdatenspeicherung (organisierte Kriminalität, Schwerkriminalität, terroristische Gewalt) nicht passt.

Im Übrigen ist Bedarf an auf Vorrat gespeicherten Telekommunikationsdaten für erfolgreiche Ermittlungen bei Stalking-Fällen auch in der Begründung der österreichischen TKG-Novelle zur Umsetzung der Richtlinie 2006/24/EG geäußert worden. Der österreichische Datenschutzrat hat in seiner Stellungnahme zum Entwurf mit großer Deutlichkeit darauf hingewiesen, dass der Tatbestand zu einem beliebten Anzeigedelikt geworden und sicherheitspolitisch völlig bedeutungslos sei[242].

4.8. Bedrohung (§ 241 StGB)

Drohungsdelikte werden zum einen durch § 241 StGB erfasst, zum anderen enthält § 126 StGB eine Strafbestimmung. Straftaten nach § 126 StGB sind in der Polizeilichen Kriminalstatistik nicht gesondert ausgewiesen. Die nachstehenden Ausführungen beziehen sich deshalb allein auf § 241 StGB.

Die polizeistatistischen Daten zeigen für die Bedrohung eine Zunahme der registrierten Taten bis etwa 2000. Die Aufklärungsquote geht seit etwa 2004, allerdings in sehr geringfügigen Schritten, zurück. Der Rückgang setzt sich bis zum Jahr 2008 fort. Eine leichte Zunahme der Aufklärungsquote wird in den Jahren 2009 und 2010 sichtbar. Die im Jahr 2008 vorhandene Möglichkeit des Rückgriffs auf gespeicherte Verkehrsdaten hat demnach keine in den Aufklärungsquoten sichtbare Veränderung mit sich gebracht.

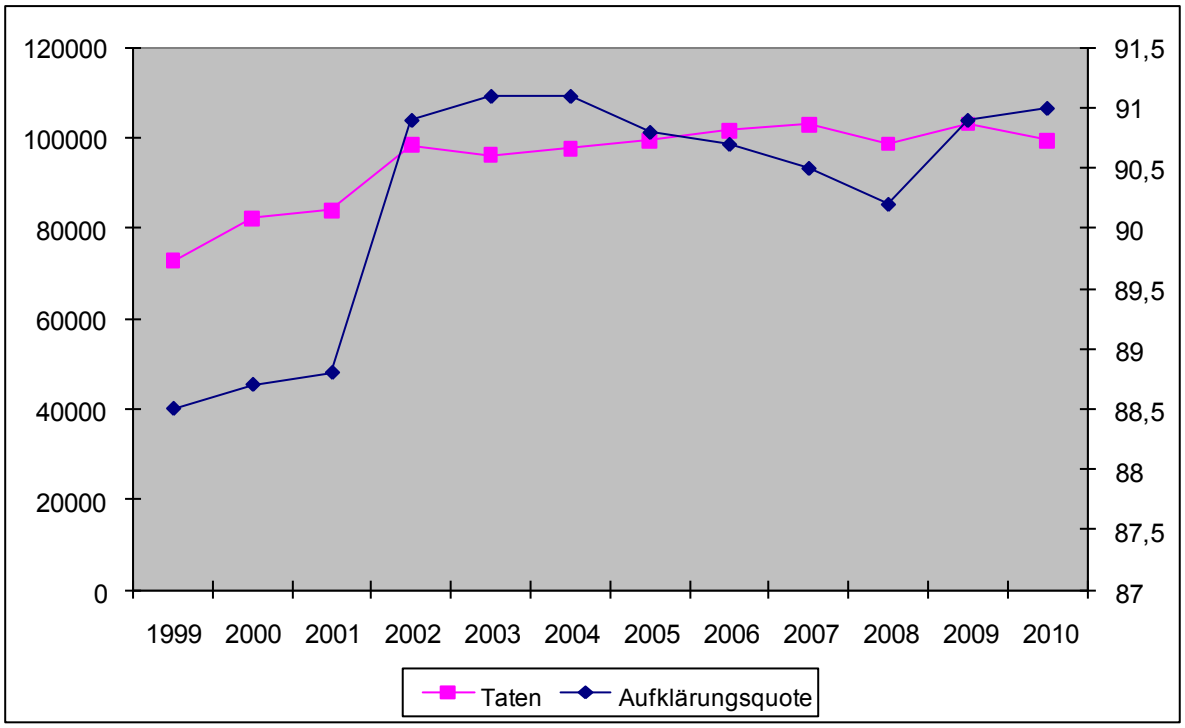
---

240 *Rusch, S.*: Das „Gesetz zur Strafbarkeit beharrlicher Nachstellung" – Allheilmittel polizeilicher Intervention bei Stalking? Lawzone 1 (2010), S. 22-30, S. 30.

241 *Etzel, T.*: § 238 StGB (Nachstellen) in der anwaltlichen Praxis. Lawzone 1 (2010), S. 17-22, S. 21.

242 Datenschutzrat: Stellungnahme zur TKG-Novelle zur Umsetzung der Richtlinie über Vorratsdatenspeicherung. GZ BKA-817304/0003-DSR/2007.

*Schaubild D-24: Fallaufkommen und Aufklärungsquoten bei Bedrohung (§ 241 StGB)**



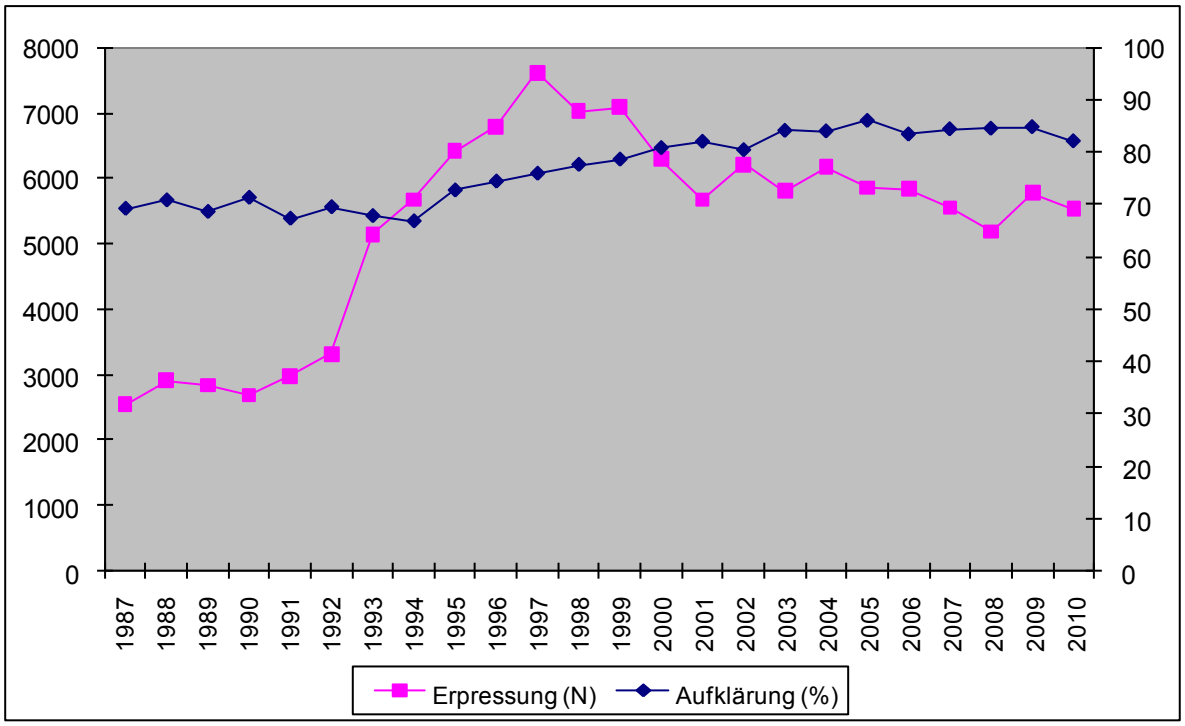
*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

Im Fallmaterial des BKA sind 5 Fälle der Bedrohung enthalten. Es handelt sich um die Androhung von Bombenanschlägen, Amoklauf und Tötungsdelikten (sie sind teilweise nach § 241, teilweise als Taten des § 126 StGB einzustufen). Die Fälle bleiben ungeklärt. Es ist aus der Dokumentation allerdings nicht unmittelbar abzuleiten, dass eine Rückverfolgung zu einer Aufklärung hätte führen können. Erwartungsgemäß kam es in keinem Fall zu einer Realisierung der Drohung.

4.9. Erpressung

Das Delikt der Erpressung verweist auf eine seit Anfang des neuen Jahrtausends stabile Aufklärungsquote. Aus den Verläufen lässt sich nichts entnehmen, was auf Veränderungen durch die Vorratsdatenspeicherung hinweisen würde.

*Schaubild D-25: Fallaufkommen und Aufklärungsquoten bei Erpressung**



*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

4.10. Weitere Delikte

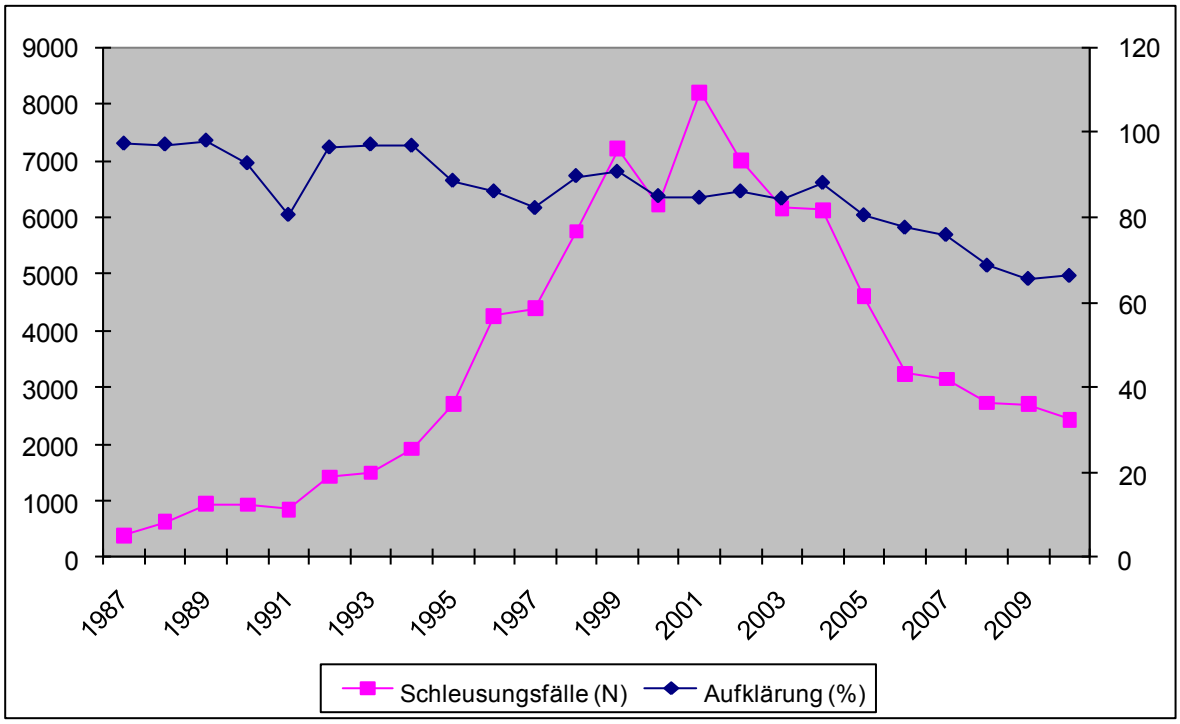
4.10.1. Banden- und gewerbsmäßig begangene Delikte

Banden- und gewerbsmäßig begangene Delikte (Diebstahl, Hehlerei, Schleusung von Ausländern, Drogendelikte) verweisen zum Teil auf organisierte Kriminalität bzw. auf kriminelle Netzwerke, in denen Tatwiederholung und die Kommunikation zwischen Tatbeteiligten besondere Bedeutung haben. Dem Fallmaterial des BKA sind insgesamt 12 (aus etwa 50) derartige Sachverhalte zu entnehmen[243]. Dabei geht es zum Teil um Fälle, die im Ausland angesiedelt sind, und für die entweder Bewegungen in Deutschland oder Kontakte nach Deutschland überprüft werden sollten. Im Wesentlichen handelt es sich um Delikte, die teilweise aufgeklärt sind, wo allerdings (begründet) vermutet wird, dass weitere Taten (oder Mittäter) zugeordnet werden können. Hier dient der Zugriff auf Verkehrsdaten einer weiteren Ausforschung eines Sachverhalts, für den allerdings weitere Ermittlungsansätze zur Verfügung stehen. Ferner liegen grundsätzlich Beweismittel vor, die zu Strafverfahren und Verurteilungen führen.

---

243 Bundeskriminalamt: Stand der statistischen Datenerhebung, a.a.O. (Fn. 164), Anhang 2.

*Schaubild D-26: Schleusung von Ausländern und Aufklärung**



*) Quelle: Bundeskriminalamt PKS-Zeitreihen für den Zeitraum von 1987 bis 2010, www.bka.de (Berichte und Statistiken).

Die Betrachtung der Entwicklung des Schleusens von Ausländern ergibt keine Hinweise dafür, dass sich durch die Einführung der Vorratsdatenspeicherung am langfristigen Trend des Rückgangs der Aufklärungsquoten etwas verändert hat. Die Entwicklungen in den registrierten Taten sind sicher zum größeren Teil durch die Verlagerung der Schengen-Grenzen bedingt.

4.10.2. Enkeltrick (Betrug)

Betrugsdelikte, die auf dem so genannten „Enkeltrick“ basieren, werden im rechtspolitischen Diskurs ebenso regelmäßig wie die Kinderpornografie als Beispiel dafür herangezogen, dass die Vorratsdatenspeicherung nicht verzichtbar sei. Geht es bei der Kinderpornografie um als besonders schutzbedürftig anerkannte Kinder, so geht es beim „Enkeltrickbetrug“ um die besondere Schutzbedürftigkeit alter Menschen. Derartige Betrugsdelikte werden aber weder in der Polizeilichen Kriminalstatistik des Bundes noch der Länder gesondert ausgewiesen. Gesamtaussagen zur Aufklärung können deshalb hierzu nicht getroffen werden. Entsprechende Daten werden offensichtlich auch nicht systematisch in Inpol oder KPMD eingegeben, so dass aussagekräftige Daten auch außerhalb der polizeilichen Kriminalstatistik nicht gewon-

nen werden können[244]. Bereits dies weist darauf hin, dass dem Enkeltrickbetrug in der polizeilichen Praxis keine zentrale Bedeutung beigemessen wird (bzw. beigemessen werden kann), handelt es sich doch um einen sehr kleinen Ausschnitt aus dem Gesamtaufkommen der Vermögensdelikte mit einem ganz geringfügigen Anteil an dem durch Betrug insgesamt verursachten Schaden.

Nur vereinzelt ergeben sich Hinweise auf die Gesamtzahl erfasster Fälle in einzelnen Bundesländern und in den Zuständigkeitsbereichen von Polizeidirektionen. Die lokal mitgeteilten Fallzahlen können teilweise in einen Bezug zum Gesamtaufkommen an Betrugsfällen gestellt werden. So werden für Nordrhein-Westfalen für das Jahr 2008 272 versuchte und 52 vollendete Taten mit einem Gesamtschaden von knapp 550.000;- € gemeldet[245]. Für Hessen wurden im Jahr 2004 140 Fälle (davon 107 Versuche) mit einem Gesamtschaden von etwa 300.000,- € registriert[246]. Dies dürfte durchschnittliche Erfahrungen sowohl für den erheblichen Anteil an Versuchen, als auch für die durchschnittliche Schadenshöhe der vollendeten Betrugsfälle sowie die bisherigen Erfahrungen in anderen Ländern (Österreich, Schweiz) und Bundesländern im Hinblick auf das Auftreten von Enkelbetrugsfällen widerspiegeln[247]. Verwiesen wird auch auf eine hohe Dunkelziffer. Sicher ist, dass Ermittlungsmöglichkeiten grundsätzlich von Anzeigen der Opfer abhängen. Das Deliktsphänomen des „Enkelbetrugs“ unterliegt starken regionalen Schwankungen, die durch entsprechende Bewegungen der Tätergruppen verursacht werden. So wird für Baden-Württemberg zwischen 2008 und 2009 eine starke Zunahme verzeichnet, mit Schwerpunkten in Karlsruhe, Stuttgart und Mannheim. Der Schaden stieg in diesem Zeitraum von 45.870.- € auf 557.900,- €[248]. Dies entspricht den Mitteilungen des Regierungspräsidiums Karlsruhe, wo zwischen 2008 und 2009 ein Zuwachs von 36 auf 74 Fälle festgestellt wurde. Die durchschnittliche Schadenssumme betrug 2009 16.000.- €, die Aufklärungsquote belief sich auf knapp 10 % (7 von 74 registrierten Straftaten)[249].

Aufklärungsergebnisse lassen sich ansatzweise den Berichten des Polizeipräsidiums Mittelfranken (Nürnberg) entnehmen. Danach kam es 2008 zu 54 Fällen, von denen 8 Fälle geklärt

---

244 Vgl. hierzu *Ludwig, J.*, Enkeltrick – Kollektive Strafvereitelung durch Unzuständigkeit? der kriminalist 38 (2006), S. 55- 60, S. 55, 59.

245 Stadtsparkasse Düsseldorf, LKA Nordrhein-Westfalen: Kampagne gegen Enkeltrick, Düsseldorf 4. März 2009.

246 Informationsveranstaltung der Polizei Marburg zum Thema -Enkeltrick-, 20.2.2008, abrufbar unter www.polizei.hessen.de; für 2005 wird von der Frankfurter Polizei ein Gesamtschaden von 185.000,- € für Frankfurt mitgeteilt, nicht jedoch die Zahl der vollendeten Delikte, vgl. S. 142.

247 Vgl. hierzu *Ludwig, J.*, Enkeltrick – Kollektive Strafvereitelung durch Unzuständigkeit? der kriminalist 38(2006), S. 55- 60; *Ludwig, J.*: Enkeltrick – Grenzen der Ermittlungen und der Prävention. der kriminalist 41 (2009), S. 4-9; www.polizei.bayern.de/schuetzenvorbeugen/senioren/index html/93155, vom 27.11.2010: 22 Fälle im Zuständigkeitsbereich der Polizeidirektion München im Jahr 2009 mit einem Gesamtschaden von 227.000 €.

248 LKA Baden-Württemberg: Polizeiliche Kriminalstatistik 2009, Stuttgart 2010, S. 10.

249 www rp.baden-wuerttemberg.de/servlet/PB/menu/1309516/index htm [Juni 2011].

werden konnten (Aufklärungsquote 14,8%). Ermittelt wurden 8 Tatverdächtige[250]. Im Jahr 2009 wurden 145 Straftaten registriert (107 Versuche), bei einem Gesamtschaden von ca. 200.000 €. Gegenüber 2008 (54 Straftaten) wird somit ein Anstieg um 91 Delikte festgestellt. Die Ursache für den starken Anstieg beim Enkeltrick wird in erweiterten Auswertungsmöglichkeiten lokalisiert. Ab Herbst 2008 sei seitens der Telekom eine Speicherung ausländischer Anrufernummern erfolgt, was in der Folge rückwirkende Recherchen zu solchen Rufnummern ermöglicht habe. Von den im Jahr 2009 registrierten Straftaten wurden 22 aufgeklärt und 5 Beschuldigte ermittelt. Insoweit beträgt die Aufklärungsquote 15,2 %. Die Aufklärungsquoten unterscheiden sich demnach im Vergleich von 2008 und 2009 nicht.

Wesentliche Informationen zu der Entstehung des Phänomens, zu Durchführungspraktiken, den grenzüberschreitenden Aktivitäten sowie zu den Tätern und der Größe der Tätergruppen lagen schon kurz nach dem ersten Auftreten des Enkelbetrugsphänomens, das auf Ende der 1990er Jahre datiert wird, vor[251]. Das spezifische Delikt des Enkeltricks wird einer ethnischen Gruppe zugeordnet, die in verschiedenen europäischen Ländern, allerdings auch in Nordamerika, lokalisiert wird. Die Größe dieser Gruppe wird auf etwa 2000 Personen geschätzt[252]. Allerdings dürfte es wohl auch Nachahmer geben. Besondere Schwerpunkte des Enkeltricks haben sich für Deutschland, die Schweiz und Österreich ergeben. Diese Schwerpunkte werden neben Hauptwohnorten der Organisatoren und Täter wohl auch durch sprachliche Bedingungen erklärt. Allerdings wird der „Enkeltrickbetrug“ in den letzten zehn Jahren auch in anderen europäischen Ländern, ferner in Nordamerika beobachtet. Der Enkeltrick reiht sich im Übrigen ein in eine ganze Reihe von Trickdiebstählen und Trickbetrügereien, die den „Zetteltrick“ oder „Wassertrick“ sowie Anderes umfassen. Im Bereich der Polizei Hannover wurden zum Beispiel im Jahr 2009 250 Fälle des Enkeltricks, 222 Fälle „falscher Stadtwerker“, 105 Zetteltrickfälle und 94 Geldwechseltrickereignisse gezählt[253]. Die Opfer des Enkelbetrugs rekrutieren sich (gezielt) aus alten Menschen, wobei das Durchschnittsalter der Opfer auf über 80 Jahre geschätzt wird[254]. Das Vorgehen besteht in der massenweise telefonischen Kontaktaufnahme aus dem Ausland mit Personen, die an Hand von Vornamen und an Hand von Recherchen über digitale Telefonverzeichnisse der Gruppe alter Menschen zugerechnet wird. Der angerufenen Person wird vorgetäuscht, dass der Anrufer/die Anruferin in einem Verwandtschaftsverhältnis oder einem Freundschaftsverhältnis (Enkel, Neffe etc.) steht und dringend Geld benötigt. Die Angerufenen werden aufgefordert, das Geld sofort zu

---

250 Polizeipräsidium Mittelfranken: Sicherheitsbericht Nürnberg 2008. Nürnberg 2009, :S. 28.

251 *Ludwig, J.*, Enkeltrick – Kollektive Strafvereitelung durch Unzuständigkeit? der kriminalist 38 (2006), S. 55- 60; *Ludwig, J.*: Enkeltrick – Grenzen der Ermittlungen und der Prävention. der kriminalist 41 (2009), S. 4-9.

252 Rudolf Mäder, Leiter des Dezernats für Betrugs- und Wirtschaftskriminalität in Bern, Interview: www.tagesschau.sf.tv/Nachrichten/Archiv/2009/08/27/Schweiz/Enkeltrick-Betrueger-ergaunern-jaehrlich-Millionen [Juni 2011].

253 www.pfiffige-senioren.de/ [Juni 2011].

254 Polizeipräsidium Mittelfranken: Sicherheitsbericht Nürnberg 2008. Nürnberg 2009, :S. 28; *Ludwig, J.*: Enkeltrick – Grenzen der Ermittlungen und der Prävention. der kriminalist 41 (2009), S. 4-9, S. 4.

beschaffen. Ist der erste Kontakt erfolgreich, werden mobile Gruppen an den Wohnort der Angerufenen herangeführt, die dann nach weiteren Anrufen, in denen mitgeteilt wird, dass der Anrufer nun verhindert sei, persönlich vorbei zu kommen, aber einen Vertrauten schicken werde, die Abholung des Geldes vornehmen. Aus dieser Vorgehensweise ergibt sich auch, dass die Anbahnungsgespräche ganz überwiegend fehlschlagen werden und ferner ein erhebliches Dunkelfeld besteht[255]. Der Polizei werden Fälle im Wesentlichen durch Anzeigen von Opfern bekannt. Die Vorgehensweise führt schließlich dazu, dass sich die Tatortschwerpunkte beständig verlagern. Dies wird auch an den Mustern der Warnungen vor Enkeltrickbetrügern durch die Polizei in Deutschland, Österreich und in der Schweiz sichtbar.

Für die Prävention wird vor allem auf die Aufklärung alter Menschen und ihrer Angehörigen[256] sowie die Zusammenarbeit mit Banken und Sparkassen gesetzt (denn die Abhebung großer Geldbeträge wird in aller Regel die Aufmerksamkeit des Schalterpersonals erregen). So gehen Ermittlungserfolge darauf zurück, dass Bankangestellte darüber informieren, dass ältere Kunden ungewöhnlich viel Geld abheben[257]. Auf Ermittlungsansätze, die an eine frühzeitige Benachrichtigung durch Banken und Sparkassen anknüpfen, zielen auch die in den letzten Jahren teilweise aufgelegten gemeinsamen Initiativen von Polizei und Finanzinstituten[258].

Die spezifische Tatanbahnung bei dem Enkeltrick verweist auf die besondere Bedeutung der Telekommunikationsdaten insbesondere für die Herstellung von Verbindungen zwischen einer Vielzahl von meist erfolglos bleibenden Einzeltaten[259]. Besondere Ermittlungsprobleme ergeben sich allerdings auch wegen der Begehung der Delikte aus dem Ausland, der Nutzung von ausländischen SIM-Karten und vor allem aus der Zersplitterung der Ermittlungszuständigkeiten in Deutschland. Die lokale Ermittlungszuständigkeit führe dazu, dass zahlreiche Einzeltaten registriert würden, die hinsichtlich der Schwere der Tatbegehung nicht ins Gewicht fielen und deshalb häufig in der Einstellung der Verfahren resultierten[260]. In den letzten Jahren werden deshalb zunehmend Projekte zentraler Ermittlungsführung durchgeführt[261]. Hierdurch sollen Tatzusammenhänge besser erkannt und eine effektivere Bekämpfung dieser Straftaten durch besonders qualifizierte und spezialisierte Beamte gewährleistet werden[262]. Jedoch wird auch betont, dass eine Zusammenführung der Verfahren für Deutschland insge-

---

255 So wurde in einem Kölner Verfahren festgestellt, dass die Angeklagte von den Niederlanden aus bis zu 1000 Telefongespräche täglich nach Deutschland geführt habe, Kölner Stadtanzeiger, „Prozess. Tausend Telefonate pro Tag“, 5.10.2009.

256 Bundeskriminalamt: Infopool Prävention. Newsletter 1/2007, S. 3.

257 www.abendblatt.de/hamburg/article788687/Enkeltrick-Polnische-Banden-agieren-bundesweit.html [27.2.2006].

258 Polizeipräsidium Mittelfranken: Sicherheitsbericht Nürnberg 2008. Nürnberg 2009, :S. 28.

259 Polizeipräsidium Frankfurt: Polizeiliche Kriminalstatistik 2008. Teil 2. Frankfurt 2009, S. 150.

260 www rp.baden-wuerttemberg.de/servlet/PB/menu/1309516/index htm; vgl. schon *Ludwig, J.*, Enkeltrick – Kollektive Strafvereitelung durch Unzuständigkeit? der kriminalist 38 (2006), S. 55- 60 [Juni 2011].

261 Polizeipräsidum Mittelfranken: Sicherheitsbericht Nürnberg 2009, Nürnberg 2010, S. 34.

262 Polizeipräsidium Mittelfranken: Sicherheitsbericht Nürnberg 2008, Nürnberg 2009, :S. 28.

samt notwendig wäre. Dies scheitere aber daran, dass entweder von vornherein Zusammenhänge nicht erkannt würden und ferner wenig Interesse an einer die Bundesländer übergreifenden zentralen Ermittlung bestehe. Insoweit kommt es wohl auch dazu, dass wegen einzelner Fälle keine Anträge auf Verkehrsdatenabfragen gestellt bzw. Gerichte diese (wegen nicht nachgewiesener Bedeutung) grundsätzlich nicht erlassen würden[263].

Im Fallmaterial des BKA hat der Enkeltrick eine gewisse Prominenz. Es geht um drei Fälle mit 12 versuchten Taten und einem vollendeten Betrugsdelikt[264]. Besondere Betonung erfährt der Enkeltrickbetrug wegen der besonderen Schutzbedürftigkeit alter Menschen, der im Einzelfall dramatischen finanziellen Auswirkungen für die Opfer und wegen der Annahme, dass durch derartige Straftaten das Vertrauen in die Sicherheit nachhaltig gestört werde.

Für Nordrhein-Westfalen lässt sich der Enkeltrickbetrug in den Zusammenhang mit dem Gesamtaufkommen an Betrugsfällen stellen. Im Zeitraum 2008 wurden in Nordrhein-Westfalen 151.117 Betrugsfälle (ohne Beförderungserschleichung) registriert, mit einem Gesamtschaden von 345.850.204,- €[265]. Enkeltricksbetrugsfälle repräsentieren somit 0,2 % der Betrugsfälle insgesamt (ohne Beförderungserschleichung) sowie 0,16 % des durch Betrugsfälle verursachten Schadens.

Im Vergleich der Entwicklungen des Enkeltrickphänomens in Deutschland, Österreich und der Schweiz, der allerdings lediglich auf Pressemitteilungen (auch solcher der Polizei) gestützt werden kann, ergibt sich nicht, dass durch die unterschiedliche Gestaltung der Vorratsdatenspeicherung (die in Deutschland 2008/2009 zur Verfügung stand, in Österreich bislang nicht implementiert wurde und in der Schweiz seit 2002/2004 Abfragen über 6 Monate in die Vergangenheit zulässt) Unterschiede in Ermittlungseffizienz (und insbesondere Auswirkungen auf das Auftreten der Täter) resultieren. Das Enkeltrickphänomen tritt seit etwa 2001[266] in der Schweiz bis heute mit denselben Schwankungen und Schwerpunktbildungen auf[267], wie sie auch in Deutschland oder Österreich beobachtet werden. Einzelne Fall- und Verfahrensbeschreibungen lassen davon ausgehen, dass eine typische Verfahrensauslösung über Opferanzeige und sich anschließende Zusammenarbeit mit der Polizei bei der Geldübergabe und als Regelfall eine Aburteilung nur einzelner Fälle auch die Lage in der Schweiz charakte-

---

263 Zusammenfassend *Ludwig, J.*: Enkeltrick – Grenzen der Ermittlungen und der Prävention. der kriminalist 41 (2009), S. 4-9, S. 7.

264 Bundeskriminalamt: Stand der statistischen Datenerhebung, a.a.O. (Fn. 164), im BKA sowie der Rechtstatsachensammlung für Bund (BKA, BPOL, ZKA) und Länder zu den Auswirkungen des Urteils des Bundesverfassungsgerichts zu Mindestspeicherungsfristen, Wiesbaden, Stand: 17.09.10.

265 Landeskriminalamt Nordrhein-Westfalen: Polizeiliche Kriminalstatistik 2008. Tabellenanhang. Düsseldorf 2009, S. 222 f.

266 Tagesanzeiger Schweiz: Wie die angeblichen Enkel die Oma und den Opa übers Ohr hauen, von *Christine Anna-Huber*. Aktualisiert am 23.08.2009.

267 Bundesamt für Polizei: Kriminalitätsbekämpfung Bund. Lage, Massnahmen und Mittel. Jahresbericht 2009, Bern 2010, Teil 1, Lage Wirtschaftskriminalität.

risieren[268]. In der Schweiz wird mit der Einrichtung einer nationalen Koordinationsstelle sowie mit Aufklärungsinitiativen, ebenso wie in Deutschland, versucht, Schutzmöglichkeiten zu verstärken, die über strafrechtliche Maßnahmen allein nicht herzustellen sind.

Durch Zusammenarbeit mit Schweizer Behörden sowie den nach der Entscheidung des Bundesverfassungsgerichts im März 2010 verfügbaren Ermittlungsmaßnahmen ist es im Übrigen im Stuttgarter Raum kürzlich gelungen, eine international operierende Gruppe von Enkeltrickbetrügern samt den die Taten dirigierenden Personen zu überführen[269], wie dies offensichtlich bereits im Sommer 2010 der Fall war[270]. Insoweit ergeben sich im Bereich des Enkeltrickbetrugs offensichtlich auch ohne Rückgriff auf gespeicherte Vorratsdaten effiziente Ermittlungsansätze.

5. Aufklärungsquote, Ermittlungseffizienz und Schutzlücken

Der Zugriff auf Vorratsdaten der Telekommunikation erfolgt lediglich in einer sehr kleinen Zahl von Verfahren. Dies ergibt sich bereits aus den insgesamt registrierten Zugriffen auf Verkehrsdaten, ferner aus vereinzelten Hinweisen, die zwar nicht in vollem Umfang nachvollziehbar sind, sich jedoch in das Gesamtbild einfügen. So teilte das Niedersächsische Innenministerium in der Antwort auf die eingangs behandelte Kleine Anfrage im Landtag mit, dass die niedersächsische Polizei zwischen 1. Juli 2010 und 10. November 2010 eine interne Erhebung durchgeführt habe. Diese habe, wie weiter oben bereits ausgeführt, ergeben, dass bei 454 gemeldeten Straftaten, in denen es aus Ermittlungsgründen erforderlich gewesen wäre, die Verbindungsdaten zu erheben, 409 Taten gar nicht mehr bzw. nur noch unzureichend aufgeklärt werden konnten. Dieser Umstand wird als Beleg dafür herangezogen, dass für eine Vielzahl von Straftaten Verkehrsdaten den einzigen Ermittlungsansatz darstellten und nach Wegfall der sogenannten Vorratsdatenspeicherung nicht mehr bzw. nur wesentlich erschwert aufgeklärt werden könnten[271]. Der Verweis auf „interne Untersuchungen“ und die Mitteilung von Zahlen wären angemessen, wenn die Zahlen begleitet wären von Informationen, die eine, wenn auch nur bescheidene, Nachvollziehbarkeit und Interpretierbarkeit mit sich bringen würden. Dies ist hier aber nicht der Fall. Denn Bezugszahlen sind nicht verfügbar. Nicht mitgeteilt wird ferner, wie die Daten erhoben worden sind oder, auf welche Straftatbestände sich die Ermittlungen bezogen. Mitgeteilt wird im Wesentlichen nur, dass 409 Straftaten in einem bestimmten Zeitraum nicht hätten aufgeklärt werden können.

Nun wurden in Niedersachsen in dem angegebenen Zeitraum (geschätzt auf der Basis der Daten von 2009) etwa 210.000 Straftaten registriert und davon wurden 84.000 nicht aufgeklärt. Bei der Annahme von 454 Fällen, in denen es erforderlich gewesen wäre, Vorratsdaten

---

268 Tagesanzeiger Schweiz: Basler Enkeltrick-Betrüger müssen hinter Gitter, 23.10.2009.

269 Stuttgarter Zeitung, „Enkeltrick-Serie. Bandenchefs hinter Gitter“. Donnerstag, 6.1.2011.

270 Stuttgarter Zeitung „Enkeltrick“-Bande. Hintermann in Polen verhaftet“, 4.8.2010.

271 Niedersächsischer Landtag − 16. Wahlperiode Drucksache 16/3056. Kleine Anfrage mit Antwort. Wie weiter mit der Vorratsdatenspeicherung?, S. 6.

abzufragen, ergibt dies eine in den Gesamtzahlen der Aufklärung somit nicht mehr wahrnehmbare Veränderung. Denn angesichts von insgesamt etwa 84.000 nicht aufgeklärter Straftaten in diesem Zeitraum spielen 409 Straftaten keine bedeutsame Rolle (0,5 %). Wie dies die Innere Sicherheit beeinflussen soll, ist nicht nachvollziehbar. Im Übrigen kann durch einen solchen Untersuchungsansatz auch nicht mit Sicherheit nachgewiesen werden, dass die Tat bei einer Rückgriffsmöglichkeit hätte aufgeklärt werden können.

Die niedersächsische Staatsanwaltschaft hat ferner im Jahr 2008 25.724 Verfahren erledigt, im Rahmen derer sich Verkehrsdatenabfragen konzentrieren dürften (Verfahren wegen organisierter Kriminalität, Staatsschutzkriminalität, politische Kriminalität, Verbreitung von Pornografie, Schleusung von Ausländern, Geldwäsche, Serien-, Gruppengewalt- und Bandenkriminalität, Verbrechen nach dem BtMG, Kapitaldelikte[272]). Verfahren wegen IuK-Delikten können deshalb nicht einbezogen werden, weil die Staatsanwaltschaftsstatistik diese nicht gesondert ausweist. Im Jahr 2009 handelte es sich um 21.352 Verfahren aus diesem Deliktsbereich (der Rückgang im Vergleich zu 2008 beruht weitgehend auf der Verbreitung pornografischer Schriften). Dies bedeutet, dass in einem Kernbereich von Verfahren, in denen sich Maßnahmen der Telekommunikationsüberwachung konzentrieren werden, im Jahr 2008 766 Verfahren mit Abfragen) in 3 % der Verfahren und 2009 (679 Verfahren mit Abfragen) in 3,3 % der Verfahren Verkehrsdatenabfragen durchgeführt wurden. Dies schließt den Rückgriff auf Vorratsdaten sowohl im Jahr 2008 als auch (unter den Bedingungen der einstweiligen Anordnung des Bundesverfassungsgerichts) im Jahr 2009 ein. Von den Abfragen des Jahres 2009 blieben ausweislich der Statistiken des Bundesamts für Justiz 53 ohne oder ohne vollständiges Ergebnis[273]. Damit wären also etwa 0,2 % der Verfahren in dem beschriebenen Deliktsausschnitt dann betroffen, wenn sich tatsächlich alle nicht oder nicht vollständig erfolgreichen Abfragen darauf konzentriert hätten.

Im Übrigen ist allerdings nur ein allgemeiner Blick auf die Entwicklung der Verfahrenserledigungen in niedersächsischen Staatsanwaltschaften möglich. In Tabelle D-1 sind die Quoten der Anklagen, Strafbefehlsanträge, der Einstellungen nach §§ 153ff. StPO, der Abgabe als Ordnungswidrigkeit und des Verweises auf den Privatklageweg sowie der Einstellungen nach § 170 Abs. 2 StPO enthalten.

Die Erledigungen zeigen zwischen 2002 und 2009 eine gleichbleibende Tendenz im Rückgang von Anklagen und Strafbefehlen und in der Zunahme der nach § 170 Abs. 2 StPO eingestellten Verfahren. Nichts deutet darauf hin, dass durch die Zugriffsmöglichkeiten auf Vorratsdaten, die im Jahr 2008 sowie im Jahr 2009 zur Verfügung standen, eine Veränderung der Tendenzen eingetreten ist.

---

272 Statistisches Bundesamt: Staatsanwaltschaftsstatistik 2008;Wiesbaden 2009, S. 24.

273 Bundesamt für Justiz: Übersicht Telekommunikationsüberwachung (Maßnahmen nach § 100g StPO) für 2009, Bonn, 28.10.2010.

*Tabelle D-1: Erledigungsstruktur in niedersächsischen Staatsanwaltschaften 2002-2009**

	An-klage	*Straf befehl*	*§§ 153 ff. StPO*	*§ 170 StPO*	*OWi u. Privat-klage*	*Insges. erledigt*
2002	12,7	12,8	28	24,7	10,7	428795
2003	12,5	12,8	27,9	24,8	9,6	451209
2004	11,5	13,3	29,3	24,4	9,4	454176
2005	11,5	13,2	29,6	24,9	9,4	458790
2006	11,4	12,6	28,8	26,2	9,4	457493
2007	11,5	11,9	27,8	26,8	10,1	468763
2008	10,9	11,3	27,5	27,4	10,2	474750
2009	10,9	10,9	27,3	28,1	10,3	464489

*) Quelle: Statistisches Bundesamt: Staatsanwaltschaftsstatistik 2002-2009. Wiesbaden 2003-2010.

Geht man schließlich davon aus, dass Niedersachsen als großer Flächenstaat eine zwar nicht repräsentative, aber doch aussagekräftige Aussage für die Größenordnungen von Vorratsdatenabfragen zulässt (Niedersachsens Anteil an der Bevölkerung betrug 2009 9,7 %, der Anteil an registrierten Straftaten ebenfalls,[274] und dass die Periode auf 12 Monate verallgemeinert werden kann, dann könnte – falls die „interne Untersuchung" tatsächlich das Aufkommen wegen fehlender Kommunikationsdaten nicht aufklärbarer Straftaten wiedergibt – bundesweit von etwa 13.000 Fällen ausgegangen werden, in denen zum Zwecke der Aufklärung auf Daten der Vorratsspeicherung hätte zurückgegriffen werden müssen.

Dem stehen allerdings Aussagen gegenüber, die mit den für Niedersachsen ermittelten und ferner mit den Sondererhebungen des Bundesamts für Justiz übereinstimmenden Daten zu der Abfragepraxis kaum in Einklang zu bringen sind. Denn es wird von Ermittlungslagen für verschiedene Deliktsbereiche ausgegangen, die sich vor dem Urteil des Bundesverfassungsgerichts in erheblich höheren Abfragewerten und Aufklärungsquoten hätten äußern müssen. So wird angenommen, dass bei den im Jahr 2008 registrierten 38.000 Fällen von IuK-Kriminalität für 80% nur elektronische Spuren vorgelegen hätten, die geeignet gewesen seien, Straftaten aufzuklären und die Straftäter zu überführen. Weitere Beweismittel seien in diesen Fällen nicht vorhanden gewesen[275]. Dies würde – und in einen solchen Zusammen-

274 Bundeskriminalamt: Polizeiliche Kriminalstatistik 2009, Wiesbaden 2010, S. 49.

275 Wetzlar-Kurier, Nr 4/29. Jahrgang, Wie geht es nach dem Karlsruher Urteil weiter mit der „Vorratsdatenspeicherung"? Ein Interview mit dem Vorsitzenden des Innenausschusses des Deutschen Bundestages, Wolfgang Bosbach, MdB, über die Entscheidung des Bundesverfassungsgerichts zum Thema „Vorratsdatenspeicherung" und ihre Folgen für die Gesellschaft und den Gesetzgeber (www.gemeinsam-gegen-stalking.de/attachments/File/karlsruher_urteil.pdf) [Juni 2011].

hang wird die Aussage gestellt - bedeuten, dass allein etwa 30.000 dieser Fälle nur bei Zugriff auf gespeicherte Verkehrsdaten hätten aufgeklärt werden können. Ferner würde dies bedeuten, dass für den Bereich der Internetkriminalität im Vergleich der Jahre 2007 und 2008 ein erheblicher Zuwachs in der Aufklärung hätte beobachtet werden müssen. Dies ist allerdings, wie die weiter oben dargestellten Zeitreihen ausweisen, gerade in den Kernbereichen des Computerbetrugs und anderer mittels Kommunikationsmitteln durchgeführter Straftaten nicht der Fall.

Auf der Ebene kriminalstatistischer Daten bietet sich schließlich noch ein Vergleich zwischen Deutschland und der Schweiz an. In der Schweiz ist seit etwa 10 Jahren eine Vorratsdatenspeicherung eingeführt, die so genannte „Randdaten" der Telekommunikation umfasst. In der Schweiz wurde im Jahr 2009 erstmals eine bundesweite polizeiliche Kriminalstatistik vorgestellt. Aus ihr und aus der deutschen polizeilichen Kriminalstatistik folgen die Daten, die in Tabelle D-2 enthalten sind. Bei aller gebotenen Vorsicht, die unterschiedliche Deliktsdefinitionen, unterschiedliche Zählweisen etc. gebieten, lässt sich doch für die in der Tabelle enthaltenen Deliktsbereiche die Aussage treffen, dass die Aufklärungsquote in Deutschland in keinem Fall unter den für die Schweiz mitgeteilten Aufklärungsquoten liegt. Vielmehr liegen die Aufklärungsquoten teilweise deutlich höher. Dies gilt auch für solche Delikte, für die die besondere Bedeutung des Zugriffs auf Telekommunikationsverkehrsdaten hervorgehoben wird (also Computerbetrug, Verbreitung von Pornografie (einschließlich Kinderpornografie oder Drohung).

*Tabelle D-2: Aufklärungsquoten in Deutschland und in der Schweiz 2009**

	Schweiz		*Deutschland*	
	Absolut	Aufklärung %	Absolut	Aufklärung %
Pornografie	1.080	85,9	11.597	85,6
Computerbetrug	4.688	33,3	22.963	34,8
Tötungsdelikte	236	88,1	2277	96,7
Einbruchsdiebstahl**	51.758	12,7	1.108.766	14,9
Raub	3.530	36,9	49.317	52,6
Erpressung	349	74,5	5.776	84,8
Menschenhandel	50	74	811	88,7
Drohung	11.686	84,5	103.211	90,9

*) Quellen: Bundeskriminalamt: Polizeiliche Kriminalstatistik 2009. Wiesbaden 2010; Bundesamt für Polizei: Polizeiliche Kriminalstatistik 2009. Bern 2010;
**) für Deutschland wurde der Diebstahl unter erschwerenden Umständen insgesamt einbezogen, weil sich eine andere Kategorie nicht anbietet.

Neuere Berichte aus der Schweiz heben im Übrigen nach wie vor besondere Ermittlungsprobleme in der Identifizierung von Tatverdächtigen und in der Beweissicherung auch bei der Vorratsdatenhaltung hervor, die mit der Verbreitung von effizienten Anonymisierungstechniken, der Nutzung öffentlicher WLAN-Netze, dem Cloud Computing und anderem zusammenhängen[276].

276 Bundesamt für Polizei: Kriminalitätsbekämpfung Bunde. Jahresbericht 2009, Bern 2010, S. 28f.

Teil E: Der Evaluationsbericht der Europäischen Kommission

1. Der Berichtsinhalt

Der Evaluationsbericht der Europäischen Kommission gliedert sich in verschiedene Teile. Dabei geht es nur in einem kurzen Abschnitt (S. 21-25) um die Evaluation im eigentlichen Sinn, das heißt, um die Auswirkungen von Verkehrsdatenabfragen auf die Ermittlungspraxis und die Strafverfolgung.

Datengrundlage des Evaluationsberichts sind vollständige (und offensichtlich den Vorgaben entsprechende) Mitteilungen aus 9 Mitgliedsländern. Insgesamt haben 19 Mitgliedsländer jedenfalls selektiv Daten mitgeteilt. Diese beziehen sich auf die Zahl der in den Jahren 2008 und/oder 2009 durchgeführten Verkehrsdatenabfragen. Auf entsprechende Anfragen hätten dann 10 Mitgliedsländer Berichte über Einzelfälle übersandt, für die Verkehrsdaten notwendig gewesen seien[277]. Der Bericht erläutert, dass die mitgeteilten Daten von unterschiedlichem Differenzierungsgrad und unterschiedlicher Aussagegüte seien. Deshalb solle jedenfalls für die Zukunft ein Erfassungssystem ausgearbeitet werden, das eine „transparente und aussagekräftige“ Untersuchung der Vorratsdatenspeicherung zulasse[278].

Die Daten sollen nach dem Bericht zeigen, dass in den Berichtsjahren 2008 und 2009 in der Europäischen Union jeweils etwa 2 Millionen Abfragen durchgeführt worden seien. Allerdings unterscheidet die Evaluation nicht zwischen der Abfrage von auf Vorrat gespeicherten Verkehrsdaten und der regulären Abfrage von Verkehrsdaten, noch lassen die Daten nach dem Zweck der Abfrage unterscheiden. Dies war angesichts der weiter oben dargestellten Entwicklungen aber auch gar nicht anders zu erwarten. Der Evaluationsbericht der Europäischen Kommission kann sich damit allein auf die Verkehrsdatenabfrage allgemein, nicht aber auf die Nutzung von auf Vorrat gespeicherten Verkehrsdaten beziehen. Erhebliche Varianz in der Abfragehäufigkeit ergebe sich, so der Bericht, aus den Daten, bei einem Minimum von 100 (mitgeteilt aus Zypern) und einem Maximum von mehr als einer Million (Polen). Jedoch wird die extreme Varianz nicht zum Anlass für die Frage genommen, ob die Varianz nicht eher auf vollständig unterschiedliche statistische Erfassungskriterien und Bezugspunkte hindeutet als auf einen unterschiedlichen Gebrauch der Abfrage von auf Vorrat gespeicherten Verkehrsdaten. Tatsächlich wird im Evaluationsbericht aber darauf hingewiesen, dass zum Beispiel Polen, die Tschechische Republik und Lettland Daten übermittelt hätten, die sich auf die Anforderung von Verkehrsdaten von jedem einzelnen Telekommunikationsunternehmen beziehen (was natürlich bei bestimmten Abfragetypen (auch wenn es sich lediglich um eine einzige Abfrage handelt) die Zahl, abhängig von der Zahl der Unternehmen in einem Land, aufbläht)[279]. Die Abfragen konzentrieren sich, auch dies ist erwartungsgemäß, auf Mobiltele-

---

277 European Commission: Report From the Commission to the Council and the European Parliament Evaluation report on the Data Retention Directive, a.a.O. (Fn. 156), S. 2.

278 European Commission: a.a.O. (Fn. 156), S. 19.

279 European Commission: a.a.O. (Fn. 156), S. 21.

fondaten. Der Abfragezeitraum betrifft im Schwerpunkt kurze Zeiträume; unterstrichen wird im Bericht, dass die Mitgliedsländer mitgeteilt hätten, auch ältere Daten könnten für Ermittlungen große Bedeutung haben. Die Bedeutung älterer Verkehrsdaten wird für drei Nutzungsstrategien hervorgehoben.

(1) Zunächst würden Verkehrsdaten in der Regel erst später erhoben als andere Beweise. Denn die Erhebung von Telekommunikationsdaten führe zu Spuren, die dann durch weitere Abfragen abgeklärt werden könnten.

(2) Sodann tendierten Untersuchungen von Fällen schwerer Kriminalität, von Serienstraftaten und organisierter Kriminalität dazu, auf länger zurückliegende Daten zuzugreifen. Denn schwere Kriminalität bedeute teilweise lange Planung auf Seiten der Täter, weshalb die Ermittler auf diese Zeiträume zugreifen müssten. Verbindungen zwischen Komplizen und zwischen verschiedenen Taten könnten ebenfalls nur auf der Grundlage von für die Vergangenheit verfügbarer Verkehrsdaten aufgeklärt werden.

(3) Im Übrigen würden komplexe Vermögensstraftaten oft erst nach Monaten angezeigt. Ausnahmsweise könnte schließlich verzögerter Bedarf bei dem Zugriff auf Verkehrsdaten aus anderen europäischen Staaten entstehen[280]. Jedoch hat sich offensichtlich kein Mitgliedsland für eine Erleichterung des zwischenstaatlichen Datenaustauschs im Falle von Verkehrsdaten ausgesprochen (vgl. hierzu auch Rahmenentscheidung 2006/960/JI)[281].

Die absolute Zahl von Abfragen, so der Evaluationsbericht, reflektiere nicht unbedingt den Wert von Verkehrsdaten für strafrechtliche Ermittlungen. Doch hätten die Mitgliedsländer ausgesagt, dass Verkehrsdaten zumindest "wertvoll" (valuable), in manchen Fällen sogar „unverzichtbar" für Prävention und Kriminalitätsbekämpfung seien. Es wird darauf hingewiesen, dass „erfolgreiche Verurteilungen" (successfull convictions, was immer auch damit gemeint sein mag) auf Schuldbekenntnis, Zeugenaussagen und forensische Beweismittel gestützt werden. Verkehrsdaten seien insoweit hilfreich, als sie dazu dienten, mit Zeugen, die anderweitig nicht hätten identifiziert werden können, Kontakt aufzunehmen, oder Hinweise auf eine Tatbeteiligung Dritter geben könnten. Mitgliedsstaaten hätten dann darauf hingewiesen, dass Verkehrsdaten dazu eingesetzt worden seien, um Personen von einem Tatverdacht zu befreien (ohne dass auf eingreifendere Maßnahmen wie eine Hausdurchsuchung habe zurückgegriffen werden müssen)[282].

In dem Bericht wird betont, es gebe keine allgemeine Definition einer „schweren Straftat", weshalb über den Gebrauch von Verkehrsdatenabfragen im Falle „schwerer Kriminalität" auch keine Aussagen gemacht werden könnten. Damit wird im Übrigen erklärt, dass sich die

---

280 European Commission: a.a.O. (Fn. 156), S. 22.

281 European Commission: a.a.O. (Fn. 156), S. 23.

282 European Commission: a.a.O. (Fn. 156), S. 23.

mitgeteilten Daten, und somit auch die Evaluation, nicht auf die Praxis der Abfrage auf Vorrat gespeicherter Verkehrsdaten für Ermittlungen bei schwerer Kriminalität (insbesondere organisierte Kriminalität und Terrorismus) beziehen lassen. Dies war aber der eigentliche Zweck der Richtlinie 2006/24. Insgesamt und vor dem Hintergrund der für die Mitgliedsstaaten verfügbaren Kriminalstatistiken gesehen – so fährt der Bericht fort - könne jedoch die Aussage getroffen werden, dass auf 100 polizeilich registrierte Straftaten etwa 11 Abfragen entfielen[283]. Würde diese Aussage auch auf Deutschland zutreffen, so müsste tatsächlich von etwa einer halben Million Abfragen in Deutschland ausgegangen werden. Folgende Schlussfolgerungen seien zur Nutzung von Verkehrsdatenabfragen möglich:

(1) Konstruktion von Beweisketten: Verkehrsdaten ermöglichen die Konstruktion von Beweisketten, indem andere Beweismittel identifiziert oder verstärkt und Alibis verifiziert werden. Zum Beleg werden verschiedene von Mitgliedsländern mitgeteilte Fälle bzw. Fallgruppen angegeben. Dazu gehören die Fälle eines „Tiger Kidnapping“ in Antwerpen[284] sowie eines Tötungsdelikts an dem Mitglied einer Motorradgang (Hells Angels) in England auf der Autobahn M40. Während das „Tiger Kidnapping“ eines Justizbeamten der Stadt Antwerpen nicht dokumentiert ist (und auch in belgischen Zeitungen nicht nachverfolgt werden konnte), wird (in anderen Quellen) über den Mord an einem Hells Angel in England ausführlich berichtet. Dabei handelt es sich um eine Sachverhaltsgestaltung, die bereits bei oberflächlicher Betrachtung nicht für den Wert von auf Vorrat gespeicherten Verkehrsdaten spricht, sondern ganz offensichtlich (wenn überhaupt) den typischen Fall eines Quick-Freeze-Verfahrens darstellt.

Nach dem von den Strafverfolgungsbehörden mitgeteilten Sachverhalt wurde der Angel auf der Autobahn M40 und auf der Rückfahrt von einer Großveranstaltung, ferner in Anwesenheit von drei weiteren Angels aus einem PKW heraus erschossen[285]. Die Polizei war unmittelbar nach der Tat am Tatort und konnte von daher sofort alle notwendigen Ermittlungsmaßnahmen einleiten. Hierzu gehörten neben der Vernehmung von Zeugen (einschließlich der Angels, die allerdings erwartungsgemäß keinerlei Angaben machten), auch die Durchsicht von CCTV-Aufnahmen und die Abfrage von Funkzellendaten. Aus Videoaufnahmen (Tankstellen) wurden das Tatfahrzeug (das wenig später ausgebrannt aufgefunden wurde und auf einen der Tatverdächtigen zurückverfolgt werden konnte[286]) und die drei Tatverdächtigen identifiziert. Funkzellenauswertungen ergaben den Hinweis, dass Mobiltelefone der drei Tatverdächtigen

---

283 European Commission: a.a.O. (Fn. 156), S. 23.

284 Tiger Kidnapping bezeichnet die Kombination von Geiselnahme (in der Regel von Familienangehörigen im Haus des Opfers) und (räuberischer) Erpressung.

285 Zur Beschreibung des Tatverlaufs *Lawrence, K.*: Investigation into the Murder of Hell’s Angel Gerard Tobin on the M40: A Murder committed by an Organised Crime Group against another. The Journal of Homicide and Major Incident Investigation 5 (2009), S. 39-52, S. 42.

286 *Lawrence, K.*: a.a.O. (Fn. 285), S. 46.

(nicht überraschend: Angehörige der Outlaws), in dieser Funkzelle zur Tatzeit eingebucht waren. Die Beweisführung gründete sich auf eine Mischung von Zeugenaussagen, Videoaufnahmen, Automatischem Kennzeichenabgleich, Telekommunikationsinhaltsüberwachung, weiterer nicht spezifizierter Informationsbeschaffung sowie Verkehrsdaten [287]. Die Besonderheiten der Tat und des Tatablaufs sprechen dafür, dass ein sofortiger Zugriff auf die Funkzellendaten die Beweismittel bzw. eher Ermittlungsansätze ohne weiteres sicher gestellt hätte (und in diesem Fall sicher gestellt hat). Nachvollziehbar ist der Ratschlag des für die Ermittlungsführung zuständigen Beamten, möglicherweise relevante Informationen (unter ihnen die Verkehrsdaten) sofort und unmittelbar abzufragen[288], was jedenfalls in diesem Fall für das Quick-Freeze-Verfahren spricht (auf Vorrat gespeicherte Verkehrsdaten sind in dem Bericht im Übrigen nicht erwähnt).

(2) Bezug genommen wird schließlich auf durch Kommunikationsgeräte begangene Straftaten (Gewaltandrohungen in Chatrooms) sowie auf Fälle des „Enkeltrickbetrugs", die aus Ungarn und Polen gemeldet worden seien[289]. Die Bezugnahme ist hier allgemein und ergibt keinerlei Möglichkeit, die Informationen und die aus ihnen gezogenen Schlussfolgerungen auf Richtigkeit, Nachvollziehbarkeit und Plausibilität hin zu überprüfen.

(3) Verwiesen wird im Bericht auch auf Fälle, in denen der einzige Weg, Ermittlungen zu beginnen, der Rückgriff auf Vorratsdaten gewesen sei. In diesem Zusammenhang wird ein Fallbeispiel aus Deutschland genannt, und zwar der unter D 5.5 detailliert beschriebene Fall eines Tötungsdelikts an einem Polizeibeamten[290]. Hier können Sachverhalt und Ermittlungsverlauf zwar nicht durch im Kommissionsbericht zur Verfügung gestellte Informationen, aber durch Zusatzdaten rekonstruiert werden, die aus der BKA-Datensammlung und darauf aufbauenden Recherchen folgen[291]. Gerade dieser Beispielsfall eignet sich allerdings, ebenso wenig wie das Hells Angels Beispiel, nicht dafür, die Notwendigkeit von Vorratsdaten (auf die in diesem Fall tatsächlich zugegriffen werden konnte) zu begründen, obwohl es sich hier um einen der Fälle schwerster Kriminalität handelt, die von Deutschland an die Kommission als die Notwendigkeit der Vorratsdatenspeicherung demonstrierend übermittelt wurde. Funkzellenabfragen, auf der Grundlage von auf Vorrat gespeicherter Verkehrsdaten, führten hier eben nicht weiter. Außerdem lagen DNA-Untersuchungsbefunde vor, die allerdings keine Übereinstimmung zwischen nachgewiesenen Spuren am Tatort und der DNA der Tatverdächtigen zeigten. Schon angesichts dieser Spurenlage ist nicht

---

287 *Lawrence, K.*: a.a.O. (Fn. 285), S. 43.

288 *Lawrence, K.*: a.a.O. (Fn. 285), S. 51.

289 European Commission: a.a.O. (Fn. 156), S. 24.

290 European Commission: a.a.O. (Fn. 156), S. 24.

291 Bundeskriminalamt: Stand der statistischen Datenerhebung, a.a.O. (Fn. 164).

nachvollziehbar, warum Funkzellendaten (wären sie tatsächlich vorhanden gewesen) dazu geführt haben sollten, nicht übereinstimmende DNA-Spuren zu kompensieren.

Aus der Tschechischen Republik wird die dort so genannte Operation "Vilma" mitgeteilt, ein Großverfahren zur Kinderpornografie und offensichtlich Teil der Operation „Rescue"[292], die über drei Jahre dauerte und in deren Verlauf mit verdeckten Maßnahmen die auf Kinderpornografie bezogenen Interaktionen in einem Forum ausgeleuchtet wurden. Im Evaluationsbericht wird (ohne dass konkrete Hinweise dafür angegeben würden) davon ausgegangen, dass dieses Verfahren ohne auf Vorrat gespeicherte Verkehrsdaten (in der Tschechischen Republik) nicht hätte initiiert werden können. Ferner wird darauf hingewiesen, dass in einigen Mitgliedsländern wegen fehlender Umsetzung der Vorratsdatenspeicherungsrichtlinie entsprechende Ermittlungen nicht hätten durchgeführt werden können. Für erfolgreiche Ermittlungen wäre der Zugriff auf bis zu 12 Monate alte Verkehrsdaten notwendig gewesen[293].

(4) Die Bedeutung von auf Vorrat gespeicherten Verkehrsdaten wird dann für die allgemeine Untersuchung von Cyberkriminalität hervorgehoben. In diesem Zusammenhang enthält der Bericht auch allgemeine Hinweise auf das Potenzial von Verkehrsdaten für die Information und Warnung von Opfern bzw. Computerbesitzern, die in Bot-Netze rekrutiert wurden[294].

(5) Statistiken, die Auskunft geben könnten über die Art von Beweismitteln, die für die Verurteilung oder den Freispruch Bedeutung haben, werden nach dem Kommissionsbericht von den Mitgliedsländern nicht geführt. Insoweit gibt es auch keine empirische Grundlage, auf der der (relative) Effekt von (auf Vorrat gespeicherten) Verkehrsdaten auf das Ergebnis von Ermittlungsverfahren beleuchtet werden könnte. Jedoch wird daran festgehalten, dass Verkehrsdaten "integral" für Ermittlungen und Strafverfahren seien. Belegt wird dies mit dem Hinweis, die Niederlande hätten mitgeteilt, dass sich zwischen Januar und Juli 2010 „historische" Verkehrsdaten in 24 Urteilen als entscheidende Beweismittel erwiesen hätten. Angesichts einer Gesamtzahl von etwa 60.000 Verurteilungen im Halbjahr in den Niederlanden[295] erscheint damit allerdings die Bedeutung von Verkehrsdaten für strafrechtliche Ermittlungen als äußerst überschaubar (0,04 %). Aus Finnland wird berichtet, dass von 3402 Abfragen 56 % „wichtig" oder „wesentlich" für die Aufklärung oder Verfolgung von Straftaten gewesen seien. Für das Vereinigte Königreich wird demgegenüber erklärt, hier hätte die Untersuchung von drei Strafverfolgungsbehörden ergeben, dass auf

---

292 www.europol.europa.eu/content/press/more-200-children-identified-and-rescued-worldwide-police-operation-465 [Juni 2011].

293 European Commission: a.a.O. (Fn. 156), S. 24.

294 European Commission: a.a.O. (Fn. 156), S. 24f.

295 *Aebi, M. F.* u. a.: European Sourcebook of Crime and Criminal Justice Statistics 2010. WODC, Den Haag 2010, S. 174.

Vorrat gespeicherte Verkehrsdaten in den „meisten, wenn nicht für alle“ Ermittlungen notwendig gewesen seien, die in Anklagen oder Verurteilungen resultierten[296]. Insoweit geht die Kommission, ohne dass dies als widersprüchlich thematisiert worden wäre, von Ergebnissen aus, die eine erfolgreiche Nutzung von Verkehrsdaten (nicht auf Vorrat gespeicherte Verkehrsdaten) in eine Bandbreite zwischen 0,04 und etwa 100% der strafrechtlichen Verfahren einordnen lassen. Vor dem Hintergrund der bislang einzigen empirischen Untersuchung des Beitrags von Verkehrsdatenabfragen zu strafrechtlichen Ermittlungen dürften die Angaben aus Finnland wohl eher eine realistische Einschätzung darstellen[297].

2. Bewertung des Evaluationsberichts der Europäischen Kommission

2.1. Die Datengrundlage des Berichts

Die Datengrundlage des Berichts besteht aus allgemeinen Statistiken zur Verkehrsdatenabfrage, aus Fällen, die von den Mitgliedsländern als die Notwendigkeit von Vorratsdatenspeicherung demonstrierend mitgeteilt wurden sowie allgemeinen Stellungnahmen zu Erfahrungen mit der Verkehrsdatenabfrage aus den Mitgliedsländern.

2.2. Statistiken

Von etwa einem Drittel der Mitgliedsländer wurden von der Europäischen Kommission nachgefragte Statistiken zur Verfügung gestellt. Die von den Mitgliedsländern übermittelten Daten erlauben keine Differenzierung nach solchen Abfragen, die sich auf Vorrat gespeicherte Verkehrsdaten beziehen, und solchen, die reguläre Verkehrsdaten anfordern. Insoweit bezieht sich die Evaluation auf die Verkehrsdatenabfrage allgemein und lässt auf der Grundlage der Statistiken von vornherein keinen Schluss darüber zu, wie und mit welchen Ergebnissen auf Vorrat gespeicherte Verkehrsdaten zu Ermittlungen beitragen. Die Daten sind dann nicht nach Delikten oder Deliktsschwere aufgeschlüsselt. Insoweit gibt es keine Möglichkeit zu überprüfen, ob Verkehrsdaten tatsächlich in dem von der Richtlinie 2006/24 geforderten Bereich schwerer Kriminalität genutzt werden. Ferner haben die Mitgliedsländer unterschiedliche Daten zur Verfügung gestellt, wobei sich aus dem Bericht nicht ergibt, um welche Daten bzw. Datenquellen es sich handelt. Die Größenordnungen der absoluten Zahlen lassen begründet vermuten, dass die Mitgliedsländer teilweise undifferenziert Informationen zu Verkehrs- und Bestandsdatenabfragen geliefert haben. Teilweise sind wohl strafrechtliche Verfahren mit Abfragen gemeldet worden, von anderen Ländern wurden Statistiken übermittelt, die nicht die Abfragen (oder das Verfahren, in dem Abfragen vorkamen) selbst zählen, sondern die mit Abfragen kontaktierten Telekommunikationsunternehmen. Schließlich ist die Art der Abfrage (Bestandsdaten, abgehende, ankommende Gespräche, Funkzellenabfragen etc.) nicht aufgeschlüsselt. Für wenige Länder ergeben sich weitergehende Informationen zu den

---

296 European Commission: a.a.O. (Fn. 156), S. 25.

297 *Albrecht, H.-J., Grafe, A., Kilchling, M.*: Rechtswirklichkeit der Auskunftserteilung über Telekommunikationsverbindungsdaten nach §§ 100g, 100h StPO. Berlin 2008.

Zeiträumen, auf die sich abgefragte Verkehrsdaten beziehen. Keine Statistik enthält Angaben zu den Ergebnissen der Verfahren (in Form von Einstellung, Verurteilung oder Freispruch), in denen es zu Verkehrsdatenabfragen gekommen ist.

2.3. Fallbeschreibungen

Der Evaluationsbericht enthält Hinweise auf verschiedene von den Mitgliedsländern mitgeteilte einzelne Fälle, die die Notwendigkeit von auf Vorrat gespeicherten Verkehrsdaten belegen sollen. Teilweise sind diese Fälle so konkretisiert, dass sie nachvollzogen werden können, überwiegend ist dies nicht möglich. So werden im Bericht zwei Tötungsdelikte angesprochen (England, Deutschland), die sich nach Überprüfung nicht als Beleg für die Notwendigkeit der Vorratsdatenspeicherung interpretieren lassen. Der englische Fall hätte sich wohl eher für das Quick-Freeze-Verfahren geeignet. In dem aus Deutschland mitgeteilten und im Bericht erwähnten Fall zeigte sich, dass auf Vorrat gespeicherte Verkehrsdaten eben nicht zu den Ermittlungen beigetragen haben.

2.4. Allgemeine Stellungnahmen der Mitgliedsländer

Die Datengrundlage wird ergänzt um allgemeine Stellungnahmen aus den Mitgliedsländern. Diese sind infolge ihrer Allgemeinheit und wegen fehlender Ansatzpunkte für eine Überprüfung kaum geeignet, eine angemessene Evaluation zu befördern. Teilweise sind die Mitteilungen aber insgesamt nicht nachvollziehbar. Dies gilt jedenfalls für die Einschätzung, auf Vorrat gespeicherte Verkehrsdaten seien in allen Ermittlungs- und Strafverfahren notwendig gewesen[298]. Dies kann schon deshalb nicht der Fall sein, weil in den meisten Verfahren von vornherein Verkehrsdaten der Telekommunikation keine Rolle spielen, entweder weil Mobiltelefone keine sachdienlichen Hinweise bieten können oder weil andere Beweismittel, insbesondere Geständnisse vollkommen ausreichen (und ferner Verkehrsdaten überlegen sind).

3. Zur Anlage der Evaluation

Aus einer methodischen Perspektive ist der von der Kommission gewählte und dann realisierte Zugang für eine Evaluation nicht geeignet. Der Zugang wäre dazu geeignet gewesen (wenn entsprechende Datenerhebungsschritte eingeleitet worden wären), die (auf Vorratsdaten gestützte) Verkehrsdatenabfrage in ihrem Umfang und in ihren Strukturen zu beschreiben, nicht aber kausale Beziehungen zwischen Vorratsdaten und Aufklärungserfolg herzustellen. Denn der Zugang war von vornherein nicht dazu geeignet, den Beitrag der Verkehrsdatenabfrage für den Erfolg von Ermittlungen zu beleuchten. Hierzu wäre im Übrigen lediglich ein Evaluationskonzept geeignet gewesen, das bei Kontrolle der unterschiedlichen Speicherungspraktiken von Telekommunikationsunternehmen (und damit auch der unterschiedlichen rechtlichen Bedingungen der Speicherung von personenbezogenen Daten) in Form von Stichprobenuntersuchungen der Frage nach der relativen Bedeutung von auf Vorrat gespeicherten Verkehrsdaten nachgegangen wäre. Die unzureichende Datengrundlage wird in der zusammen-

---

298 European Commission: a.a.O. (Fn. 156), S. 25.

fassenden und die Zukunft ansprechenden Bewertung des Evaluationsergebnis auch sichtbar gemacht, wenn zuerst darauf hingewiesen wird, dass die auf die von den Mitgliedsländern zur Verfügung gestellten Daten gestützten Befunde in verschiedener Hinsicht begrenzt seien[299] und dann betont wird, dass für die Zukunft ein Instrument entwickelt werden müsse, mit dem der Nutzen der Vorratsdatenspeicherung überprüft werden könne[300].

4. Die analytischen Teile des Berichts

Angesichts der prekären Datenlage war zu erwarten, dass die analytischen Teile des Evaluationsberichts eher bescheiden ausfallen. Die Aussage, auf Vorrat gespeicherte Verkehrsdaten würden in signifikanter Weise zur Prävention und zur Kriminalitätsbekämpfung beitragen, Unschuldige entlasten und Opfer schützen[301], stützt sich im Kern auf die Beobachtung, dass von der (allgemeinen) Verkehrs- und Bestandsdatenabfrage in erheblichem Umfang Gebrauch gemacht wird. Die Aussage zur Effizienz gründet sich demnach offensichtlich auf eine einfache Annahme, nämlich die Annahme, dass dann, wenn im Verlaufe strafrechtlicher Ermittlungen bestimmte Informationsbeschaffungsmethoden praktiziert werden, diese Praktiken auch tatsächlich nützlich waren (denn ansonsten hätten die Ermittlungsbehörden davon ja keinen Gebrauch gemacht).

Zu offensichtlichen Widersprüchen (England: in nahezu allen Verfahren werden Verkehrsdaten benötigt[302]; Niederlande: 24 Verurteilungen (von mutmaßlich 60.000 Verurteilungen), für die Verkehrsdaten notwendig waren[303]) wird im Bericht nicht Stellung genommen. Derartige Widersprüche lassen sich an Hand der Datenlage auch gar nicht auflösen. Die uneingeschränkte und positive Bewertung der Vorratsdatenspeicherung verträgt sich schließlich kaum mit der Stellungnahme zu anonymen Prepaid SIM-Karten, die in Europa offensichtlich nach wie vor erhebliche Bedeutung haben und für die Handlungsbedarf nicht gesehen wird[304], obwohl der Nutzen der Vorratsdatenspeicherung von vornherein und maßgeblich davon abhängen dürfte, ob und inwieweit es gelingt, die Anonymität in der Telekommunikation zu unterbinden.

5. Zusammenfassende Bewertung des Kommissionsberichts

(1) Der Evaluationsbericht der Europäischen Kommission geht davon aus, dass die Vorratsspeicherung von Telekommunikationsdaten signifikant zur Sicherheit in Europa beigetragen habe.

---

299 European Commission: a.a.O. (Fn. 156), S. 31.
300 European Commission: a.a.O. (Fn. 156), S. 19.
301 European Commission: a.a.O. (Fn. 156), S. 31.
302 European Commission: a.a.O. (Fn. 156), S. 25.
303 European Commission: a.a.O. (Fn. 156), S. 25.
304 European Commission: a.a.O. (Fn. 156), S. 25.

(2) Die Evaluation der Europäischen Kommission konnte sich allerdings wegen der fehlenden Differenzierung zwischen auf Vorrat gespeicherten und anderen Verkehrsdaten von vornherein nicht auf eine Bewertung der Vorratsdatenspeicherung beziehen. Der Bericht enthält nur solche Daten, die allein die Praxis allgemeiner Verkehrsdatenabfragen beschreiben.

(3) Die Beschreibung der Nutzung von Verkehrsdaten bezieht sich auf Daten aus etwa einem Drittel der Mitgliedsländer. Ganz überwiegend können die Mitgliedsländer nicht einmal über einfache Strukturen der Verkehrsdatenabfrage Auskunft geben.

(4) Die Statistiken zur Verkehrdatenabfrage lassen nicht unterscheiden zwischen Bestandsdaten und Verkehrsdaten im engeren Sinn. Ferner werden verschiedene Abfragearten nicht differenziert.

(5) Die Beschreibung der Nutzung von Verkehrs- und Bestandsdaten unterscheidet nicht nach der Deliktsart oder -schwere. Die Evaluation enthält keine Aussage darüber, ob und inwieweit Vorratsdaten oder allgemeine Verkehrsdaten der Telekommunikation für Ermittlungen im Bereich schwerer Kriminalität Bedeutung haben.

(6) Die von den Mitgliedsländern übermittelten Statistiken lassen in keinem Fall eine Aussage darüber zu, ob und in welchem Ausmaß (allgemeine) Verkehrsdaten in strafrechtlichen Ermittlungsverfahren zur Aufklärung von Straftaten beigetragen haben (oder nicht).

(7) Die über die wenig aussagekräftigen Statistiken hinausgehenden Informationen und Fallberichte sind weitgehend nicht nachvollziehbar und deshalb als Grundlage für eine Evaluation nicht geeignet.

Teil F: Aktuelle Situation der Verkehrsdatenabfrage aus der Sicht der Praxis

1. Situationsbeschreibung aus der Sicht der Ermittler

Die folgenden Ausführungen basieren auf den Interviews mit den Vertretern der Polizeibehörden des Bundes und der Länder. Gegenstand der ausführlichen Gespräche waren sowohl der repressive als auch der präventive Einsatz der Verkehrsdatenabfrage.[305] Die Ausführungen der Gesprächspartner konzentrierten sich dabei im Wesentlichen auf dieselben Kernfragen, insbesondere was den Bedarf und den Zugang zu Verkehrsdaten betrifft.

Quantitativ hat der präventive Einsatz im Vergleich zu den Abfragen im Rahmen der Strafverfolgung allerdings eine wesentlich geringere Bedeutung. Die konkreten Angaben hierzu unterscheiden sich eher graduell und bewegen sich zwischen Anteilen von ca. 85 % und mehr[306] für die repressiven Beschlüsse. Zu beachten ist dabei allerdings im Hinblick auf die Zielsetzung der Gefahrenabwehr, dass die unter Umständen betroffenen Rechtsgüter – insbesondere die Rettung von Leib und Leben in Suizid- und Amoksituationen – einen sehr hohen Stellenwert haben und vergleichsweise niedrige Anwendungszahlen daher per se kein hinreichender Maßstab zur Einordnung der Bedeutung der Maßnahme sein sollten. Einige Bundesländer – Berlin, Bremen, Nordrhein-Westfalen, Sachsen und Sachsen-Anhalt – haben bislang allerdings keine entsprechende Ermächtigungsgrundlage. Eine besondere Situation besteht weiterhin im Hinblick auf die besondere Aufgabenbeschreibung für das Bundeskriminalamt und die Bundespolizei. Im Übrigen wird auch auf das Auftreten repressiv-präventiver Gemengelagen hingewiesen, die eine Abgrenzung im Einzelfall schwierig erscheinen lassen. Aus praktischen Gründen werden Anfragen offensichtlich auch dann eher auf der Grundlage der StPO beantragt. Die Situationsbeschreibung konzentriert sich daher im Wesentlichen auf den repressiv orientierten Einsatz der Verkehrsdatenabfrage. Besondere Aspekte im Kontext des präventiven Einsatzes sind jedoch berücksichtigt und werden im Rahmen der Darstellung explizit benannt.

Zu Illustrationszwecken wurden einige exemplarische Beispielsfälle aus den Transskripten exzerpiert. Sie sollen sowohl typische Delikts- und Gefahrenkonstellationen als auch gängige Ermittlungsprobleme illustrieren[307], mit denen die Behörden nach dem Wegfall der Vorratsdatenspeicherung nach eigenen Angaben konfrontiert sind. Die Fallbeschreibungen sind in direkter Rede wiedergegeben und finden sich in einer doppelseitigen Übersicht unter Pkt. 1.2.2. Auf die Beispiele wird im weiteren Text unter ihrer jeweiligen Nummer mehrfach Bezug genommen.

---

305 Die den Gesprächen zugrunde liegenden Interviewleitfäden sind in Anhang B dokumentiert.

306 Lediglich die hessischen Beamten gaben den Anteil präventiver Abfragen mit geschätzten ca. 33 % deutlich höher an.

307 Es handelt sich nicht um eine repräsentative Auswahl. Eine systematische Analyse der vom BKA derzeit erhobenen Realfälle ist im zweiten Halbjahr in Ergänzung zu der vorliegenden qualitativen Erhebung geplant.

1.1. Allgemeine Folgeneinschätzung

Zu Beginn der Expertengespräche wurden alle Gesprächspartner um eine generelle Einschätzung der Auswirkungen des Wegfalls der Vorratsdatenspeicherung aus ihrer jeweiligen Arbeitsperspektive gebeten. Die Frage war den Teilnehmern vorab zusammen mit dem Interviewleitfaden zugestellt worden, um eine angemessene Überlegungs- und Vorbereitungszeit sicherzustellen. Es handelt sich insoweit also um keine spontanen Äußerungen. Vorgegeben wurden leicht nachvollziehbare Antwortkategorien. Diese folgen methodologisch freilich keiner streng skalierten Kategorisierung, wofür die Problemstellung insgesamt zu komplex erschien. Die ermittelten Antworten zeigen daher ein grobes Meinungsbild auf, eignen sich aber nicht für weitergehende statistische Auswertungen.

Wie aus den Voten in Tabelle F-1 erkennbar wird, äußerten sich die Vertreter der Polizeibehörden, die ja die einsatznächste Ebene im Hinblick auf die Maßnahmen repräsentiert, im Vergleich zu den anderen Befragten am eindeutigsten. Dies zeigt sich an beiden Enden: während die Zahl derjenigen, die die Erfahrungen in dem Zeitraum seit dem 2.3.2010 für zu kurz halten, um die Situation eindeutig einschätzen zu können, sehr niedrig ist, fällt auf der anderen Seite auch das Votum am eindeutigsten aus. Damit heben sie sich erkennbar von den Justizvertretern ab. Sowohl auf der Richter- als auch auf der Staatsanwaltschaftsebene werden die Auswirkungen vorsichtiger (relativ halten doppelt so viele Staatsanwälte den Zeitpunkt für ein abschließendes Votum für zu früh) als auch in der Bewertung differenzierter beurteilt.

*Tabelle F-1: Generelle Einschätzung: „Wie beurteilen Sie die praktischen Auswirkungen des Wegfalls der Vorratsdaten gem. §§ 113a und 113b TKG für Ihre Arbeit?“**

	sehr hoch	hoch	eher gering	sehr gering	keinerlei Auswirkungen	noch nicht abschätzbar	k.A.	Gesamt
Polizei**	56	10	1	0	0	5	5	77
StA***	13	9	5	0	0	4	0	31
Richter	1	2	1	0	0	1	0	5
Gesamt	70	21	7	0	0	10	5	113

**) Mehrfachnennungen bei Polizei und StA. Dies war etwa der Fall, wenn eine Person unterschiedliche Arbeits- oder Deliktsbereiche repräsentierte.*
***) inkl. Bundespolizei und BKA.*
****) inkl. Bundesanwaltschaft.*

Gefragt nach den Gründen für das so dezidierte (und nahezu einhellige) Votum wurde zuallererst auf diejenigen Delikts- bzw. Einsatzbereiche der Verkehrsdatenabfrage verwiesen, in denen der Wegfall der Vorratsdaten am deutlichsten zu spüren ist. Hierzu zählt insbesondere die IuK-Kriminalität (im engeren, teilweise auch im weiteren Sinne). Die Vertreter aus Schleswig-Holstein vermelden hier für ihr Bundesland einen Anteil von mehr als 90 % der Fälle, in denen die Anfragemöglichkeit aufgrund der veränderten Speichersituation bei den Anbietern weggebrochen sei; in einigen anderen Bundesländern erscheint der Anteil niedri-

ger, aber gleichwohl deutlich (siehe dazu auch unten Pkt. 1.5.). Gerade bei diesen Straftaten sei der Zugriff auf retrograde Verkehrsdaten die einzige Möglichkeit, verantwortliche Personen zu identifizieren. Ein Experte aus Baden-Württemberg beschrieb die aktuelle Situation im Internet mit einem bildlichen Vergleich: *„Straßenverkehr ohne Kfz.-Kennzeichen"*. Gerade in diesem Bereich habe das Urteil das BVerfG einen rapiden Einschnitt in die polizeiliche Tätigkeit gebracht.

Einige Gesprächspartner äußerten Unverständnis vor allem für die sofortige und übergangslose Löschungsanordnung, die so nicht erwartet worden sei. Dies verweist auch auf eine ganz persönliche empfundene Betroffenheitskomponente, die bei einigen Gesprächspartnern deutlich spürbar war. Verwiesen wurde dann auf gefühlte Auswirkungen, weil die kriminalistische Arbeit erheblich erschwert werde. Einer der Befragten verglich die Konsequenzen für die Ermittlungsarbeit mit dem Herausoperieren des Rückgrads. Ein anderer berichtete von *„großem Frust"* bei der Polizei, die zugleich mit enttäuschten Reaktionen bei Opfern konfrontiert werde, wenn Verfahren bereits am Anfang wieder eingestellt werden müssten.

Diese Situation tritt nach vielen Einzelbeschreibungen weitgehend übereinstimmend überall dort zutage, wo die IP-Adresse vormals den ersten Ermittlungsansatz geliefert habe und wo aktuell kein erfolgversprechender Ermittlungsansatz mehr verfügbar sei. Dies betreffe auch niedrigschwelligere Straftaten wie den E-Bay-Betrug. In solchen Fällen reiche die Speicherfrist von vier bis sieben Tagen, die einige TK-Unternehmen implementiert hätten, nicht aus. Auch in Fällen des Computerbetruges bemerke das Opfer regelmäßig erst mit Verzögerung, dass sein Konto leer geräumt wurde. Zu dem Zeitpunkt, zu dem bei der Polizei Anzeige erstattet werde und der Vorgang den zuständigen Sachbearbeiter erreiche, seien sieben Tage regelmäßig verstrichen. Ein Gesprächspartner führt aus, er habe seit dem 2.3.2010 genau einen Fall bearbeitet, in dem die Sieben-Tage-Frist ausreichend gewesen sein.

Zahlreiche Praktiker führen ergänzend aus, dass die aktuelle Situation auch nicht mit der Zeit vor Einführung der Vorratsdatenspeicherung vergleichbar sei. Dies sei nicht nur Folge des veränderten Speicher- und Auskunftsverhaltens der Provider, sondern auch die Konsequenz der zwischenzeitlich fortgeschrittenen technischen Entwicklung. Eine Neuerung mit weitreichenden Konsequenzen, die der Gesetzgeber bis dato nicht erkannt habe, sei das IP-Sharing über die Portnummer. Große Provider wie z.B. Vodafone, die über UMTS oder Nachfolgeprotokolle Zugänge zum Internet anbieten, lösten ihre IP-Adressen auf und nutzen dazu die Port- Nummern[308]. Diese seien bis heute im TKG nicht genannt und daher nicht speicherungsrelevant. Die Situation werde ferner dadurch verschärft, dass sich die Zugangstechnik und die Tarif- und Abrechnungspraxis deutlich verändert hätten. *„Früher sind die Leute über das Modem ins Internet gegangen, dabei sind Kosten entstanden und die entsprechenden Daten wurden zur Kostenerhebung i.d.R. etwa drei Monate gespeichert. Heute hat jedermann*

---

308 Siehe für weitere Einzelheiten zu dieser Problematik unten Pkt. 1.2.4.

eine Flatrate, da werden zu Abrechnungszwecken keine Daten mehr benötigt." Dies gelte nicht nur für den Internetbereich, sondern ebenso für den Festnetz- und Mobilfunkbereich.

Ein weiterer Punkt, der neben den spezifischen Problembereichen, die im Weiteren im Detail dargestellt werden, zu einer allgemeinen latenten Unzufriedenheit beizutragen scheint, sind Unsicherheiten, die mit der Unkontrollierbarkeit der Speicherpolitik der Unternehmen im Zusammenhang zu stehen. Der Umstand, dass die Unternehmen weithin selbst definieren können, welche Daten sie wie lange speichern, hat dazu geführt, dass sich ganz verschiedene, aus der Außenperspektive nicht – und schon gar nicht mit rechtlichen Kriterien – nachvollziehbare Systeme entwickelt haben, die zudem nicht statisch sind, sondern, parallel zu der permanenten Änderung und Vermehrung der Tarifmodelle, einem ständigen Wandel unterworfen sind. Änderungen werden von den Providern scheinbar auch nicht immer hinreichend und nicht regelmäßig kommuniziert, sondern müssen in den Dienststellen in eigener Recherchearbeit fortlaufend fortgeschrieben werden. Ein exemplarisches Muster einer solchen Speicherfristenauflistung des LKA NRW ist unter Pkt. 1.4. abgedruckt.[309] Das macht den Umgang mit Verkehrsdatenabfragen offenbar zusätzlich mühsam und den Abfrageerfolg – und damit den Sinn der Maßnahme – unkalkulierbar. Unter solchen Rahmenbedingungen wird der oft zufällige, im Wesentlichen von der jeweiligen Speicherpraxis determinierte Abfrageerfolg bzw. Misserfolg dann in der rechtlichen Bewertung als willkürlich empfunden.

Einzelne Gesprächspartner aus Dienststellen, die schwerpunktmäßig im Bereich der IuK-Kriminalität arbeiten, räumen freilich eine graduelle Verbesserung ihrer Situation infolge des Urteils vom März 2010 ein. Für sie war der Erlass der einstweiligen Anordnung im März 2008 die noch einschneidendere Zäsur. Denn zwischenzeitlich seien für sie Daten von allen Straftaten, die nicht in den Katalog gem. § 100a StPO fallen, nahezu unzugänglich gewesen. Zeitweise sei der gesamte IuK-Bereich, in dem die retrograden Verkehrsdaten zumeist der einzigen Ermittlungsansatz seien, weggebrochen.

1.2. Bedeutung der Verkehrsdaten und ihre Erreichbarkeit nach der derzeitigen Rechtslage

1.2.1. Quantitative Bedeutung der Bereiche Festnetztelefonie, Mobilfunk und Internet

Zu Beginn der spezifischen Problemanalyse sollten die Befragten dann zu der Bedeutung der Verkehrsdatenabfrage im Zuge der (repressiven und präventiven) Polizeiarbeit und der derzeitigen tatsächlichen Erreichbarkeit der Daten Stellung nehmen. Dabei sollte zunächst die aktuelle Bedeutung der verschiedenen Telekommunikationsbereiche, also Festnetz, Mobilfunk und Internet, im Rahmen der Ermittlungstätigkeit eingeordnet werden.

Übereinstimmend wird ausgeführt, dass alle Kommunikationsbereiche und -arten grundsätzlich relevant seien. Eine prozentuale Einschätzung sei allerdings nicht möglich. Vor allem im

---

309 Siehe unten Tabelle F-2.

klassischen Kriminalitätsbereich und bei der organisierten Kriminalität finde die Kommunikation nach wie vor über Handy und auch im Festnetz statt, sodass beide Bereiche für die Ermittlungen wesentlich sind. Das klassische Festnetz spiele auch weiterhin eine Rolle in der Täter-Opfer-Relation. Als Beispiele wurden Entführungen (erpresserischer Menschenraub) und v.a. der Enkeltrick genannt. Im letzteren Fall seien alte Menschen das durchgängige Opferprofil. Diese hätten in der Regel einen klassischen Festnetzanschluss bei der Deutschen Telekom. Dort sei jedoch, wie bei den meisten Anbietern, der entscheidende Ermittlungsansatz über die Anrufernummer entfallen (siehe auch Beispiel 4). Die Bedeutung des Festnetzes folge im Übrigen auch aus dem Umstand, dass die Deutsche Telekom noch immer der Netzbetreiber mit den meisten Kunden sei.

Relativ nehme der Festnetzbereich gegenüber dem immer noch zunehmenden Mobilfunksektor gleichwohl ab. Dieser allgemeine Trend sei in Deutschland nach wie vor ungebrochen. Entsprechend seien sowohl die Verkehrsdatenüberwachung als auch die Überwachung nach § 100a StPO in diesem Bereich ungebrochen stark. Die Täter arbeiteten und bewegten sich mobil. Dies gelte freilich nur für den klassischen Telefonie-Bereich. Zunehmende Bedeutung erlange daneben Datenkommunikation im Internet. Diese neuen Kommunikationsformen (Voice-Over-IP), die auf unterschiedlichen Übertragungswegen abgewickelt würden (Skype, ICQ, MSN etc.), hätten den Ermittlungsalltag bereits erreicht. Diese Entwicklung führe dazu, dass Festnetz und Internet kaum noch zu trennen seien. Technisch ersetze das Internet dabei immer mehr das Festnetz, das bei einigen Providern technisch zunehmend über das Internet betrieben werde. Verknüpfungen ergäben sich im Übrigen auch auf der Grundlage vieler Tarifmodelle wie Doppel-Flatrates für Telefon und Internet, sog. Homezone-Tarifen und UMTS-Verbindungen, die sich für den Nutzer zuhause wie ein Festnetzanschluss darstellen, Ergänzungskarten u.v.a.m.

Ob konkrete Kommunikationsformen von bestimmten Tätern genutzt werden, vermochten die Befragten nicht konkret zu bestimmen. Jedenfalls existierten keine klassischen Täterprofile für die unterschiedlichen Kommunikationsformen. Das Nutzungsverhalten hänge ebenso wie die Bemühungen um Anonymisierung hingen im Einzelfall von der Bildung bzw. Persönlichkeit des Täters, insbesondere seiner Technikaffinität ab. Solche Täter loteten vor Tatbegehung aus, inwieweit Möglichkeiten bestehen, sie als Täter zu identifizieren. Gewisse Häufungen sagen einige freilich im Bereich der IuK-Kriminalität. Überdurchschnittliches IT-Knowhow zur Nutzung neuester Verschleierungstechniken bei der elektronischen Kommunikation haben einige der Befragten auch bei Tätern aus dem rechts- und linksextremen Milieu sowie dem Umfeld des islamistischen Terrorismus festgestellt. Mitglieder entsprechender Gruppierungen würden sich auch gezielt über die Wirkungsweise von IMSI-Catchern und über die Bedingungen der Verkehrsdatenerhebung zu informieren.

Beispiel 1: Tötungskriminalität

Ermittlungen in einem Tötungsdelikt aus dem Februar 2010, bei dem die Ermittlungen noch vor dem Urteilvom 2.3.2010 begonnen wurden. Damals stand noch mehr Zeit zur Verfügung um zu selektieren, welche Daten zu Beginn benötigt werden und welche eventuell erst später beantragt werden müssen. Im Laufe der Ermittlungen, als sich die neue Entwicklung abzeichnete, hatte sich die Situation geändert. Nun sahen sich die Ermittler gezwungen, bereits am Anfang der Ermittlungen ein Maßnahmenpaket zu schnüren, in der Hoffnung, dass die tatsächlich benötigten Informationen dabei sind. Es werden nun viel mehr Daten bereits in den ersten Tagen eingeholt, um Verkehrsdaten mangels längerer Speicherfristen überhaupt nutzen zu können.

Beispiel 2: Wirtschaftskriminalität

Betrug zum Nachteil von Wertpapieranlegern. Im Zuge der Ermittlungen gab es Hinweise auf andere Straftaten, bei denen sich die Täter bei den Opfern per Telefon als angebliche Vermögensberater gemeldet hatten (wobei dies oft von Callcentern geschah) und persönliche Daten erfragt hatten, mit denen vermögensschädigende Wertpapiergeschäfte (Schaden für die Bank: € 1,1 Mio.) getätigt wurden. Die einzige Spur ist in diesen Fällen der Verbindungsanruf bei der Bank. Ohne Verkehrsdaten gibt es in derartigen Fällen zumeist keine Ermittlungsansätze. Über Funkzellenauswertung bzw. den Einsatz eines IMSI-Catchers würde zusätzlich in Rechte nicht betroffener Menschen eingegriffen, was bei Vorliegen der Vorratsdaten teilweise vermeidbar wäre.

Beispiel 3: Steuerhinterziehung

Steuerhinterziehung mit Schadenshöhe im zweistelligen Millionenbereich durch hierarchisch strukturierte Tätergruppierungen. Die Mittelsmänner zu identifizieren, bereitet aktuell erhebliche Schwierigkeiten: Die Kontakte wurden ursprünglich per (Mobil-)Telefon geknüpft. Durchsuchungen bei Tatverdächtigen könnten Aufmerksamkeit erregen bzw. weitere Mittäter warnen. Eine Auswertung der retrograden Verbindungsdaten des originären Täters wäre die einzige Maßnahme um die Strukturen zu ermitteln und so einen Verlust von Beweismitteln zu verhindern.

Beispiel 4: Enkeltrick

Im Beispiel des Enkeltricks agieren oft polnischen Tätergruppen, die vom Ausland aus hier anrufen. Gleichzeitig steht in Deutschland ein Läufer bereit, der anschließend das Geld abholt. Diese Gruppierungen können ohne Ermittlung der Verkehrsdaten nicht mehr identifiziert werden. Viele der betagten Opfer bemerken den Betrug erst zu einem späteren Zeitpunkt, nach Gesprächen mit Angehörigen oder Bekannten. In der Zwischenzeit kann die Datenlöschfrist bereits überschritten sein.

Beispiel 5: Grenzüberschreitender Kfz.-Diebstahl

Im Raum Nürnberg ist seit einiger Zeit ein starker Anstieg an PKW-Diebstählen zu verzeichnen. Es ist bekannt, dass die Täter vor, während und nach der Tat kommunizieren. Die Kfz. werden kurzgeschlossen und nach Tschechien gefahren. Die einzige Möglichkeit, die Täterstrukturen zu ermitteln und nachzuweisen, führt über die Kommunikation. Ohne gespeicherte Kommunikations- bzw. Standortdaten fühlen sich die Ermittler hilflos. Als alternative Maßnahme könnten Polizeistreifen versuchen die Täter auf frischer Tat zu fassen. Das ist aber anhand der Größe des Gebiets unrealistisch.

Beispiel 6: Baustellenplünderung

Seriendiebstähle von teuren Baumaschinen durch eine reisende ausländische Tätergruppe in einem größeren Umkreis auf sächsischen Baustellen. Retrograde Verkehrs- (in diesem Fall v.a. Funkzellen-) Daten waren hier der einzig zielführende erste Ermittlungsansatz. Bei derart komplexen Fällen dauert es allerdings eine gewisse Zeit, bis überhaupt erkennbar wird, ob und von wem Daten erhoben werden müssen. Ohne diese Informationen fehlt auch der Ansatzpunkt für eine Observation.

Beispiel 7: Produkterpressung

Eine Firma wird per E-Mail mit der Drohung erpresst, dass ein Teil des Warensortiments vergiftet werde, wenn nicht ein bestimmter Geldbetrag überwiesen würde. Der Täter hatte ein Online-Konto mit fiktiven Personalien eröffnet, auf das das Geld überwiesen werden sollte. Zunächst wurden die IP-Daten zu der Kontoeröffnung angefordert, doch der Täter hatte sich getarnt und sich anonymisiert. Mit weiter zurückliegenden, retrospektiven Daten hätte er ermittelt werden können. Am Ende konnte er über andere, früher begangene Delikte – ebenfalls über die Auswertung retrograder Daten – ermittelt werden.

Beispiel 8: Abfrageversuch bei präventiver Einsatzlage ohne explizite polizeirechtliche Grundlage

In einem Internetforum wurde ein Suizid angekündigt. Die IP-Adresse konnte ermittelt werden, da der Suizident zu dieser Zeit online noch aktiv war. Der zuständige Netzbetreiber hat sich jedoch geweigert, diese IP-Adresse nach dem Bestandsdatum aufzulösen, da es an einer Rechtsgrundlage fehlte. Eine Straftatsituation war nicht gegeben. Drei Stunden später war es Kollegen auf andere Weise – nämlich über das Auflösen eines E-Mail-Accounts – gelungen, an das Bestandsdatum zu kommen. Zu diesem Zeitpunkt war der junge Mann dann aber schon tot. Er wurde tot auf der Tastatur liegend aufgefunden. Der Fall wurde in der Presse ausführlich aufgegriffen. Zwei Jahre zuvor hatte es in dem betreffenden Bundesland einen vergleichbaren Fall gegeben.

Beispiel 9: Gemischt präventive-repressive Einsatzlage

Nachts wurde mit einer großkalibrigen Waffe in das Schaufenster eines kleinen Ladens geschossen. Am nächsten Tag wurde eine Morddrohung per SMS an den Inhaber gesandt. Aus strafrechtlicher Perspektive ist der Fall als Sachbeschädigung und Bedrohung zu qualifizieren, also keine schweren Straftaten, sodass die Schwelle für eine Verkehrsdatenabfrage nicht überschritten war. Mangels präventiver Ermächtigungsgrundlage in dem betreffenden Bundesland liefen die Ermittlungen im Ergebnis ins Leere.

Beispiel 10: Kinderpornographie

Die inkriminierten Bilddateien werden in diesem Bereich häufig im Wege des File-Sharing eingestellt und verbreitet. Für die dafür notwendigen E-Mail-Accounts werden oft falsche Kontaktdaten hinterlegt, sodass die hinter den Kommunikationsinhalten bzw. der Tathandlung stehenden Personen nur anhand der IP heraus ermittelt werden können. Die Täter legen sich hierzu regelmäßig mehrere sog. „Wegwerf"-Accounts mit gefaketen Bestandsdaten an, um sich auf kinderpornografischen Foren zu registrieren. Die E-Mail-Adresse nutzen sie zumeist nur zu diesem Zweck. Wenn die Polizei später Kenntnis von dem Sachverhalt bekommt, ist es nach dem Wegfall der Vorratsdatenspeicherung nicht mehr möglich, über die Login-Daten den tatsächlichen Inhaber der E-Mail-Adresse zu ermitteln. Einige Ermittler sprechen gerne von „Donald-Duck-Accounts".

Beispiel 11: Pädophilie in Netzwerken

Auch bei Pädophilie in Netzwerken sind falsche Anmeldedaten häufig. Ein unter falschem Namen angemeldeter Täter nutzte das Netzwerk, um mit jungen Mädchen in Kontakt zu treten. Nach einiger Zeit verabredete er sich mit ihnen, um sie zu vergewaltigen. Die Aufklärung war nur durch den Zugriff auf retrograde Daten möglich. In einem ähnlichen Fall wurde ein 14jähriges Mädchen als vermisst gemeldet, das zuvor über SchülerVZ mit einem erwachsenen Mann gechattet hatte. Die IP-Adressen konnten zwar ermittelt werden, die Identifizierung wurde von dem Provider jedoch abgelehnt. Das Mädchen konnte nicht gefunden werden.

Beispiel 12: Live-Übertragung eines Sexualdelikts

In einem Internetforum wurde von einem Mann angekündigt, er werde eine junge Frau vergewaltigen und die Vergewaltigung live im Internet übertragen. Mithilfe der retrograden Daten hätte der Mann möglicherweise ermittelt werden können. Mangels gespeicherter Daten war dies jedoch nicht möglich. Ob die Vergewaltigung tatsächlich stattgefunden hat, ist nicht bekannt.

1.2.2. Kriminalitätsbereiche, in denen die Telekommunikation eine besondere Rolle spielt

Die Gesprächspartner sollten im nächsten Schritt Kriminalitätsbereiche benennen, bei deren Begehung elektronische Kommunikation typischerweise eine Rolle spielt. Neben den Delikten, die über Kommunikationsmittel begangen werden, so die einhellige Auskunft, könne Telekommunikation grundsätzlich in allen Deliktsbereichen eine Rolle spielen. Eine scharfe Zuordnung zu Phänomenen sei nicht möglich. So könne es vorkommen, dass sich Täter heute auch im Bereich 'klassischer' Kriminalität ein Tatmittel über das Internet besorgen. Grundsätzlich könne man unter den heutigen Lebensbedingungen bei keiner Deliktsart ausschließen, in der nicht zu irgendeinem Zeitpunkt kommuniziert werde. Das beginne bei Beleidigung oder Stalking. Auch bei Erpressungen (siehe Beispiel 7) und selbst bei Tötungsdelikten werde zwangsläufig irgendwann ein Telekommunikationsmedium genutzt. Als Beispiel wird über ein Ermittlungserfahrungen in einer Mordserie in Zusammenhang mit kurdischen Rauschgifthändlern berichtet, in deren Verlauf aus dem Ausland 50 oder 100 Prepaid-Karten zur Verschleierung geordert worden seien, diese seien dann jede halbe Stunde gewechselt worden. Als Ausnahme sehen einige am ehesten klassische Beziehungstaten, die spontan erfolgen; dort spiele Kommunikation für das Tatgeschehen selbst gar keine Rolle.

Bei allen kommunikationsrelevanten Delikten kann dann nach der Funktion der Kommunikation unterschieden werden. Auf der einen Seite erfolgt die Kommunikation täterseitig, also intern. Dies könne im Planungsstadium, während der Tatausführung oder danach geschehen. Davon ist, auf der anderen Seite, die Kommunikation zu unterscheiden, die auf die Opfer zielt. So riefen Täter vor Begehung eines Einbruchdiebstahls häufig in der Wohnung an, in die sie später einbrechen wollten, um auf diese Weise sicherzustellen, dass niemand zu Hause ist. Ebenso bedeutsam sei die Anbahnungs-Kommunikation, die gezielt zur Kontaktaufnahme erfolge. Bei Geiselnahmen, Entführungen und Erpressungen meldete sich der Täter heute zumeist über das Telefon bei dem Opfer, manchmal auch per E-Mail. Auch beim Enkeltrick (siehe Beispiel 4) und anderen Betrügereien zu Lasten älterer Menschen finde kein physischer Kontakt statt, sondern ausschließlich telefonischer. Alle genannten Kommunikationsvarianten könnten ein entscheidender Ermittlungsansatz sein; dabei spiele keine Rolle ob die Kommunikation in einem Fall Tatbestandsrelevanz besitze oder 'bloße' Ermittlungsmaßnahme sei.

Weitere Unterschiede seien dann entlang der technischen Umstände festzustellen, beispielsweise ob Mobilfunk oder Festnetz genutzt werde oder ob sich ein Täter noch alter Technik, also leitungsvermittelter Kommunikation (analog, ISDN) bediene oder sich bereits im Bereich der breitbandigen Kommunikation mit DSL-Anschlüssen bewege. Auch im Bereich der mobilen Kommunikation gebe es vielfältige Varianten, indem fremde Anschlüsse angezapft, Hot-Spots oder Internet-Cafés genutzt werden. Dies alles habe dann jeweils spezifische Implikationen im Rahmen der Datenaufklärung.

Ein Gesprächspartner erklärte den Kern der Problematik wie folgt: *„Wir leben im Zeitalter der @-Generation. Das soziale Leben verlagert sich mehr und mehr ins Internet. Die Jugend*

kauft nicht mehr bei Karstadt, sondern im Internet. Es besteht also nicht primär das Risiko, dass die Jugendlichen Kaufhausdiebstähle begehen, sondern dass Delikte im Internet begangen werden. Gerade bei Warenbetrug bzw. Warenkreditbetrug ist eine deutliche Verlagerung ins Internet zu erkennen. Die Zahl der Raubüberfälle und Einbrüche geht zurück. Der ordentliche, intelligente Kriminelle benutzt heute Geldautomaten und moderne Kommunikationsmittel. Darin besteht heute die basispolizeiliche Arbeit."

1.2.3. Daten- und Abfragearten, ihre Bedeutung für die Ermittlungsarbeit und ihre Verfügbarkeit

Im Folgenden wurden die Bedeutung der verschiedenen Datenarten und Abfragearten im repressiven und präventiven Ermittlungskontext analysiert sowie die Konsequenzen der weggefallenen Vorratsdatenspeicherung bezogen für den Abfrageerfolg.

Hierzu wurde zunächst erklärt, dass die Bedeutung der einzelnen Tools stets von Tat und Tatort abhängig sei. Sei der Tatort im virtuellen Raum angesiedelt, dann gebe es grundsätzlich auch nur dort Spuren. Sei der Tatort nicht virtuell, gibt es regelmäßig noch andere Spuren, die Ermittlungsansätze bieten könnten. V.a. im Bereich der professionellen Bandenkriminalität würden jedoch sehr wenige Spuren hinterlassen, weil diese Täter das kriminalistische Potenzial der Polizei gut kennen würden. Das bedeute, dass es immer weniger Spuren gefunden oder, wie z.B. im Bereich des Skimming, durch den Abbau der Geräte wieder verwischt würden. Im Bereich der Verkehrsdaten ließen sich aber auch in diesen Fällen noch Spuren finden. Wenn diese Identifizierungsmöglichkeiten wieder wegfielen, würden viele Ermittlungen in solchen Fällen regelmäßig ins Leere laufen. Es sei also eine immer stärkere Verlagerung der Spuren zu beobachten, von der klassischen Spur zu Kommunikationsspuren

1.2.3.1. Retrograde Daten

Im Mittelpunkt der weiteren Problembeschreibung steht ganz deutlich die Situation bei den retrograden Daten. Hier werden der größte Bedarf und zugleich die gravierendsten Auswirkungen lokalisiert.

Essentielle Bedeutung haben retrograde Daten nach der Erfahrung der Polizeipraktiker bei einer Vielzahl von Delikten. Dies umfasse alle Delikte des in § 100a StPO sowie die IuK-Kriminalität, die über § 100g Nr.2 StPO erfasst sind. Explizit genannt werden ergänzend

- Hackerkriminalität,
- Phishing, Skimming, Carding,
- Propagandadelikte im Internet,
- Raubdelikte,
- schwere Gewalt- und Tötungsdelikte,
- sonstige Kapitaldelikte,
- Kinderpornographie, Kindesmissbrauch (vgl. Beispiele 10 und 11),

- Wirtschaftsbetrug,
- Rauschgiftbeschaffungsfahrten und Drogenkriminalität im Allgemeinen,
- organisierte Einbruchskriminalität, bandenmäßige Einbruchskriminalität,
- die übrigen Bereiche der organisierten Kriminalität,
- Enkeltrick (vgl. Beispiel 4)[310],
- Terrorismus,
- Staatsschutzdelikte,
- Verstöße gegen das Kriegswaffenkontrollgesetz und andere nebenstrafrechtliche Deliktsbereiche.

Auch für den Bereich der Gefahrenabwehr[311] werden übereinstimmend verschiedene Situationen aufgezählt, in denen typischerweise der Zugriff auf retrograde Daten erforderlich sei. Hierunter fielen insbesondere

- Bedrohung des öffentlichen Friedens,
- Amoklagen bzw. Amokandrohungen,
- Geiselnahmen,
- Terroristische Gefahrenlagen,
- Verdacht auf oder explizite Ankündigung von Suizid,
- Vermisstenfälle,
- häusliche Gewalt,
- Stalking,
- Aktivitäten in social communities, insbes. Kontaktanbahnung durch Pädophile,
- Computersabotage,
- Botnetzbekämpfung.

In allen genannten Deliktsbereichen und Gefahrenlagen erscheinen retrograde Daten als das entscheidende Instrument zur Gewinnung eines Anfangsverdachts und zum Einstieg in die Ermittlungen bzw. zur Vorbereitung und Durchführung gefahrenabwehrender Maßnahmen. So zeigten etwa die Erfahrungen bei Tötungsdelikten, dass es in etwa 90 % der Fälle zuvor Kontakte zwischen Täter und Opfer gegeben habe. Prinzipiell seien sowohl Verbindungsdaten (Internet und Telefonie) als auch Geodaten von Bedeutung. Die gelte insbesondere für Delikte, bei denen das Kommunikationsgerät das zentrale Tatinstrument ist. Speziell bei den Internetdelikten sind ferner die Bestandsdaten eine primäre Erkenntnisquelle. Nur durch Einblick in die Verkehrsdaten könne eine Zuordnung zwischen dynamischer IP und Bestandsdatum hergestellt werden. Diese verkehrsdatengestützte Erkenntnisgewinnung sei nun deutlich erschwert, in vielen Fällen sogar unmöglich geworden.

---

310 Einige Bundeländer ordnen das Phänomen mittlerweile der organisierten Kriminalität zu oder ordnen die Bedeutung knapp unterhalb der Schwelle zur OK ein.

311 Dies schließt gefahrenabwehrende Interventionen bei Straftaten (präventiv-repressive Mischsituationen) mit ein.

Denn durch die Beschränkung der Verkehrsdatenabfrage auf Daten, deren Zielsetzung unternehmensbezogen und damit ganz anders gelagert ist als die Bedürfnisse der staatlichen Gefahrenabwehr und Strafverfolgung, haben sich spürbare Einschränkungen für die Praxis ergeben. Auf der Grundlage des § 96 TKG gehen ganz offenbar viele Abfragen ins Leere, weil die jeweils benötigten Daten nicht abrechnungsrelevant sind. Dabei erkennen die befragten Praktiker durchaus an, dass Netzbetreiber und Provider ihre Speicherpraxis nach dem rechtlichen Rahmen ausrichteten, der ihnen vorgegeben sei. Insbesondere seien sie gemäß § 96 TKG explizit dazu verpflichtet, die Daten zu löschen, sobald sie nicht mehr abrechnungsrelevant sind. Die Speicherung von Gerätenummern liege ebenso wenig im Interesse der Anbieter wie die nicht-anonymisierte Übermittlung von Kontaktdaten mit den entsprechenden Nummern; das letztere entspreche auch nicht den vertragsrechtlichen Bestimmungen zwischen dem Provider und dem Kunden. Aus alledem ergebe sich für die Unternehmen ein gewisser Löschungsdruck.

Durch den Wegfall der Speicherverpflichtung, verbunden mit genuin unternehmensspezifischen Charakteristika, die sich in der Hauptsache nach der implementierten Technik sowie den angebotenen Tarifstrukturen definieren, ist aus Ermittlersicht eine gewisse Willkürlichkeit entstanden, ob und wie lange Daten erreichbar sind. Die nachfolgenden Beschränkungen wurden besonders erwähnt:

- Bei eingehenden Daten seien die größten Ausfälle zu verzeichnen. Da diese in der Regel nicht gebührenrelevant seien, würden sie meist überhaupt nicht gespeichert. Sofern sie in einzelnen Fällen doch gebührenrelevant sind, würden sie dann meist nur wenige Tage gespeichert. Aus kriminalistischer Perspektive seien in vielen Fällen nicht nur die Verkehrsdaten des sog. A-Teilnehmers, sondern auch jene des Gesprächspartners, des sog. B-Teilnehmers, relevant. Mit einer Abfrage habe man die gesamte Kommunikation ermitteln können. Nunmehr sei ein gesonderter Beschluss für die Daten über diesen zweiten Anschluss erforderlich; dies sei freilich nur möglich, wenn dieser bekannt sei. Die Verkehrsdaten eingehender Anrufe seien ferner unerlässlich bei den schon erwähnten opferseitigen Ermittlungsansätzen.
- Im Hinblick auf die letztgenannte Konstellation sei zudem bei einem großen Universalanbieter das mögliche Ersatzinstrument zur Anruferidentifizierung, die Zielwahlsuche, nicht mehr möglich.[312]
- Im Mobilfunkbereich fehlten vermehrt Standort-/Geodaten. Dies betreffe u.a. Zellwechsel, die bei einigen Anbietern generell nicht gespeichert würden. Mit dem Wegfall der Daten zu eingehenden Verbindungen fielen im Übrigen meist auch die Geodaten der B-Teilnehmer weg.
- Im Flatratebereich seien häufig sämtliche Daten unerreichbar.

---

312 Die Befragten bestätigten übereinstimmend, dass es sich hierbei um ein Sonderphänomem speziell bei der Deutschen Telekom handele. Bei anderen Anbietern sei die Zielwahlsuche möglich und auch zu Zeiten der Vorratsdatenspeicheung stets möglich gewesen.

- Systematische Ausfälle würden ferner bei IMEI- und IMSI-Kennungen sowie bei IP-Adressen auftreten. In diesen Bereichen seien häufig gar keine Daten mehr zu erlangen.
- Speziell bezogen auf die IP-Adressen ergebe sich daraus das Folgeproblem, dass die zur Identifikation erforderliche Verknüpfung mit den Bestandsdaten nicht mehr möglich sei (sieh dazu auch gleich unten Pkt. 1.2.3).
- Ein weiteres Problem im Bereich der IP-Adressen sei das immer häufigere IP-Sharing, das eine Zuordnung zu individuellen Nutzern unmöglich mache. Diese Konstellation trete zum einen bei WLAN-Hotspots für den Zugriff auf das mobile Internet über UMTS auf (siehe hierzu auch gleich unten Pkt. 1.2.4.). Zum anderen gebe es inzwischen bereits diverse Provider, die generell keine eigenen IP-Kontingente mehr besäßen, sondern sich von Zweit- oder Drittanbietern bedienten. Die Zuordnung wechsele in diesen Fällen so dynamisch, dass Ermittlungsbeamte keine verbindliche Struktur und damit auch keinen Ermittlungsansatz mehr finden könnten. Hinter einer einzigen IP-Adresse könnten unter Umständen 1.000 oder 10.000 oder mehr zeitgleiche einzelne Zugriffe auf das Internet stecken. Als konkretes Beispiel benennt ein Interviewpartner die Firma 1&1, die in großem Stil Telefonica-IPs gemietet hätte. Im Hinblick auf die günstigere Kostenstruktur sei zu erwarten, dass dieses Geschäftsmodell weiter zunehmen werde.

Neben dem Totalausfall bestimmter Datenkategorien erscheint die Speicherfrist als besonders problematischer Punkt. Über die Vielzahl der Unternehmen und teilweise auch regionalen Unterschiede hinweg lasse sich als längste Speicherfrist, in der Verkehrsdaten mit relativer Sicherheit noch erreichbar seien, ein Zeitraum von 7 Tagen festhalten. Ein Provider speichere neuerdings wieder vermehrt 30 Tage, doch das sei reiner Goodwill. Gerade bei kleineren Anbietern würden Daten aus Kapazitätsgründen nur für maximal drei Tage gespeichert. Ansonsten gebe es zwar auch in zahlreichen anderen Konstellation eine 30-Tage-Grenze; diese sei aber weder systematisch noch unternehmensbezogen nachvollziehbar oder kalkulierbar; dasselbe gelte für längere Fristen, die allerdings nur punktuell anzutreffen seien. Ein Experte spitzt die Situation mit dem Hinweis darauf zu, dass die Aufklärung beispielsweise in Missbrauchsfällen derzeit davon abhänge, *„ob der Täter Kunde bei Arcor oder bei der Deutschen Telekom ist“*.

Einigkeit besteht in dem Befund, dass insbesondere die 7-Tages-Frist für eine zielführende Ermittlungsarbeit im Bereich der Verkehrsdatenabfrage regelmäßig nicht ausreichend sei. Das gelte insbesondere für diejenigen Deliktsbereiche, in denen das Anzeigeverhalten typischerweise sehr verzögert sei (z.B. Phishing, E-Bay-Betrug, Enkeltrick, vgl. Beispiel 4). Abfragemöglichkeiten seien in diesen Bereichen nahezu unmöglich geworden. Denn die Kommunikationsspuren müssten in solchen Fällen sehr weit retrograd vorhanden sein. Für den Bereich Computerbetrug verzeichnet z.B. das LKA Baden-Württemberg für 2010 bislang bereits einen Anstieg der nicht aufklärbaren Fälle um 70 %. Täter, die im vergangenen Jahr noch hätten ermittelt werden können, seien heute nicht mehr greifbar und könnten ihre Be-

trugsserien fortsetzen. Einige Gesprächspartner äußerten die Vermutung, dass professionellen Tätern inzwischen bereits bekannt sei, bei welchen Anbietern nichts gespeichert wird, und dieses Wissen gezielt für Straftaten genutzt werde. Einige Provider würden teilweise sogar damit werben, keine Daten zu speichern. Des Weiteren würden entsprechende Informationen über Foren verbreitet.

Aufgrund der aktuellen Speicherpraxis ergeben sich nach den Schilderungen der betreffenden Beamten auch spezifische Probleme im präventiven Anwendungsbereich der Verkehrsdatenabfrage. Als konkrete Beispiele werden etwa Erpressungen und Amokandrohungen benannt, die typischerweise per Telefon oder im Internet ausgelöst werden. Hier sei die Ermittlung der Urheber in der Regel unmöglich geworden, da die ermittlungsrelevanten Informationen nicht oder nur unzureichend gespeichert würden. Als weiteres Beispiel wird auf Fälle mit akuter Suizidgefahr hingewiesen. Dort seien zur Ermittlung des Standortes regelmäßig Geodaten notwendig. Neben Echtzeitdaten zur Ermittlung des aktuellen Aufenthaltsortes betreffe das auch retrograde Standortdaten, etwa wenn es – bei abgeschaltetem Handy – um die Identifizierung möglicher Aufenthaltsorte auf der Grundlage der zuletzt eingeloggten Funkzelle gehe. Ohne Hinweise auf zumindest eine konkrete Funkzelle sei der Standort faktisch kaum ermittelbar. Retrograde Geodaten seien darüber hinaus von Bedeutung, weil eine Funkzellenabfrage in Echtzeit oft nicht möglich sei, da der Anbieter diese Informationen oft nicht speichere. Gleiches gelte sinngemäß für Maßnahmen zur Ermittlung des Aufenthaltes vermisster Personen. Im Beispielsfall 11 sei die Suche nach einem vermissten Mädchen, das sich mutmaßlich mit einem pädophilen Täter getroffen hatte, erfolglos geblieben, weil zwar die relevanten IP-Adressen ermittelt worden seien, der Provider sich aber geweigert habe, diese nach den Bestandsdaten aufzulösen. Ein Interviewpartner formuliert die Situation in solchen Fallkonstellation drastisch wie folgt: *„Wir können lediglich bei dem jeweiligen Unternehmen anrufen und fragen, ob es bereit ist […] das Leben seines Kunden zu retten oder nicht. Wenn der Provider dazu nicht bereit ist und die Herausgabe der erforderlichen Daten ablehnt, kommen wir auf diesem Weg nicht weiter“* (siehe auch Beispiel 8).

1.2.3.2. Echtzeit- und zukunftsgerichtete Daten

Gerade der präventive Bereich wie auch gemischt präventiv-repressive Einsatzlagen (vgl. Beispiel 9) werden an erster Stelle als Beispiel für Situationen genannt, in denen – anstelle oder neben retrograden – Echtzeitdaten wichtig seien. Diesbezüglich haben die Interviewpartner in der großen Mehrheit bislang keine unmittelbaren Auswirkungen durch das Urteil vom 2.3.2010 zu vermelden. Ein Gesprächspartner verweist jedoch auf eine indirekte Auswirkung. Durch den Wegfall der retrograden Daten sei ein wichtiges Element für die Vorbereitung aller Echtzeitmaßnahmen, auch der Datenabfrage in Echtzeit, entfallen. Damit könne das Ziel einer Echtzeitmaßnahme oft gar nicht bestimmt werden.

Darüber hinaus werden einige Probleme aufgezeigt, die in keinen unmittelbaren Zusammenhang mit dem BVerfG-Urteil aufweisen. Dies betrifft vor allem technisch bedingte Einschränkungen, insbesondere bei der Standortabfrage in Echtzeit. § 100g Abs. 1 S. 3 StPO sei

weitgehend totes Recht, da bislang keine Technik existiere, die eine gezielte Ausleitung von Standortdaten in Echtzeit ermögliche. Hier fehle eine entsprechende technische Richtlinie. Verkehrsdaten und bestimmte Inhaltssignale (SMS-Texte, etc.) könnten nicht getrennt werden, sodass stets ein 100a-Beschluss erforderlich sei. Daher sei der Begriff eigentlich irreführend. Faktisch handele es sich um kurzfristige retrograde Daten. Diese würden zumeist im Rahmen von Maßnahmen gem. § 100a StPO von der Polizei selbst erhoben. Faktisch erscheint die Echtzeitabfrage des § 100g StPO als Sonderkonstellation, die ausschließlich auf die Abfrage der Standortdaten ausgerichtet und nur unter den Voraussetzungen einer Katalogtat möglich ist.

Speziell bezogen auf das Internet wird als zusätzliches Problem beschrieben, dass man von der gerade aktiven Verbindung Kenntnis haben müsse, um überhaupt zeitgleich eine Abfrage vornehmen zu können. Die Echtzeitdaten würden aber in einem ganz anderen technischen Bereich eines Netzbetreibers verwaltet. Die für Verkehrsdatenabfragen zuständige Sicherheitsabteilung sei in der Regel ausschließlich für die Abfrage-Systeme zuständig, nicht für die Live-Systeme. In den Netzüberwachungszentren, die für die Echtzeitdaten zuständig seien, überwögen häufig datenschutzrechtliche Bedenken. Aus diesem Grund seien schon Auskünfte verweigert worden, obwohl die betreffende Zielperson zeitgleich im Internet aktiv gewesen sei (vgl. Beispiel 8).

In rechtlicher Hinsicht könnte zudem zweifelhaft sein, ob die so abgefragten Daten überhaupt Verkehrsdaten sind oder es sich nicht eigentlich um eine technische Kommunikation zwischen einem Endgerät und dem System des Netzbetreibers handelt. Somit zähle es eigentlich nicht als Verkehrsdatensatz. Man müsse nicht in die abrechnungsrelevanten Daten schauen, sondern in das Echtsystem, ob es aktuell eine Rückmeldung vom System über den Zellbereich gibt, in dem sich das Handy gerade aufhält.

Auf positive Erfahrungen verwies ein Vertreter aus Berlin. Die dort 2007 eingeführte präventive Ermächtigungsgrundlage für die Standortabfrage (§ 25a ASOG) spreche gezielt von der „Standortbestimmung bei Telekommunikationsendgeräten“ und vermeide damit den Begriff Verkehrsdaten. Diese Maßnahme werde mangels Kommunikation nicht als Eingriff in die Kommunikation gewertet und erhalte keinen Verweis auf § 113 TKG. Ein Netzanbieter habe für diese Abfragen einen eigenen Vordruck erstellt und führe diese auch aus. Andere Netzbetreiber würden die Vordrucke inzwischen kennen und ebenfalls bearbeiten.

Keinerlei Auswirkungen sehen die Befragten im Übrigen im Hinblick auf die Abfrage zukunftsgerichteter Daten. Diese hätten freilich einen recht geringen Einsatzbereich und seien vor allem im Rahmen von längerfristigen Strukturermittlungen von Bedeutung.

1.2.3.3. Bestandsdatenauskünfte

Einschneidend erscheinen hingegen die Auswirkungen auf Bestandsdatenauskünfte nach § 113 TKG. Die meisten Unternehmen würden der nicht unumstrittenen Rechtsauffassung folgen, Auskünfte nach § 113 dürften im Zusammenhang mit einer Verkehrsdatenabfrage

gegenwärtig nicht gegeben werden, da der explizite Verweis auf § 96 TKG fehle. Alle Befragten verweisen auch übereinstimmend auf evidente Probleme speziell in diesem Bereich. Die praktischen Konsequenzen würden speziell in einer Konstellation spürbar: die TK-Unternehmen weigerten sich in aller Regel, IP-Adressen nach den Bestandsdaten aufzulösen. Gerade hier fehle aber in vielen Fällen jeder andere Ermittlungsansatz. Siehe hierzu auch oben die Beispiele 8 und 11 sowie die rechtlichen Ausführungen in Teil B.

Im Hinblick auf alle Arten der Bestandsdatenabfrage gem. §§ 111 bis 113 TKG wird ferner auf die grundsätzliche Problematik mit unrichtigen Identitätsangaben verwiesen. Die beim Kauf bzw. der Aktivierung einer Prepaid-Karte vorgesehene Angabe der Personalien werde oftmals entweder gar nicht verlangt oder die angegebenen Personalien würden nicht überprüft. Oft würden Nutzer Namen erfinden (dies seien häufig sogar leicht erkennbare Phantasienamen, wie sie auch in Internet-Foren verbreitet seien) oder die Namen unbeteiligter Dritter verwenden (Familie, Verwandte, Bekannte, Unbekannte). Einige Gesprächspartner berichten von Fällen, in denen solche Personen dann von weiteren, teilweise einschneidenden Maßnahmen wie Durchsuchungen betroffen waren. Insbesondere die Phantasienamen, zu deren Verwendung in manchen Internet-Foren aktiv aufgerufen werde[313], bereiteten zunehmend Probleme.[314] Auch bei Prepaid-Karten, die über Tauschbörsen weitergereicht werden, seien die Bestandsdaten dann wertlos. Dasselbe gelte bei der Verwendung ausländischer Karten. Eine umfassende Verifizierungspflicht in diesem Bereich wird daher als wünschenswert bezeichnet.

Vergleichbare Identifizierungsprobleme bestünden ferner in Bezug auf E-Mail-Accounts, bei denen Phantasienamen ein weit verbreitetes Phänomen seien. Manche Ermittler sprechen dann auch von *„Donald-Duck-Accounts“* (siehe auch die Fallbeschreibung in Beispiel 10). Hier gebe es zusätzlich das Problem, dass viele Provider ihren Sitz im Ausland hätten und es oftmals keine weiteren Verzeichnisse gebe.

1.2.4. Sonstige technische Fragen

Besonders erörtert wurden dann einzelne weitere technische Fragestellungen, die den Erfolg der Verkehrsdatenerhebung ebenfalls beeinflussen können. Zunächst ging es um besondere Probleme der Identifizierbarkeit, die bei der mobilen Nutzung des Internets auftreten können, insbesondere dann, wenn öffentliche WLAN-Anschlüsse genutzt werden (z.B. in Cafés und Gaststätten, in Hotels oder im ICE).

Nach Auskunft der Befragten ergäben sich ermittlungstechnisch auf den ersten Blick keine Unterschiede, ob das Internet von zuhause oder vom Handy aus genutzt werde; in beiden

---

313 Bei einer probehalber durchgeführten Suche während der Durchführung der Studie konnten beispielsweise unter www hackerboard.de/off-topic-zone/41817-prepaid-falsche-daten-angeben html in der Tat entsprechende Anleitungen gefunden werden [Juni 2011].

314 Ein Interviewpartner verweist auf Erhebungen der Bundesnetzagentur, nach der mindestens 10 % aller Prepaid-Nutzer falsche Personalien angäben. Diese Prozentangabe konnte nicht verifiziert werden.

Fällen müssten grundsätzlich die gleichen Daten ermittelt werden. Im Hinblick auf die telekommunikationstechnischen Konsequenzen ergäben sich hingegen deutliche Unterschiede. Bei dem Zugang zum Internet über Mobilfunk träten, häufig auch kumuliert, die schon beschriebenen Probleme aus der Nutzung von Flatrates und dem zunehmendem Aufkommen von IP-Pools auf. Die rechtliche Speicherverpflichtung habe bislang nur die IP-Adresse erfasst. Bei Mehrfachnutzung einer IP im UMTS-Netz sei hingegen die Port-Nummer das entscheidende technische Datum. Ohne Speicherung des Ports könne eine ermittelte IP-Adresse nicht mehr eindeutig einem konkreten Nutzer zugeordnet werden. Der Endnutzer sei dann nicht mehr identifizierbar. Diese Situation könne im Übrigen nicht nur bei der mobilen Internet-Nutzung auftreten, sondern auch bei der Handy-Nutzung. Handele es sich um duale Handys, sei es meist vom Zufall abhängig, ob sich das Gerät an einem bestimmten Standort über das Festnetz, GPRS, oder UMTS-Hotspots einwähle. Eine ähnliche Problematik stelle sich bei SIM-Boxen, die gerne zur Spurenverwischung genutzt würden.

Diskutiert wurde dann der mögliche kriminalistische Wert von Verbindungsdaten, die auf Wunsch des Kunden anonymisiert werden (indem die drei letzten Ziffern durch ein X ersetzt werden). Hier zeigte sich ein differenziertes Meinungsbild. Während einige Gesprächspartner mit Hinweis auf den fehlelenden Beweiswert solche Daten als vollkommen wertlos bezeichnen, erkennen andere zumindest einen gewissen Indizwert, der insbesondere im Zuge längerfristig angelegter Strukturermittlungen durchaus, wenn auch eingeschränkt, nützlich sein könnte. So könnten auf ihrer Basis beispielsweise Informationen über das Land und die Stadt des Gesprächsteilnehmers gewonnen werden. Darüber hinaus könnten sie in Fällen, in denen eine Nummer im Voraus bekannt sei, ungeachtet der drei ge-x-ten Endziffern, Anhaltspunkt für eine übereinstimmende Identität sein. Unbrauchbar seien sie freilich, wenn es um die konkrete Zuordnung von Nummern gehe.

Prinzipiell stellen die Interviewpartner, ungeachtet des gestiegenen Flatrateanteils, eine Zunahme dieser Konstellation fest. Im Übrigen existierten auch hier anbieterabhängige Unterschiede. Zum Teil würden die gespeicherten Nummern sofort anonymisiert, einige andere Unternehmen würden die XXX nach 7 Tagen einsetzen, während andere wiederum zumindest bis zum nächsten Abrechnungsdatum die vollständigen Nummern vorhalten und in dieser Form auch herausgeben würden. Zweifel wurden vereinzelt dahingehend zum Ausdruck gebracht, ob die entsprechenden Daten selbst nicht zumindest bei einigen Unternehmen in Gänze vorhanden wären und erst zur Herausgabe an die Behörden gezielt anonymisiert würden.

Nicht ganz einheitlich ist das Meinungsbild zu den Konsequenzen aus dem Wegfall der Speicherpflicht für Ort und Zeit der Aktivierung von SIM-Karten. Diese in § 113a Abs. 2 Nr. 4a TKG explizit geregelten Merkmale sind, abgesehen von den eingehenden Verbindungen, das einzige Datum, das nicht unter § 96 subsumierbar ist.[315] Einige Gesprächspartner führen aus,

---

315 Siehe dazu Teil B, insbes. Tabelle B-1.

dass diese Information in der Regel nicht besonders aussagekräftig sei, da es vom Zufall abhängen könne, wo die Karte aktiviert wird. Im Einzelfall, insbesondere dann, wenn es ansonsten keinerlei andere Ansatzpunkte gebe, könne das Datum weiterhelfen. Einige andere Ermittler verweisen auf einen nützlichen Indizwert, der etwa in Fällen des Enkeltrickbetruges in der Vergangenheit bereits zu weiterführenden Erkenntnissen geführt habe. So komme es vor, dass ein Täter aus dem Ausland einreise, eine SIM-Karte kaufe und sie aktiviere. Sowohl das Datum wie auch der Ort der Aktivierung seien dann bedeutsam, um den Ablauf der Tat insgesamt nachvollziehen zu können. In anderen Fällen könne eine vermehrte Aktivierung neuer Prepaid-Karten durch einen bestimmten Verdächtigen ein Indiz dafür sein, dass der Eintritt in das konkrete Vorbereitungsstadium begonnen habe. In dem aktuellen, bundesweit bekannt gewordenen Berliner Pokerraub-Fall sei eine der beteiligten Personen kurz vor dem Tatzeitpunkt von einer Vertragsnutzung plötzlich zu der Verwendung von Prepaid-Karten übergegangen. Ferner helfe die Information, in Fällen in denen Tätern eine Vielzahl von verschiedenen Prepaid-Karten nutzen, eine Übersicht zu bekommen, welche Karten aktiviert wurden. Im Einzelfall könne es schließlich auch ein entlastendes Indiz sein, wenn ein Verdächtigter zu einem betreffenden Zeitpunkt die Karte zwar in seinem Besitz, aber noch nicht aktiviert hatte.

Abschließend verweist ein Gesprächspartner auf eine technische Konstellation, die speziell in Grenzregionen auftreten kann. So könne sich ein Handy beispielsweise in der Bodensee-Region in Österreich oder der Schweiz einwählen. Dann könnten Verkehrsdaten nur über den Rechtshilfeweg beantragt werden. Dies sei überhaupt nur bei rechthilfefähigen Delikten möglich. Im Erfolgsfalle könne es mehrere Wochen dauern, bis Daten aus dem Ausland geliefert würden.

1.3. Mögliche Substitute für die Verkehrsdatenabfrage

Die Beurteilung der möglichen – das heißt aus Ermittlersicht vor allem: praktikablen und zielführenden, konkrete Erfolge versprechenden – Substitute ist zunächst danach zu differenzieren, welche Datenarten ausfallen.

1.3.1. Retrograde Daten

Einhellig bekunden die Ermittler, dass retrograde Telekommunikations-Daten, die nach ihrer Löschung verloren sind, durch andere Daten in aller Regel nicht ersetzt werden könnten. Auch mit anderen Mitteln seien Informationen mit vergleichbarem Indiz- bzw. Beweiswert meist nicht erreichbar. Ein in der Vergangenheit stattgefundenes Gespräch könne auf andere Weise weder recherchiert noch verwertbar belegt werden.

Etwas anders könnte sich die Situation im Einzelfall im Hinblick auf Standortdaten darstellen. Bei bekannten Tatorten könnten die Spuren mit den üblichen klassischen Ermittlungsmethoden aufgenommen und ausgewertet werden. Gerade bei der Tatortarbeit falle allerdings immer wieder auf, dass bei professionellen und organisierten Tätergruppen immer weniger Spuren hinterließen; dies gelte für Form- und andere klassische Spuren ebenso wie für DNA-

Spuren. In solchen Situationen sei mit den Standortdaten dann ein neuer, zusätzlicher Ermittlungsansatz entstanden – dieser sei somit gerade selbst ein Substitut gewesen, und zwar eines mit hohem Beweiswert. Der Wegfall dieses kommunikationsbezogenen Spurenansatzes wirke sich gerade in solchen Fällen spürbar aus.

1.3.2. Echtzeit- und zukunftsgerichtete Daten

Differenzierter wird die Situation im Hinblick auf Echtzeitdaten und künftig anfallende Daten beschrieben. Zunächst wurde einhellig darauf hingewiesen, dass im IP-Bereich insoweit keine Substitute denkbar seien. Dort seien Erhebungen prinzipiell in die Vergangenheit gerichtet, Echtzeit- und zukunftsgerichtete Daten spielten keine Rolle.[316]

Hingegen gebe es im Telefoniebereich, abhängig von der jeweiligen Fallkonstellation und den konkreten Ermittlungszielen, unter Umständen Möglichkeiten, die erforderlichen Informationen auf andere Weise zu generieren.

Am häufigsten wird dabei die Telekommunikationsüberwachung genannt. Dabei richtet sich das Interesse an dieser Stelle zunächst nicht auf die Frage, welche weiteren Auswirkungen die Nichtverfügbarkeit von Verkehrsdaten auf die Anordnungspraxis im Bereich der § 100a-Maßnahmen als solche hat (siehe zu dieser Frage gleich unten Pkt. 1.5.). Im Vordergrund steht hier vielmehr, ob und in welchen Situationen eine Inhaltsüberwachung eine Verkehrsdatenabfrage tatsächlich *ersetzen* kann. Während einige Ermittler eine solche Möglichkeit mit dem Hinweis ablehnen, die Durchführung einer TKÜ mit dem Ziel, damit primär vor allem Verkehrsdaten zu generieren, als weder sachgerecht noch verhältnismäßig prinzipiell ablehnen, erscheint die Maßnahme anderen Ermittlern durchaus als denkbares – und tatsächlich eingesetztes – Substitut, mit dem die latenten Lücken, die durch den Wegfall der Vorratsdatenspeicherung entstanden sind, eventuell ausgeglichen werden könnten. Sobald eine TKÜ geschaltet sei, fielen als Nebenprodukt die entsprechenden Verkehrsdaten gleichzeitig mit an. Als Vorteil kann darüber hinaus erscheinen, dass die Daten dann bei den Behörden anfielen, sodass sie unmittelbar zur Verfügung stünden, und zwar, anders als im Abfragefall, in – 'echter' – Echtzeit (sozusagen live). So entfällt der Zwischenschritt der Abfrage bei den TK-Unternehmen mit allen ihren Verzögerungen und Unwägbarkeiten.

Voraussetzung für eine solche Maßnahme sei freilich das Vorliegen eines Katalogdeliktes und der anderen Voraussetzungen des § 100a StPO. Nicht prognostizierbar sei dann aber gleichwohl der Ertrag. So müsse man darauf hoffen, dass auch in Zukunft über den abgehörten Anschluss Kommunikation zwischen den Zielpersonen stattfinde. Auf diese Weise könne dann beispielsweise auch die Tatzugehörigkeit eines bestimmten Handynutzers verifiziert werden. Zur Identifikation von Personen tauge die Maßnahme daher nur sehr bedingt. Den-

316 Die einzige Ausnahme ist wohl die E-Mail-Überwachung, die aber als Inhaltüberwachung angelegt ist und in dem vorliegenden Kontext daher außer Betracht bleiben soll.

noch werde sie insbesondere bei schwereren Straftaten nun vermehrt beantragt. Als konkrete Beispiele werden Serienstraftaten und Staatsschutzdelikte genannt.

Als besondere Variante kommt dabei bei einigen Dienststellen offenbar auch die Auslandskopfüberwachung zum Einsatz.[317] Diese setzt konzeptionell beim B-Teilnehmer an und könnte damit, zumindest in bestimmten Ermittlungskonstellationen mit Auslandsbezug, u.a. die derzeit problematische Zielwahlsuche ersetzen. Allerdings erscheinen die Nutzenbewertung und der Umfang der Nutzung sehr unterschiedlich. Einerseits äußerten mehrere Gesprächspartner Zweifel an dem Nutzen, insbesondere in Massenverfahren und den meisten präventiv relevanten Gefahrenlagen. Eine weitere Einschränkung ergebe sich aus dem erforderlichen Auslandsbezug. Eine Ausnahmestellung hinsichtlich der Anwendungsdichte nimmt offenbar Baden-Württemberg ein. Dort habe die Zahl der AKÜ-Maßnahmen um etwa 900 % zugenommen. Teilnehmer aus anderen Bundesländern wissen dagegen eher von vereinzelten Anwendungen zu berichten. Ein praktisches Hindernis seien schließlich Kapazitätsprobleme bei den Anbietern. Einige Gesprächspartner berichten von Wartezeiten von bis zu einem halben Jahr. Ein großer Anbieter führe nicht einmal eine Warteliste, sondern vergebe freie Kapazitäten jeweils neu nach dem 'first come'-Prinzip.

Mehrheitlich und mit Nachdruck weisen die Ermittler freilich auf den Mehraufwand hin, den eine ('ersatzweise') TKÜ im Vergleich mit der Verkehrsdatenabfrage mit sich bringe. Denn es müssten zwingend stets auch die Inhalte ausgewertet werden. Eine Falldokumentation ohne entsprechende Protokolle könne spätestens in der Hauptverhandlung nicht bestehen. Dieser Auswertungsdruck bringe, kombiniert mit der zusätzlichen Problematik des Kernbereichsschutzes, einen erheblichen zusätzlichen Personalaufwand mit sich.

Eine weitere Alternative könnte eine § 100g-Maßnahme auf der Basis einer Ausleitung an die Behörde sein. Auch in dieser Konstellation, wie sie das Gesetz in § 100g Abs. 3 StPO ausdrücklich vorsieht, könnte die Datenerhebung in Eigenregie der Behörden erfolgen. In mindestens einer Dienststelle wird diese Möglichkeit salopp *"Mini-TKÜ"* genannt. Die entsprechende Technik sei derzeit aber nur bei einem großen TK-Anbieter implementiert. Einschränkend wird ferner darauf hingewiesen, dass eine solche Möglichkeit überhaupt nur in Bezug auf Festnetzanschlüsse realisierbar sei. Mangels Filtermöglichkeit hinsichtlich SMS-Nachrichten übertrage das Signal beim Mobilfunk zumindest potenziell stets Inhaltsdaten, sodass eine solche Maßnahme dann – wie alle Echtzeitabfragen im Mobilfunkbereich (vgl. oben Pkt. 1.2.3.2.) – wiederum nur auf der Grundlage eines § 100a-Beschlusses durchgeführt werden könne.

Speziell auf den Einsatz in Echtzeit ist schließlich der IMSI-Catcher angelegt. Er kann daher grundsätzlich auch im präventiven Bereich nützlich sein. Allerdings beschränkten sich die Einsatzmöglichkeiten schon wegen des hohen personellen und finanziellen Aufwandes auf wenige Einzelfälle. Ein IMSI-Catcher koste mehr als eine Million Euro und binde drei Perso-

---

317 Vgl. §§ 3 u. 4 TKÜV. Ausführlicher zur Auslandskopfüberwachung *Kilchling* 2006.

nen für die Bedienung. Schon im Hinblick auf diesen Aufwand sei das Instrument meist nicht praktikabel. Auch wegen der rechtlichen Anforderungen (vgl. § 100i StPO), scheide die Maßnahme in vielen Fällen, in denen eine § 100g-Abfrage möglich wäre, aus. Ergänzend wird zudem auf den beschränkten technischen Einsatzbereich verwiesen. Notwendige Voraussetzung seien örtliche und personenbezogene Anknüpfungspunkte, beispielsweise eine bereits bekannte Zielperson.

Alle eben genannten Punkte lassen nach Ansicht der befragten Beamten auf die Observation übertragen und diese ebenfalls nicht als allgemein taugliches Substitut zum Ersatz von Verkehrsdaten erscheinen.

1.3.3. Bestandsdaten

Zielführende Substitute für die anderweitige Ermittlung der Bestandsdaten sehen die Ermittler nicht. Dies gelte insbesondere für die weitgehend weggefallene Auflösung der IP-Adresse nach den Bestandsdaten. Ein Beamter aus Baden-Württemberg führt hierzu aus, nur mit einer Art "Bestandsdatenerzwingungsverfahren" würde man gegenwärtig eine Chance haben, diese Informationen von den TK-Anbietern zu erhalten.

Theoretisch seien allenfalls Einzelfälle im Bereich der IuK-Kriminalität denkbar, in denen die Identifizierung auch mit herkömmlichen Ermittlungsmethoden ohne Zugriff auf die Bestandsdaten möglich erscheine. Berichtet wurde hierzu von einem konkreten Fall, in dem über die IP-Adresse ein konkreter Computer in einem Internet-Café identifiziert werden konnte. Mit Hilfe konservativer Ermittlungsmethoden (Beschlagnahme des Rechners, DNA-Auswertung am Rechner, Vernehmungen von Personal) in Kombination mit einer Funkzellenauswertung zum Versendezeitpunkt sei es schließlich gelungen, den Verdächtigen zu finden. Ein solcher Ermittlungsaufwand erscheint freilich nur bei sehr gravierenden Fällen vertretbar; in der Vielzahl der 'herkömmlichen' IuK-Verdachtsfälle ist dies selbstredend nicht realistisch.

Ein Gesprächspartner spitzt sein Unverständnis über die Weigerung der Unternehmen, Bestandsdatenanfragen auch bei akuten Gefahrenlagen wie Amokdrohungen nicht zu beauskunften, auf das Beispiel zu, dass er den Einsatz von SEK-Kräften an Schulen als Substitut für einen verweigerten Zugriff auf die Verkehrs- und Bestandsdaten eines konkreten Gefährders definitiv nicht für den milderen Eingriff halte.

1.4. Praktische Erfahrungen im Kontakt mit den TK-Anbietern

Die Erfahrungen, die die befragten Ermittler von ihren Kontakten mit den Telekommunikationsanbietern berichten, sind sehr unterschiedlich ausgeprägt und werden von einer Vielzahl verschiedener Faktoren beeinflusst. Während einige berichten, schon vor dem Urteil des Bundesverfassungsgerichts vom 2.3.2010 seien immer wieder Probleme aufgetreten und diese hätten nach dem Urteil eher noch zugenommen, können andere kaum von Problemen oder Veränderungen seit dem Wegfall der Vorratsdatenspeicherung berichten. Sofern Probleme

auftreten, wird übereinstimmen konzediert, dass die Ursache nicht unbedingt in einer fehlenden Kooperationsbereitschaft der Telekommunikationsanbieter zu suchen sei; vielmehr habe auch auf Unternehmensseite die Verunsicherung darüber, welche Daten sie in Folge des BVerfG-Urteils konkret herausgeben dürfen, zugenommen. Zudem spielten Datenschutzerwägungen und der schon erwähnte Löschungsdruck, der von Kundenseite ebenso befördert werden könne wie von dem kritischen öffentlichen Diskurs, eine Rolle.

1.4.1. Das Auskunftsverhalten der Telekommunikationsanbieter

Nach Ansicht der meisten Ermittler könne man daher vor einer grundsätzlichen Bereitschaft der Anbieter zur Zusammenarbeit mit den Gefahrenabwehr- und Strafverfolgungsbehörden ausgehen. Allerdings hätten manche Unternehmen nach dem Urteil zunächst überhaupt keine Anfragen mehr beauskunftet. Nach einiger Zeit – wohl nachdem die TK-Anbieter das Urteil analysiert und ihre Rechte und Pflichten herausgearbeitet hätten – habe sich die Lage wieder etwas entspannt und die meisten Anfragen würden inzwischen, sofern Daten vorhanden seien, wieder beauskunftet. Einige Interviewpartner äußern freilich auch Zweifel, ob Negativauskünfte tatsächlich immer der wahren Speichersituation entsprächen. Als problematisch wird insgesamt aber nicht so sehr die Zusammenarbeit als solche beschrieben, sondern die Tatsache, dass generell nur noch sehr wenige Daten gespeichert würden.

In der Mehrzahl der Fälle seien die Telekommunikationsanbieter durchaus bemüht, den gesetzlichen Vorgaben zu Folgen. Diese Vorgaben seien aus Ermittlersicht derzeit aber unzureichend und unbefriedigend, da sie den Unternehmen einen sehr großen Spielraum bei der Festlegung der Speicherpraxis eröffne. Daher sei es weitgehend dem Zufall überlassen; ob Gefahrenlagen abgewendet, Straftaten verhindert und Verbrechen aufgeklärt werden könnten. An die Stelle einer einheitlichen Speicherfrist von sechs Monaten sei nun eine Vielzahl von individuellen Speicherfristen getreten, die kaum noch überschaubar sei. Diese würden teilweise in kurzen Intervallen revidiert und die Änderungen zudem häufig unzureichend kommuniziert. Nur wenige Anbieter informierten die Behörden aktiv und in eindeutiger Weise.[318] Die meisten Ermittlungsbehörden führen Tabellen über die individuellen Speicherfristen der einzelnen Telekommunikationsanbietern, die laufend nachrecherchiert und entsprechend aktualisiert werden müssten. Bedingt durch das Auftreten einer Vielzahl kleinerer, oft regionaler Anbieter ergäbe sich in den verschiedenen Bundesländern jeweils eine eigene, von anderen Ländern abweichende Situation. Ein Beispiel ist nachfolgend als Tabelle F-2 reproduziert.[319] Anhand dieser Tabellen werde derzeit in jedem Einzelfall überlegt, ob eine Verkehrsdatenabfrage erfolgversprechend sein und beantragt werden könnte. Zu berücksichtigen sei dabei, dass auch Negativauskünfte („Die Daten sind nicht mehr in unserem System vorhanden; sie wurden bereits gelöscht.“) nur gegen Entgelt erteilt würden.

---

318 Ein konkretes Beispiel ist in Anhang C reproduziert.

319 Die dort aufscheinende Varianz in den Speicherzeiten deckt sich im Wesentlichen mit den Ergebnissen der Bundesnetzagentur, sieh oben Tabelle C-5.

Tabelle F-2: Arbeitsübersicht des LKA Niedersachsen über die Speicherfristen einiger wichtiger Anbieter

Speicherfristen von [retrograden] Verkehrsdaten (abrechnungsrelevante Daten nach § 96 TKG)					
Änderungen in rot dargestellt.					
Herausgeber: LKA NI Dez. 23 (ESB) und PD OL (KOST FZVD)					Stand: 29.07.2010
Abfrageparameter	**T-Mobile D 1**	**Vodafone Arcor D 2**	**E-Plus**	**Telefonica O 2**	**Telekom**
Rufnummer gehend	30 Tage	Geliefert werden alle VD (mit IMEI, IMSI, GEO-Daten) **1-7 Tage** (vollständig) **8-90 Tage** nur Notrufe **8-30 Tage** (alle abgehenden + ankommenden gebührenpflichtigen) **31-110 Tage** (Anonymisiert nach Kundenwunsch) **111-210 Tage** alle noch gespeicherten Verkehrsdaten ohne IMEI, Geo-Daten **Abgehende Verkehrsdaten** werden zu Funkzellen, IMEI-Nummern und ausländischen Rufnummern **nur noch 80 Tage rückwirkend** festzustellen.	ca. 80 Tage nach Monatswechsel + aktueller Monat (3 + 1)	**1-7 Tage** (alle ein- und ausgehenden Verkehrsdaten mit IMEI, IMSI, Funkzelle, IP-Adresse, Datenvolumen Anrufversuche und Notrufe) **8-30 Tage** (nur noch Abrechnungs-relevante Daten **ohne IP-Adresse, IMEI, Anrufversuche und Notrufe**. Eingehende Anrufe nur aus Fremdnetzen mit A- und B-Teilnehmer, Zeitpunkt und Dauer) **31-182 Tage** (Anonymisiert bzw. gelöscht nach Kundenwunsch B-Rufnummer letzte 3 Stellen durch x ersetzt. Dies gilt auch für Internationales Roaming)	in der Regel 80 Tage
Rufnummer kommend					nein
Funkzelle gehend					
Funkzelle kommend					
IMEI					
IMSI					
Serviceproviderkunden gehend (eigenes Netz)	bis max. 180 Tage *			182 Tage ohne Anonymisierung	
Serviceproviderkunden kommend (eigenes Netz)					
Roaming-Teilnehmer gehend (eigenes Netz)	30 Tage			**1-7 Tage** (alle ein- und ausgehenden Verkehrsdaten mit IMEI, IMSI, Funkzelle, IP-Adresse, Datenvolumen Anrufversuche und Notrufe) **8-30 Tage** (nur noch Abrechnungsrelevante Daten **ohne IP-Adresse, IMEI, Anrufversuche und Notrufe.** Eingehende Anrufe nur aus Fremdnetzen mit A- und B-Teilnehmer jedoch nur Zeitpunkt und Dauer) **31-182 Tage** (Anonymisiert bzw. gelöscht nach Kundenwunsch B-Rufnummer letzte 3 Stellen durch x ersetzt. Dies gilt auch für Internationales Roaming)	
Roaming-Teilnehmer kommend (eigenes Netz)					
Abweichungen bei Pre-Paid					
Abweichungen bei Post-Paid					
Abweichungen IMEI bei Pre-Paid	30 Tage **nur kommend**				
Abweichungen bei Flatrate	ca. 30 Tage *		keine Angabe		Im Fall einer Flatrate kann es sein das keine Verkehrsdaten vorhanden sind.
Speicherung Anrufversuche	30 Tage (gehend + kommend **nur bei Pre-Paid**)	nein	nein	7 Tage	nein
Auskunft Zuordnung IP-Adresse >> Kunde	nein	keine Angabe	nein	7 Tage	7 Tage
Anonymisierung von Daten auf Kundenwunsch	ja	ja (ab 31. Tag)	ja	ja	ja***
Bemerkungen	* VD (gehend / kommend) bleiben mind. 30 Tage erhalten. Nach Rechnungslauf sind nur noch abrechnungsrelevante VD (gehende) zw. min. 30 und max. 180 Tagen vorhanden. Die Speichdauer/-zeiten "oberhalb" der 30 Tage orientieren sich am Kundenauftrag-/wunsch.	Verkehrsdaten im **Festnetzbereich** (vormals ARCOR) : 1-90 Tage **alle ein- u. ausgehenden** Verkehrsdaten.			Die Telekom ist technisch nicht mehr in der Lage Zielwahlsuchläufe zu machen. **Ein Zielsuchlauf kann jedoch bei den vier Mobilfunk-netzbetreibern ersatzweise durchgeführt werden.**
Notizen	Hinweis: Weitere Aktualisierungen / Differenzierungen sind zu erwarten. Netzbetreiberangaben zu den "Leerfeldern" liegen derzeit nicht vor.				***Das Anrufziel kann u.U. um die letzten drei Stellen verkürzt sein.

Dass die Auskunfts- bzw. Kooperationsbereitschaft der Telekommunikationsanbieter mit deren Größe zusammenhinge, lasse sich nicht beobachten. Manche Gesprächspartner berichteten, dass die großen Anbieter besonders kooperativ seien; andere haben mit den kleinen Anbietern bessere Erfahrung gemacht. Die meisten Ermittler können keinen generellen Unterschied feststellen; vielmehr hänge die Kooperationsbereitschaft zumeist von dem einzelnen Mitarbeiter ab.

1.4.2. Probleme

Neben der unsicheren Speichersituation bemängeln die Ermittler vor allem, dass Anträge zum Teil erst sehr spät umgesetzt werden. Viele Provider seien überlastet und lieferten Daten aus diesem Grund später oder unvollständig. Während eine Funkzellenabfrage von manchen Providern bspw. in zwei Tagen beauskunftet werde, könne derselbe Vorgang bei anderen Unternehmen hingegen zwei Wochen beanspruchen.

Problematisch sei zudem, dass oft sehr große Datenmengen immer noch per Fax übermittelt würden, obwohl sie später automatisiert verarbeitet werden müssten. Das bedeute für die Ermittler, dass sie alle Daten einscannen oder manuell in die Systeme eingeben müssten. Würden die Daten standardisiert und auf sicherem elektronischem Weg übermittelt werden, könnte die Ermittlungsarbeit in vielen Fällen noch zügiger und damit noch effektiver voranschreiten.

Bemängelt wird des Weiteren, dass speziell seit dem Wegfall der Vorratsdatenspeicherung die Durchführung einer Zielwahlsuche bei einem großen Anbieter vielen derzeit nicht mehr möglich sei, weil die entsprechende Technik abgebaut wurde. Dadurch würden Ermittlungen in vielen Bereichen erheblich erschwert oder ganz unmöglich.

In Einzelfällen sei es ferner vorgekommen, dass Telekommunikationsunternehmen mitunter eine weitreichende Prüfung der übermittelten Beschlüsse bzw. Eilanordnungen für sich in Anspruch nähmen, beispielsweise hinsichtlich des Vorliegens einer Gefahrenlage. So etwas gehe über die von den Unternehmen selbst beschriebene grobe formale Prüfung hinaus, gegen die nichts einzuwenden wäre. Freilich seien dies eher seltene Vorkommnisse.

Wiederholt wurde den Gefahrenabwehrbehörden hingegen mitgeteilt, dass das im konkreten Fall einschlägige Landesgesetz nicht für den Telekommunikationsanbieter gelte, weil er seinen Sitz in einem anderen Bundesland habe und sich daher nicht zur Beauskunftung des Beschlusses in der Lage sähe.

1.5. Veränderungen in der Ermittlungspraxis

Der Gesprächsleitfaden sah weiterhin einige Schätzfragen hinsichtlich konkreter Veränderungen in der Ermittlungspraxis vor. Fast keiner der Interviewpartner sah sich zu dem Zeitpunkt der Gespräche allerdings in der Lage, Zu- bzw. Abnahmeentwicklungen einigermaßen verlässlich zu quantifizieren oder auch nur zu schätzen. Stattdessen wurde von persönlichen

Erfahrungen und Trends in der jeweiligen Dienststelle bzw. dem jeweiligen Arbeitsbereich berichtet.

Bezogen auf Verkehrsdatenabfragen wird die Häufigkeit von Negativauskünften generell als hoch eingeschätzt. Das gelte insbesondere für den Bereich der IuK-Kriminalität. Explizite Schätzungen über die aktuelle Häufigkeit von Negativauskünften schwanken zwischen etwa 50 Prozent bezogen auf Kinderpornographie (z.B. Rheinland-Pfalz) und ca. 60 % (z.B. Baden-Württemberg) bzw. mehr als 90 % (z.B. Sachsen-Anhalt, Schleswig-Holstein) bezogen auf IP-Abfragen im Allgemeinen. Ein Experte aus Nordrhein-Westfalen führte hierzu ergänzend aus, es sei im Bereich der Internet-Straftaten derzeit fast sinnlos, überhaupt noch Anzeigen aufzunehmen. Die Ermittler aus Baden-Württemberg haben die Entwicklung der Negativauskünfte über einen längeren Zeitraum beobachtet: nach ihren Angaben lag der Anteil 2007 bei 13,7 %, 2008 bei 25,3 %, 2009 bei 9,8 %[320] und 2010 bislang bei 59,3 %. Anfragen seien hier in Einzelfällen selbst dann nicht beauskunftet worden, wenn der Verdächtige zum Zeitpunkt der Kontaktaufnahme zum Provider noch online war.

Die Konsequenzen, die aus dieser Entwicklung in der Ermittlungsarbeit gezogen werden, sind augenscheinlich sehr unterschiedlich. Dies gilt sowohl im Hinblick auf die Verkehrsdatenabfrage als auch bei der Telekommunikationsüberwachung.

Was zunächst die Abfragen gem. § 100g StPO betrifft, so gibt es auf der einen Seite Länder bzw. Dienststellen, die einen Rückgang der Abfragen verzeichnen. Dort wird in mutmaßlich erfolglosen Fällen, in denen die Löschung der Daten wahrscheinlich erscheint, von vornherein darauf verzichtet, einen Beschluss zu erwirken. In den Wochen unmittelbar nach dem Urteil vom 2.3.2010 scheint dies im Übrigen eine verbreitete, auch aus Enttäuschung und Unsicherheit gespeiste Haltung gewesen zu sein. Inzwischen hat sich die Situation insoweit wieder normalisiert. Zahlreiche Interviewpartner berichten sogar von einer dezidiert entgegengesetzten Strategie. In ihren Dienststellen gehe die generelle Marschrichtung jetzt dahin, in allen Fällen, in denen Verkehrsdaten potenziell relevant sein könnten, als erste Maßnahme sofort eine Abfrage zu beantragen, um eventuellen Datenverluste weitestmöglich vorzubeugen. Handlungsleitend ist hier der Zeitdruck, der durch die teilweise sehr kurzen Speicherfristen eingetreten sei. Dieser Zeitdruck bestehe vor allem im IP-Bereich, aber auch bei Funkzellenabfragen. Hier könne man nur dann realistisch eine positive Auskunft erwarten, wenn der Beschluss nach spätestens 3 Tagen beim TK-Anbieter vorliege. Die Zeit für Tatortaufklärung und die Vorprüfung, ob die Abfrage eventuell auf bestimmte wenige Funkzellen beschränkbar wäre, stehe schlichtweg nicht mehr zur Verfügung. Notfalls müsse, auch in polizeirechtlichen Gefahrensituationen, ein Eilbeschluss erwirkt werden. Einige Gesprächspartner äußern sich freilich skeptisch, ob eine vermehrte Antragstellung nach § 100g StPO tatsächlich handlebar sei. Im Hinblick auf Massenverfahren, etwa im IuK-Bereich, sei eine

---

320 Der einmalige Rückgang wurde nachvollziehbar mit der Sondersituation bei den Straftaten gem. § 100g Abs. 1 Nr. 2 StPO während der Zeit der einstweiligen Anordnung erklärt.

solche "Streuschuss"-Strategie mit Blick auf den Aufwand jedenfalls auf Dauer nicht vorstellbar. Für realistisch halten aber auch diese Kollegen eine schnelle und generelle Abfragepraxis jedenfalls im Kapitaldeliktsbereich. Insbesondere bei Tötungsdelikten sei die § 100g-Abfrage nunmehr tatsächlich zumeist die routinemäßig eingeleitete Erstmaßnahme geworden.

Überlegungen zur späteren Verwertbarkeit abgefragter Daten spielen für die Ermittler in diesem Stadium meist nur eine untergeordnete Rolle. Mangels Einblick in den internen Speicherbedarf der Unternehmen sei es unmöglich zu beurteilen, ob die dort vorhandenen Daten zu Recht oder zu Unrecht gespeichert werden. Rechtliche Erwägungen betreffend die Subsidiarität und Verhältnismäßigkeit einer Maßnahme würden, soweit erforderlich, vorab mit der Staatsanwaltschaft als antragstellender Behörde abgestimmt. Die Prüfung der materiellen Voraussetzungen falle insgesamt in die Zuständigkeit von Staatsanwaltschaft und Gericht. Die Zusammenarbeit wird insoweit durchweg als im Allgemeinen problemlos beschrieben. Die Justiz habe die erschwerten Rahmenbedingungen bei der Verkehrsdatenabfrage zur Kenntnis genommen und trage den beschriebenen Veränderungen in der Abfragepraxis zumeist Rechnung.

Vergleichbar gegenläufige ermittlungspraktische Strategien und Entwicklungen wurden auch im Bereich der Inhaltsüberwachung gem. § 100a StPO erkennbar. Auf der einen Seite wird auf Rückgänge verwiesen, die darauf zurückzuführen seien, dass aufgrund fehlender Verkehrsdaten konkrete Zielpersonen bzw. Zielanschlüsse nicht mehr identifiziert werden können bzw. ein konkreter Tatverdacht nicht mehr generiert werden kann. Ebenso plausibel erscheinen auf der anderen Seite Szenarien, die einen Anstieg begründen lasen aus dem Wegfall der Filterfunktion von Verkehrsdaten im Vorbereitungsstadium der Maßnahme. Zahlreiche Interviewpersonen haben immer wieder auf diese ermittlungstechnische Funktion der Daten hingewiesen, die in der Vergangenheit regelmäßig zur Bestimmung und Eingrenzung der Überwachungsziele genutzt worden seien. Auch insoweit entfaltet die Telekommunikationsüberwachung heute wohl zumindest in Teilbereichen eine größere Streubreite als zuvor. Anstatt einer gezielt ausgewählten Person werden dann alle mutmaßlich zu einem näheren Verdächtigenkreis zählenden Personen überwacht. Hinzu kommt als weitere Möglichkeit eine Zunahme durch diejenige Fälle, in denen die TKÜ tatsächlich als Substitut eingesetzt wird (siehe dazu oben Pkt. 1.3.). Dämpfend dürfte sich freilich in allen Fällen der im Vergleich zur Verkehrsdatenabfrage engere Anwendungsbereich des § 100a StPO auswirken.

Aussagefähige Zahlen, auf deren Grundlage die hier wiedergegebenen Szenarien verifiziert werden könnten, liegen wie erwähnt nicht vor. Nur wenige Interviewpartner konnten insoweit konkrete Zahlen berichten. Danach war in Mecklenburg-Vorpommern von März bis Juni 2010 im Vergleich zu demselben Zeitraum 2009 ein Rückgang der § 100g-Maßnahmen um 54 % zu verzeichnen; zeitgleich sei bei denen gemäß § 100a StPO eine Zunahme um 20 % festgestellt worden. Ihre Kollegen aus Bremen gaben einen Rückgang der § 100g-Maßnahmen um etwa 40 % an. Im Gegensatz hierzu berichteten die Vertreter aus Sachsen von einem – allerdings nicht konkret quantifizierbaren – Anstieg bei den statistisch erfassten § 100g-Maßnahmen.

Abschließend wiesen einige der Praktiker auch auf mögliche Fernwirkungen bei anderen Maßnahmen hin. Das Fehlen von Verkehrsdaten könne erhebliche mittelbare Auswirkungen haben. Informationen, die aus Verkehrsdaten generiert werden, können neben den schon mehrfach erwähnten Hauptzwecken (Identifikation, Standortermittlung, Tatzeitbestimmung) vielfältigen Ermittlungszwecken dienen, bspw. als Standortdaten für die Durchführung von Observationen, zur Alibiüberprüfung, als Anhaltspunkt zur Überprüfung des Wahrheitsgehalts von Aussagen, als Vorhalt in Vernehmungen oder als Anhaltspunkt zur Ermittlung des modus operandi bei bestimmten Straftaten (z.B. das Erkennen des Einsatzes von Zweit-, Begleit-, Vorabfahrzeugen). Im präventiven Einsatzbereich sei es durch das Fehlen von IP-Daten bspw. unmöglich geworden, bei der Ermittlung von Botnetzen die infizierten Computer zu identifizieren und deren Besitzer vor den Trojanern zu warnen.

Das Fehlen von Verkehrsdateninformationen könne ferner zur Durchführung eingriffsintensiverer Maßnahmen zwingen, um das gleiche Ziel zu erreichen. So müssten manchmal zu einem früheren Zeitpunkt, als es ermittlungstaktisch eigentlich wünschenswert wäre, offene Maßnahmen ergriffen werden, was insbesondere im Bereich der Schwerstkriminalität den Ermittlungserfolg in Gänze gefährden könne. In dem aktuell bearbeiteten Fall eines Gesprächspartners könne eine geplante Durchsuchung nicht stattfinden, weil sie die noch unentdeckten Tatteilnehmer warnen würde. Der ermittlungstaktische Vorteil, der mit der Heimlichkeit der Verkehrsdatenabfrage verbunden sei, komme in der aktuellen Diskussion oft zu kurz. Die Heimlichkeit könne im Übrigen auch eine Schutzfunktion haben. So werde der Tatverdacht gegen eine Person, deren Alibi auf der Grundlage von Funkzellendaten später bestätigt wird, niemals nach außen erkennbar. Ohne Verkehrsdaten werde hingegen regelmäßig eine offene Alibiüberprüfung bei Dritten erforderlich sein, was ein sehr viel schwerwiegenderer Eingriff in die Privatsphäre sein könne; denn so erlangten gegebenenfalls Arbeitgeber und andere Personen erst Kenntnis von einem Verdacht, was mutmaßlich nicht im Interesse des Betroffenen sein werde.

1.6. Erwartungen an den Gesetzgeber

Die abschließende Frage nach den Erwartungen der Ermittler an den Gesetzgeber ergibt Einigkeit darüber, dass eine Neuregelung der Vorratsdatenspeicherung möglichst zügig erfolgen solle. Diese müsse sich inhaltlich an den Vorgaben des Bundesverfassungsgerichts orientieren.

1.6.1. Speicherungsumfang

Als problematisch wird die gegenwärtige Ausrichtung der Speicherung an der Abrechnungsrelevanz gesehen. Die Neuregelung müsse daher die zunehmende Bedeutung von Flatrates berücksichtigen, die dazu führe, dass die Telekommunikationsanbieter Verkehrsdaten nur noch in sehr eingeschränktem Umfang zu Abrechnungszwecken benötigen und nach § 96 TKG speichern. Die Entwicklung gehe weg von der Speicherung einzelner Verbindungen.

Ein besonderes Anliegen der Ermittler ist der gesamte Bereich der Internetkriminalität. Ohne den Zugriff auf retrograde Daten fehle in diesem Bereich jeglicher Ermittlungsansatz. Die Spuren, die die Täter im Internet hinterlassen, seien oft der einzige Ansatz zur Aufklärung solcher Straftaten. Aus diesem Grund wird nachdrücklich gefordert, dass bezogen auf den Bereich der Internetkommunikation technische Nachbesserungen gegenüber der alten Regelung vorgenommen werden. Eine Lücke sei hier insbesondere das bei der mobilen Internetnutzung an öffentlichen Anschlüssen praktizierte IP-Sharing. Hier sei eine Regelung zur Speicherung der Ports unentbehrlich. Ferner sei dringend erforderlich, dass die dynamische IP-Adresse in Verbindung mit der Anschlusskennung als Bestandsdatum qualifiziert und diese Daten von der Speicherungspflicht erfasst werden.

1.6.2. Zugriffsvoraussetzungen

Eindeutige Regelungen werden auch hinsichtlich der Zugriffsbefugnisse gewünscht. Es müsse klar geregelt werden, wer in welchen Fällen zur Abfrage der gespeicherten Daten berechtigt ist.

Im Hinblick auf die materiellen Zugriffsvoraussetzungen halten die Ermittler einen abgeschlossenen Deliktskatalog nicht für sinnvoll. Aufgrund der Schwere des Grundrechtseingriffs sei es grundsätzlich zwar wünschenswert einen Katalog, der jenem des § 100a StPO ähnlich sein könnte, aufzustellen und dadurch den Zugriff auf die gespeicherten Daten grundsätzlich auf Fälle der schweren Kriminalität zu beschränken. Andererseits dürfe die Schaffung eines Deliktskataloges nicht dazu führen, dass einzelne Phänomenbereiche vollständig wegfallen und Straftaten, die typischerweise mittels Telekommunikationsendgeräten begangen werden, nicht mehr verhindert oder verfolgt werden können. Diese Straftaten seien zwar häufig der leichten bis mittleren Kriminalität zuzuordnen, könnten ohne den Zugriff auf retrograde Verkehrsdaten aber nicht mehr aufgeklärt werden. In vielen Fällen ergebe sich überhaupt erst gerade aus der Analyse retrograden Verkehrsdaten die eigentliche Schwere einer Straftat. Oft lasse sich nur anhand der in der Vergangenheit stattgefundenen Kommunikation nachweisen, dass bspw. kein einfacher Diebstahl, sondern ein Bandendiebstahl vorliegt oder dass es sich bei einer Person nicht um einen Einzeltäter handelt, sondern sein Handeln der organisierten Kriminalität zuzuordnen ist. Ein abgeschlossener Katalog berge die Gefahr, dass die Schwere einer Straftat nicht nach außen erkennbar sei, die Straftat daher nicht von dem Katalog erfasst und daher nur die 'Spitze des Eisberges' abgebrochen werde, während das darunterliegende Tätergeflecht nicht ermittelt und gefasst werden könne. Insbesondere der Bereich der sozialschädlichen Massendelikte dürfe dabei nicht außer Acht gelassen werden. Ein Deliktskatalog als Ersatz für die gegenwärtige Generalklausel des § 100g Abs. 1 Nr. 2 StPO würde zudem im Widerspruch zu der Notwendigkeit stehen, diesen Bereich entwicklungsoffen zu definieren. Aus der raschen technologischen Entwicklung im Bereich der elektronischen Medien ergäben sich fast zwangsläufig fortlaufend neue Deliktsformen.

Zur Lösung dieses Problems wurden verschiedene Lösungsmöglichkeiten aufgezeigt. Denkbar wäre zunächst, für die Abfrage der gespeicherten Daten zwei Kriterien nebeneinander

aufzustellen: einerseits solle nach der Qualität einer Straftat gefragt werden, andererseits nach den Ermittlungsmöglichkeiten in dem jeweiligen Phänomenbereich unabhängig von der Schwere der einzelnen Tat. Auf dieses Weise könnte für den ersten Bereich ein Katalog geschaffen werden, der all diejenigen Straftaten erfasst, die so schwer wiegen, dass sie einen Rückgriff auf die gespeicherten Daten rechtfertigen. Gleichwohl wäre im Rahmen der zweiten Kategorie ein Zugriff auf die gespeicherten Daten auch dann möglich, wenn die Schwelle zur Katalogtat zwar nicht eröffnet ist, die Straftat ohne diesen Zugriff aber nicht verhindert oder verfolgt werden kann.

Ein anderer Vorschlag stellt auf die Schwere der verursachten Rechtsgutverletzung ab. Danach könnte der Zugriff auf die gespeicherten Daten in all denjenigen Fällen eröffnet werden, in denen die Schädigung des Opfers eine bestimmte Schwelle überschreitet. Dabei könnten einerseits Schädigungen körperlicher oder psychischer Art, andererseits aber auch Schäden materieller Art berücksichtigt werden. Dieser Ansatz würde es ermöglichen, den volkswirtschaftlichen Schaden eines Kriminalitätsbereiches zu berücksichtigen.

Weit überwiegend wird weiter gefordert, dass die Formulierung des § 100g Abs. 1 Nr. 2 StPO neben einem Katalog bestehend bleibt. Andernfalls würden die Ermittlungen im gesamten Bereich der Computerkriminalität, in dem die Schwelle des § 100a StPO regelmäßig nicht überschritten wird, weitgehend ins Leere laufen oder ganz unmöglich werden. Dasselbe würde für Beleidigungs- und Stalking-Fälle gelten, auch wenn sie im Einzelfall schwerwiegende Folgen hätten.

Von manchen Ermittlern wird die Einführung eines Kataloges generell abgelehnt und für wenig sinnvoll erachtet. *„Je spezieller man versucht, ein Gesetz auszugestalten, desto schwieriger wird dessen Umsetzung“,* warnt ein Gesprächspartner. Zudem gebe es nur sehr wenige Delikte, für die die Vorratsdatenspeicherung in Einzelfällen nicht von Bedeutung sein könnte. Einzelne Straftatbestände von der Verkehrsdatenabfrage auszuschließen könne im Einzelfall schwerwiegende Folgen haben. Zudem müsse eine neue Regelung der Vorratsdatenspeicherung möglichst technikneutral sein. In der Regel sei es dem Gesetzgeber nicht möglich, schnell genug auf technische Neuerungen zu reagieren und die Gesetze dem technischen Fortschritt umgehend anzupassen. Die technischen Rahmenbedingungen könnten innerhalb kürzester Zeit so weit voranschreiten, dass Normen schon kurze Zeit nach ihrem Erlass nicht mehr aktuell sind. Daher sei nur eine möglichst generelle, technikneutrale Formulierung zielführend.

Im Hinblick auf mögliche Straftatenkataloge wird als weitere Alternative eine Differenzierung nach bestimmten Abfragearten angeregt. So könne beispielsweise für die Zielwahlsuche ein eigener Katalog geschaffen werden. Angesichts des eng begrenzten Personenkreises, der von einer Zielwahlsuche betroffen ist, sei diese Maßnahme deutlich weniger eingriffsintensiv als andere Formen der Verkehrsdatenabfrage. Dann könnten in diesen speziellen Katalog auch niedrigschwelligere Delikte wie beispielsweise der Enkeltrick oder Stalking aufgenommen werden, ohne dass die Maßnahme unverhältnismäßig erscheine.

Viele der Praktiker bringen auch deutlich zum Ausdruck, dass der Grundrechtseingriff bei einer Verkehrsdatenabfrage deutlich unter jenem der Telekommunikationsüberwachung liege und ein Katalog auch unter diesem Gesichtspunkt generell weniger restriktiv sein müsste.

Speziell im Bereich der Internetkommunikation sollte zudem zumindest der Zugriff auf Bestandsdaten generell, d.h. auch bei allen unterschwelligen Delikten, möglich sein. Die Eine Orientierung an der Zugriffsschwelle des § 100a StPO sei nicht sachgerecht. Andernfalls werde die Aufklärung sämtlicher Vermögens- und Fälschungsdelikte, die über das Internet begangen werden, praktisch unmöglich.

Im Bereich der Gefahrenabwehr sollte ein Zugriff auf die gespeicherten Verkehrsdaten immer dann möglich sein, wenn eine Gefahr für Leib oder Leben einer Person oder für bedeutende Sachwerte besteht.

1.6.3. Speicherdauer

Die vor dem Urteil des Bundesverfassungsgericht gültige Speicherdauer von sechs Monaten wird überwiegend als sachgerecht und ausreichend, im Hinblick auf bestimmte Situationen zum Teil aber auch als zu kurz bezeichnet. Insbesondere zur Bekämpfung der organisierten Kriminalität und im Bereich des Staatsschutzes wird eine längere Speicherfrist als wünschenswert erachtet. Hier dienten die Daten vorwiegend der Aufdeckung von Täterstrukturen und Beziehungsgeflechten. Hierfür sei eine Zugriffsmöglichkeit auf länger zurückliegende Verkehrsdaten sehr wichtig. Auch insoweit werden vereinzelt Überlegungen dahingehend geäußert, ob nicht auch im Hinblick auf die Zugriffsdauer eine deliktsbezogene Differenzierung sinnvoll sein könnte. Zumindest für Einzelfälle wäre der Rückgriff auf noch ältere Daten wünschenswert. Eine mögliche Differenzierung könnte regelungstechnisch auf der Speicher- wie auf der Zugriffsseite gelöst werden. Einig waren sich schließlich alle Befragten, dass die bisherige Sechsmonatsfrist die absolute Untergrenze sei. Kürzere Speicher- oder Zugriffsfristen seien am ehesten im präventiven Aufgabenbereich vertretbar.

1.6.4. Quick Freeze

Sofern das Quick-Freeze-Verfahren den Ermittlern überhaupt bekannt war, bestand Einigkeit darüber, dass diese Methode kein Substitut für die Vorratsdatenspeicherung darstellen könne. Verlorene retrograde Daten könnten auf diese Weise jedenfalls nicht ersetzt werden. Ob die benötigten Daten noch vorhanden sind und überhaupt eingefroren werden können, hänge – sofern es keine allgemeinverbindlichen Speicherungspflichten gäbe – von der individuellen Speicherpraxis des jeweiligen Telekommunikationsunternehmen ab. Das Quick-Freeze-Verfahren als solches könne die unbefriedigende Lage, wie sie derzeit bestehe, nicht entscheidend verändern. Wichtig sei vor allem Rechtssicherheit, die vor allem durch die Unabhängigkeit von der Organisationshoheit der an privatrechtlichen Interessen orientierten Anbieter erreicht werden könne. Solange der staatliche Zugriff auf Daten von der willkürlichen Speicherpraxis der Telekommunikationsunternehmer bzw. deren Vereinbarungen mit dem

Kunden abhänge, könne eine Gleichbehandlung in der Gefahrenabwehr und der Strafverfolgung nicht erreicht werden.

Ob das Quick-Freeze-Verfahren neben der Vorratsdatenspeicherung implementiert werden sollte, wird eher skeptisch bewertet. Teilweise wird die gesetzliche Normierung des Quick-Freeze-Verfahren neben der Vorratsdatenspeicherung für entbehrlich erachtet, da ein echter Mehrwert nicht erkennbar sei. Alle erforderlichen Daten würden dann hinreichend lange gespeichert werden, sodass es keinen Bedarf gebe, Daten zusätzlich einzufrieren. Einen sinnvollen Einsatzbereich sehen Befürworter des Quick-Freeze-Verfahrens in Fällen, in denen andernfalls wegen Ablauf der Speicherfrist die Löschung droht.

1.6.5. Sonstiges

Die befragten Ermittler haben wiederholt darauf hingewiesen, dass eine 24/7-Bereitschaft bei den Telekommunikationsanbietern, wie sie für Anfragen nach § 100a StPO wohl bereits besteht, auch für die Abfrage von Verkehrsdaten unbedingt erforderlich sei. Es wurde daher wiederholt der Wunsch geäußert, dass eine durchgängige Erreichbarkeit der Telekommunikationsanbieter gesetzlich vorgeschrieben wird. Dies sei v.a. bei plötzlichen Gefahrenlagen (Eingang einer Suizidankündigung oder der Androhung eines Amoklaufs am Wochenende) unentbehrlich. Zudem sollte eine verbindliche Frist normiert werden, binnen welcher die Anfragen der berechtigten Stellen beauskunftet werden müssen.

Zwecks Vereinheitlichung der Beauskunftungspraxis wird zudem vorgeschlagen, dass mittels einer technischen Richtlinie den Gefahrenabwehr- und Strafverfolgungsbehörden einerseits, sowie den Providern andererseits genaue technische Vorhaben zur Erhebung, Speicherung und Übermittlung der Daten gemacht werden. Dies bezieht sich insbesondere auf eine Vereinheitlichung der Antragsformulare sowie ein einheitlichen Datenformat und die Übertragung auf einem gesicherten elektronischen Weg.

Angemahnt wird ferner ein technischer Standard für die Erhebung und Übertragung von Geodaten.

2. Situationsbeschreibung aus der Sicht der Staatsanwälte

In den Gesprächen mit den Staatsanwälten wurden alle wesentlichen Einschätzungen der Polizeibeamten über die ermittlungstechnischen Auswirkungen bestätigt. Größeren Raum nahmen in den Lageanalysen der Staatsanwälte erwartungsgemäß rechtliche Aspekte wie z.B. die Beweisfunktion der Verkehrsdaten im Kontext der Anklage oder Erwägungen zur gerichtlichen Verwertbarkeit ein. Diese zusätzlichen Aspekte stellen einen Schwerpunkt der nachfolgenden Ausführungen dar.

2.1. Allgemeine Folgeneinschätzung

Wie bereits erwähnt, werden die Folgen etwas zurückhaltender bewertet als aus der 'Front-Perspektive' der Polizeibeamten (siehe dazu oben Pkt. 1.1. einschließlich Tabelle F-1). Im Verhältnis zu jenen ist der Anteil derer, die den Zeitpunkt für zu früh halten, um ein endgültiges Urteil abzugeben, etwas höher. Inhaltlich decken sich die Problem- und Folgenbeschreibung beider Gruppen gleichwohl in allen wesentlichen Punkten. Die Ermittlungsarbeit der involvierten Staatsanwälte sei, parallel zu derjenigen der Polizeibeamten, in vielen Bereichen erheblich erschwert, aber nicht ganz unmöglich geworden.

Spürbare Konsequenzen ergäben sich sowohl im Hinblick auf den Speicherumfang als auch auf die Speicherfristen. Diese seien inzwischen so kurz, dass sie häufig schon verstrichen seien, wenn ein Vorgang zur Staatsanwaltschaft kommt. Manche Daten seien überhaupt nicht mehr zu erhalten, andere nur während eines kurzen Zeitraumes. Beides beeinflusse die Ermittlungsarbeit wesentlich, da in der Folge zusätzliche Überlegungsschritte und Maßnahmen erforderlich werden könnten, die nach der schulmäßigen Ermittlungsroutine eigentlich nicht, anders oder zu einem anderen Zeitpunkt angezeigt wären. Die Ermittlungstaktik und der Ablauf der Ermittlungen werden somit durch externe Umstände – die abrechnungsorientierte Speicherpolitik der TK-Unternehmen – wesentlich mitbestimmt.

Bezogen auf konkrete Informationen werden vor allem der Verlust der eingehenden Nummern, der teilweise Verlust auch der Zielwahlsuche sowie die Ausfälle bei den IP-Adressen und den Funkzelleninformationen, insbes. den Geodaten beklagt. Als problematisch wird darüber hinaus die Echtzeitabfrage erkannt. Anders als gesetzlich in § 100g Abs. 3 StPO vorgesehen, seien Echtzeitdaten im Bereich der Telefonie derzeit nur über Maßnahmen gem. § 100a StPO zu erlangen, im Bereich des Internets überhaupt nicht.

Besonders betroffen sind nach übereinstimmender Einschätzung der Gesprächspartner die Ermittlungen in allen Delikten, die per Computer begangen werden, sowie in alle Delikten, die von mehreren Tätern begangen werden und daher Kommunikation erfordern.

Dies wirke sich dann an erster Stelle bei den Ermittlungen im Bereich der Internet-Kriminalität aus, deren Aufklärung von der Verbindung von IP-Adresse und Anschlussinhaber abhängig sei. Als konkrete Beispiele werden genannt Kinderpornographie, Phishing und Betrug im Internet. Ein Dezernent berichtet von einem völligen Stillstand der Ermittlungen im IP-Bereich.

Deutlich spürbar sind die Einschnitte nach übereinstimmender Ansicht zahlreicher Gesprächspartner auch bei der Verfolgung von Kapitaldelikten. Diese seien häufig zunächst Unbekannt-Sachen. Hier sei die Erhebung von Standortdaten von ebenso großer kriminalistischer Bedeutung wie klassische Kommunikationsdaten. Der Wegfall der eingehenden Daten betreffe konkret insbesondere die Verfolgung von Drohanrufen, Erpresseranrufen und Enkeltrickbetrügern.

Vergleichbar erscheint die Situation ferner bei den Organisationsdelikten, mit denen die Bundesanwaltschaft vorrangig konfrontiert ist. So werde bspw. die Gründung einer terroristischen Vereinigung meist nur durch – konspirative – Kommunikation verwirklicht.

Insgesamt wird die Situation derzeit als diffus und unbefriedigend bezeichnet. Unterschiedliche Speicherfristen, Zeitdruck und unsichere Erfolgsaussichten haben in der Kumulation einen negativen Einfluss auf die Ermittlungsarbeit. Diese Unübersichtlichkeit, in welcher Ermittlungserfolge von Zufälligkeiten abhängig geworden seien, hätte ein Ausmaß an Rechtsunsicherheit mit sich gebracht, die einer der befragten Staatsanwälte auch als Gerechtigkeitslücke bezeichnet hat.

2.2. Bedeutung der Verkehrsdaten und ihre Erreichbarkeit nach der derzeitigen Rechtslage

Nach übereinstimmender Einschätzung der meisten Gesprächspartner haben die Einschnitte Rückwirkungen auf alle ermittlungstaktischen Zielsetzungen einer Verkehrsdatenabfrage. Genannt werden insbesondere die Identifizierung von Personen und Strukturen – bspw. Ermittlung und Identifizierung von weiteren, bislang unbekannten Mittätern oder sonstigen Beteiligten, insbesondere auch Hintermännern –, die Rekonstruktion von Bewegungsabläufen, die Zuordnung einzelner scheinbar isolierter Tatkomplexe, die Vorbereitung und Auswahl anderer Ermittlungsmaßnahmen (insbesondere auch solcher nach § 100a StPO), die Rekonstruktion von Bewegungsabläufen, die Überprüfung des Wahrheitsgehaltes von Alibis und anderen Aussagen, sowie der Vorhalt in Vernehmungen, etc.

Als Konsequenz aus den Veränderungen sehen sich die Staatsanwälte nun vor die Aufgabe gestellt, eingehender zu prüfen, wann die Maßnahme zulässig und erfolgversprechend ist und wann nicht. Gleichzeitig sei aufgrund der kurzen Speichefristen größere Eile geboten. Der daraus folgende sehr große Zeitdruck erzwinge schnelles Handeln und führe zu Ungenauigkeiten und der Notwendigkeit, bei der Prüfung der Anregungen und der Begründung der Anträge großzügiger zu sein. Zahlreiche Staatanwälte weisen darauf hin, dass eine erschöpfend tiefe Begründung und rechtliche Absicherung der Maßnahmen unter solchen Rahmenbedingungen nur bedingt möglich sei; auch die Gerichte könnten in Eilfällen maximal eine summarische Prüfung vornehmen. Trotz des Zeitdruckes sei man natürlich weiterhin darauf bedacht, die Qualität der Begründungen zu halten. Dennoch sehe eine unter Zeitdruck verfasste Eilanordnung eben anders aus als ein in Ruhe verfasster Beschluss. Noch nicht konkret belegbar, aber denkbar erscheint ferner, dass die Eilbedürftigkeit bzw. der zugrunde liegende drohende Datenverlust als Faktum selbst Eingang in den Begründungskontext findet, um die Erforderlichkeit i.S.v. § 100g Abs. 1 S. 1 oder 2 StPO zu begründen.

Spürbar wird dieser Zeitdruck offenbar auch bei der Bundesanwaltschaft. Der befragte Bundesanwalt beschreibt, dass die Anforderungen, die die Ermittlungsrichter beim BGH im Hinblick auf die rechtlichen Erörterungen erwarteten, stetig höher geschraubt würden. Während noch vor wenigen Jahren bei Anträgen gem. §§ 100a oder 100g StPO eine

Sachverhaltsschilderung und die Bezugnahme auf die einschlägigen Rechtsvorschriften ausreichend gewesen seien, würden inzwischen umfangreiche Sachverhaltsdarstellungen mit Beweiswürdigung nebst umfangreichen Aktenvorlagen verlangt, um alleine den Tatverdacht zu rechtfertigen. Die Erfüllung dieser Anforderungen innerhalb der kurzen Speicherfristen bereite erhebliche Schwierigkeiten.

2.2.1. Rechtmäßigkeit der Datenspeicherung

Die Rechtmäßigkeit der Speicherung bei den Anbietern wird in keiner der Dienststellen, die die Befragten repräsentieren, explizit überprüft. Zur Begründung wird übereinstimmend ausgeführt, dies sei mangels Einblick in die Kundenverhältnisse und die Abrechnungsrelevanz konkreter Daten auch gar nicht möglich. Man gehe daher allgemein von einer rechtmäßigen Speicherpraxis der Unternehmen aus. Mitunter wird darauf hingewiesen, dass man Daten dann nicht in ein Strafverfahren einführen würde, wenn im Einzelfall eine rechtswidrige Speicherung bekannt würde. Einen solchen Fall habe es bislang aber nicht gegeben. Etwas zurückhaltender äußert sich lediglich der befragte Bundesanwalt. In seiner Behörde werde in jedem Einzelfall kritisch geprüft, ob Daten rechtmäßig erlangt wurden.

Allgemein herrscht auf der staatsanwaltlichen Ebene auch die Rechtsauffassung vor, dass vor dem 2.3.2010 abgefragte und erhaltene Daten verwertbar seien. Zur Begründung verweisen die Gesprächspartner auf die ursprüngliche Rechtmäßigkeit der Speicherung und Erhebung unter den Bedingungen, wie sie das BVerfG in seiner einstweiligen Anordnung festgesetzt habe.[321] Zahlreiche Generalstaatsanwaltschaften haben inzwischen auch entsprechende Rundverfügungen herausgegeben. Gegenteilige Gerichtsentscheidungen waren keinem der Befragten bekannt.

Auch ein mögliches Fernwirkungsverbot im Hinblick auf weiterführende Erkenntnisse, die aus weiteren Ermittlungsmaßnahmen generiert wurden, die durch ehemalige Vorratsdaten ausgelöst wurden, kann keiner der teilnehmenden Staatsanwälte erkennen.

2.3. Mögliche Substitute für die Verkehrsdatenabfrage

Auch bei der Erörterung möglicher Substitute stimmen die befragten Staatsanwälte im Wesentlichen mit den Polizeibeamten überein. Alternative Ermittlungsstrategien sind für sie nur dort vorstellbar, wo die Verkehrsdaten unterstützende Funktion haben. Als Beispiele schildern einige Beamte Situationen bei der Vorbereitung des Einsatzes technischer Mittel und der Wohnraumüberwachung. So sei die Vorbereitung einer Maßnahme nach § 100c StPO schwieriger geworden, da häufig nicht mehr wie früher auf der Grundlage von Geodaten der Aufenthaltsort der verdächtigen Person zeitnah ermittelt werden könne um sicherzustellen, dass diese nicht zuhause ist. Auch bei der Präparierung von Fahrzeugen hätten die Daten Aufschluss darüber gegeben, wie sich der Verdächtige bewegt und wann er wahrscheinlich

---

321 So inzwischen auch der BGH, siehe oben Fn. 82

mit dem Fahrzeug unterwegs ist. Diese Vorbereitungen müssten nunmehr durch Observation durchgeführt werden und seien dadurch viel aufwendiger geworden.

In allen Fällen, in denen die Verkehrsdaten originären Beweiswert hätten und in dieser Funktion bspw. im Kontext einer Anklagebegründung relevant sind, seien sie nicht ersetzbar. Hier blieben stets Lücken in der Tatsachenfeststellung. Es hängte dann vom Einzelfall ab, ob diese überbrückbar sind oder nicht.

Für retrograder Daten konnte auch hier keiner der Befragten ein praxistaugliches Substitut erkennen. Ein Staatsanwalt belegt dies anschaulich mit dem Hinweis auf das einzig denkbare, 'natürliche' Substitut für fehlende Telefonverkehrsdaten: die im Wege einer Durchsuchung sichergestellte Telefonrechnung. Außer in dem glücklichen Ausnahmefall eines Zufallsfundes sei dies freilich keine realistische Option.

Spiegelbildlich zu den Berichten der Ermittler ergibt sich auch in den Gesprächen mit den Staatsanwälten ein differenziertes Bild, was die mögliche Ersatzfunktion speziell der TKÜ gem. § 100a StPO anbetrifft. Einigkeit besteht in der Einschätzung, dass diese als Substitut zur Ermittlung retrograde Verkehrsdaten ausscheide. Uneinigkeit besteht hingegen in der Beurteilung der Tauglichkeit im Hinblick auf zukunftsgerichtete Daten. Während einige Gesprächspartner die TKÜ – zum Teil unter expliziter Einbeziehung der Auslandskopfüberwachung – als grundsätzlich geeignetes Substitut bewerten, sind andere zwar nicht generell ablehnend, aber doch skeptischer. Die Letzteren verweisen auf das ganz spezifische Ermittlungsziel der TKÜ, nämlich die Inhaltsüberwachung von Kommunikation. Bei der Verkehrsdatenauswertung gehe es hingegen um die Aufklärung von Personenzusammenhängen und die Erstellung von Bewegungsbildern. Überwachung mit TKÜ sei dann als Ausweichmaßnahme denkbar, wenn andere Wege der Informationsgewinnung aussichtslos erscheinen. Solche Substitute könnten theoretisch sein: die 7-Tagesdaten gem. § 100 TKG – diese seien freilich nicht vollständig und würden zu kurz gespeichert – oder die Bestandsdaten gem. § 113 TKG – diese beträfen aber nur das Vertragsverhältnis und seien für Ermittlungszwecke nicht ausreichend. Daher bliebe in der Praxis tatsächlich häufiger als zuvor nur der Weg über Maßnahmen gem. § 100a StPO.

Ein Staatsanwalt verweist kritisch darauf, dass die fehlende Filterfunktion der Verkehrsdatenauswertung auch zu der schon von einigen Polizeibeamten erwähnten Streuwirkung bei den Abhörmaßnahmen führen könne. Er beschreibt den fiktiven Fall eines Beschuldigten, dem 20 Anschlüsse zuzuordnen seien. Eigentlich müsste bei allen 20 Anschlüssen eine TKÜ geschaltet werden, um dann festzustellen, welchen oder welche er aktuell nutze. Die anderen wären in der Zwischenzeit aufwendig überwacht worden, obwohl sie nicht mehr benutzt werden. Oder es wären Unbeteiligte überwacht worden, weil man manchmal erst nach einigen Tagen merke, dass man die falsche Person überwacht. Oftmals fehlten freilich tragfähige Erkenntnisse, um überhaupt eine TKÜ beantragen zu können. Ein Dezernent aus Bayern berichtet, dass dort zur Vorbereitung von § 100a-Maßnahmen jetzt im Einzelfall ein IMSI-Catcher eingesetzt werde, um die Anschlussnummer (bekannter) Verdächtiger herauszubekommen.

Ein Dezernent aus Mecklenburg-Vorpommern fasst die Konsequenzen auf der Basis seiner Erfahrungen kurz so zusammen: Vorbereitung und Beantragung von Maßnahmen gem. § 100g StPO und als Folge des engen ermittlungstechnischen Zusammenhangs der beiden Maßnahmen auch gem. § 100a StPO seien schwieriger geworden, die Durchführung sei gleich schwierig geblieben, und der Ertrag sei geringer geworden.

Vor dem Hintergrund der Schwierigkeiten in dem Zugang zu den Verkehrsdaten ist in einigen Behörden die Tendenz feststellbar, eine Abfrage gar nicht erst zu veranlassen – jedenfalls dann nicht, wenn zu erwarten ist, dass keine Daten mehr vorhanden sind oder jedenfalls nicht herausgegeben würden. Dies betreffe vor allem den Bereich der kleineren und mittleren Kriminalität. Wo keine Substitute greifbar sind, bleibe aus staatsanwaltlicher Sicht dann das Schließen der Akte regelmäßig die einzige Option.

Große Skepsis herrscht auch bei diesen Gesprächspartnern im Hinblick auf den Zusatzwert eines Quick-Freeze-Verfahrens. Die schon von Ermittlerseite vorgebrachten Argumente wiederholten sich hier sinngemäß.

2.4. Auskunftsverhalten der Telekommunikationsanbieter

Einig sind sich die Staatsanwälte mit den Ermittlern auch in der allgemeinen Einschätzung, dass die Auskunftsbereitschaft der Telekommunikationsanbieter seit dem Urteil geringer geworden sei. Die Unternehmen seien schon immer sperrig gewesen und nunmehr in der Verweigerung der Zusammenarbeit noch selbstbewusster geworden. Dabei wird die Frage nach möglichen Unterschieden zwischen kleinen und großen Anbietern wiederum unterschiedlich beantwortet. Einige beurteilen die letzteren tendenziell als kooperativer, andere die ersteren. Einig ist man sich in der Bewertung, dass im Hinblick auf die gegenwärtige, eher kritische öffentliche Diskussion letztlich kein Unternehmen in den Verdacht geraten möchte, zu eng mit den Strafverfolgungsbehörden zu kooperieren. Befürchtet werde ein Kundenverlust, weshalb einige, meist kleinere Anbieter diesen Aspekt mitunter sogar als Werbeargument nutzten. Auch setze die allgemeine Löschungsverpflichtung für nicht explizit abrechnungsrelevante Daten die Unternehmen unter Druck.

Generell wird auch konzediert, dass von einer kompletten Kooperationsverweigerung nicht die Rede sein könne. Mehrere Staatsanwälte beklagen aber eine deutlich verzögerte Bearbeitung der Anfragen. Eine Standardauskunft könne gut und gerne 14 Tage dauern. Kritisiert wird ferner, dass viele Anbieter für § 100g-Beschlüse keinen Bereitschaftsdienst hätten. Dies wirke sich umso spürbarer aus, als die Unternehmen vor Einführung der Vorratsdatenspeicherung speziell auch in Eilsituationen kooperativer gewesen seien und Daten eingefroren hätten, bis ein entsprechender Beschluss vorlag. Hierzu seien sie jetzt im Allgemeinen nicht mehr bereit

Die Staatsanwälte bestätigen dann auch die von Ermittlerseite vorgetragenen Probleme hinsichtlich der Bestandsdatenauskünfte. Die frühere Problematik, dass Unternehmen hierfür einen § 100g-Beschluss verlangt hätten, habe sich infolge der in diesem Punkt inzwischen

eindeutigen Rechtsprechung entspannt. Eine ganz andere Frage sei freilich, ob die Unternehmen nach dem 2.3.2010 berechtigt sind, die IP-Adresse nach den Bestandsdaten aufzulösen. Viele weigerten sich bislang, dies zu tun.

Einige Gesprächspartner bestätigen auch, dass die Überprüfung von Beschlüssen durch Unternehmen nach wie vor zu beobachten sei; einige Staatsanwälte sprechen diesbezüglich dezidiert von einer Anmaßung eigener Prüfungskompetenz. Dies sei vor allem bei den großen Anbietern zu beobachten. Einige Staatsanwälte berichten von einzelnen Fällen, in denen Unternehmen zur Herausgabe hätten gezwungen werden müssen. Die Auskunft, dass keine Daten vorhanden seien, sei heute eine alltägliche Erfahrung. Einige der Befragten beobachten nach eigenen Angaben zwei Ausnahmen: wenn mit Durchsuchung gedroht werde und wenn die Unternehmen selbst Geschädigte seien oder ihre eigenen Interessen berührt sähen. In mehreren der Gespräche berichteten einzelne Dezernenten unabhängig voneinander, dass sie anlässlich konkreter Ermittlungen festgestellt hätten, dass von Telefonzellen – gleichsam dem "Prototyp der Prepaid-Konstellation" (so ein Dezernent aus Baden-Württemberg) – stets sehr weit zurückreichende retrograde Daten vorrätig gewesen seien. Mehrfach wird schließlich die Vermutung geäußert, dass Daten zumindest in einzelnen Situationen nicht herausgegeben würden, obwohl sie existierten.

Interessanterweise berichten einige Kollegen aus Nordrhein-Westfalen von abweichenden Erfahrungen mit den auf Kundenwunsch hin anonymisierten (XXX-) Daten. Die Anonymisierung betreffe lediglich das Anbieter-Kunden-Verhältnis. Die Ermittlungsbehörden in NRW bekämen die Daten in der Regel in der Originalform geliefert.

2.5. Veränderungen in der Ermittlungspraxis

Sehr uneinheitlich fallen auch bei den Staatsanwälten die Schätzungen aus, was die konkreten Veränderungen bei dem Aufkommen der Maßnahmen betrifft. Die Angaben aus den Bundesländern differieren untereinander und entlang verschiedener Deliktsbereiche. Insgesamt ergibt sich daraus ein sehr uneinheitliches Bild, das noch keine große Aussagekraft beanspruchen kann.

Nur die Gesprächspartner aus Rheinland-Pfalz konnten Angaben zu der Häufigkeit von nicht kompensierbaren Negativauskünften machen. Sie schätzen den Anteil bei der IuK-Kriminalität auf 80 %, bei speziellen Delikten wie Phishing auf bis zu 100 %. Ermittlungen in Fällen herkömmlicher Kriminalität seien im Hinblick auf andere Ermittlungsmaßnahmen nicht so hart betroffen. Hier liege der Anteil nicht kompensierbarer Ausfälle z.B. im Drogenbereich bei ca. 25 %.

Was die Entwicklung bei den Maßnahmen gem. §§ 100a und 100g StPO betreffe, so sei ebendort bislang keine Veränderung bei den § 100a-Maßnahmen zu beobachten gewesen. Dasselbe wird für Berlin berichtet. Dort liegen ebenso wie in Rheinland-Pfalz noch keine Schätzungen für § 100g-Maßnhamen vor. Gefühlt seien diese dort aber jedenfalls weniger geworden. Ein Vertreter aus Niedersachsen meldete einen Rückgang der § 100g-Beschlüsse

um ca. 30 %. Daten über einen möglichen Anstieg bei § 100a-Beschlüssen lägen dort nicht vor, eine Zunahme würde aber nicht überraschen. Aus Hamburg wurden Einbrüche bei beiden Maßnahmen berichtet, und zwar bei den §100g-Beschlüssen um geschätzte 25 %, bei den § 100a-Beschlüssen um geschätzte 10 %. Mecklenburg-Vorpommern verzeichnet im IuK-Bereich einen Rückgang der Abfragen je nach Deliktsart zwischen 10 und 100 %, bei der allgemeinen Kriminalität um 70 %. Auch der Vertreter der Bundesanwaltschaft konstatiert einen deutlichen Rückgang der § 100g-Anträge, nicht jedoch bei § 100a StPO.

Selbst innerhalb eines Landes kann es zu unterschiedlichen Wahrnehmungen kommen. Während einige Gesprächspartner aus Baden-Württemberg von einem Rückgang bei den Anträgen gem. § 100g StPO in der Größenordnung zwischen 50 % und 70-80 % berichten, sieht ein anderer keine größeren Veränderungen. Gesunken sei aber auf jeden Fall der Ertrag der Abfragen. Einigkeit besteht hingegen in der Beurteilung der § 100a-Maßnahmen. Hier seien bislang keine nennenswerten Veränderungen zu beobachten.

2.6. Erwartungen an den Gesetzgeber

Vergleichsweise kurz fielen, wiederum im Vergleich zu dem Meinungsbild bei den Polizeibeamten, auch die Erwartungen an eine mögliche Neuregelung aus.

Übereinstimmend und nachdrücklich wird für die Beibehaltung einer Generalklausel für den Bereich der IuK-Kriminalität votiert. Die Zugriffsmöglichkeit könnte für im Einzelfall tatsächlich niedrigschwellige Fälle mit einem rechtlichen Korrektiv begrenzt werden, etwa in Form einer Schwereklausel; diese könne man konkret etwa an der Schadenshöhe oder an sonstigen (gravierenden) Auswirkungen in dem Einzelfall (opferbezogen, gesellschaftsbezogen oder bezogen auf die öffentliche Sicherheit bzw. die Rechtsordnung) orientieren. Sehr häufig wurde dabei ganz generell, wie schon in den Interviews mit den Ermittlern, auf die Bedeutung der Opferperspektive hingewiesen. Als alternatives oder weiteres Qualifizierungsmerkmal im Bereich der einfacheren Kriminalität könnte die Begrenzung auf wiederholte Tatbegehung definiert werden. So wäre dann etwa der Enkeltrick mit erfasst.

Einige Dezernenten stellen die Klassifizierung von Straftaten anhand des Straftatbestandes – und damit das Katalogprinzip – prinzipiell in Frage. Dies sei kein hinreichendes Kriterium. Denn der abstrakte Straftatbestand indiziere nicht automatisch die tatsächliche Schwere einer Straftat. Als Beispiel wird die Nichtkatalogtat der Nachstellung genannt. Nach dem Alltagsverständnis eher minderschwere Sachverhalte könnten anhand der formalen Kriterien als vermeintlich schwer zu klassifizieren sein – ein Beispiel kann hier das Abziehen auf dem Schulhof sein, das als Raub Katalogdelikt gem. §§ 100a und g StPO ist – und umgekehrt; ob beispielsweise eine Straftat nach § 243 StGB eine Einzeltat oder Teil einer Einbruchsserie sei und personale oder geographische Bezüge zu anderen Taten aufweise, könne häufig erst auf der Grundlage einer Verkehrsdatenerhebung ermittelt werden.

Die Zugriffsvoraussetzungen könnten auch für verschiedene Deliktsbereiche und verschiedene Daten- bzw. Abfragearten gestaffelt definiert werden. Auch ein Katalog mit Eröffnungsklausel wird vorgeschlagen.

Einigkeit herrscht in den verschiedenen Gesprächen ganz unabhängig voneinander, dass eine Orientierung an dem § 100a-Katalog wegen der geringeren Eingriffsqualität nicht sachgerecht wäre.

Auch im Hinblick auf die schon von den Polizeibeamten identifizierte Regelungslücke wird eine gesetzliche Nachbesserung angemahnt.

Die überwiegende Mehrheit der Befragten einschließlich des Vertreters der Bundesanwaltschaft hält die Sechsmonatsfrist ebenfalls für ausreichend. Nur ein Dezernent sprach sich für eine allgemeine Anhebung auf 12 Monate aus. Übereinstimmend meinen alle, dass drei Monate zu knapp bemessen wären.

Abschließend brachten einige Interviewpartner das Modell einer zentralen Speicherung bei einer staatlichen Agentur zur Sprache. Die Telekommunkationsunternehmen hätten die Klage gegen die Vorratsdatenspeicherung teilweise unterstützt und seien nicht neutral. Mit der Übernahme der durch eine solche Agentur entfiele insbesondere die Problematik, die Speichersituation bei den Unternehmen ständig neu erforschen zu müssen. Ein Staatsanwalt aus Bayern verweist auf weitere Vorteile, die darin bestünden, dass es dauerhafte Ansprechpartner und einen zügigeren, in sicheren rechtlichen Bahnen verlaufenden Arbeitsablauf mit einheitlichen Standards gäbe. Die Kollegen aus Niedersachsen machen in diesem Kontext auch auf ein Geheimhaltungsproblem aufmerksam. Die Geheimhaltung sei momentan nicht gewährleistet, da die Privaten, die die Beschlüsse umsetzen, konkrete Kenntnisse von den nicht selten brisanten Ermittlungsgegenständen erlangten. Auch diese Problematik könne bei Schaffung einer staatlichen Stelle entschärft werden.

3. Situationsbeschreibung aus der Sicht der Richter

Befragt wurden als keine Kontrollgruppe fünf Richter, die neben ihrer Funktion als erkennende Richter allesamt eine weitere Funktion als Ermittlungs-, Haft- oder Eildienstrichter ausüben. Ihre Wahrnehmung kann lediglich als Momentaufnahme gelten und eignet sich nicht für Verallgemeinerungen.

3.1. Allgemeine Folgeneinschätzung

Den Stellungnahmen lässt sich entnehmen, dass die Richterschaft, aufgrund ihrer Ferne zu dem unmittelbaren operativen Geschehen durchaus erwartungsgemäß, weniger mit den ermittlungstechnischen Konsequenzen des Urteils vom 2.3.2010 konfrontiert ist als die anderen Berufsgruppen. Ein Kollege erklärt die relative Gelassenheit der Richterschaft in dieser Frage damit, dass Ermittlungsrichter das persönliche Enttäuschungserlebnis eines Staatsanwaltes,

für den bestimmte Daten verloren sind, nicht kennen würden. Aus ihrer Perspektive als Eil- bzw. Ermittlungsrichter und damit als richterliches Kontrollorgan stünden Fragen der Begründetheit, gegebenenfalls auch Begründbarkeit von Abfrageanträgen und -beschlüssen unter erschwerten ermittlungspraktischen Rahmenbedingungen, (weiterhin) im Vordergrund. Allgemein sind die befragten Richter der Auffassung, dass die antragstellenden Staatsanwaltschaften ihre Praxis offenbar sehr schnell an die neue Rechtslage angepasst und ihre Anträge entsprechend umgestellt hätten. Bei der Abfrage von Verkehrsdaten nach § 100g StPO werde nunmehr einheitlich auf § 96 TKG anstatt auf § 113a TKG verweisen. Hier sei lediglich ein Textbaustein angepasst worden. Das sei rechtlich zulässig und nicht zu beanstanden.

Von spürbaren Auswirkungen berichten die Richter hingegen mit Blick auf ihre Erfahrungen als erkennende Richter. Hier fehle oft ein wichtiges Element zur Überführung von Tätern, bringt ein Richter die einhellig geäußerte Meinung auf den Punkt. Erkenntnisse, die mithilfe der retrograden Daten erlangt werden konnten und die in vielen Fällen auch zielführend waren, stünden nicht mehr zur Verfügung, sodass verschiedene Taten nicht mehr aufgeklärt werden könnten. In Anbetracht des kurzen Zeitraumes seit dem Urteil des Bundesverfassungsgerichts können die Richter bislang allerdings nur von relativ wenigen konkreten Fällen berichten, in denen die retrograden Daten zur Klärung des Falles definitiv gefehlt hatten. Sie weisen jedoch darauf hin, dass unbekannt bleibe, in welchen Fällen die gespeicherten Daten möglicherweise zum Ziel geführt hätten. Andererseits wisse man auch nicht, wie viele Daten in den entsprechenden Fällen tatsächlich noch hätte erlangen können, wenn die Vorratsdatenspeicherung nicht weggefallen wäre.

3.2. Veränderungen in der Antrags- und Anordnungspraxis

Die Antragspraxis der Ermittlungsbehörden hat sich seit dem Wegfall der Vorratsdatenspeicherung nach der Beobachtung der befragten Richter nur bedingt verändert. Ein Richter berichtet, dass in seinem Tätigkeitsbereich die Anzahl der Anträge nach § 100a StPO zugenommen habe. Hinsichtlich der von dem Wegfall der Vorratsdatenspeicherung unmittelbar betroffenen Verkehrsdatenabfrage nach § 100g StPO ergibt sich ein uneinheitliches Bild: während ein Richter berichtet, in seinem Tätigkeitsbereich würden mindestens gleich viele Anträge nach § 100g StPO wie vor dem BVerfG-Urteil vom März 2010 bearbeitet werden, berichten zwei andere von einem Rückgang der Anträge nach § 100g StPO. Ein weiterer Kollege beobachtet freilich eine deutliche Zunahme der Eilanträge. Sofern von einem generellen Anstieg der Antragszahlen in Bereich des § 100g StPO berichtet wird, sei dies wahrscheinlich auf den schon längerfristig erkennbaren Trend zurückzuführen, dass viele Straftäter mittlerweise immer mehr Handys besäßen. Ein Zusammenhang mit dem Wegfall der Vorratsdatenspeicherung könne daraus eher nicht hergestellt werden. Vielmehr habe das Urteil des Bundesverfassungsgerichts, jedenfalls kurzfristig, eher zu einem Rückgang der Anträge nach § 100g StPO geführt. Ein Richter beziffert den Rückgang in seinem Arbeitsbereich sogar mit fast 100%. Ansonsten seien hinsichtlich der Abfragepraxis der Ermittlungsbehörden keine Veränderungen zu beobachten.

Die Frage, ob die faktische Eilbedürftigkeit der Verkehrsdatenabfrage im Hinblick auf die kurze Speicherfrist von ca. drei bis sieben Tagen Auswirkungen auf die Antragspraxis der Ermittlungsstellen einerseits und die Anordnungspraxis der Gerichte andererseits hatte, wird von allen befragten Richtern übereinstimmend verneint. Zwar sei bei Anträgen ein erhöhter Zeitdruck festzustellen (*„man muss sich heute mit den Beschlüssen wirklich beeilen"*). Inhaltlich würden die eingehenden Anträge aber auch heute *„jedes Mal auf Herz und Nieren geprüft. Nachlässigkeiten lassen wir nicht zu"*, betonte ein Gesprächspartner; *„abgenickt wird nichts"*, drückt es ein anderer aus. Sofern eine Verkehrsdatenabfrage nach § 100g StPO beantragt wird, würden an die Begründung dieselben Anforderungen gestellt werden, wie es auch vor dem Wegfall der Vorratsdatenspeicherung der Fall war. Die Qualität der Anträge habe sich aufgrund der faktischen Eilbedürftigkeit nicht verändert.

Ob die beantragten bzw. die übermittelten Daten auch tatsächlich rechtmäßig im Sinne von § 96 TKG gespeichert waren, wird von den Gerichten nicht überprüft. Die befragten Richter weisen darauf hin, dass ihnen eine dahingehende Prüfung nicht möglich sei, da die Erforderlichkeit der Speicherung ebenso wie die Speicherdauer von den betriebsinternen Abläufen der Telekommunikationsanbieter abhängig sei. Insoweit werde allgemein von einer rechtmäßigen Speicherpraxis der Telekommunikationsunternehmen ausgegangen.

3.2.1. Alte Vorratsdaten

Hinsichtlich des Umgangs mit Daten, die nach der alten Rechtslage vor dem 2.3.2010 nach § 113a TKG rechtmäßig gespeichert wurden, war zunächst eine gewisse Unsicherheit festzustellen. Keiner der befragten Richter hatte bislang einen Fall bearbeitet, in dem diese Frage hätte entschieden werden müssen. Spontan neigten einige von ihnen aber, anders als die Staatsanwälte[322] und anders als der BGH[323], einhellig der Auffassung zu, die eine Verwertbarkeit derartiger Daten verneint hatte und von einem Beweisverwertungsverbot ausgegangen war. Das hat sich inzwischen geändert.

3.3. Mögliche Substitute für die Verkehrsdatenabfrage

Auf der Grundlage der gegenwärtigen Rechtslage sehen die befragten Richter keine ausreichenden Substitute für die Vorratsdatenspeicherung. Im Rahmen von § 100 TKG würden zwar viele Daten immerhin für ca. sieben Tage gespeichert, das sei jedoch in vielen Fällen nicht ausreichend. Auf der Grundlage des § 96 TKG würden nur die abrechnungsrelevanten Daten gespeichert. Im Rahmen der tatrichterlichen Perspektive seien jedoch häufig darüber hinausgehende Daten erforderlich, um eine bestimmte Beweisführung hieb- und stichfest begründen zu können. § 100a StPO sei als mögliches Substitut nur im Hinblick auf zukünftig stattfindende Kommunikationsvorgänge hilfreich. Retrograde Daten können mit der Telekommunikationsüberwachung nicht erfasst werden. Darüber hinaus stelle eine Maßnahme

---

322 Siehe dazu oben Pkt. 2.2.1.

323 Siehe dazu oben Fn. 82

nach § 100a StPO einen deutlich schwereren Eingriff dar als eine Verkehrsdatenabfrage, weshalb die Maßnahme zudem nur bei Vorliegen einer Katalogtat angeordnet werden könne. Für die Erlangung retrograder Daten gebe es somit nach der gegenwärtigen Rechtslage kein der Vorratsdatenspeicherung adäquates Mittel.

Ob die Einführung eines Quick-Freeze-Verfahrens sinnvoll wäre, konnten die befragten Richter mangels detaillierter Kenntnisse nicht beurteilen.

3.4. Auskunftsverhalten der Telekommunikationsanbieter

Zur Auskunftsbereitschaft der Telekommunikationsanbieter konnten sich die befragten Richter nur bedingt äußern. Regelmäßig seien es die Ermittlungsbehörden, die mit diesen in Kontakt stünden. Allerdings sei bekannt, dass verschiedene Telekommunikationsanbieter regelmäßig die Beauskunftung von Anfragen verweigerten und Beschlüsse nicht umsetzten. Daran habe sich durch das Urteil des Bundesverfassungsgerichts vom 2.3.2010 jedoch nichts geändert. Diese Probleme seien sowohl vor der Einführung der Vorratsdatenspeicherung, während der Geltung der §§ 113a, b TKG und auch nach dem Wegfall dieser Normen aufgetreten. Ab und zu hätten einzelne Anbieter auch Beschwerde gegen richterliche Beschlüsse eingelegt; diese seien aber immer verworfen worden. Teilweise seien sogar Zwangsgelder verhängt worden.

3.5. Erwartungen an den Gesetzgeber

Eine möglichst baldige Wiedereinführung der Vorratsdatenspeicherung wird von den Gesprächspartnern als dringend erforderlich erachtet. Teilweise wird vorgeschlagen, §§ 113a, b TKG in ihrer bisherigen Fassung sollten an die Vorgaben des Bundesverfassungsgericht angepasst werden, ansonsten aber möglichst unverändert bleiben. Ein anderer Gesprächspartner ist der Ansicht, vor einer Neuregelung solle untersucht werden, ob tatsächlich alle in der alten Norm genannten Datenarten zu Gefahrenabwehr- bzw. Strafverfolgungszwecken tatsächlich erforderlich und ihre Speicherung wünschenswert sind. Übereinstimmend wird ein offener Katalog befürwortet, mit dem neben exemplarisch aufgelisteten Straftaten bei Bedarf auch andere Fälle vergleichbarer Schwere erfasst werden. Eine Anlehnung an die aus dem StGB bekannte Regelbeispieltechnik wäre aus Sicht der Richter wünschenswert. Der Katalog selbst könne dann auf wirklich gravierende Straftaten beschränkt werden.

4. Situationsbeschreibung aus Sicht der TK-Anbieter

Die Einschätzung der Auswirkungen des BVerfG-Urteils vom 2.3.2010 auf die Speicher- und Abfragepraxis fällt bei den befragten TK-Anbietern ebenso unterschiedlich aus wie die allgemeine Situationsbeschreibung und die Vorstellungen zu einer künftigen Neuregelung.

4.1. Veränderungen in der Abfragepraxis

Diese Unterschiede zeigen sich exemplarisch bei der Frage nach etwaigen Veränderungen in der Abfragepraxis. Während ein großer Universalanbieter keine Unterschiede feststellen konnte, haben zwei weitere eine Zunahme im Anfragevolumen wahrgenommen, die bei gleichbleibender Anzahl von Verkehrsdatenabfragen mit einem Anstieg bei der TKÜ erklärt wurde. Das vierte Großunternehmen berichtete hingegen von gegenteiligen Erfahrungen. Dort habe man bei Anfragen betreffend Festnetzdaten einen massiven Rückgang beobachtet, bezüglich ausgehender Anrufe um ca. 70 %, bezüglich eingehender um nahezu 100 %. Der Rückgang wird im Mobilfunkbereich auf ca. 10 % geschätzt, für das Internet auf etwa 50 %. Diese Unterschiede können speziell bei der Entwicklung der Verkehrsdatenabfragen zumindest teilweise mit einer unterschiedlichen Speicherpolitik der Unternehmen nach dem Wegfall der §§ 113a/b TKG erklärt werden. Wie sich aus den Gesprächen mit den Ermittlern ergeben hat, werden unternehmensspezifische restriktive Speicher- und Beauskunftungspraktiken, insbesondere wenn sie von Unternehmensseite offensiv kommuniziert werden, wahrgenommen und in künftigen Anfragesituation auch entsprechend antizipiert. Nicht begründbar sind damit allerdings die unterschiedlichen Beobachtungen zu der Zunahme im § 100a-Bereich; hier meint das zweite Unternehmen, eine solche speziell nur in Bayern beobachten zu können.

Bei den kleineren Anbietern speziell im Festnetz- und Internetbereich ist die Wahrnehmung ebenfalls unterschiedlich. Während das eine Unternehmen aus heutiger Sicht das Abfragevolumen mit dem aus der Zeit vor der einstweiligen Verfügung vergleicht und nur für dieses Interimszeitraum (März 2008 bis Februar 2010) einen Rückgang beobachtet hat, stellte das andere einen Rückgang fest. Dieser wird, ähnlich wie bei dem schon erwähnten Universalanbieter, mit Lerneffekten aus der zunächst großen Zahl eigener Negativauskünfte nach dem 2.3.2010 erklärt.

4.2. Aktuelle Speicherpraxis

Die Speicherpraxis der Unternehmen ist sehr vielfältig und ergibt unter Berücksichtigung der Vielfalt unterschiedlicher Tarifmodelle ein sehr unübersichtliches Gesamtbild. Eine Übersichtstabelle einer niedersächsischen Polizeidienststelle ist unter Pkt. 1.4.1. reproduziert. Uneinheitlich ist ferner die Praxis bei den Anonymisierungen nach Kundenwunsch gem. § 96 Abs. 4 TKG. Zum Teil werden die drei Endziffern bereits nach 3 bis 7 Tagen ge-x-t, zum Teil erst später. Wird ein Einzelverbindungsnachweis gewünscht, sind die Daten bei zwei der großen Anbieter bis zu 80 bzw. 90 Tage verfügbar, während dies bei dem dritten bis zu 182 Tage der Fall ist. 7 Tage ist auch bei den beiden internetzentrierten Unternehmen ein entscheidendes Datum; so lange werden dort IP-Adressen gespeichert. Einer der Universalanbieter handhabt IP-Adressen wie auch IMEI- und IMSI-Kennungen entsprechend, während der zweite IP-Adressen über Festnetz 30 Tage speichert, über Mobilfunk hingegen nur bis zum Verbindungsende. Bei dem dritten werden IP-Daten, IP-Zuordnungen und E-Mail-Verbindungsdaten gar nicht mehr gespeichert. Auch die von zahlreichen Ermittlern für den Bereich des

mobilen Internets thematisierten Probleme bei Port-Nummern und Mac-Adressen werden hier bestätigt. Diese werden zumindest bei einigen Anbietern tatsächlich überhaupt nicht gespeichert. Uneinheitlich gestaltet sich auch die Speicherfrist bei Funkzellenabfragen. Im Übrigen zeigt sich für abrechnungsrelevante Verkehrsdaten eine gewisse Häufung der Löschfristen nach 30 Tagen. Ein weiterer Anbieter hält die Daten bis 80 Tage nach Rechnungsversand vor, was eine Gesamtspeicherdauer von 90 Tagen plus den aktuellen Monat ergibt. Noch schwerer zu verallgemeinern ist die Handhabung eingehender Verbindungen. Mindestens ein Anbieter speichert auch diese. Bei den anderen sind sie aber nur noch in den ersten 3 bis 7 Tagen abrufbar; das ist die Speicherfrist für das Störungsmanagement (vgl. § 100 TKG).

4.2.1. Abrechnungsrelevanz bei Flatrates und Prepaid-Karten

Besondere Aufmerksamkeit galt der Frage nach der tatsächlichen Abrechnungsrelevanz von Flatrates und Prepaid-Karten. Diese können, in unterschiedlicher Konstellation, nahezu in allen Bereichen elektronischer Kommunikation relevant sein.[324] Anders als mitunter kommuniziert wird, kann auch in diesem Bereich, zumindest in einigen Konstellationen, die Vorhaltung von Daten für Abrechnungszwecke erforderlich sein. Ein Gesprächspartner erläutert hierzu, dass Kommunikationsvorgänge, die im Endkundenverhältnis auf einer Flatrate basierten, im Inter-Carrier-Verhältnis tatsächlich abrechnungsrelevant seien und häufig minutenweise abzurechnen seien. Eines der befragten großen Unternehmen speichert Verkehrsdaten bei Inlandsgesprächen auf Flatratebasis daher zumindest für wenige Tage, bei Auslandsgesprächen für längere Zeit. Im Mobilfunkbereich werden dort sowohl aus- wie auch eingehende Verbindungen 30 Tage lang gespeichert. Ein anderer Anbieter berichtet von einer ähnlichen Praxis; ein weiterer speichert auch diese regulär[325]. Alle Daten, die für die Abrechnung mit anderen Carriern notwendig seien, würden gespeichert, einschließlich der roamingrelevanten eingehenden Gespräche am Handy im Ausland. Vor diesem Hintergrund führt ein Unternehmen aus, dass es Flatrates im Hinblick auf die Abrechnungserfordernisse im Mobilfunk faktisch nicht gebe. Anders sei die Situation im Internet; dort gebe es fast ausschließlich Flatrate-Verträge.

Uneinheitlich sind die Auskünfte dann im Hinblick auf die Kommunikation mit Prepaid-Karten. Während einer der Universalanbieter auf die Notwendigkeit der Speicherung zur exakten Dokumentation des Guthabenverbrauchs verweist, verfolgt der andere einen abweichenden technischen Ansatz. Dort würden die verbrauchten Einheiten sowohl auf der Karte selbst als auch auf dem virtuellen Konto sofort automatisch gelöscht. Mögliche Einwendungen würden gem. §§ 45e u. i TKG behandelt.[326] Entsprechend werden auch die Daten betreffend SMS- und MMS-Nachrichten behandelt, wo die meisten Tarife sowohl bei Flatrates als auch im Prepaid-Bereich (zahlenmäßig ggf. volumenmäßig) limitiert sind. Das heißt, dass

---

324 Siehe oben Teil C, Pkt. 5.

325 Dort fallen lediglich Anrufversuche heraus.

326 Danach genügt der Nachweis, dass Billing-Kette und Abrechnungssystem normgemäß arbeiten.

auch insoweit der eine Anbieter Verkehrsdaten zum Nachweis darüber speichert, dass und wie das limitierte Guthaben aufgebraucht wurde, der andere hingegen nicht.

Diese tarifbezogenen Detailinformationen haben ermittelnde Beamte selbstredend meist nicht. Die uneinheitliche Speicherpraxis im Falle von Flatrates und Prepaid-Karten macht die Erfolgsaussichten von Verkehrsdatenabfragen ex ante noch ein Stückweit unkalkulierbarer. Immerhin bleibt aber auch in diesem Bereich eine gewisse Chance, insbesondere wenn man an die hohe Anzahl bei SMS- und MMS-Aufkommen[327] berücksichtigt.

4.3. Mögliche Substitute für die Verkehrsdatenabfrage

Auf die Frage, ob und bei welchen anderen Abfragearten ein erhöhtes Volumen beobachtet wird, werden im Wesentlichen drei Punkte benannt. Neben der schon erwähnten Telekommunikationsüberwachung gem. § 100a StPO stellen zwei Unternehmen auch eine Zunahme speziell bei der Auslandskopfüberwachung gem. § 4 TKÜV fest. Mehrfach wird schließlich auf eine Zunahme der Verkehrsdatenabfragen auf präventiv-polizeilicher Rechtsgrundlage verwiesen, auch wenn diese Abfragen insgesamt selten seien. Ein Interviewpartner meint allerdings, hier besonders in Niedersachsen ein entsprechendes 'Umschwenken' beobachten zu können. Entsprechende Anfragen aus Niedersachsen würden allerdings nicht beauskunftet, da das dortige Polizeigesetz explizit auf §§ 113a/b TKG verweise.[328] Alle Befragten konzedieren im Übrigen, dass retrograde Daten durch keine derzeit mögliche andere Maßnahme ersetzt werden könnten.

Unterschiedlich sind die Meinungen zur der Möglichkeit der Quick-Freeze-Technik als mögliche Alternative. Während der Repräsentant eines großen Anbieters auf gute Erfahrungen, die einige Länder mit einer solchen Speicheroption gemacht hätten, verweist, sprechen sich zwei andere sehr dezidiert gegen die Einführung aus. Zur Begründung wird auf die potenzielle Missbrauchsgefahr verwiesen. Anwälte könnten das Instrument z.B. zur Vorbereitung von Abmahnungen, v.a. im Bereich der Urheberrechtsverletzungen, missbrauchen. Sollte ein Quick-Freeze-Verfahren o.ä. eingeführt werden, sei eine Antragsflut zu befürchten, die den Betrieb der TK-Unternehmen lahmlegen würde.

4.4. Prüf- und Beauskunftungspraxis

Angesprochen auf die generelle Beauskunftungspraxis betonen die Gesprächspartner übereinstimmend, dass die Anbieter den Ermittlungsbehörden nach wie vor alle abgefragten Daten lieferten, sofern entsprechende Datenbestände vorhanden seien. In Umsetzung des Urteils des BVerfG vom 2.3.2010 seien die Daten, die auf der Grundlage von § 113a TKG gespeichert waren, gelöscht und die entsprechenden Speicherprogramme ausgesetzt worden. Darüber

---

327 Diese machen in Deutschland ein Vielfaches im Vergleich zur Sprachkommunikation aus. 2009 wurden hierzulande 34 Mrd. SMS-Nachrichten versandt. Bundesnetzagentur, Jahresbericht 2009, S. 92.

328 Eine solche Verweisung kann § 33a nds. SOG allerdings nicht entnommen werden.

hinausgehende Einschränkungen in der Beauskunftungspraxis gebe es nicht. Daher würden alle vorhandenen Daten im Abfragefall zur Verfügung gestellt, auch wenn sie nicht abrechnungsrelevant sind. Ein Zitat, das sinngemäß alle Antworten zu dieser Thematik repräsentiert, lautete „wir speichern, wozu wir gesetzlich verpflichtet sind, und geben heraus, wozu wir gesetzlich verpflichtet sind“. Der Repräsentant eines Universalanbieters verweist in diesem Zusammenhang explizit auf das Risiko, dass die Staatsanwaltschaft ansonsten bei dem Verdacht, dass vorhandene Daten zurückgehalten werden, einen Durchsuchungsbeschluss erwirken könnte.

Unterschiedlich fallen im Detail die Angaben zu der Prüfdichte bei eingehenden Beschlüssen aus. Übereinstimmend wird berichtet, dass alle Beschlüsse auf ihre formale Richtigkeit hin überprüft würden. Genannt werden als Kriterien übereinstimmend zunächst Formalien wie insbesondere Namen, Datum und Unterschrift. Problematisch seien Beschlüsse, auf denen handschriftliche Änderungen vorgenommen worden sind. Könne nicht aufgeklärt werden, von wem diese stammten, würde die Beauskunftung mitunter verweigert. Ein Vertreter beschreibt die Prüfungsintensität in seinem Unternehmen als Prüfung auf Plausibilität und offensichtliche Mängel. Bei einigen Anbietern wird allerdings weitergehend auch überprüft, ob tatsächlich eine Katalogstraftat vorliegt. Ein besonderer Kritikpunkt in diesem Zusammenhang ging dahin, dass die Interpretation des § 100g Abs. 1 Nr. 2 StPO (mittels Telekommunikation begangene Straftat) schwierig sei. Ein Gesprächspartner gibt ferner an, in seinem Unternehmen werde auch die in dem Beschluss angegebene Rechtsgrundlage geprüft. Ob die zuletzt genannten Prüfkriterien tatsächlich noch als „grobe formale Prüfung“ angesehen werden können, mag zweifelhaft erscheinen.

Drei der sechs Gesprächspartner räumen im Übrigen ein, dass es bei Eilanordnungen vermehrt zu Problemen kommen könne. Hier herrsche mitunter Unsicherheit darüber, ob und wann eine Anfrage eines richterlichen Beschlusses bedürfe und wann nicht. Schwierigkeiten bereiteten in diesem Bereich auch die Übermittlungen per Fax. Diese seien nicht selten nur schlecht lesbar, was ihre Bearbeitung erschweren könne.

4.5. Unternehmensstrategien im Hinblick auf eine mögliche Neuregelung und Erwartungen an den Gesetzgeber

Uneinheitlich erscheint schließlich auch die unternehmerische Strategie im Hinblick auf die weitere gesetzliche Entwicklung im Bereich der Verkehrsdatenabfrage. Übereinstimmend wurde berichtet, dass das Personal für den Betrieb der Hard- und Software zur Vorratsdatenspeicherung abgezogen wurde. Die implementierte Technik wurde bei einigen Unternehmen teilweise abgebaut, bei anderen wird die Systeminfrastruktur in Erwartung einer Neuregelung vorgehalten. Ein Gesprächspartner schätzt, dass etwa 50 % der ursprünglich eingesetzten Investitionen verloren sein dürften. Ein anderer berichtet, dass die Technik nunmehr für die Beauskunftung der abrechnungsbezogenen Daten eingesetzt werde. Technische Angaben zum Speichervolumen, das aktuell für die Verkehrsdatenspeicherung notwendig sei, konnten nur die Vertreter der großen Universalanbieter machen. In allen Fällen wird der Anfall auf

mehrere Terabite veranschlagt. Ein weiteres großes Unternehmen beziffert die notwendige Speicherkapazität auf 300 bis 500 Millionen Datensätze pro Tag.

Der Vertreter der Deutschen Telekom berichtete ferner, dass die Technik zur Zielwahlsuche, die mit Einführung der Vorratsdatenspeicherung für überflüssig erachtet und daher demontiert worden sei, gegenwärtig wieder implementiert werde.

Im Hinblick auf eine mögliche gesetzliche Neuregelung haben die Interviewpersonen auf eine Vielzahl von Punkten hingewiesen, die aus der Perspektive ihrer Unternehmen Berücksichtigung finden sollten. Das erste Petitum ging dahin, dass die zur Zeit der Vorratsdatenspeicherung geltende Doppelspurigkeit – Speicherung gem. § 113a und §§ 96ff. TKG – wegfallen sollte. Würde tatsächlich eine neue Vorratsdatenspeicherung eingeführt, sollte die Zugriffsmöglichkeit der Behörden auf abrechnungsrelevante Verkehrsdaten unbedingt wegfallen. Dies erfordere eine parallele Datenspeicherung und eine doppelte Verwaltung. Die Befragten fordern auch übereinstimmend eine klarere Definition als bislang, welche konkreten Daten zu speichern sind, einschließlich einer Klarstellung, dass Anfragen, die darüber hinausgehen, nicht beauskunftet werden müssen. Ein Interviewpartner regt in diesem Zusammenhang eine Beschränkung auf solche Datenarten an, die ermittlungstechnisch tatsächlich von Bedeutung sind. Als Beispiel verweist er auf Ermittlungen im Internetbereich, bei denen die Erfahrung zeige, dass IP-Adressen und Zeitstempel die maßgeblichen Parameter seien, die die Ermittler bräuchten. Von verschiedener Seite wird schließlich für kurze Speicherfristen plädiert. Die ursprüngliche Sechsmonatsfrist sei aus Unternehmenssicht zu lang. Die Möglichkeit, Abfragen zügig zu veranlassen, wird von einem der Gesprächspartner als verwaltungstechnisches Problem der Strafverfolgungsbehörden bezeichnet, das mit organisatorischen Maßnahmen zu lösen sei.

Mit Blick auf den sachlichen Anwendungsbereich wird, auch insoweit dezidiert anders als von Ermittlerseite, mehrheitlich eine Kataloglösung favorisiert. Insbesondere die aktuelle Fassung des § 100g Abs. 1 Nr. 2 StPO wird als für die Unternehmen schwer nachvollziehbar bezeichnet.

In formaler Hinsicht wird zum einen eine klare und abschließende Regelung gewünscht, wer zur Abfrage von Verkehrsdaten berechtigt sein solle. Mehrere Personen regen darüber hinaus eine Konzentration auf Seiten der berechtigten Stellen zu schaffen. Heute sei die Kompetenz bei den Abfrageberechtigten nicht überall gleich. Mit zentralen Stellen, wie sie z.B. in Bayern bestünden, habe man hingegen die Erfahrung gemacht, dass die zuständigen Personen deutlich besser informiert seien. Die Abfragen hätten eine höhere Qualität, wodurch deutlich weniger Rückfragen erforderlich seien, sodass sich auf Anbieterseite ein geringerer Aufwand ergebe. Ein Interviewpartner hält im Übrigen eine Vereinheitlichung im Hinblick auf den Richtervorbehalt für wünschenswert; ein solcher solle generell für alle Abfragen gelten; damit könnten Rechtsunsicherheiten wie insbesondere bei den Eilanordnungen, vermieden werden.

Zuletzt setzten sich die Unternehmensvertreter auch mit verfahrenstechnischen Fragen auseinander. Ähnlich wie von Ermittlerseite wird auch hier ausgeführt, dass es hilfreich wäre, wenn das Verfahren verpflichtend definiert und vereinheitlicht würde. Über die bisherige Umsetzungsrichtlinie[329] hinaus müssten sämtliche Anfrage- und Antwortformate verbindlich definiert und der elektronische Austausch genereller Standard für alle Abfragearten werden. Wie bei vielen anderen Gelegenheiten auch, wird von den Anbietern die Entschädigungsproblematik angesprochen. Die Unternehmen, so eine dezidierte Meinungsäußerung, bräuchten keine Vorratsdatenspeicherung; deshalb sollten alle anfallenden Kosten – Anschaffung, Instandhaltung und Beauskunftung – auf kostendeckendem Niveau erstattet werden. Der Vertreter eines Universalanbieters beziffert die Investitionskosten für die nun wieder außer Funktion gesetzte Vorratsdatenspeicherung für sein Unternehmen auf € 12 Mio. Ein anderer verweist auf die Kosten für die zusätzlichen Kosten für die Vernichtung. Dieser Aufwand sei ausschließlich fremden, nämlich staatlichen Interessen geschuldet.

Uneinheitlich sind schließlich die Ansichten zu dem optimalen Speicherort für Verkehrsdaten. Einige halten mit Verweis auf Aspekte des Datenschutzes eine zentrale Speicherung für vorzugswürdig, andere sehen gerade den Datenschutz besser über die gegenwärtige dezentrale Speicherung bei den Unternehmen gewährleistet. Hier wird allerdings auch die Befürchtung laut, dass zusätzliche Sicherheitsanforderungen ein weiterer kostentreibender Faktor seien. Zwei Unternehmensvertreter verweisen auch mit Nachdruck darauf, dass es sich um die Daten der eigenen Kunden handele; diese Verantwortung wolle man nicht abgeben.

---

329 Anm.: Gesprächspartner nimmt mutmaßlich auf die TKÜV Bezug.

Teil G: Situation im Ausland

1. Einleitung

Betrachtet man die europäischen und außereuropäischen Entwicklungen zur Abfrage und Speicherung von Telekommunikationsverkehrsdaten, dann lässt sich auch feststellen, dass die Europäische Union bei der Einführung von Regelungen zur Verkehrsdatenvorratsspeicherung eine Vorreiterrolle gespielt hat und heute noch spielt. Die Diskussion der Vorratsspeicherung hat sich auf Europa konzentriert[330].

Die Implementierungsdebatten in den Mitgliedsstaaten lassen deutlich erkennen, dass Strafverfolgungs-, Gefahrenabwehr- und Datenschutzgesichtspunkte die Gesetzgebung maßgeblich bestimmen, und nicht genuin wirtschaftspolitische Überlegungen, wie bei einer EU-Richtlinie als Instrument zur Binnenmarktregulierung eigentlich zu erwarten wäre. Jedenfalls wird das ursprüngliche Ziel der Richtlinie, einheitliche Rahmenbedingungen für die Telekommunikationsunternehmen zu schaffen, angesichts des derzeitigen Stands der Umsetzung noch nicht erreicht[331]. Heute werden jedenfalls in der die Richtlinie umsetzenden Gesetzgebung der Mitgliedsländer ein erhebliches verfassungsrechtliches Problempotential sowie deutliche Unterschiede gesehen[332].

Die Abfrage von Telekommunikationsverkehrsdaten hat sich international zu einer Standardmaßnahme in strafrechtlichen Ermittlungen und bei der strategischen Informationsbeschaffung zu Zwecken der Gefahrenabwehr und -analyse entwickelt. Dieser Prozess reflektiert die zunehmende Verbreitung von (mobilen) Telekommunikationsmitteln, die Digitalisierung und die aus digitalen Spuren resultierenden detaillierten und validen Informationen zu individuellem Verhalten sowie Beziehungsmustern. Rechtspolitische Debatten zur Nutzung von Verkehrsdaten für Zwecke der Strafverfolgung und der Gefahrenabwehr sind auch dadurch gekennzeichnet, dass für Verkehrsdaten grundsätzlich von einer im Vergleich zu Kommunikationsinhalten weniger signifikanten Eingriffsintensität ausgegangen wird.

---

330 In Argentinien wurde im Jahr 2004 eine Vorratsspeicherung für zehn Jahre eingeführt, kurz darauf aber wieder suspendiert, vgl. Decreto 357/2005: Suspéndese la aplicación del Decreto Nº 1563 del 8 de noviembre de 2004.

331 Vgl. hierzu auch Council of European Professional Informatics Societies: Position Paper on Data Retention. Brüssel 2008.

332 www.FAZ net.de, vom 27. Juni 2010: Vorratsdatenspeicherung. Die Richtlinie, nach der sich nicht alle richten.

2. Die Entwicklung in den Common Law Staaten USA, Kanada, Australien und Neuseeland

Der Common Law Bereich, und hier die USA, Kanada Australien und Neuseeland, hat sich bislang darauf beschränkt, anlassbezogene Regeln des Zugriffs auf Verkehrsdaten einzuführen bzw. den Zugriff auf Bestands- und Verkehrsdaten im Rahmen der Überwachung der Telekommunikation selbst zu nutzen[333].

In den USA hatten die Anschläge vom 11. September 2001 in Gestalt des Patriot Act 2001 zwar zu weitreichenden Erweiterungen der Exekutivbefugnisse auch in der Telekommunikationsüberwachung geführt[334]. Jedoch sind die Verpflichtung zur Erfassung von Bestandsdaten und die Vorratsspeicherung von Verkehrsdaten zu diesem Zeitpunkt nicht ins Auge gefasst worden[335]; die anlassbezogenen Zugriffe auf Verkehrsdaten sind auf 90 Tage begrenzt, bei einer einmaligen Verlängerungsmöglichkeit um 90 Tage.

In den USA wird dabei ein Verfahren praktiziert, das auch in Europa zuweilen als Alternative zur Vorratsdatenspeicherung vorgeschlagen wird. Es handelt sich um das so genannte „Quick Freeze“ oder „Data Freeze-Verfahren“[336]. Darunter versteht man ein (auch im Übereinkommen des Europarats über Computerkriminalität enthaltenes) Verfahren (vgl. hierzu im Einzelnen 2.3.2.2.), in dem die Daten einer verdächtigen Person ab dem Zeitpunkt einer polizeilichen Anordnung gegen ein Telekommunikationsunternehmen (oder Internetserviceprovider) gespeichert und damit „eingefroren“ werden[337]. Hier geht es im Kern um eine allgemeine Verkehrsdatenabfrage, mit der ab dem Zeitpunkt einer Anordnung auf noch vorhandene und entstehende Telekommunikationsverbindungen zugegriffen wird. Insoweit werden durch ein solches Verfahren allerdings gerade solche Daten nicht erfasst, auf die die Vorratsspeicherung abzielt, nämlich Daten, die aus betrieblichen Zwecken heraus nicht gespeichert werden

---

333 Die größere Zurückhaltung deckt sich im Übrigen mit Umfrageergebnissen, nach denen die nordamerikanische Bevölkerung stärker als diejenige kontinentaleuropäischer Länder am Schutz persönlicher Daten interessiert ist, vgl. hierzu The Surveillance Project: Global Privacy of Data, International Survey. Queens University Belfast 2006, S. 11.

334 *Ringland, K.*: The European Union’s Data Retention Directive and the United States’s Data Preservation Laws: Finding the Better Model, 5 Shidler J. L. Com. & Tech. 13 (2009), http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/427/vol5_no3_art13.pdf?sequence=1 [Juni 2011].

335 *Crump, C.:* Data Retention: Privacy, Anonymity, and Accountability Online. Stanford Law Review 56 (2003), S. 191-229.

336 Stenographischer Bericht des BT, 19. Sitzung in der 16. Wahlperiode, 16.2.2006, S. 1419; *Dix, A.*: Informations- und Kommunikationskriminalität. Kriminalistik 2004, S. 81-85, S. 82.

337 *Büllingen, F.*: Vorratsspeicherung von Telekommunikationsdaten im internationalen Vergleich, DuD 2005, S. 349-353, S. 350; *Sierck, G., Schöning, F., Pöhl, M.*: Wissenschaftliche Dienste des Deutschen Bundestages, Gutachten zur „Zulässigkeit der Vorratsdatenspeicherung nach europäischem und deutschem Recht“. Berlin 2006, S. 14.

und solche, die vor der in der Vorratsspeicherungsregelung vorgesehenen Frist von Telekommunikationsunternehmen gelöscht werden[338].

Die Verkehrsdatenabfrage ist in den USA auf Bundesebene in Titel 18, Art. 2703(f) des US-Gesetzbuches geregelt. Danach kann jede staatliche Behörde Telekommunikationsunternehmen oder Internetserviceprovider anweisen, anfallende Verkehrsdaten für einen Zeitraum von bis zu 90 Tagen zu speichern. Die Anweisung kann um weitere 90 Tage verlängert werden. Der Zugang zu den gespeicherten Daten wird dann über eine gerichtliche Anordnung ermöglicht.

Im Jahr 2006 lebte in den USA die Debatte über eine Verkehrsdatenspeicherung in den USA auf, beschränkt auf Internetverbindungen und angefacht durch Fälle der Kinderpornografie sowie der sexuellen Ausbeutung von Kindern in online-Kommunikation über das Internet[339]. Ein Gesetzesantrag im Bundesstaat Colorado, der die Vorratsspeicherung für Internetverbindungen zum Zwecke der Aufklärung gegen Kinder gerichteter Straftaten im Internet vorsah, fand im Jahr 2006 allerdings im Parlament keine Mehrheit[340]. Die kontroverse Diskussion über die Vorratsspeicherung von Internetverbindungsdaten[341] konzentrierte sich allerdings weiter auf Fälle der Vorbereitung sexuellen Missbrauchs durch Internetkontakte. Insbesondere das FBI fordert eine Speicherungspflicht der bei Internetserviceprovidern (ISP) anfallenden Verkehrs- und Nutzerdaten für eine Dauer von zwei Jahren. Im Jahr 2007 wurde auf Bundesebene ein Entwurf zu einem Gesetz „Internet Stopping Adults Facilitating the Exploitation of Today's Youth Act (SAFETY)" eingebracht, der eine Speicherungspflicht für Internetserviceprovider vorsieht, jedoch über das Entwurfsstadium nicht hinausgekommen ist. Die Konzentration der Diskussion über eine Vorratsdatenspeicherung auf den Schutz von Kindern vor sexueller Ausbeutung und beschränkt auf Internetkommunikation lässt im Vergleich zu Europa Unterschiede in Überwachungs- und Strafverfolgungsinteressen, allerdings auch andere politische Rahmenbedingungen erkennen, die die Durchsetzung einer der Richtlinie 2006/24 vergleichbaren Gesetzgebung bislang wenig realistisch erscheinen lässt. Die für die Bush Administration registrierte Unterstützung der systematischen Speicherung von Telekommunikationsverkehrsdaten in der Europäischen Union wird aus einer kritischen Per-

---

338 Stenographischer Bericht des BT, 19. Sitzung in der 16. Wahlperiode, 16.2.2006, S. 1426; Commission Staff Working Document, Annex to the: Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC, Extended Impact Assessment, {COM(2005) 438 final}, Brüssel, 21. 9. 2005, S. 12; European Working Party on Information Technology Crime: Expert Statement, Overview of vital traffic data necessary for investigations for which the EWPITC asks the general retention by telecommunication operators and telecommunication access and service providers. Interpol, 2001; Stenographischer Bericht des BT, 19. Sitzung in der 16. Wahlperiode, 16.2.2006, S. 1427

339 *Petersen*, *R.:* Toward a U.S. Data Retention Standard for ISPs. EDUCAUSE Review 2006, S. 78-79.

340 Cyber Security Industries Alliance: Data Retention: Get the Facts. Arlington, 2007.

341 Vgl. hierzu Center For Democracy and Technology: Mandatory Data retention – Invasive, Risky, Unnecessary, Ineffective. Washington 2006.

spektive auch als Versuch einer „Politikwäsche“ interpretiert, mit der ein national konfliktträchtiges rechtspolitisches Thema durch internationale Organisationen aufgegriffen und über diese auf die nationale Ebene zurückgeschleust werden soll[342].

Seit dem 11.09.2001 haben sich Hinweise auf die systematische Sammlung von Telekommunikationsverkehrsdaten durch amerikanische Geheimdienste und das FBI ergeben, für die umstritten ist, ob sie durch die Gesetzeslage gedeckt sind, da sie offensichtlich nicht nur Auslandsverbindungen erfassen. Doch entstand keine Debatte über eine generelle Vorratsdatenspeicherung von Verkehrsdaten der Telekommunikation. Dies wird teilweise erklärt mit dem in den USA kaum ausgeprägten gesetzlichen Schutz persönlicher Daten, die im privaten Sektor anfallen, was dazu führt, dass Telekommunikationsunternehmen und Internetserviceprovider sehr weitgehende Datensammlungen betreiben, die in die Quick-Freeze-Speicherungs- und Abfragestrategien der Sicherheits- und Strafverfolgungsbehörden einbezogen werden können. Hinzu tritt eine besondere Geschichte in der Zusammenarbeit zwischen Staat und privatem Sektor in der Strafverfolgung und Gefahrenabwehr[343]. Ferner unterliegen so genannte „National Security Letters“, deren Anwendungsbereich durch den Patriot Act deutlich erweitert wurde, kaum einer Kontrolle; insbesondere ist kein Erfordernis einer gerichtlichen Anordnung oder Bestätigung der Anweisungen zur Herausgabe vorgesehen. National Security Letters können durch das FBI sowie weitere Behörden erlassen werden und enthalten Anweisungen an Telekommunikationsunternehmen, Internetserviceprovider und andere Unternehmen, die personenbezogene (Transaktions-) Daten speichern, zu bestimmten Personen vorhandene Informationen herauszugeben (und über die Herausgabe Stillschweigen zu bewahren). Dies kann auch nicht tatverdächtige Personen betreffen, solange die Daten für Ermittlungen in Terrorismus- oder Spionagefällen von Nutzen sind[344]. Von solchen Anweisungen wurde im Jahr 2006 in knapp 50.000 Fällen Gebrauch gemacht[345]. Die Datenabfrage erstreckte sich ganz überwiegend auf Telekommunikations- und Internetverkehrsdaten sowie Bestandsdaten zu den Kunden von Telekommunikationsunternehmen[346].

In Kanada wurde bereits anlässlich der Konsultationen zum Gesetz über die Modernisierung von Ermittlungstechniken (Modernization of Investigative Techniques Act, MITA, 2005) darauf hingewiesen, dass weder an die Einführung von „Know Your Customer“ Regeln noch von Verpflichtungen zur Speicherung von Bestands- oder Verkehrsdaten gedacht werde. Der

---

342 *Stanley J.*: The Surveillance-Industrial Complex: How the American Government Is Conscripting Businesses and Individuals in the Construction of a Surveillance Society. American Civil Liberties Union, New York 2004, S. 15.

343 *Stanley J.*: a.a.O., 2004, S. 3.

344 U.S. Department of Justice, Office of the Inspector General: A Review of the FBI’s Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006. Office of the Inspector General, Washington, März 2008.

345 U.S. Department of Justice, Office of the Inspector General: a.a.O., 2008, S. 9.

346 U.S. Department of Justice, Office of the Inspector General: a.a.O., 2008, S. 109 f.

Entwurf des Modernisierungsgesetzes MITA[347], mit dem die Umsetzung der Cyber Konvention des Europarats erfolgen sollte und das Telekommunikationsunternehmen verpflichtet hätte, die Kommunikationstechnik an Erfordernisse der Strafverfolgung anzupassen, fiel aus formellen Gründen 2005 aus dem Gesetzgebungsverfahren[348]. Das Vorhaben ist 2009 wieder aufgegriffen worden. Der „Investigative Powers For The 21st Century Act", der nach der 2. Lesung im Herbst 2009 wie der vorangegangene Entwurf wegen Vertagung des Parlaments im Januar 2010 aus dem Gesetzgebungsverfahren herausgefallen ist (und deshalb neu eingebracht werden muss), sieht, in bewusster Abhebung zur Richtlinie 2006/24/EG der Europäischen Union[349], keine umfassende Speicherungspflicht von Verkehrsdaten vor. Im Falle begründeten Tatverdachts oder begründeten Verdachts, dass eine Straftat begangen werden wird, sind Ermittlungsbeamte der Polizei dazu befugt, Telekommunikationsunternehmen anzuweisen, bestimmte Verkehrsdaten zu speichern (preservation demand). Insoweit handelt es sich um eine Form des weiter oben angesprochenen Quick-Freeze-Verfahrens. Die Anweisung kann nur einmal erfolgen und ist auf einen Zeitraum von 21 Tage beschränkt. Die richterliche Anordnung der Speicherung (preservation order) hat eine (einmalige) Gültigkeitsdauer von 90 Tagen. Die (polizeilichen) Anordnungen der Aufbewahrung von Verkehrsdaten sollen die endgültige Beschlagnahme bzw. den richterlichen Beschluss zur Herausgabe gewährleisten[350]. Die Canadian Association of Chiefs of Police setzt sich seit den 1990er Jahren für eine Modernisierung der Telekommunikationsüberwachungsgesetzgebung (die aus den 1970er Jahren stammt) und vor allem für den einfachen Zugang (ohne richterliche Anordnung) von Bestandsdaten der Telekommunikation ein. Dabei wird besonderer Bedarf an Telekommunikationsverkehrsdaten für Ermittlungen gegen kriminelle Gangs und organisierte Kriminalität sowie den Schutz von Kindern vor Sexualstraftätern im Internet hervorgehoben[351].

Australien[352] hat bislang ebenso wie Neuseeland[353] keine Speicherungspflicht für Telekommunikationsverkehrsdaten implementiert. Die Abfrage von Telekommunikationsdaten setzt

---

347 Zusammenstellung der Unterlagen aus dem Anhörungsverfahren in Nevis Consulting Group Inc., 2003.

348 *Gilbert, D., Kerr, I.R., McGill, J.*: The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers. Criminal Law Quarterly 51(2007), S. 469-507, S. 483ff.

349 Bill C-46, Legislative Summary: Investigative Powers for the 21st Century Act. Library of Parliament, Ottawa 2009, S. 6.

350 Bill C-46, Legislative Summary: Investigative Powers for the 21st Century Act. Library of Parliament, Ottawa 2009, S. 6.

351 *Canadian Association of Chiefs of Police:* Media Release. "Canadian Association of Chiefs of Police calls on Government to update Canada's Lawful Access laws". www.cacp.ca/index/viewsearch?contentId=405; *Canadian Association of Chiefs of Police*: Letter to the Prime Minister of Canada. Re: Modernization of Canada's Electronic Surveillance Laws (Lawful Access): Access to Subscriber Information. www.cacp.ca/index/viewsearch?contentId=731 [Juni 2011].

352 *Mallesons, S. J.*: Australia. In: Global Legal Group (Hrsg.): Telecommunication Laws and Regulations 2010. www.ICLG.co.uk, S. 38-44 [Juli 2010].

eine richterliche Anordnung voraus. In Australien wird derzeit aber eine der Richtlinie 2006/24 vergleichbare Gesetzgebung erörtert[354]. Die australische Bundesanwaltschaft hat im Jahr 2008 anlässlich einer nationalen Konferenz über Telekommunikation mitgeteilt, dass in Überlegungen eingetreten werde, wie eine der Richtlinie 2006/24 entsprechende Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten in Australien umgesetzt werden könne[355]. Jedoch gehen entsprechende Überlegungen wohl weiter zurück. Berichtet wird, dass die Bundesanwaltschaft seit mehr als 10 Jahren mit Telekommunikationsunternehmen Gespräche darüber führt, wie ein Vorratsdatenspeicherungsregime umgesetzt werden könne[356]. Im Vordergrund steht die Befürchtung, dass die Entwicklung der Telekommunikation zu einer Reduzierung der von Unternehmen gespeicherten und damit auch für Gefahrenabwehr oder Strafverfolgung zugänglichen Verkehrsdaten führen werde[357]. Ein Antrag auf Zugang zu den Dokumenten, die aus den bisherigen Konsultationen mit Telekommunikationsunternehmen resultierten, wurde zunächst negativ beschieden und schließlich mit einem weitgehend zensierten Dokument beantwortet, aus dem sich wenig inhaltliche Informationen ergeben[358].

3. Entwicklungen in Europa

In England/Wales wird der Zugang zu Telekommunikationsdaten (einschließlich Bestands- und Verkehrsdaten) in Teil I, Kapitel 2 des Gesetzes zur Regelung von Ermittlungsbefugnissen geregelt (RIPA, Regulation of Investigatory Powers Act 2000)[359]. Der Zugang wird erlaubt für Polizeibehörden, Zoll, Geheimdienste und die Finanzbehörden. RIPA bezieht sich auf drei Arten von Telekommunikationsdaten: Verkehrsdaten, Nutzungsdaten und Nutzerdaten. Ein Code of Practice legt die Bedingungen fest, unter denen Angehörige der genannten

---

353 *Webb, M.G.F.*: New Zealand. In: Global Legal Group (Hrsg.): Telecommunication Laws and Regulations 2010. www.ICLG.co.uk, S. 190-195 [Juli 2010].

354 www.ZDNet.com.au [16. Juni 2010].

355 http://www.ag.gov.au/www/agd/agd nsf/Page/AbouttheDepartment_Speeches_2008_NationalTelecommunicationsConferenceBrisbane-14August2008?open&query=about%20the%20department%20speeches%20telecommunications%20conference [Juni 2011].

356 www.securecomputing.net.au/News/217843,feds-launch-online-privacy-inquiry.aspx [Juni 2011].

357 Attorney-General's Department: Carrier-Carriage Service Provider Data Set. Consultation Paper. Version 1.0.

358 Vgl. Attorney-General's Department: Carrier-Carriage Service Provider Data Set. Consultation Paper. Version 1.0; abrufbar unter www.images.smh.com.au/file/2010/07/23/1710367/Secret-Document.PDF?rand=1279847709475 [Juli 2010].

359 *Walker, C., Akdeniz, Y.:* Anti-Terrorism Laws and Data Retention: War is Over? Northern Ireland Legal Quarterly 54(2003), S. 159-182.

Behörden auf diese Datenbestände zugreifen dürfen.[360] Die Polizei selbst (genau bestimmte Dienstgrade) hat das Recht, Abfragen anzuordnen. Bis zur Einführung der Pflicht zur Verkehrsdatenspeicherung beruhte die Speicherung der Verkehrsdaten auf freiwilligen Vereinbarungen, die der Innenminister mit Telekommunikationsversorgern abschließen konnte. Die Möglichkeit der Einführung zwingender Vorschriften sind bereits in RIPA sowie im Anti-Terrorism, Crime and Security Act 2001 angelegt. Für bestimmte Verkehrsdaten war von den meisten Telekommunikationsfirmen in England eine Speicherung von zwölf Monaten vorgesehen. Insoweit wurden die Bedürfnisse der Strafverfolgungspraxis in Kombination mit RIPA offensichtlich auch ohne gesetzlichen Zwang zur Speicherung weitgehend erfüllt. Zum 1. Oktober 2007 sind dann die Data Retention (EC Directive) Regulations 2007 in Kraft getreten, die in Umsetzung der EU-Richtlinie 2006 die Pflicht zur Speicherung von Verkehrsdaten für einen Zeitraum von 12 Monaten vorsehen. Zum 6. April 2009 traten weitere Vorschriften in Kraft (Electronic Communications. The Data Retention [EC Directive] Regulations 2009), die sich auf Internetverbindungen beziehen. Im Jahr 2009 hat das englische Innenministerium ein Dokument zur Konsultation aufgelegt, aus dem sich Hinweise ergeben, dass die Vorratsspeicherungsbestimmungen angesichts schneller technischer Entwicklungen beträchtlich erweitert werden soll[361]. Noch unter der vormaligen Labor-Regierung war dies Teil eines Programms zur Modernisierung der Überwachung (Interception Modernization Programme), das bei Investitionen von 2 Milliarden GBP bis zum Jahr 2016 realisiert werden sollte. Die neue konservativ-liberale Regierung scheint allerdings an der vollständigen Umsetzung des Programms wenig Interesse zu haben und ist programmatisch wohl eher auf eine Reduzierung von präventiv angelegten und möglichst umfassenden Datensammlungen ausgerichtet[362].

Berichte zu englischen Erfahrungen mit der Abfrage gespeicherter Verkehrsdaten verweisen auf verschiedene Fallgruppen, in denen von einem erheblichen Nutzen der Abfrage und mittelbar der Vorratsdatenspeicherung ausgegangen wird. Dabei geht es zunächst um die über oder durch Telekommunikationstechnik begangene Straftaten, die keinen anderen Kontakt zwischen Täter und Opfer und damit keine anderen Ermittlungsansätze mit sich brachten[363]. Sodann handelt es sich ganz allgemein um die Identifizierung von Tatverdächtigen, ihre

---

360 *Rowland, D.*: Data Retention and the War Against Terrorism – A Considered and Proportionate Response? The Journal of Information, Law and Technology 2004; www2.warwick.ac.uk/fac/soc/law/elj/jilt/2004_3/rowland/ [Juni 2011].

361 Secretary of State for the Home Department: Protecting the Public in a changing Communications Environment. London, April 2009; zu kritischen Punkten vgl. vor allem London School of Economics Policy Engagement Network: Briefing on the Interception Modernisation Programme. London 2009.

362 *Cameron, D., Clegg, N.*: The Coalition: our programme for government. Cabinet Office, London, S. 11: Unter dem Punkt "Civil Liberties" wird ein Ende der Speicherung von Internet- und Emaildaten ohne vernünftige Gründe angekündigt.

363 *Gaspar, R.*: NCIS Submission on Communications Data Retention Law. On behalf of A.C.P.O. and A.C.P.O (S), H.M. Customs and Excise Security Service, Secret Intelligence Service, and G.C.H.Q. Looking to the Future. Clarity on Communications Data Retention Law. Submission to the Home Office For Legislation on Data Retention. London, 21. August, 2000, Nr. 2.1.3.

„kriminellen“ Kontakte, Beziehungen zwischen Tatverdächtigen, Einordnung Tatverdächtiger in Zeit und Raum sowie die Feststellung von Bankkonten und Hinweise auf Geldwäscheaktivitäten. Eine zweite Fallgruppe betrifft Tötungsdelikte (sowie generell Todesfälle), für die die Analyse von Kommunikationsdaten der Toten Erkenntnisse zu Bewegungen und Kontakten vor dem Todeseintritt liefern kann. Für Opfer von Sexualdelikten wird die Verbesserung der Beweislage in Fällen genannt, in denen der Täter vorgibt, vorherigen Kontakt zum Opfer gehabt zu haben. In diesem Zusammenhang wird auch darauf hingewiesen, dass gerade Opfer von Sexualstraftaten erfahrungsgemäß – und dies wird durch die Opferforschung gestützt – nicht sofort Anzeige erstatten, sondern mitunter erst nach mehreren Monaten. Schließlich werden der Schutz von Kindern in „Online-Umgebungen” und die präventiven und repressiven Strategien des „Child Exploitation and Online Protection Centre”[364] als herausragende Anwendungsfelder der Nutzung von Telekommunikationsverkehrsdaten betont[365]. Die Identifizierung von Nutzern von Prepaid-Simkarten wird ebenfalls als Grund für eine langfristige Speicherung von Verkehrsdaten herangezogen.

Systematische empirische Untersuchungen zur Nutzung gespeicherter Verkehrsdaten liegen über die allgemeine Statistik hinaus nicht vor[366]. Im Übrigen sind die bisherigen Angaben zu den Straftaten, die Anlass zur Abfrage von Verkehrsdaten gaben, allgemein gehalten. Hinsichtlich der Bewertung der Speicherungsdauer, die in England (bei der Interesse verschiedener Sicherheitsbehörden an einer sehr viel weiter gehenden Speicherungsdauer[367]) auf 12 Monate festgelegt wurde, werden unterschiedliche Stellungnahmen abgegeben[368]. Jedenfalls ist nach derzeitigen Schätzungen lediglich ein kleiner Teil der Abfragen auf Zeiträume, die über 2 Monate zurückreichen, bezogen[369].

In der Schweiz wurde durch das Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs 2000 eine Speicherungspflicht mit einer Dauer von 6 Monaten eingeführt. Art. 23 des im Mai 2010 eingebrachten Vorentwurfs zu einem Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) sieht nunmehr neben der Ausdehnung der Speicherungspflichten auf Internetzugangsdaten auch eine Erweiterung der Speiche-

---

364 www.ceop.gov.uk/ [Juni 2011]; vgl. auch Child Exploitation and Online Protection Centre: Annual Review 2009-2010. London 2010

365 Explanatory Memorandum to the Data Retention (EC Directive) Regulations 2009. London 2009, No. 859, S. 2.

366 Zusammenfassend *Walker, C.*: Data retention in the UK: Pragmatic and proportionate, or a step too far? computer law & security review 25(2009), S. 325-334.

367 *Gaspar, R.*: a.a.O., 2000, Nr. 6.1.1.

368 Home Office: A Consultation Paper – Transposition of Directive 2006/24/EC. London 2008, S. 10, wo von der Notwenigkeit einer mindestens zwölfmonatigen Speicherung ausgegangen wird, sowie die kritische Stellungnahme von Walker, C.: a.a.O., 2009, S. 331 f.

369 *Milford, P.*: The retention of communications data: a view from industry. PLC IP& IT, 19. 11. 2008, www.ld.practicallaw.com/5-384-0822 [Juli 2010], geht von weniger als 2% aus.

rungsdauer auf 12 Monate vor[370]. Finnland und die Tschechische Republik haben ebenfalls eine Speicherungsdauer von 6 Monaten angesetzt. Auch Rumänien hatte sich für eine 6-Monatsfrist der Speicherung mit dem Gesetz no. 298/2008 entschieden, das nunmehr aber durch die Entscheidung des Verfassungsgerichts für nichtig erklärt wurde (siehe dazu gleich unten Pkt. 4.4.).

Frankreich, Dänemark und Spanien haben eine Speicherungsdauer von 12 Monaten eingeführt (Frankreich: Décret n° 2006-358 du 24 mars 2006 relatif à la conservation des données des communications électroniques[371]; Spanien: Gesetz zu Conservación de datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones (Nr. 25/2007), vom 18. Oktober 2007). Italien (Dekret 259/2003, "Codice delle comunicazioni elettroniche", Dekret 196/2003, "Codice in materia di protezione dei dati personali, sowie das so genannte "decreto Pisanu") und Irland haben bereits längere Speicherungsfristen implementiert, und zwar Italien mit einer Dauer von 2 Jahren (mit Verlängerungsmöglichkeit bis zu 4 Jahren für Telefondaten, Internetverbindungsdaten: 6 Monate) und Irland von 3 Jahren (allerdings ebenfalls begrenzt auf Telefonverbindungsdaten; Irish Criminal Justice (Terrorist Offences) Act, 2005). In Irland wurde im Juli 2009 ein Reformgesetz vorgelegt (Communications [Retention of Data] Bill 2009), das die Speicherung von Telefondaten auf 2 Jahre und die von Internetverbindungen auf 1 Jahr festsetzt[372]. Am 29. April 2010 ging der Entwurf in die Zweite Lesung. Am 5. Mai 2010 wurde eine Klage der Digital Rights Ireland Limited gegen das Vorratsdatengesetz vor dem Obersten Gericht zugelassen, mit der die Aufhebung des Gesetzes wegen Verstoßes gegen die Europäische Menschenrechtskonvention (Art. 8) angestrebt wird[373].

In den Niederlanden war zunächst in einem Gesetzesentwurf zur Umsetzung der Europäischen Richtlinie eine Speicherungszeit für Telefon- und Internetverbindungsdaten von 18 Monaten vorgesehen. Die Vorlage ist vom niederländischen Datenschutzbeauftragten kritisch gewürdigt worden, der unter Berufung auf neuere Stellungnahmen der Art. 29 Arbeitsgrup-

---

370 Vorentwurf Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vom 30. 4. 2010 sowie Erläuternder Bericht zur Änderung des Bundesgesetzes vom 6. Oktober 2000 betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF) http://www.ejpd.admin.ch/content/ejpd/de/home/themen/sicherheit/ref_gesetzgebung/ref_fernmeldeueberwachung html [Juni 2011].

371 Frankreich hat im Übrigen im Gesetz Nr. 2006-64 vom 23. Januar 2006 (relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers), Journal Officiel du 24 janvier 2006 mit dem Wegfall des Richtervorbehalts den Zugang zu Verkehrsdaten erleichtert (gebilligt durch das Verfassungsgericht, vgl. Conseil Constitutionelle, Décision n° 2005-532 DC vom 19. Januar 2006).

372 Kritisch hierzu Irish Council for Civil Liberties: Submission on the Communications (Retention of Data) Bill 2009, as initiated November 2009. Dublin 2009. insbesondere aus der Perspektive von Art. 8 der EMRK sowie der Entscheidung des EGMR S. and Marper v. UK, Application nos. 30562/04 and 30566/04, 4 December 2008.

373 The High Court, Draft Judgement/Ruling of Justice William McKechnie, 2006/3785P, 5. 5. 2010.

pe[374] eine Orientierung am Minimum der EU Richtlinie für angemessen ansieht, im Übrigen aber ebenso wie die Europäischen Datenschutzbeauftragten bei der Vorratsspeicherung von Verkehrsdaten Art. 8 der Europäischen Menschenrechtskonvention als berührt betrachtet[375]. Eingeführt wurde schließlich eine Speicherungsdauer von 12 Monaten[376]. Neuere Stellungnahmen des niederländischen Justizministeriums verweisen ebenso wie die vormalige Laborregierung in England in der Begründung des Modernisierungsprogramms der Überwachung, auf Veränderungen der Telekommunikationstechnik, die auch neue Probleme und Anforderungen für die Überwachung zum Zwecke der Strafverfolgung mit sich brächten. Jedenfalls klingen in der Mitteilung zur Evaluation der Umsetzung der Richtlinie 2006/24 des niederländischen Justizministeriums an die Europäische Kommission erhebliche Zweifel an der Effizienz der derzeitigen Regelungen an.[377]

Der Umsetzung der Europäischen Richtlinie in Österreich war ein langjähriger Streit vorausgegangen, ob zum Vorrat gespeicherte Verkehrsdaten eventuell auch für die Verfolgung von weniger schweren Straftaten insgesamt und im Besonderen von Urheberrechtsverletzungen genutzt werden sollten. Der österreichische Datenschutzrat ebenso wie die Rechtsanwaltskammer und andere Berufs- und Standesorganisationen die Vorratsdatenspeicherung grundsätzlich ab.[378].Die vom Infrastrukturministerium verantwortete und im Vorbereitungsstadium vom Ludwig-Boltzmann-Institut für Menschenrechte begleitete Gesetzesänderung entschied sich für eine 6-monatige Speicherfrist bei gleichzeitiger Begrenzung des Zugriffs auf schwere Straftaten (siehe dazu gleich unten Pkt. 4.3.). Dasselbe gilt für das – vom Parlament inzwischen wieder ausgesetzte – Umsetzungsgesetz in Schweden (Pkt. 4.5.).

Belgien ist bislang nicht über das Stadium eines Entwurfs hinausgekommen.[379] Im Entwurf wird eine Speicherungsdauer nicht fixiert. Vielmehr soll diese durch ein Dekret festgelegt werden[380]. Der Plan einer baldigen Umsetzung der Richtlinie im Hinblick auf die EU-Ratspräsidentschaft Belgiens im zweiten Halbjahr 2010[381] konnte wegen der Vakanz in der

---

374 Article 29 Arbeitsgruppe Opinion 3/2006 sowie Opinion 4/2005.

375 Opinion from the Dutch Data Protection Authority (Dutch DPA) [College bescherming persoonsgegevens (CBP)] Legislative proposal (Bill) for implementation of the European Directive on Data Retention, Pertaining to the tender letter of 22 January 2007, S. 2.

376 Wet van 18 juli 2009 Staatsblad van het Koninkrijk der Nederlanden 2009.

377 Ministerie van Justitie: evaluatie van de Richtlijn 2006/24/EG. Schreiben an Commissioner Cecilia Malmström, Europäische Kommission vom 1. Juli 2010; allerdings sind dem Schreiben keine Angaben über die niederländische Praxis der Nutzung gespeicherter Verkehrsdaten zu entnehmen.

378 www.computerwelt.at/detailArticle.asp?a=125962&n=4, 15.01.2010 [Juni 2011].

379 L'avant-projet de loi et au projet d'arrêté royal en matière de rétention de données et au projet d'arrêté royal relatif à l'obligation de collaboration (A/09/012).

380 Kritisch hierzu La Commission de la protection de la vie privée: Avis n° 20/2009 du 1er juillet 2009; www.privacycommission.be/fr/docs/Commission/2009/avis_20_2009.pdf [Juni 2011].

381 Ministère de Justice: Note de Débat Conçernant la Rétention de Données. Bruxelles 2010.

Neubildung einer Regierung auf der nationalen Ebene nicht verwirklicht werden (zu der Situation in Belgien auch gleich unten Pkt. 4.1.).

Insgesamt gesehen war somit bislang im Prozess der Implementierung der Europäischen Richtlinie ein Trend zur Vereinheitlichung der durch sicherheitspolitische Erwägungen begründeten Rahmenbedingungen der Telekommunikation (wie durch die Richtlinie beabsichtigt) nicht angelegt. Unsicherheit und Unterschiede werden deutlich, wenn die Zielsetzung der Schaffung gleicher Rahmenbedingungen für den Wettbewerb der Telekommunikationsunternehmen in das Blickfeld rückt. Dies wird gerade in der Behandlung von mit der Implementierung der Vorratsspeicherung entstehenden Kosten sichtbar. Die englische Regelung von 2007 sieht in § 10 vor, dass das Innenministerium Kosten, die aus der Umsetzung der Vorratsspeicherung folgen, ersetzen kann. Die Übernahme der Kosten steht jedoch unter der Bedingung der Mitteilung der Kosten durch die Betreiberfirma und der Verständigung zwischen Unternehmen und Regierung über die Höhe der Aufwendungen. In Frankreich werden gestaffelte Tarife eingeführt (Art. R. 213-1 Décret n° 2006-358 du 24 mars 2006), in die auch die mit der Implementierung der Vorratsspeicherung verbundenen Kosten aufgenommen werden sollten. Damit hat die französische Gesetzgebung auf eine Entscheidung des Verfassungsgerichts reagiert, das im Jahr 2000 grundsätzlich festgestellt hat, dass der Staat die durch öffentliche Interessen begründete Verpflichtung zur Schaffung von Abhörkapazitäten in Telekommunikationsunternehmen nicht entschädigungslos setzen darf.[382] Der österreichische Entwurf stellt darauf ab, dass Mehrkosten nicht absehbar seien und enthält sich einer Regelung.[383] Das spanische Gesetz sieht vor, dass alle Kosten für Anpassungsmaßnahmen auf der Seite der Telekommunikationsunternehmen zu deren Lasten gehen[384].

4. Länderberichte zu ausgesuchten Rechtsordnungen

4.1. Belgien

Belgien gehört zu den Ländern, welche die Richtlinie 2006/24/EG bislang nicht umgesetzt haben. Gründe hierfür sind einerseits der innenpolitische Dissens über die Umsetzung der Richtlinie per se, andererseits aber auch die insgesamt angespannte innenpolitische Situation, welche seit Juni 2007 in diversen Regierungskrisen und schließlich der Einsetzung einer kommissarischen Regierung im Frühling 2010 ihren Niederschlag gefunden hat.

Zwar wurden bereits diverse, zum Teil sehr weitgehende Umsetzungsvorschläge und Entwürfe für ein entsprechendes Änderungsgesetz vorgelegt, diese sind in der Bevölkerung und bei

---

382 Entscheidung Nr. 2000-441, DC vom 28. Dezember 2000.

383 61/ME XXIII. GP - Ministerialentwurf – Materialien, S. 1.

384 Boletin Oficial de Las Cortes Generales, VIII LEGISLATURA, Serie A: PROYECTOS DE LEY 11 de junio de 2007 Núm. 128-9, S. 67.

Bürgerrechtsorganisationen jedoch auf massive Kritik gestoßen. Widerstand kommt auch von den Internetanbietern, die nicht bereit sind, die bei der Datenspeicherung anfallenden hohen Kosten zu tragen. Besonders umstritten ist ferner die Reichweite der zu implementierenden Richtlinie. Der Ausschuss für den Schutz des Privatlebens (Privacy Commission)[385] hat bereits negative Gutachten über den Entwurf für eine Gesetzesänderung eingeholt.

Obwohl die Richtlinie 2006/24/EG bislang nicht förmlich umgesetzt wurde, ist die Europäische Kommission der Ansicht, dass die derzeit in Belgien bestehende Rechtslage den Vorgaben der Richtlinie genügt.[386]

4.1.1. Zugriffsmöglichkeiten auf Verkehrsdaten nach der akuellen Rechtslage

Die Speicherung und der Zugriff auf Verkehrsdaten richten sich derzeit nach dem Telekommunikationsgesetz von 2005.[387] Ausgangspunkt ist eine generelle Löschungs- bzw. Anonymisierungsverpflichtung für sämtliche Verkehrsdaten. Art. 122 § 1 Abs. 1 belg. TKG lautet in der offiziellen deutschen Übersetzung wie folgt: *Sobald Verkehrsdaten, die sich auf Teilnehmer beziehungsweise Endnutzer beziehen, für die Übertragung einer Nachricht nicht mehr benötigt werden, werden sie von den Betreibern aus ihren Verkehrsdaten gelöscht oder anonymisiert.*

Dabei werden Verkehrsdaten in Art. 2 Nr. 6 belg. TKG legal definiert als *„Daten, die zum Zwecke der Weiterleitung einer Nachricht über ein elektronisches Kommunikationsnetz oder zum Zwecke der Fakturierung einer solchen Nachricht verarbeitet werden“*. Elektronische Kommunikationsnetze sind gem. Art. 2 Nr. 3 belg. TKG *„aktive oder passive Übertragungssysteme und gegebenenfalls Vermittlungsstellen oder Leitwegeinrichtungen sowie anderweitige Ressourcen, die die Übertragung von Signalen über Kabel, Funk, optische oder andere elektromagnetische Ausrüstungen ermöglichen, soweit sie zur Übertragung von anderen als Rundfunk- und Fernsehsignalen verwendet werden“*. Aus der Gesetzesbegründung zum belg. TKG ergibt sich, dass diese Definitionen auch die Internetkommunikation mit erfassen sollen.

Von der generellen Speicher- und Anonymisierungspflicht des Art. 122 § 1 Abs. 1 belg. TKG machen Art. 122 § 1 Abs. 2 und Art. 122 §§ 2-4 belg. TKG eine Ausnahme, sofern die Daten für Abrechnungszwecke benötigt werden und der Kunde der Speicherung seiner Daten zugestimmt hat oder die Daten zu Zwecken der Strafverfolgung benötigt werden. Art. 126 § 1 belg. TKG sieht vor, dass *„der König die Bedingungen fest(legt), unter denen Betreiber im*

---

385 Siehe oben Fn. 380. Informationen unter www.privacycommission.be [Juni 2011].

386 Ludwig-Boltzmann-Institut für Menschenrechte, Rechtsvergleichende Analyse im Hinblick auf die Umsetzung der Richtlinie 2006/24/EG über die Vorratsdatenspeicherung, S. 8.

387 Loi relative aux communications électroniques (Gesetz über die elektronische Kommunikation); eine deutsche offizielle in deutscher Sprache wurde im belgischen Staatsblatt vom 26. Januar 2007 veröffentlicht; online abrufbar unter: www.ibpt.be/GetDocument.aspx?forObjectID=2141&lang=de [Juni 2011].

Hinblick auf Verfolgung und Ahndung strafrechtlicher Verstöße […] Verkehrs- und Identifizierungsdaten von Endnutzern aufzeichnen und aufbewahren". Ein entsprechendes königliches Dekret ist bislang allerdings nicht ergangen, sodass derzeit keine Daten speziell zu Strafverfolgungszwecken gespeichert werden. Über Art. 126 § 1 belg. TKG wäre es jedoch möglich, die Vorgaben der RL 2006/24/EG in das belg. TKG zu implementieren.

Die Verarbeitung von Standortdaten richtet sich nach Art. 123 belg. TKG. Sie dürfen nur anonymisiert verarbeitet werden, es sei denn, die Verarbeitung erfolgt im Zusammenhang mit der Bereitstellung eines Dienstes und der Teilnehmer hat in diese Form der Verarbeitung eingewilligt. Ausnahmen sind gem. Art. 123 § 5 belg. TKG bei der Bearbeitung von Notrufen möglich.

Explizit verboten sind die vorsätzliche Kenntnisnahme von Inhalten, die vorsätzliche Identifizierung der Gesprächspartner sowie jede Form der Verwendung von vorsätzlich oder nicht vorsätzlich erlangten Daten, Art. 124 belg. TKG. Das rechtswidrige Abhören von Telefongesprächen sowie die rechtswidrige Verwendung von Inhaltdaten durch Beamte werden in Art. 259bis belg. Strafgesetzbuch (SGB) unter Strafe gestellt; für Nichtbeamte enthält Art. 314bis belg. SGB einen entsprechenden Straftatbestand. Art. 259bis Abs. 5 belg. SGB hält weitreichende Sonderregelungen für Geheimdienste bereit. Desweiteren normiert Art. 125 belg. TKG diverse Ausnahmen für die in Art. 124 belg. TKG, Art. 259bis und Art. 314bis belg. SGB niedergelegten Grundsätze. Besonders hervorzuheben ist Art. 125 § 1 Nr. 1 belg. TKG, welcher Art. 124 belg. TKG, Art. 259bis und Art. 314bis belg. SGB für nicht einschlägig erklärt, sofern *„das Gesetz die erwähnten Handlungen erlaubt oder auferlegt"*. Auch diese Norm eröffnet eine Möglichkeit zur Umsetzung der RL 2006/24/EG in das belg. TKG.

Hinsichtlich der zulässigen Speicherdauer besteht in Belgien derzeit keine genaue Regelung. Gemäß Art 126 § 2 belg. TKG ist für deren Erlass der König zuständig[388]; das entsprechende königliche Dekret wurde bislang aber noch nicht angenommen. Die tatsächlichen Speicherfristen der einzelnen Telekommunikationsanbieter variieren daher aktuell sehr stark und ergeben sich nur aus den allgemeinen Geschäftsbedingungen der Unternehmen. So speichert beispielsweise Belgacom Verkehrsdaten bis zu 12 Monate; Kundendaten hingegen werden von Belgacom bis zu 10 Jahre nachdem der Kunde seine Vertragsbeziehungen zu dem Unternehmen beendet hat, gespeichert. Base speichert beide Datenarten einheitlich bis zu zwei Jahre nach Beendigung der Vertragsbeziehung. Mobistar legt keine maximale Speicherdauer fest, sondern behält sich vor, sämtliche Daten so lange zu speichern, wie dies notwendig ist.

---

388 Art. 126 § 2 belg. TKG lautet wie folgt: „Aufzubewahrende Daten und Dauer dieser Aufbewahrung, die bei öffentlich zugänglichen Telefondiensten zwischen zwölf und sechsunddreißig Monaten liegen muss, werden vom König nach Stellungnahme des Ausschusses für den Schutz des Privatlebens und des Instituts durch einen im Ministerrat beratenen Erlass festgelegt."

Der Zugriff auf die zu Abrechnungszwecken gespeicherten Daten wird in zwei Artikeln des belgischen Strafprozessgesetzbuches (SpGB) geregelt.[389] Art. 46bis belg. SpGB regelt, unter welchen Voraussetzungen ein Staatsanwalt auf die Kundendatenbank eines TK-Anbieters zugreifen darf. Er ist in all denjenigen Fällen einschlägig, in denen keine Zwangsmaßnahmen durchgeführt werden. Ist hingegen die Durchführung von Zwangsmaßnahmen erforderlich, ist der Zuständigkeitsbereich des Ermittlungsrichters eröffnet. In diesen Fällen richtet sich die Abfrage der gespeicherten Daten nach Art. 88bis belg. SpGB.

4.1.2. Die Bedeutung der Vorratsdatenspeicherung in Belgien

Die beiden Experten, mit denen im Rahmen der vorliegenden Studie gesprochen wurde, äußerten sich übereinstimmend dahingehend, dass eine einheitliche und verpflichtende Regelung zur Vorratsdatenspeicherung unabdingbar sei. Bemängelt wird v.a., dass jeder Anbieter nur diejenigen Daten speichere, die er für Abrechnungszwecke benötigt. Diese seien für eine effektive Strafverfolgung in der Regel nicht ausreichend. Insbesondere würden aufgrund neuer Tarifmodelle immer weniger Verbindungsdaten gespeichert werden. Auch die uneinheitliche Speicherdauer stelle ein großes Problem für die Ermittlungsbehörden dar. Da manche Anbieter die Daten nach eigenen Angaben so lange speicherten, wie dies im Einzelfall notwendig sei, ohne sich auf eine konkrete Speicherdauer festzulegen, könnten die Ermittler vorab nicht einschätzen, welche Daten ihnen zur Verfügung stehen. Aus diesem Grund sei es dringend notwendig, gesetzlich festzulegen, welche Daten die Telekommunikationsanbieter für welchen Zeitraum speichern müssen. Eine Speicherdauer von zwei Jahren wird dabei als unabdingbar erachtet; grundsätzlich sollten die Daten so lange wie möglich gespeichert werden.

Verbindungsdaten könnten grundsätzlich für die Aufklärung aller Straftaten von Bedeutung sein. In erster Linie werden hier sämtliche Formen der Computerkriminalität genannt; in diesem Bereich gebe es oft keine anderen Spuren als die Verkehrsdaten und daher auch keine anderen Ermittlungsansätze als die Daten. Aber auch bei einem zunächst als niedrigschwellig eingestuftes Delikt wie z.B. einem einfachen Diebstahl könne sich dann bei der Analyse von Verkehrsdaten herausstellen, dass eine größere kriminelle Vereinigung dahinter stehe. Die Analyse der Kommunikationsstrukturen sei daher bei vielen Straftaten Voraussetzung für eine umfassende Aufklärung. Problematisch sei zudem, dass die Polizei aufgrund eines verzögerten Anzeigeverhaltens der Opfer oft verzögert Kenntnis von einer Straftat erlangt. Damit könnten Verluste gerade bei den retrograden Daten auftreten, die für die Aufklärung von besonders großer Bedeutung seien.

Abschließend wird explizit darauf hingewiesen, dass Vorratsdaten auch zur Entlastung eine große Rolle spielen könnten. So könne bspw. die Unschuld eines Beschuldigten nachgewiesen werden, wenn dessen Computer gehackt und zur Begehung von Straftaten genutzt wurde.

---

389 Für den einschlägigen ersten Teil des belg. SpGB ist keine offizielle Übersetzung ins Deutsche verfügbar.

4.2. Bulgarien

In Bulgarien wurde die Richtlinie zur Vorratsdatenspeicherung durch das Gesetz über die elektronischen Meldungen (im Folgenden: EMG)[390], welches am 22.05.2007 in Kraft getreten ist, umgesetzt. Danach müssen die Telekommunikationsunternehmen alle in einer Verordnung genannten Daten zu Strafverfolgungszwecken sowie zum Schutz der nationalen Sicherheit zwölf Monate lang speichern, Art. 251 EMG. Explizit ausgenommen von dieser Speicherpflicht sind Inhaltsdaten jeglicher Art.

4.2.1. Verordnung Nr. 40 über die Datenspeicherung

Die zu speichernden Daten wurden gem. Art. 251 EMG in der Verordnung Nr. 40 über die Datenspeicherung vom 07.01.2008[391] (im Folgenden: VO40), welche ausdrücklich auf die Richtlinien 2006/24/EG und 2002/58/EG verweist, festgelegt. Im Einzelnen sind dies gem. Art. 3 VO40:

- für Festnetz und Mobilfunk die Rufnummer des anrufenden Anschlusses, Name und Anschrift des Teilnehmers bzw. des registrierten Benutzers
- bei der Internetnutzung (inkl. E-Mail und Internettelefonie): die zugewiesene Benutzerkennung, die Benutzerkennung und Rufnummer, welche jeder Meldung im öffentlichen Telefonnetz zugewiesen werden, sowie Name und Anschrift des Teilnehmers bzw. des registrierten Benutzers, dem eine IP-Adresse, eine Benutzerkennung oder eine Rufnummer zum Zeitpunkt der Kommunikation zugewiesen war
- die Rufnummer des angewählten Anschlusses sowie bei Zusatzdiensten wie Rufum- oder -weiterleitung die Nummer(n), an die der Anruf weitergeleitet wird, ferner Name und Anschrift der Teilnehmer bzw. registrierten Benutzer
- Benutzerkennung des Nutzers von Internettelefoniediensten, die Rufnummer des Empfängers sowie Name und Anschrift des Teilnehmers bzw. des registrierten Benutzers, ferner die Benutzerkennung des Empfängers einer Meldung
- Datum und Uhrzeit von Beginn und Ende einer Telekommunikationsverbindung bzw. bei der Nutzung von Internetdiensten Datum und Uhrzeit der An- und Abmeldung bei dem Internetzugangsdienst bzw. dem E-Mail-Provider bzw. dem Anbieter des Internettelefoniedienstes unter Bezugnahme einer bestimmten Zeitzone, zusammen mit der dem Nutzer zugewiesenen dynamischen oder statischen IP-Adresse sowie die Benutzerkennung des Teilnehmers bzw. des registrierten Benutzers
- das verwendete Telefon- und Mobilfunknetz bzw. der genutzte Internetdienst bei der Nutzung von Internet, E-Maildiensten und Internettelefonie
- die Rufnummer des anrufenden und des angerufenen Anschlusses bei der Nutzung eines Festnetzes

---

390 Staatsblatt Nr. 41 vom 22.05.2007.

391 Staatsblatt Nr. 9 vom 29.01.2008.

- bei der Nutzung eines Mobiltelefons darüber hinaus die IMSI- und die IMEI-Nummer des anrufenden und des angerufenen Mobiltelefons; im Falle voraus bezahlter anonymer Karten ferner Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Kennung der Funkzelle, in der der Dienst erstmals aktiviert wurde
- bei der Nutzung des Internets sowie von E-Mail- oder Internettelefoniediensten die angerufene Telefonnummer (Dial-Up), der digitale Teilnehmeranschluss (DSL) bzw. ein sonstiger Endpunkt der Verbindung
- die Funkzelle, in der sich der Nutzer bei Beginn der Verbindung befindet, sowie die Funkzellen, die während des Zeitraums, in dem die Verbindungsdaten gespeichert werden, genutzt werden.

Gem. Art. 5 Abs. 1 VO40 müssen die Telekommunikationsunternehmen einen passiven technischen Zugang durch ein Computerterminal für die operativ-technische Informationsdirektion des Innenministeriums bereitstellen. Abs. 2 verpflichtet die Telekommunikationsunternehmen zur Herausgabe der gespeicherten Daten, sofern dies zur Strafverfolgung erforderlich ist und von der Polizei, der Staatsanwaltschaft oder einem Gericht beantragt wird. Werden die Daten hingegen zum Schutz der nationalen Sicherheit benötigt, müssen die Telekommunikationsanbieter nach Art. 5 Abs. 3 VO40 den Diensten Zugang zu den gespeicherten Daten gewähren. Schließlich beinhaltet Abs. 4 noch eine ausdrückliche Verpflichtung, die Daten so zu speichern, dass bei Eingang einer entsprechenden Anfrage eine schnelle Weiterleitung der Daten an die zuständige Stelle gewährleistet ist. Art. 2 Abs. 1 VO40 wiederholt die bereits in Art. 251 Abs. 1 EMG normierte Speicherdauer von zwölf Monaten.

Besonders hervorzuheben ist Art. 6 VO40. Nach dieser Norm sollen alle Telekommunikationsunternehmen dem Innenminister bis zum 31. März eines jeden Jahres folgende Informationen bereitstellen:

- die Anzahl der Fälle, in denen den zuständigen Gefahrenabwehr- bzw. Strafverfolgungsorganen Daten bereitgestellt wurden
- die Dauer der Datenspeicherung von der Erhebung der Daten an bis zum Abfrage dieser Daten durch die zuständige Stelle
- sowie die Anzahl von Fällen, in denen eine Anfrage nicht beauskunftet wurde.

Diese Informationen stellt der Innenminister einmal pro Jahr der Europäischen Kommission zur Verfügung. Die bereitgestellten Angaben dürfen keine personenbezogenen Informationen enthalten.

4.2.2. Die Entscheidung des Obersten Verwaltungsgerichts vom November 2008

Im März 2008 rügte eine Nichtregierungsorganisation die Konventions- und Verfassungswidrigkeit der VO40 vor dem Obersten Verwaltungsgericht erster Instanz. Diese Beschwerde

wurde abgelehnt, ohne dass sich das Gericht zu den Art. 32 und 34 der bulg. Verfassung oder zur Art. 8 EMRK äußerte.[392]

Daraufhin wurde eine Kassationsbeschwerde vor dem Obersten Verwaltungsgericht zweiter Instanz eingelegt.[393] Dieses erklärte Art. 5 der VO40 am 12.11.2008 für gesetzeswidrig und hob ihn daher auf.[394]

Das Gericht kritisierte v.a., dass in Art. 5 VO40 von einem „passivem technischen Zugang" gesprochen werde. Dies sei nicht richtig, da der Zugang den zuständigen Behörden erst aufgrund einer schriftlichen Anfrage derselben möglich sei. Ferner begrenze Art. 5 VO40 den Zugriff nicht auf bestimmte Daten; dass die Daten für die „operativ-technische Informationstätigkeit" erforderlich sind, sei zu weit gefasst und biete keinen ausreichenden Grundrechtsschutz. Dies sei mit Art. 32 Abs. 1 der bulg. Verfassung, der die Unantastbarkeit des privaten Lebens der Bürger sowie die Nichteinmischung des Staates in das Privat- und Familienleben gewährleistet, nicht vereinbar. Ferner bemängelt das Gericht, dass kein Schutz vor einem Missbrauch der Daten in Art. 5 VO40 vorgesehen sei. Die angegriffene Norm verstoße daher gegen Art. 8 EMRK, gegen die Richtlinie zur Vorratsdatenspeicherung selbst sowie gegen die Art. 32 und 34 der bulg. Verfassung.

Von den Klägern war u.a. beanstandet worden, dass der Begriff der „schweren Straftaten" aus der EU-Richtlinie 2006/24/EG in der VO40 durch jenen der „Straftaten" ersetzt worden war. Dies wurde von dem Gericht jedoch nicht beanstandet, da der Begriff der Straftaten jenem des Art. 34 Abs. 2 bulg. Verfassung sowie des Art. 251 Abs. 1 EMG entspreche.

4.2.3. Die Änderungen des EMG

Nach dem Urteil des Obersten Verwaltungsgerichtes zweiter Instanz wurde am 06.03.2009 das EMG erstmals geändert.[395] Darin wurden v.a. ein Richtervorbehalt eingeführt und der Zugriff auf die Vorratsdaten zur Aufklärung von schweren Straftaten und Computerstraftaten begrenzt. Es folgten fünf weitere Versuche, das EMG zu ändern, bis am 17.02.2010 eine weitere Gesetzesänderung beschlossen wurde.[396]

Als besonders wichtige Neuerungen sind hervorzuheben, dass die Strafverfolgungsbehörden keinen direkten Zugriff mehr auf die gespeicherten Daten haben, wie das im Rahmen des „passiven technischen Zugangs" möglich sein sollte. Vielmehr bedarf jeder Zugriff auf gespeicherte Daten nun einer richterlichen Anordnung. Andererseits wurden der Kreis der zur

---

392 Entscheidung Nr. 8767; online verfügbar unter: www.aip-bg.org/pdf/reshenie_vas170708.pdf [Juni 2011].

393 Siehe: www.aip-bg.org/pdf/kas_jalba_naredba40.pdf [Juni 2011].

394 Entscheidung Nr. 13627; online verfügbar unter: www.aip-bg.org/pdf/reshenie%2013627_december%2008.pdf [Juni 2011].

395 Gesetzblatt Nr. 17 vom 06.03.2009.

396 Am 10.05.2010 in Kraft getreten.

Anordnung berechtigten Gerichte erheblich erweitert, sodass nun fast alle Regional- und Bezirksgerichte eine Verkehrsdatenabfrage anordnen können.

Welche Daten konkret gespeichert werden müssen, ist in dem neuen Art. 250a EMG nicht mehr so detailliert geregelt, wie dies in Art. 5 VO40 der Fall gewesen war. Vielmehr werden hier nur sechs Oberpunkte gebildet, deren genauer Inhalt nicht näher spezifiziert wird. So müssen nun all diejenigen Daten gespeichert werden, die notwendig sind

- zur Verfolgung und Identifizierung des Ursprungs einer Verbindung
- für die Identifikation einer Verbindungsrichtung
- zur Bestimmung von Datum, Uhrzeit und Dauer einer Verbindung
- zur Bestimmung der Verbindungsart
- zur Identifikation des Endgerätes sowie
- zur Bestimmung der genutzten Funkzelle.

Eine inhaltliche Änderung gegenüber der alten Norm in Art. 3 VO40 war damit aber wohl nicht bezwewckt worden.

Die Speicherdauer beträgt nach wie vor zwölf Monate. Neu ist hingegen die gesetzlich festgelegte Beauskunftungsfrist von 72 Stunden. Allerdings wurde nach Inkrafttreten des neuen Gesetzes eine Weisung des Innenministers erlassen, nach welcher die anfragebe-rechtigten Beamten die Beauskunftungsfrist selbst festlegen dürfen.[397] Auf diese Weise soll sichergestellt werde, dass dringende Fälle vor weniger dringenden Fällen bearbeitet werden. Die Kommunikation zwischen den berechtigten Stellen, dem zuständigen Gericht und den Telekommunikationsunternehmen hat nach dem neuen Gesetz auf elektronischem Weg zu erfolgen. Dadurch sollen die Beauskunftung beschleunigt und die Effektivität der Straf-verfolgung gesteigert werden. Werden die erlangten Daten von den berechtigten Behörden nicht zur Strafverfolgung genutzt, müssen sie nach sechs Monaten vernichtet werden.

Desweiteren wurden detaillierte Regelungen zum Datenschutz, zur Errichtung von Kontroll-stellen[398], sowie zur Information von Bürgern bei unrechtmäßigen Zugriffen geschaffen.

Im April 2010 wurde in Art. 171a bulg. Strafgesetzbuch ein neuer Straftatbestand geschaffen[399], welcher den rechtswidrigen Zugriff auf oder die rechtswidrige Verwendung von Verkehrsdaten, die nach dem EMG gespeichert und verarbeitet werden, unter Strafe stellt. Diese kann sich auf bis zu drei Jahren Freiheitsstrafe belaufen, sofern die Tat zu eigennützigen Zwecken begangen wird, liegt die Höchststrafe sogar bei fünf Jahren Freiheitsstrafe.

---

397 www.crc.bg/files/_bg/Zapoved_po_ZES_MVR_PravnaRamka.pdf [Juni 2011] (vgl. Art. 21 Punkt 11 des Gesetzes des Innenministeriums und Art. 250e Abs. 2 EMG).

398 Siehe: www.cpdp.bg/index.php und www.cpdp.bg/en/index.php [Juni 2011].

399 Staatsblatt Nr. 26 vom 06.04.2010.

Erwähnenswert ist eine weitere Gesetzesänderung, welche mit Wirkung vom 15.09.2009 in Kraft getreten ist.[400] Danach ist der Erwerb von vorausbezahlten Diensten, v.a. also von Prepaid-Karten, seit dem 1.1.2010 nur nach einer vorherigen Registrierung des Kunden möglich. Wer vor dem 1.1.2010 vorausbezahlte Dienste erworben hat, muss sich bis spätestens zum 31.12.2010 bei dem jeweiligen Kommunikationsunternehmen unter Angabe seines Namens, seiner Anschrift und seiner EGN[401] bzw. bei seiner Passnummer registrieren lassen. Sofern eine solche Registrierung nicht bis zum 31.12.2010 durchgeführt wird, soll der entsprechende Dienst, beispielsweise die SIM-Karte, gesperrt werden und nur noch das Absetzen von Notrufen möglich sein.

4.2.4. Abfragepraxis

Im Mai 2011 hat die parlamentarische Kommission für Rechtsfragen, die auch für die Kontrolle der Verkehrsdatenabfragen zuständig ist[402], einen Bericht über die Häufigkeit der Abfragen gem. Art. 250a EMG veröffentlicht.[403] In den Bericht flossen die Ergebnisse aus den Registern der Gerichte und von drei Telekommunikationsunternehmen[404] ein. Danach wurden zwischen dem 20. April 2010 und dem 20. April 2011 insgesamt 21.714 Anfragen auf Zugriff von Verkehrsdaten registriert. 378 Anfragen wurden von den Gerichten abgelehnt (1,7 %). Die übrigen Anfragen mündeten in insgesamt 21.605 richterliche Anordnungen. Diese vergleichsweise hohe Anzahl von Verkehrsdtenabfragen wird von der Kommission als bedenklich bewertet. Offensichtlich habe die letzte Gesetzesänderung zu einer verstärkten Nutzung der Zugriffsmöglichkeiten geführt. Das Gremium ruft die Errmittlungsbehörden und Justizorgane zu einem zurückhaltenderen Gebrauch auf und kündigt eine verstäkte Kontrolle der Abfragepraxis auf.

4.3. Österreich

Österreich hat lange gezögert, die EU-Richtlinie 2006/24/EG in das nationale Recht umzusetzen. Ein erster Gesetzesentwurf zur Änderung des Telekommunikationsgesetzes (öTKG) 2003 war zunächst im November 2009 vorgelegt worden.[405] Nach der Verurteilung durch den EuGH im Zuge des Vertragsverletzungsverfahrens[406] und einer Analyse des BVerfG-Urteils vom 2.3.2010 hat der österreichische Nationalrat am 28.4.2011 nunmehr die

---

400 Staatsblatt Nr. 74 vom 15.09.2009.

401 Spezielle Nummer, die jeder bulgarische Staatsbürger bei seiner Geburt zugewiesen bekommt.

402 Art. 261b EMG.

403 Bericht Nr. 153-03-61 vom 13.5.2011, www.parliament.bg/bg/parliamentarycommittees/members/226/reports/ID/27 [Juni 2011].

404 GLOBUL, M-TEL, WIWAKOM.

405 Die Entwürfe und eine Vielzahl von Stellungnahmen sind abrufbar unter www.parlinkom.gv.at/PG/DE/XXIV/ME/ME_00117/pmh.shtml [Juni 2011].

406 Rechtsache C-189/09, Urteil vom 29.7.2010, ABl. C 246/8 vom 11.9.2010.

Novellierung verabschiedet.[407] Eingeführt wird eine sechsmonatige Speicherpflicht nach exakt festgelegten Parametern. Das Gesetz[408] ist am 19.5.2011 in Kraft getreten, die Speicherpflicht selbst wird erst zum 1.4.2012 wirksam werden.[409] Die TK-Anbieter haben nach dem Gesetz Anspruch auf Erstattung von 80 Prozent der Personal- und Sachaufwendungen für die Umsetzung.[410] Ergänzende Änderungen wurden in der österreichischen StPO vorgenommen.[411] Eingefügt wurde u.a. eine eigene Rechtsgrundlage für den Zugriff auf Vorratsdaten, die im Wesentlichen auf die bisherige Regelung verweist (siehe dazu gleich unten Pkt. 4.3.1.1.).

Die Problembeschreibung, die sich aus dem Expertengespräch ergibt (siehe unten Pkt. 4.3.2.), bezieht sich auf die gegenwärtig noch maßgebliche Rechtslage.

4.3.1. Zugriffsmöglichkeiten auf Verkehrs- und Vorratsdaten

4.3.1.1. Auskunft über Daten

Das österreichische Recht unterscheidet künftig nicht nur telekommunikationsrechtlich, sondern auch bei der strafprozessualen Regelung des Zugriffs auf gespeicherte Daten zwischen Verkehrs- und Vorratsdaten. Die Vorratsdatenspeicherung selbst ist in § 102a öTKG geregelt, § 102b bestimmt, dass die Auskunft über Vorratsdaten ausschließlich auf der Grundlage der öStPO erfolgen darf.[412]

Rechtsgrundlage für die Abfrage von Verkehrsdaten ist § 135 Abs. 2 öStPO. Nach dieser Vorschrift ist die Auskunft über Daten einer Nachrichtenübermittlung zulässig. Hierunter fällt gem. § 134 Nr. 2 öStPO die Auskunft über Verkehrsdaten, Zugangsdaten und Standorten eines Telekommunikationsdienstes oder eines sog. Dienstes der Informationsgesellschaft[413]. Letzteres erfasst sämtliche Vorgänge im Internet. § 134 verweist für die Begriffsbestimmungen weiter auf das öTKG: danach sind

- „Verkehrsdaten“ Daten, die zum Zwecke der Weiterleitung einer Nachricht an ein Kommunikationsnetz oder zum Zwecke der Fakturierung dieses Vorgangs verarbeitet werden (§ 92 Abs. 3 Ziff. 4 öTKG),

---

407 1074 der Beilagen XXIV. GP.

408 Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 - TKG 2003 geändert wird, BGBl I 2011/27 vom 18.5.2011.

409 § 137 Abs. 4 öTKG neu.

410 § 94 Abs. 1 öTKG neu.

411 Bundesgesetz, mit dem die Strafprozessordnung 1975 und das Sicherheitspolizeigesetz geändert werden, BGBl I 2011/33 vom 20. 5. 2011.

412 § 102c enthält ferner die erforderlichen Protokollierungs- und Datenschutzbestimmungen. Die §§ 102a bis 102c öTKG-neu sind in Anhang D abgedruckt.

413 § 1 Abs. 1 Ziff. 2 des österr. Notifikationsgesetzes.

- „Zugangsdaten“ jene Verkehrsdaten, die beim Zugang eines Teilnehmers zu einem öffentlichen Kommunikationsnetz bei dem Betreiber entstehen und für die Zuordnung der zu einem bestimmten Zeitpunkt für eine Kommunikation verwendeten Netzwerkadressierungen zum Teilnehmer notwendig sind (§ 92 Abs. 3 Ziff. 4a öTKG), und
- „Standortdaten“ Daten, die in einem Kommunikationsnetz verarbeitet werden und die den geografischen Standort der Telekommunikationsendeinrichtung eines Nutzers eines öffentlichen Kommunikationsdienstes angeben (§ 92 Abs. 3 Ziff. 6 öTKG).

Soweit es sich bei den Verkehrsdaten um Vorratsdaten handelt, wird künftig § 135 Abs. 2a öStPO als eigene spezielle Rechtsgrundlage maßgeblich sein. Hierfür wurde mit § 134 Ziff. 2a öStPO eine eigene Verweisnorm auf die Legaldefinition des öTKG zu Vorratsdaten geschaffen. Danach sind

- „Vorratsdaten“ Daten, die ausschließlich aufgrund der Speicherverpflichtung gemäß § 102a öTKG gespeichert werden (§ 92 Abs. 3 Ziff. 6b öTKG).

Das Telekommunikationsgesetz enthält zudem eine gesetzliche Definition der Bestandsdaten, für deren Erhebung, ähnlich wie im deutschen Recht, eigene Regeln gelten (siehe dazu unten Pkt. 4.3.2.). Diese heißen in Österreich

- „Stammdaten“ und sind definiert als alle personenbezogenen Daten, die für die Begründung, die Abwicklung, Änderung oder Beendigung der Rechtsbeziehungen zwischen dem Benutzer und dem Anbieter oder zur Erstellung und Herausgabe von Teilnehmerverzeichnissen erforderlich sind; dies sind:

  a) Familienname und Vorname,
  b) akademischer Grad,
  c) Wohnadresse,
  d) Teilnehmernummer und sonstige Kontaktinformation für die Nachricht,
  e) Information über Art und Inhalt des Vertragsverhältnisses,
  f) Bonität (§ 92 Abs. 3 Ziff. 3 öTKG).

Auf die Verkehrsdaten darf gemäß § 135 Abs. 2 öStPO nur in vier enumerativ aufgezählten Fällen zugegriffen werden. Das ist möglich zunächst bei Verdacht einer Entführung, wenn angenommen werden kann, dass diese so beendet werden kann (Ziff. 1). Diese Konstellation ist sehr selten. Von Bedeutung können in einem solchen Kontext nach Auskunft des befraten Experten des österr. Bundeskriminalamtes vor allem Standortdaten und Gerätekennungen (IMSI-Nummern) sein. Die Maßnahme darf sich dabei nur gegen den mutmaßlichen Täter richten. Ergänzend kann in derartigen Fällen auch präventivrechtlich auf Verkehrsdaten zugegriffen werden.[414] Die Maßnahme bezieht sich dann gezielt auf das Opfer (bzw. dessen –

---

414 § 53 Abs. 3a österr. Sicherheitspolizeigesetz (SPG). Voraussetzung ist eine gegenwärtige Gefahr für Leben oder Gesundheit eines Menschen. Dies wurde im Zuge des StPO- und SPG-Änderungsgesetzes 2011 ausdrücklich auf Vorratsdaten erweitert.

meist mobile – Endgeräte) als unmittelbares Ziel der Gefahrenabwehrmaßnahme. Die zweite Fallgruppe erlaubt die Verkehrsdatenabfrage zur Aufklärung einer Straftat mit einer Mindeststrafe von 6 Monaten und mit – ausdrücklicher – Zustimmung des Inhabers der technischen Einrichtung (Ziff. 2). Dies zielt in der Praxis vor allem auf Bedrohungssituationen und ist mithin für Straftaten gedacht, bei denen die Maßnahmen von der Opferseite her eingesetzt werden wie im klassischen Fall der Fangschaltung.

Die dritte und für die Ermittlungspraxis wichtigste Einsatzmöglichkeit bezieht sich auf die Aufklärung einer vorsätzlich begangenen Straftat, für die eine Mindeststrafe von einem Jahr droht (Ziff. 3). Insoweit stellt das Gesetz eine allgemeine Ermächtigung zur Verfügung; sie steht aber unter dem Vorbehalt einer abstrakten Mindesttatschwere, die derjenigen bei der Inhaltüberwachung[415] entspricht.[416] Damit fallen zahlreiche Deliktsgruppen aus dem Bereich der IuK-Kriminalität aus dem Anwendunsgbereich heraus (siehe dazu gleich unter Pkt. 4.3.2.). Die Maßnahme muss darauf abzielen, Verkehrsdaten des Beschuldigten zu ermitteln, ist aber nicht, wie unter Ziff. 1, auf dessen Sphäre beschränkt. Formal ist die Ermächtigung, was den möglichen Adressatenkreis betrifft, mithin weiter als die deutsche Regelung in § 100a Abs. 3 StPO.

Die vierte Variante wurde mit der 2011er Änderung in die öStPO aufgenommen (Ziff. 4). Sie ermöglicht den Zugriff, wenn auf Grund bestimmter Tatsachen zu erwarten ist, dass dadurch der Aufenthalt eines flüchtigen oder abwesenden Beschuldigten, der einer vorsätzlich begangenen, mit mehr als einjähriger Freiheitsstrafe bedrohten strafbaren Handlung dringend verdächtig ist, ermittelt werden kann.

Die Zugriffsmöglichkeiten der Ziff. 1 bis 4 beziehen sich auf Verkehrsdaten, mit Ausnahme der Ziff. 1 können in diesen Fällen künftig auch Vorratsdaten abgefragt werden.[417]

Weitere Voraussetzungen sind in Fällen der Ziff. 1 dringender Tatverdacht sowie die Annahme, dass sich die Daten auf Nachrichten beschränken, von denen anzunehmen ist, dass sie zur Zeit der Freiheitsentziehung tatsächlich vom Beschuldigten übermittelt, empfangen oder gesendet werden. In den übrigen Varianten muss lediglich zu erwarten sein, dass durch die Maßnahme die Aufklärung der Straftat gefördert werden kann. Im Falle der Ziff. 3, die auch den Datenzugriff außerhalb der Sphäre des Beschuldigten erlaubt, verlangt das Gesetz ferner, dass aufgrund bestimmter Tasachen angenommen werden kann, dass durch den Zugriff Daten des Beschuldigten ermittelt werden können.

---

415 § 135 Abs. 3 öStPO; dazu unten Pkt. 4.3.1.2.

416 Österreich folgt dem Höchststrafensystem; anders als im deutschen Recht konstituiert die einjährige Mindeststrafe daher nicht die Verbrechensgrenze (vgl. § 17 öStGB). Faktisch fallen die Tatbestände mit einer solchen Mindeststrafandrohung aber meist doch in den Verbrechensbereich.

417 § 135 Abs. 2a öStPO-neu.

4.3.1.2. Überwachung von Nachrichten

§ 135 Abs. 3 öStPO regelt die Inhaltsüberwachung von Nachrichten. Die Maßnahme ist in § 134 Nr. 3 öStPO definiert als das Ermitteln des Inhalts von Nachrichten (§ 92 Abs. 3 Ziff. 7 öTKG), die über ein Kommunikationsnetz (§ 3 Ziff. 11 öTKG) oder einen sog. Dienst der Informationsgesellschaft[418] ausgetauscht oder weitergeleitet werden. Verkehrsdaten dürfen bei diesen Maßnahmen mit erhoben werden. Gleiches gilt für die Stammdaten. Die überwachten Anschlüsse werden zum Bundesministerium des Innern ausgeleitet, wo die Überwachung zentral für ganz Österreich durchgeführt wird.

Die vom Gesetz vorgesehenen Fallkonstellationen sind ähnlich denen für die Verkehrsdatenabfrage (Ziff. 1 bis 3; insoweit identisch mit Abs. 2 Ziff. 1 bis 3); zusätzlich ist die Maßnahme möglich bei Straftaten einer kriminellen oder terroristischen Vereinigung oder Organisation[419] (ebenfalls Ziff. 3) sowie zur Auffindung flüchtiger Personen bei Verdacht einer vorsätzlichen Straftat mit Strafandrohung von mehr als einem Jahr (Ziff. 4). In den Fällen der Ziff. 3 muss dringender Tatverdacht bestehen und darüber hinaus anzunehmen sein, dass die dringend tatverdächtige Person Inhaber oder mutmaßlicher Nutzer des überwachten Anschlusses ist; der überwachte Anschluss muss entweder Ursprung oder Ziel der überwachten Komunikation sein. Die Voraussetzungen sind somit sowohl im Hinblick auf den notwendigen Verdachtsgrad als auch im Hinblick auf die technischen Voraussetzungen enger als bei der Verkehrsdatenabfrage gem. § 135 Abs. 2 Ziff. 3 öStPO. Als mögliches Substitut für Fälle, in denen von den Anbietern keine Verkehrsdaten erhältlich sind, erscheint sie daher von vornherein wenig praktikabel.

4.3.1.3. Formalia

§§ 137, 138 öStPO regeln die formellen Voraussetzungen für Ermittlungsmaßnahmen nach § 135 öStPO. Abfrage-[420] bzw. anordnungsberechtigt[421] ist der Staatsanwalt auf der Grundlage einer richterlichen Bewilligung. Die Überwachung ist zu befristen.[422] Anders als die deutsche sieht die österr. StPO allerdings keine fix vorbestimmten Überwachungszeiträume vor. Der gewählte Zeitraum, der im Falle der Verkehrsdatenabfrage auch retrograd sein kann, muss für die Erreichung ihres Zwecks voraussichtlich erforderlich sein.[423] Neuerliche Anordnungen sind jeweils zulässig, soweit aufgrund bestimmter Tatsachen anzunehmen ist, dass die weitere Durchführung der Maßnahme Erfolg haben würde.

---

418 § 1 Abs. 1 Ziff. 2 des österr. Notifikationsgesetzes. Siehe dazu oben Pkt. 4.3.1.1.

419 §§ 278 bis 278b öStGB.

420 Bei Verkehrsdatenabfragen gem. § 135 Abs. 2 öStPO.

421 Bei Inhaltsüberwachungen gem. § 135 Abs. 3 öStPO.

422 *Fabrizy, E.*, Kurzkommentar zur StPO, 10. Aufl., Wien 2008, § 137, Rn. 3.

423 § 137 Abs. 3 öStPO.

Im Übrigen darf nur auf solche Verkehrsdaten zugegriffen werden, die der Betreiber rechtmäßig verarbeitet oder gespeichert hat.[424] Dabei sind §§ 96 und 99 öTKG zu beachten, wonach Verkehrsdaten grundsätzlich nicht gespeichert werden dürfen und vom Betreiber nach Beendigung der Verbindung unverzüglich zu löschen oder zu anonymisieren sind. Nur für Abrechnungszwecke[425] darf ausnahmsweise nach § 99 Abs. 2 TKG für eine gewisse Zeit gespeichert werden. Weitergehend als unter § 96 des deutschen TKG sind die Anbieter in Österreich nicht nur berechtigt, sondern verpflichtet, die Daten bis zum Ablauf jener Frist zu speichern, innerhalb derer die Rechnung rechtlich angefochten werden oder der Anspruch auf Zahlung geltend gemacht werden kann. Diese Daten sind im Streitfall einer Schlichtungsstelle unverkürzt zur Verfügung zu stellen. Wird dort ein Verfahren über die Höhe der Entgelte eingeleitet, dürfen die Daten bis zur endgültigen Entscheidung über die Höhe der Entgelte nicht gelöscht werden. Nach Auskunft des befragten Experten beim österr. Bundeskriminalamt beträgt die Einspruchsfrist 6 Wochen; zusammen mit der Rechnungsstellungsfrist sind Verkehrsdaten damit meist für einen Zeitraum von ca. 3 Monaten verfügbar. Dies gilt freilich nur für Fälle, in denen eine Rechnungstellung notwendig ist.

4.3.2. Gegenwärtige Praxis der Verkehrsdatenabfrage

Der vom österr. Bundesministerium für Inneres und dem österr. Bundesministerium für Justiz herausgegebene Sicherheitsbericht beleuchtet die Praxis der Verkehrsdatenabfrage für die Jahre 2008 und 2009 anhand von konkreten Zahlen.[426] Danach wurden im Jahr 2009 von den Staatsanwaltschaften 5.341 Anträge auf die gerichtliche Bewilligung von Anordnungen einer Auskunft über Daten einer Nachrichtenübermittlung (Verkehrsdatenabfrage) und Überwachung von Nachrichten (TKÜ) gestellt (Tabelle G-1). 5.227 dieser Anträge wurden gerichtlich bewilligt; das entspricht einem Anteil von 98 %. Von diesen bezogen sich 4.013 Anträge bzw. 3.928 Bewilligungen auf Verkehrsdatenabfragen. Das ist, bezogen auf die tatsächlich bewilligten Abfragen, eine Zunahme gegenüber 2008 um 27 % (n = 835). Auffallend ist neben dem signifikanten Anstieg um mehr als ein Viertel in nur einem Jahr insbesondere der im Vergleich zu Deutschland wesentlich größere Abstand zwischen der Anzahl der Inhaltsüberwachungen (Spalte 2) und den mehr als dreimal häufigeren Verkehrsdatenabfragen (Spalte 3).

---

424 Vgl. auch *Fabrizy, E.*, Kurzkommentar zur StPO, 10. Aufl., Wien 2008, § 137, Rn. 4.

425 Dies gilt für die Verrechnung von Entgelten einschließlich der Entgelte für Zusammenschaltungen.

426 Bundesministerium für Inneres u. Bundesministerium für Justiz, Bericht der Bundesregierung über die innere Sicherheit in Österreich (Sicherheitsbericht 2009).

*Tabelle G-1: Telekommunikationsbezogene Überwachunsgmaßnahmen in Österreich in den Jahren 2008/09**

	1. Insgesamt		2, Überwachung von Nachrichten		3. Auskunft über Daten einer Nachrichten-übermittlung		4. Gegen bekannte Täter (insgesamt)		5. Gegen unbekannte Täter (insgesamt)	
	StA'liche Anträge	Gerichtliche Bewilligungen	StA'liche Anträge	Gerichtliche Bewilligungen	StA'liche Anträge	Gerichtliche Bewilligungen	StA'liche Anträge	Gerichtliche Bewilligungen	StA'liche Anträge	Gerichtliche Bewilligungen
2008	4.229	4.073 (96 %)	1.009	980 (97 %)	3.220	3.093 (96 %)	2.942	2.844 (97%)	1.287	1.229 (95 %)
2009	5.341	5.227 (98 %)	1.328	1.299 (98 %)	4.013	3.928 (98 %)	3.873	3.793 (98 %)	1.468	1.434 (98 %)

*) Quelle: Sicherheitsbericht 2009, Teil II, S. 156f.

In dem Expertengespräch wurde die Frage nach den gegenwärtig auf der Grundlage von § 99 öTKG gespeicherten und für die Ermittlungsbehörden zugänglichen Daten weiter vertieft. Auch in Österreich sehen sich die Behörden mit dem Problem konfrontiert, dass die tatsächliche Speicherpraxis ganz wesentlich von den individuellen technischen Bedingungen bei den Anbietern abhängen. Dadurch seien insbesondere die Daten eingehender Telefonate meist nicht greifbar. Gerade diese seien aber für die Praxis von großer Bedeutung, sodass diesbezüglich eine zusätzliche (Vorrats-) Speicherpflicht für besonders notwendig erachtet wird. Lücken bestünden weiterhin bei Flatrates, wo Verkehrsdaten aus technischen Gründen zwar kurzfristig gespeichert würden, aber eben nicht länger als 7 Tage. In Österreich seien Flatrates heute im Bereich des Internets Standard, mit Ausnahme des mobilen Internets über UMTS; aber auch dort sei die Tendenz zu Flatratetarifen inzwischen ansteigend. Generell sei zu der Problematik der Speicherdauer im Übrigen festzustellen, dass die von den Providern angegebenen Speicherzeiträume seit Beginn der öffentlichen Diskussion um die Vorrats-datenspeicherung in Österreich deutlich kürzer geworden seien: Die Entwicklung sei hier von 6 Monaten auf aktuell etwa 2 bis 3 Monate zurückgegangen.

Zukunftsgerichtete Abfragen gestalteten sich in der Praxis mitunter schwieriger, da die Daten nicht einfach in regelmäßigen Intervallen geliefert würden. Für jede einzelne Lieferung sei jeweils eine neue Anordnung erforderlich.

Im Hinblick auf den deliktischen Anwendungsbereich werden ebenfalls Lücken identifiziert. Durch das relativ hoch angesetzte Mindeststraferfordernis von einem Jahr sei die Durchführung von Verkehrsdatenabfragen nahezu im gesamten Cybercrime-Bereich gesperrt.

Auch bei Kinderpornographie, Computerbetrug und dem herkömmlichen Betrug läge die Mindeststrafe für die Grundtatbestände bei nur 6 Monaten. Auch beim Enkeltrick – in Österreich „Neffentrick“ genannt – hänge es von den Umständen des Einzelfalles ab, ob Qualifikationsmerkmale erfüllt sind. Am einfachsten sei die Annahme einer Qualifikation im Bereich der Kinderpornographie.

Problemlos gestaltet sich in Österreich die Standortabfrage. Funkzellen würden aus technischen Gründen stets in Verbindung mit dem Datum und der Uhrzeit gespeichert. Auch bei Echtzeiterhebungen ergeben sich keine technischen Probleme. Rechtlich umstritten ist mitunter die präventive Abfragevariante.[427] Auf dieser Grundlage würden, beispielsweise bei Suizidgefahr oder Bombendrohungen, für einen kurzen Zeitraum Verkehrsdaten einschließlich der Standortdaten, IMEI-Nummern oder IP-Adressen beauskunftet. In diesem Zusammenhang werde in der politischen Diskussion mitunter diskutiert, ob damit die StPO umgangen werden könnte. Dies sei theoretisch tatsächlich möglich, werde von den Behörden aber nicht praktiziert, nicht zuletzt auch im Hinblick darauf, dass eine solche Umgehung als Amtsmissbrauch strafbar wäre.

Deutlich mehr Probleme haben die Behörden offenbar mit Bestandsdatenabfragen[428]. Diese dürften nur beauskunftet werden, wenn dafür kein Eingriff in Verkehrsdaten notwendig ist. Ein solcher Eingriff liege nach einer Entscheidung des Obersten Gerichtshofes nicht vor, wenn die Auswertung der Verkehrsdaten beim Betreiber selbst erfolgt, ohne nach außen zu gelangen. Denn in diesen Fällen werde keine Auskunft über die Verkehrsdaten verlangt, sondern über Stammdaten. Ob der Anbieter dafür Verkehrsdaten auswerten muss, spiele insoweit keine Rolle. Diese ständige Rechtsprechung werde von einigen Anbietern bis heute nicht zur Kenntnis genommen. Dies könne zu der unbefriedigenden Situation führen, dass manche Anbieter die Stammdaten zu einer dynamischen IP-Adresse auf Ersuchen der Staatsanwaltschaft herausgeben, andere hingegen darauf beharrten, eine richterliche Bewilligung einzuholen. Dabei stelle sich dann mitunter das Folgeproblem, dass einige Richter, da es sich bei dieser Auskunft nach ständiger Rechtsprechung eben nicht um eine Auskunft nach § 135 öStPO handele, nicht in der Lage sähen, eine solche – nach dieser Rechtsauffassung überflüssige und somit formal falsche – Bewilligung zu erteilen. Es komme infolgedessen regelmäßig vor, dass die Ermittlungsbehörden die Daten im Ergebnis gar nicht erhielten.

Kontroversen mit den Rechtsabteilungen der Anbieter ergäben sich ferner aufgrund der Tatsache, dass das öTKG noch ein richterliches Auskunftsersuchen vorsieht. Nach Inkrafttreten der neuen öStPO 2008 werde die Abfrage aber, nach richterlicher Bewilligung, vom Staatsanwalt angeordnet. Trotzdem weigerten sich einige Anbieter nach wie vor, einem Auskunftsverlangen der Staatsanwaltschaft ohne richterliche Bewilligung zu entsprechen.

---

427 Siehe oben Pkt. 4.3.1.1. u. Fn.414.

428 „Stammdaten“ gem. § 92 Abs. 3 Ziff. 3 öTKG.

Gefragt nach der generellen Kooperationsbereitschaft der Anbieter wurde das Auskunftsverhalten im Bereich der Sprachtelefonie im herkömmlichen Sinne als problemlos beschrieben. Über die schon geschilderten Probleme hinaus gebe es in Einzelfällen Schwierigkeiten bei der Online-Standortbestimmung. Zwar sei die Mitwirkungspflicht der Anbieter in § 94 TKG 2003 explizit geregelt; die ausführende Überwachungsverordnung sei bislang aber nicht erlassen worden. Unbefriedigend sei ganz generell, dass die Speicherfristen nicht festgelegt seien. Diese würden von den Anbietern nicht kommuniziert und seien Änderungen unterworfen. Der Experte ergänzt, er sei sich sicher, dass Auskünfte über das Vorhanden- bzw. Nichtvorhandensein von Datenbeständen nicht immer der Wahrheit entsprächen.[429] Es sei nicht plausibel, dass einzelne Datensätze selektiv und in täglichen oder kurzen Intervallen gelöscht würden; dies geschehe mutmaßlich automatisiert und zu bestimmten Stichtagen.

Abschließend erläutert der Gesprächspartner, dass aus Ermittlersicht eine sechsmonatige Speicherfrist nur für etwa 70% der Fälle ausreichend sei. Für den übrigen Anteil, v.a. Fälle aus dem Bereich organisierter Kriminalität im Internet, sei dieser Zeitraum nicht ausreichend, insbesondere dann nicht, wenn sich die Server im Ausland befänden.

4.4. Rumänien

Rumänien hatte die Richtlinie 2006/24/EG durch das Gesetz Nr. 298/2008[430] vom 26. November 2008 über die Speicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kummunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden und zur Änderung des Gesetzes Nr. 506/2004 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, umgesetzt. Mit Urteil vom 8.10.2009 hat der rumänische Verfassunsgerichtshof das Gesetz zur Vorratsdatenspeicherung für verfassunsgwidrig erklärt. Seitdem richtet sich die Verkehrsdatenabfrage nach den allgemeinen strafprozessualen Bestimmungen.

4.4.1. Gesetz Nr. 298/2008 über die Speicherung von Daten

Das Gesetz Nr. 298/2008 über die Speicherung von Daten war in sechs Kapitel gegliedert und enthielt allgemeine Bestimmungen (*dispoziții generale*, Kap. I), Regelungen über die Speicherung von Daten (*reținerea datelor,* Kap. II), über das Ersuchen auf Übermittlung der auf Vorrat gespeicherten Daten (*procedura solicitării datelor reținute,* Kap. III), über die Kontrollbehörde (*autoritatea de supraveghere,* Kap. IV), über Sanktionen (*regimul sanctionator,* Kap. V) sowie abschließende Bestimmungen (*dispoziții finale,* Kap. VI).

Das Gesetz sah eine Pflicht für Anbieter von elektronischen Kommunikationsdiensten zur vorsorglichen, anlasslosen Speicherung von Daten für einen Zeitraum von sechs Monaten ab

---

429 Das wörtliche Zitat der Transkription lautet: „Wir wissen, dass sie uns anlügen. Wir können es aber nicht beweisen."

430 Veröffentlicht im Monitorul Oficial, Teil I, Nr. 780 vom 21. November 2008.

dem Zeitpunkt der Erfassung vor. Die Vorratsspeicherung von Daten hatte auf eigene Kosten der Kommunikationsdienste zu erfolgen.

Gem. Art. 1 II Gesetz Nr. 298/2008 sollten Verkehrs- und Standortdaten (*date de trafic şi de localizare*) von natürlichen und juristischen Personen sowie damit in Verbindung stehende Daten (*date conexe*), die zur Feststellung des Abonnenten oder Verbrauchers notwendig sind, gespeichert werden. Eine nähere Bestimmung, um welche Daten es sich mit dem Ausdruck „damit in Verbindung stehende Daten" handelt, sah das Gesetz nicht vor. Stattdessen teilte Art. 3 I Gesetz Nr. 298/2008 die zu speichernden Daten in folgenden Kategorien ein: sämtliche Daten, die zur Verfolgung und Identifizierung der Quelle der Kommunikation notwendig sind, Daten zur Identifizierung des Empfängers, Daten im Hinblick auf Datum, Uhrzeit und Dauer der Kommunikation, Daten zur Feststellung der Kommunikationsart sowie Daten zur Feststellung der Kommunikationsgeräte. Die Speicherung umfasste nach Auskunft des befragten Experten[431] auch sämtliche Daten, die im Zusammenhang mit der Nutzung des Internets anfallen. Der *Inhalt* der Daten durfte dabei jedoch nicht gespeichert werden. Am Ende der Speicherfrist müssen sämtliche Daten gem. Art. 11 III Gesetz Nr. 298/2008 irreversibel vernichtet werden.

Ein Ersuchen auf Übermittlung der auf Vorrat gespeichterten Daten konnte erst nach der Eröffnung des Ermittlungsverfahrens gestellt werden. Für das Ersuchen war gem. Art. 16 I Gesetz Nr. 298/2008 ein Richtervorbehalt vorgesehen; bei Gefahr im Verzug konnte es gem. Art. 16 II ausnahmsweise von der Staatsanwaltschaft gestellt werden. Die auf Vorrat gespeicherten Daten sollten der Ermittlung (*cercetare*), Aufdeckung (*descoperire*) und Verfolgung (*urmărire*) schwerer Straftaten dienen. Art. 2 I f) Gesetz Nr. 298/2008 definierte schwere Straftaten wie folgt: Delikte im Sinne von Art. 2 b) des Gesetzes Nr. 39/2003 über die Prävention und Verfolgung organisierter Kriminalität, Delikte im Sinne von Kapitel IV des Gesetzes Nr. 535/2004 über die Prävention und Verfolgung von Terrorismus sowie Straftaten gegen die Sicherheit des Staates gem. Art. 155–173 rum. StGB.

Konventionelle Kriminalität und Internet-Kriminalität im Sinne des deutschen Verständnisses der IuK-Kriminalität im engeren und weiteren Sinne waren nicht erfasst.

4.4.2. Entscheidung des Verfassungsgerichtshofs vom 8. Oktober 2009

Der rumänische Verfassungsgerichtshof (*Curtea Constituțională a României*) verhandelte in öffentlicher Sitzung vom 8. September 2009 über die Verfassungsmäßigkeit des Gesetzes Nr. 298/2008 über die Speicherung von Daten und hat dieses mit der Entscheidung Nr. 1.258[432] vom 8. Oktober 2009 als Ganzes für verfassungswidrig erklärt. Zur Begründung führte der

---

431 Nationale Direktion zur Korruptionsbekämpfung bei der Staatsanwaltschaft beim Hohen Gericht für Kassation und Justiz.

432 Veröffentlicht im Monitorul Oficial, Nr. 798 vom 23. November 2009. Die Entscheidung wurde ins Deutsche übersetzt und ist abrufbar unter: www.vorratsdatenspeicherung.de/content/view/342/79/ [Juni 2011]. Die Übersetzung wurde zum Teil übernommen.

Verfassungsgerichtshof aus, dass das Gesetz Nr. 298/2008 gegen das Recht auf Privatsphäre (*drept la viață intimă*) gem. Art. 26 der rum. Verfassung, gegen das Brief-, Post- und Fernmeldegeheimnis (*drept la secretul corespondenței*) gem. Art. 28 rum. Verfassung, gegen das Recht auf freie Meinungsäußerung (*drept la liberă exprimare*) gem. Art. 30 rum. Verfassung sowie gegen Art. 8 EMRK verstößt.

Der gesetzlichen Verpflichtung zur *dauerhaften* Speicherung von persönlichen Daten stehen die Persönlichkeitsrechte, insbesondere das Recht auf Privatsphäre, auf freie Meinungsäußerung und auf Schutz personenbezogener Daten entgegen; im Hinblick auf diese Rechte besteht der weithin anerkannte Grundsatz, dass die Vertraulichkeit zu garantieren und zu respektieren ist und dass den Staat in dieser Hinsicht vor allem negative Pflichten treffen, nämlich so weit wie möglich von Eingriffen in die Ausübung des Rechts oder der Freiheit abzusehen. Ausnahmen von diesem Grundsatz sind – in begrenztem Umfang – möglich, soweit dies mit der Verfassung und internationalen Übereinkommen vereinbar ist. Das Gesetz Nr. 298/2008 stellt eine solche Ausnahme dar.

Die rechtliche Verpflichtung zur *dauerhaften* Speicherung von persönlichen Daten, wie sie das Gesetz zur Datenspeicherung vorsieht, macht jedoch nach Ansicht des Gerichtshofes die Ausnahme vom Grundsatz des Schutzes des Rechts auf Privatsphäre und des Rechts auf freie Meinungsäußerung zur absoluten Regel (*regulă absolută*). Damit werden Bestimmungen über die Speicherung von Daten als Regel eingeführt, die die Strafprozessordung (*Codul de procedură penală, C.p.p.*) nur als strenge Ausnahme vorsieht. Die fortlaufende Aufbewahrung von Daten für die Dauer von sechs Monaten ab ihrer Erfassung, um gegebenenfalls auf richterliche Anordnung auf die in der Vergangenheit angefallenen – und nicht nur auf die zukünftig anfallenden – Daten zugreifen zu können, steht hierzu im Widerspruch. Die Bestimmung einer positiven Verpflichtung, welche die fortwährende Einschränkung des Rechts auf Privatsphäre und auf vertrauliche Korrespondenz vorsieht, führt zur Beseitigung des Kerngehalts dieses Rechts, indem die Schutzvorkehrungen zur Gewährleistung der Ausübung des Rechts beseitigt werden. Natürliche und juristische Personen, d.h. Massenanwender elektronischer Kommunikationsdienste, sind *ununterbrochen* dieser Einmischung in die Ausübung ihrer Rechte auf vertrauliche Korrespondenz und freie Meinungsäußerung ausgesetzt, ohne dass noch eine Möglichkeit einer freien und unzensierten Manifestation dieser Rechte besteht, außer im Wege direkter Kommunikation, was jedoch einen Ausschluss von den heutigen Kommunikationsmitteln bedeutet.

Das Gesetz Nr. 298/2008 verstößt nach der Entscheidung überdies gegen den Grundsatz der Verhältnismäßigkeit, der verfassungsrechtlich in Art. 53 II rum. Verfassung verankert ist. Dieser Grundsatz gebietet, dass das Maß der Grundrechtsbeschränkung der Situation entsprechen muss, die zu ihrer Anwendung geführt hat, und dass die Grundrechtsbeschränkung mit dem Zeitpunkt des Wegfalls ihres Grundes beendet werden muss. Das Gesetz sieht demgegenüber eine Verpflichtung zur *dauerhaften* Speicherung von persönlichen Daten ab dem Zeitpunkt seines Inkrafttretens vor, ohne die Notwendigkeit in Betracht zu ziehen, dass die Speicherung mit dem Wegfall des Grundes beendet werden muss, der zu ihrer Einführung

geführt hat. Der Eingriff in die freie Ausübung des Rechts findet ununterbrochen statt und unabhängig davon, ob bestimmte Tatsachen vorliegen, welche die Maßnahme rechtfertigen, um eine schwere Straftat zu verhindern oder, nachdem sie begangen worden ist, aufzuklären.

Ein weiterer Aspekt, der zu einer ungerechtfertigten Beschränkung des Rechts auf Privatsphäre führt, ist nach der Wertung des Gerichtshofes die Tatsache, dass das Gesetz Nr. 298/2008 nicht nur zur Feststellung von Personen verpflichtet, die eine Nachricht über einen beliebigen Kommunikationsweg senden, sondern auch zur Feststellung des Empfängers dieser Nachricht. Der Empfänger wird einer Vorratsspeicherung von Daten über sein Privatleben ausgesetzt, ohne dass eine Handlung oder Willensäußerung von seiner Seite vorläge. Die Vorratsdatenspeicherung erfolgt nur wegen des Verhaltens einer anderen Person, des Anrufers, dessen Handlungen der Empfänger nicht kontrollieren kann, um sich beispielsweise vor Bösgläubigkeit, kriminellen Absichten, Belästigungen usw. zu schützen. Obwohl der Empfänger die passive Seite der Kommunkationsbeziehung darstellt, kann er aufgrund der Beziehung zum Anrufer ungewollt zum Ziel staatlicher Strafverfolgungsmaßnahmen werden. Auch aus dieser Sicht erscheint die im Gesetz geregelte Einmischung in die Privatsphäre des Einzelnen dem Gericht zu exzessiv.

Der Gerichtshof betont weiter, dass nicht eine im Einzelfall gerechtfertigte Nutzung von Daten, unter den Bedingungen des Gesetzes Nr. 298/2008, das Recht auf Privatsphäre oder freie Meinungsäußerung auf eine nicht hinnehmbare Weise verletzen würde, sondern vielmehr die *ununterbrochene, allgemein anwendbare gesetzliche Verpflichtung* zur Vorratsdatenspeicherung. Diese Maßnahme betrifft alle Personen gleichermaßen, ob sie eine strafbare Handlung begangen haben oder nicht, ob gegen sie ein strafrechtliches Ermittlungsverfahren geführt wird oder nicht. Sie birgt darüber hinaus die Gefahr in sich, dass die Unschuldsvermutung (*prezumția de nevinovăție*) ausgehebelt wird, und dass *a priori* sämtliche Nutzer elektronischer Kommunikationsdienste und öffentlicher Kommunikationsnetze unter den Verdacht gestellt werden, terroristische oder sonstige schwere Straftaten begangen haben zu können.

Nach alledem hatte das Gesetz Nr. 298/2008 einen zu weiten Anwendungsbereich, der mit den Bestimmungen der Rumänischen Verfassung und darüber hinaus auch mit der Europäischen Menschenrechtskonvention nicht vereinbar ist.

4.4.3. Abhören und Registrieren nach geltendem Recht

4.4.3.1. Regelungen in der Strafprozessordnung

Nachdem das Gesetz Nr. 298/2008 für verfassungswidrig erklärt wurde, kann die Erfassung und Auswertung von Daten grundsätzlich nur noch nach den Bestimmungen der Strafprozessordnung erfolgen.

Die Strafprozessordnung sieht in den Art. 91^1–91^6 C.p.p. detaillierte Regelungen zum Abhören und Registrieren von Gesprächen, Telefongesprächen, oder Gesprächen, die mit sonstigen Mitteln der Kommunikation durchgeführt werden, vor; hierunter fallen auch die Kommunika-

tion und die Bewegung im Internet. Art. 91[1] ff. C.p.p. dient ebenso als Rechtsgrundlage für das Abrufen von Echtzeitdaten. Dem Registrieren muss aber zwingend ein Abhören vorangehen; eine reine Verkehrsdatenerhebung ist nicht statthaft.

Die Inhalts- und Verkehrsdatenüberwachung („Abhören und Registrieren") ist gem. Art. 91[1] C.p.p. nur auf Antrag desjenigen Staatsanwalts, der die Ermittlungen führt oder überwacht,[433] und nur auf richterliche Anordnung bei folgenden Delikten zulässig: Straftaten gegen die nationale Sicherheit (*infracțiuni contra siguranței naționale*), die im Strafgesetzbuch und in anderen Spezialgesetzen geregelt sind, Drogenhandel (*infracțiuni de trafic de stupefiante*), Waffenhandel (*infracțiuni de trafic de arme*), Menschenhandel (*infracțiuni de trafic de persoane*), terroristische Handlungen (*acte de terorism*), Geldwäsche (*spălare a banilor*), Geldfälschung (*falsificare de monede*), Straftaten gem. Gesetz Nr. 78/2000 zur Prävention, Aufdeckung und Sanktionierung der Korruption sowie im Falle einer anderen schweren Straftat oder einer Straftat, die mittels eines elektronischen Kommunikationsmittels begangen wurde.

Die Notwendigkeit der richterlichen Anordnung einer Maßnahme nach Art. 91[1] C.p.p. kann entweder durch die Feststellung von Tatsachen begründet sein (*pentru stabilirea situației de fapt*) oder wenn es um die Feststellung oder Lokalisierung von Teilnehmern geht, die nicht durch andere Mittel ermittelt werden können (*pentru că identificarea sau localizarea participanților nu poate fi făcută prin alte mijloace*) oder weil andere Ermittlungsarten zu spät kommen würden (*pentru că cercetarea ar fi mult întârziată*).[434]

Die richterliche Anordnung zum Abhören und Registrieren von Gesprächen darf gem. Art. 91[1] III C.p.p. 30 Tage nicht überschreiten. Eine Verlängerung der Anordnung ist möglich, sie darf jedoch gem. Art. 91[1] V C.p.p. insgesamt 120 Tage nicht überschreiten. Die Staatsanwaltschaft entscheidet über eine sofortige Beendigung der Maßnahme, sobald die gesetzlichen Voraussetzungen nicht mehr vorliegen.

Art. 91[2] C.p.p. bestimmt die Organe, die das Abhören und Registrieren durchführen. In der Regel wird das Abhören und Registrieren von einem Staatsanwalt selbst durchgeführt; er kann jedoch auch ein anderes Ermittlungsorgan mit der Durchführung beauftragen. Bei Gefahr im Verzug kann ausnahmsweise der Staatsanwalt, der die Maßnahmen leitet, eine vorläufige Anordnung erteilen; allerdings darf ein Abhören und Registrieren auf der Grundlage eine staatsanwaltlichen Eilanordnung nicht länger als 48 Stunden dauern. Innerhalb dieser 48 Stunden muss der Staatsanwalt die Angelegenheit dem Richter zur weiteren Entscheidung vorlegen.

---

433 Das Erfordernis, dass der Antrag von dem konkreten Staatsanwalt, der die Ermittlungen führt oder überwacht, gestellt werden muss, wurde 2006 in Art. 91[1] C.p.p. aufgenommen. Vor der Gesetzesänderung reichte der Antrag eines beliebigen Staatsanwalts aus. Siehe *Neagu, I.*, Tratat de procedură penală, Partea generală, Ediția a II–a, revăzută şi adăugită, Bucureşti 2010, S. 490.

434 *Neagu, I.*, Tratat de procedură penală, Partea generală, Ediția a II–a, revăzută şi adăugită, Bucureşti 2010, S. 491.

Art. 91^3–91^6 C.p.p. enthalten Bestimmungen über die Niederschrift der Abhör- und Registriermaßnahmen und über andere Formen der Aufzeichnung/Registrierung, inklusive visueller Aufzeichnung.

Eine offizielle Statistik über Maßnahmen der Telekommunikationsüberwachung einschließlich der Verkehrsdatenauswertung gem. Art. 91^1–91^6 C.p.p. liegt nicht vor.

4.4.3.2. Regelungen im Nebengesetz

Das Gesetz Nr. 51/1991[435] über die nationale Sicherheit Rumäniens erweitert im Bereich der Staatssicherheit die Möglichkeit des Abhörens von Gesprächen, Telefongesprächen, oder Gesprächen, die mit sonstigen Mitteln der Kommunikation, inklusive des Internets, geführt werden, unter Einhaltung der Vorschriften der Strafprozessordnung. Zulässig ist demnach das Abhören von Gesprächen für eine Dauer von bis zu 6 Monaten bei Straftaten, die die Sicherheit des Staates gefährden. Unter letztere fallen beispielsweise Handlungen zur Abschaffung oder Beeinträchtigung der Souveränität, der Einheit, der Unabhängigkeit oder Unteilbarkeit des rumänischen Staates, Handlungen mit dem Ziel, einen Krieg gegen Rumänien zu provozieren, sowie Spionagehandlungen, u.ä. Das Abhören erfolgt auf schriftlichen Antrag der Organe der Staatssicherheit und auf Anordnung besonderer Staatsanwälte, die vom Generalbundesanwalt zum Erlass solcher Anordnungen beauftragt sind. Auf Antrag kann der Abhörzeitraum von 6 Monaten mehrmals um jeweils 3 Monate verlängert werden.[436]

Eine offizielle Statistik über Maßnahmen der Telefonüberwachung gem. Gesetz Nr. 51/1991 liegt derzeit nicht vor.

4.4.3.3. Probleme in der Praxis

Nach der gegenwärtigen Rechtslage können Verkehrsdaten in Rumänien offiziell nur noch auf der Grundlage von Art. 91^1–91^6 C.p.p. erhoben werden. Dieser regelt, wie beschrieben, das Abhören und Registrieren von Gesprächen, Telefongesprächen oder Gesprächen, die mit sonstigen Mitteln der Kommunikation wie beispielsweise dem Internet geführt werden. Der Überwachungszeitraum ist auch deutlich kürzer als die ursrüngliche Speicherdauer von 6 Monaten. Ein Abhören und Registrieren bis zu 6 Monaten ist nur ausnahmsweise in Fällen möglich, die unter die Bestimmungen des Gesetzes Nr. 51/1991 über die nationale Sicherheit Rumäniens fallen.

Der Rekurs auf die Inhaltsüberwachung bedeutet zunächst, dass – rein formal betrachtet – der deliktische Anwendungsbereich der Verkehrsdatenüberwachung wesentlich breiter ist, als er auf der Grundlage des Gesetzes Nr. 298/2008 über die Speicherung von Daten war. Neben Drogen-, Waffen-, Menschenhandel, Geldfälschung und Geldwäsche sind Maßnahmen jetzt vor allem auch möglich bei Straftaten, die mittels eines elektronischen Kommunikationsmit-

---

435 Veröffentlicht im Monitorul Oficial, Nr. 163 vom 07. August 1991.

436 Siehe zum Ganzen Art. 13 des Gesetzes Nr. 51/1991.

tels begangen werden. Als wenig hilfreich wird aus der Perspektive der Ermittlungspraxis das Fehlen einer eigenen Rechtsgrundlage alleine für die Erhebung von Verkehrsdaten betrachtet. Diese rechtliche Situation führe dazu, dass zwingend auch Inhaltsüberwachungen durchgeführt werden müssen. Das sei gerade im Bereich der IuK-Kriminalität zu aufwendig und zugleich zu wenig zielführend. Die Verkehrsdatenauswertung habe im Übrigen eine ganz andere Zielrichtung, nämlich die Rekonstruktion von Kommunikation in der Vergangenheit. Zu diesem vergangenheitsbezogenen Ermittlungsziel könne die auf Inhalte bezogene Telekommunikationsüberwachung, die nur die Gegenwart und die Zukunft abdeckt, nichts beitragen. Dies werde bei der IuK-Kriminalität besonders augenfällig, gelte im Grundsatz aber auch für Ermittlungen in den anderen Deliktsbereichen.

Mit dem Wegfall der gesetzlichen Pflicht, Daten auf Vorrat zu speichern, haben die Ermittlungsorgane keine Möglichkeit mehr, von den Diensteanbietern die Herausgabe von Daten förmlich zu verlangen. Freilich gesteht der Gespächspartner ein, dass einzelne Anbieter im Einzelfall aus Kulanz durchaus kooperationsbereit seien. Allerdings seien Speicherumfang und -fristen unklar. Diese Praxis bringe es im Übrigen mit sich, dass die verfahrensbezogenen Garantien des Gesetzes zur Vorratsdatenspeicherung, das die Abfrage an den förmlichen Beginn eines staatsanwaltlichen Ermittlungsverfahrens geknüpft hatte, heutzutage leerliefen. Denn nunmehr komme es vor, dass die Behörden von den Unternehmen Daten ohne besonderes Verfahren auf eine einfache schriftliche Anfrage hin zur Verfügung gestellt bekämen. Damit könnten auch die entsprechenden Bestimmungen der Art. 91^1–91^6 C.p.p. umgangen werden, in denen festgelegt ist, ab wann richterliche und staatsanwaltliche Zwangsmaßnahmen überhaupt angeordnet werden dürfen.[437]

Generell nicht mehr ermittelbar seien auf dem Wege der Abfrage bei den TK-Anbietern allerdings Daten über eingehende Telefonate. Daher werden die Auswirkungen des Urteils für die polizeiliche Arbeit nach der auch den deutschen Interviewpartnern vorgegebenen Skala insgesamt als sehr hoch bewertet.

4.5. Schweden

Schweden gehört zu der Gruppe von EU-Mitgliedsländern, die die Richtlinie 2006/24/EG bislang nicht umgesetzt haben. Zwar wurde nach längerem innenpolitischen Streit[438] und in Folge der Verurteilung Schwedens durch den Europäischen Gerichtshof vom 4.2.2010 in dem von der EU-Kommission angestrengten Vertragsverletzungsverfahren[439] nach der Reichstagswahl 2010 ein Gesetzentwurf[440] vorgelegt, der sich an der Mindestspeicherdauer von 6 Monaten orientiert (siehe dazu unten Pkt. 4.5.3.). Er wird allerdings nicht wie ursprünglich

---

437 Dies ist die formale Eröffnung des Ermittlungsverfahrens (*urmărire penală*).

438 Vgl. etwa MMR-Aktuell 2010, 298689.

439 Rechtssache C-185/09, Urteil vom 4.2.2010, ABl. C 80/6 vom 27.3.2010.

440 Regeringens proposition 2010/11:46 [Gesetzentwurf zur Vorratsdatenspeicherung zur Strafverfolgung und zur Durchführung der Richtlinie 2006/24/EG].

vorgesehen zum 1.7.2011 in Kraft treten. Mit Beschluss vom 16.3.2011 hat der schwedische Reichstag das Inkrafttreten um (zunächst) ein Jahr aufgeschoben.[441] Der Beschluss, getragen von der Umweltpartei, der Linkspartei und den sog. Schwedendemokraten, zeigt erneut, dass das Land ungeachtet des politischen Drucks von Seiten der EU nach wie vor weit von einem innenpolitischen Minimalkonsens in der Frage der Vorratsdatenspeicherung entfernt ist.

4.5.1. Zugriffsmöglichkeiten auf Verkehrsdaten nach der gegenwärtigen Rechtslage

Die gegenwärtige Rechtslage in Schweden[442] ist von der Ausgangssituation her der aktuellen Situation in Deutschland vergleichbar. Mangels explizit geregelter Speicherpflicht können die Strafverfolgungsbehörden und die Polizei unter bestimmten Umständen auf Verkehrsdaten zugreifen, über die die Netzbetreiber im Rahmen der gesetzlichen Bestimmungen verfügen; dies betrifft namentlich Daten, die zu Abrechnungszwecken gespeichert sind. Einzelheiten dazu werden im schwedischen Datenschutzgesetz (PUL)[443], dem Telekommunikationsgesetz (LEK)[444] sowie dem Prozessgesetzbuch (RB)[445] geregelt, die sich inhaltlich teilweise überschneiden.

Nach dem RB ist eine Verkehrsdatenabfrage nur dann zulässig, wenn die Maßnahme der Verfolgung und Aufklärung einer Straftat dient. Möglich ist der Zugriff auf retrograde wie auf Echtzeitdaten. Seit dem 1. Oktober 2004 darf eine Verkehrsdatenabfrage bei jeder Anlasstatdurchgeführt werden, für die eine Mindeststrafe von sechs Monaten Freiheitsstrafe angedroht ist. Darüber hinaus ist die Abfrage generell zulässig bei einigen enumerativ aufgezählten Katalogtaten, u.a. Datenbeeinträchtigung[446] und Kinderpornographie[447].[448] Die Maßnahme muss stets verhältnismäßig sein. Bei allen übrigen Straftaten, die unter dem Sechsmonatsminimum bleiben, dürfen lediglich Bestandsdaten abgefragt werden. Eine Verkehrsdatenabfrage ist dann unzulässig.

Nach dem LEK ist eine Verkehrsdatenabfrage auch zur Erfüllung präventiv-polizeilicher Aufgaben zulässig. Verkehrsdatenabfragen nach dem LEK bedürfen – anders als jene nach dem RB – keiner richterlichen Anordnung und können von der Polizei eigenständig durchgeführt werden.

---

441 Reichstagsbeschluss 2010/11:JuU14.

442 Siehe auch das Reformgutachten des schwedischen Verkehrsdatenausschusses: Lagring av trafikuppgifter för brottsbekämpning, SOU 2007:76.

443 Personuppgifslag (PUL), 1998:204.

444 Lag om elektronisk kommunikation (LEK), 2003:389.

445 Rättegångsbalk (RB), 1942:740.

446 4. Kapitel § 9c des Kriminalgesetzbuches (Brottsbalken – BrB).

447 16. Kapitel § 10a BrB.

448 27. Kapitel § 19 RB.

Welche Daten die Telekommunikationsunternehmen speichern dürfen, wird im 6. Kapitel des Telekommunikationsgesetzes geregelt.[449] Die §§ 5 bis 7 enthalten Bestimmungen zu der Art der Speicherung und der Anonymisierung der Daten. Eine Anonymisierung entfällt nach § 8, wenn sofern Behörden oder Gerichte diese Daten benötigen, „um Streitigkeiten zu lösen". Die Zugriffsmöglichkeiten gehen mithin über den reinen Strafverfolgungszweck hinaus. Zu den abfrageberechtigten Behörden gehören u.a. die Polizei, die Finanzpolizei, die Küstenwacht sowie die Zollbehörden.

Bislang existiert keine gesetzliche Regelung zur Kostentragung. In der Praxis werden die bei der Verkehrsdatenabfrage entstandenen Kosten den Telekommunikationsunternehmern aber erstattet.

4.5.2. Situation aus der Perspektive der Praxis

Aktuelle Statistiken zu der Häufigkeit der Abfragen oder der Art der abgefragten Daten liegen nicht vor. Nach Angaben des größten Anbieters TeliaSonera waren im Jahr 2004 ca. 68% der Verkehrsdatenabfragen auf Mobilfunkdaten bezogen, ca. 30% der Anfragen betrafen das Festnetz und nur 2% Internetdienste; 85% der abgefragten Daten bezogen sich auf einen retrograden Zeitraum von bis zu drei Monaten, weitere 10% waren nicht älter als sechs Monate, und lediglich 0,5% der abgefragten Informationen betrafen einen Zeitraum, der länger als ein Jahr zurücklag.[450]

Das Expertengespräch wurde, ebenso wie in Österreich, vor der jüngsten Gesetzesänderung durchgeführt und hat daher die gegenwärtige Rechtslage als Ausgangspunkt. Die beiden Interviewpartner äußerten zunächst Probleme mit der Zugriffsbeschränkung auf Straftaten mit einer Mindeststrafandrohung von 6 Monaten. Dies schränke die Anwendung unter Berücksichtigung des schwedischen Straftarifsystems von vornherein auf schwere Straftaten ein. Zahlreiche Deliktskategorien aus dem Bereich der IuK-Kriminalität, insbesondere der Internetbetrug, bleiben unterhalb dieser Schwelle, sodass in solchen Fällen zwar Bestands-, aber keine Verkehrsdaten abgefragt werden könnten. Hier bestehe, mit Ausnahme von Ermittlungen in dem Bereich der Kinderpornographie, eine klare Anwendungslücke. Insoweit seien nach derzeitigem Kenntnisstand auch keine gesetzlichen Erweiterungen zu erwarten.

Bezogen auf die verschiedenen Datenarten wird eine weitere Lücke in Bezug auf die eingehenden Gespräche gesehen. Diese würden derzeit, wie in Deutschland, mangels Abrechnungsrelevanz nicht gespeichert. Dasselbe gelte darüber hinaus in der Regel auch bei abgehenden Anrufen, sofern der Teilnehmer eine Flatrate habe oder Prepaid-Karten benutze. Geodaten seien hingegen in der Regel vorhanden. Eine weitere Hürde sei dann aber in allen Fällen, dass die Telekommunikationsanbieter – auch insoweit der Situation in Deutschland

---

449 Damit wurde auch die EU-Richtlinie 2002/58/EG umgesetzt.

450 Alle Angaben nach *Holst, Thomas (TeliaSonera)*, Retention of Communication Data to Fight Crime and Terrorism; www.quintessenz.at/doqs/000100003005/2004_06_14,data-retention-adhoc-meeting_swedisch_teliasonera_presentation.pdf [Juni 2011].

vergleichbar – keine einheitliche Speicherpraxis entwickelt hätten. Die Ermittlungsbehörden seien im Übrigen vollständig von den Unternehmen abhängig, da in Schweden keine technische Möglichkeit existiere, um Verkehrsdaten selbst zu erheben. Dies gelte auch für die Ermittlung von Echtzeit- und zukünftigen Daten. Anders als in Deutschland scheinen die Daten, soweit denn eine Speicherung erfolgt, bei den meisten Anbietern allerdings für einen Dreimonatszeitraum verfügbar zu sein. Probleme in der Kommunikation mit den Anbietern werden insoweit nicht thematisiert; die Frage nach konkreten Erfahrungen mit mangelnder Kooperationsbereitschaft wurde explizit verneint. Allerdings schränkt einer der Gesprächspartner seine Aussage dahingehend ein, dass die Berufung der Firmen auf das Nichtvorhandensein von Daten bzw. auf bereits erfolgte Löschungen nicht überprüfbar sei. Zweifel an dem Wahrheitsgehalt entsprechender Einwendungen, wie sie Ermittler aus Deutschland und Österreich vereinzelt zum Ausdruck gebracht haben, scheinen in Schweden jedenfalls unbekannt zu sein.

Mögliche Substitute für eine erfolglose oder im konkreten Fall unzulässige Verkehrsdatenabfrage sehen die Befragten nicht. Sowohl der Indiz- als auch der Beweiswert von Verkehrsdaten seien durch andere Ermittlungsmaßnahmen nicht ersetzbar. Einzig durch die [klassische] Telefonüberwachung ließen sich vergleichbare Erkenntnisse gewinnen; diese Maßnahme scheide allerdings häufig aus, wenn die Zielanschlüsse nicht zuvor durch eine Verkehrsdatenauswertung identifizierbar seien. Darüber hinaus sei in diesem Zusammenhang zu beachten, dass die Verkehrsdatenabfrage im Gegenteil immer häufiger als Substitut für die Telekommunikationsüberwachung benötigt werde. Dieser Bedeutungszuwachs ergebe sich für die Ermittlungspraxis aus der deutlichen Zunahme verschlüsselter Kommunikationsverbindungen, vor allem in der Internettelefonie. Allenfalls in wenigen Einzelfällen könnten gegebenenfalls die Beschlagnahme von Mobiltelefonen und ihre anschließende Auswertung als alternativer Ermittlungsansatz in Betracht kommen. Dies setze aber zum einen voraus, dass man gegen bekannte Verdächtige ermittle, zum anderen müsse man das Durchsuchungsobjekt oder zumindest einen konkreten Durchsuchungsort kennen. Da sei in den wenigsten Fällen eine realistische Option.

Ganz dezidierten Widerspruch bringen die beiden Experten schließlich bei der Frage nach dem möglichen Potenzial des Quick-Freeze-Verfahrens zum Ausdruck. Ein Zusatznutzen sei nicht zu erkennen. Dieses Instrument mit seinem Fokus auf aktuell bzw. künftig anfallende Daten sei in Anbetracht des ermittlerischen Bedarfs an retrograden Daten untauglich. Insbesondere im Hinblick auf die aktuellen Lücken in der Speicherpraxis erscheint es den Befragten als untaugliches Instrument. Es könne lediglich ein Hilfsmittel sein, um ohnehin existierende Daten festzuhalten; fehlende Information könne es aber nicht generieren. Aus diesen Gründen plädieren beide Interviewpersonen für eine möglichst zügige Einführung der ausnahmslosen sechsmonatigen Vorratsdatenspeicherung auch in Schweden.

4.5.3. Die künftige Rechtslage

Das neue Gesetz beschränkt sich im Wesentlichen auf Ergänzungen im 6. Kapitel des Telekommunikationsgesetzes. Neben einigen Definitionen[451] sieht das Gesetz künftig eine allgemeine Speicherpflicht von 6 Monaten für Verkehrsdaten vor.[452] Ferner wird noch einmal explizit auf die derzeit existierenden Zugriffsvoraussetzungen in § 19 des 27. Kapitels verwiesen.[453] Auch im Hinblick auf den Anwendungsbereich der Verkehrsdatenabfrage werden sich keine Änderungen ergeben.

Anders als bislang wird dann der Kostenersatz für die Telekommunikationsanbieter eine gesetzliche Grundlage haben.[454]

---

451 6. Kapitel §§ 1, 3a und 5 LEK.

452 6. Kapitel §§ 16a und 16g LEK.

453 6. Kapitel § 16c LEK.

454 6. Kapitel § 16e LEK.

Teil H: Schlussfolgerungen

Die in der vorliegenden Untersuchung herausgearbeiteten Ergebnisse zeigen das Bild einer Momentaufnahme. Die Lage ist gegenwärtig gekennzeichnet durch eine noch sehr unsichere statistische Datengrundlage, das Fehlen systematischer empirischer Untersuchungen und sehr unterschiedliche Einschätzungen bei den unmittelbar betroffenen Praktikern, wie sie in den qualitativen Interviews zum Ausdruck kommen.

1. Datengrundlagen und Diskurse

1. Gegenwärtig können die Auswirkungen des BVerfG-Urteils vom 2.3.2010 noch nicht mit belastbaren Zahlen quantifiziert werden. Die derzeit verfügbaren statistischen Zahlen repräsentieren einen Zeitraum, in dem infolge der einstweiligen Anordnung durch das BVerfG Sonderbedingungen herrschten. So war mit den IuK-Delikten in dieser Periode der Zugriff auf die Vorratsdaten in diesem Segment nahezu vollständig versperrt. Ferner dürften die geringen Anteile erfolgloser Verfahren nicht auf die aktuelle Situation übertragbar sein.

2. Die Untersuchung von Schutzlücken bei Wegfall der Vorratsdatenspeicherung von Telekommunikationsverkehrsdaten kann auch im Hinblick auf die Auswirkungen auf Aufklärungsquoten nur eingeschränkt erfolgen. Dies ist bedingt durch das Fehlen von spezifischen empirischen Untersuchungen, die Nichterfassung von verfahrensbezogenen Daten zur Abfrage von Verkehrsdaten sowie Vorratsdaten oder IP-Adressen und die im Zusammenhang mit besonderen Deliktsphänomenen nur bruchstückhaft vorliegenden (und erfassten) Informationen zur Aufklärungsquote.

3. Der Diskussion zu Nutzen und Konsequenzen der Vorratsdatenspeicherung kann entnommen werden, dass geeignete Daten, die zu einer quantitativen Überprüfung der Auswirkungen der Vorratsdatenspeicherung auf die Aufklärungsquote führen könnten, bislang nicht erfasst werden, und im Übrigen auch nicht systematisch erfasst werden sollen.

4. Die Resultate der bis heute vorliegenden Antworten auf Anfragen zu dem Nutzen der Vorratsdatenspeicherung in Landtagen lassen ferner davon ausgehen, dass entsprechende statistische Erfassungen deshalb nicht vorgenommen worden sind und nicht vorgenommen werden, weil sie als zu kostenträchtig angesehen werden.

5. Für die Europäische Kommission deutet sich in diesem Zusammenhang ein besonderes Problem an. Daten, die zur Evaluation der Richtlinie 2006/24/EG dienen könnten, sind bislang nicht geliefert worden und können nicht geliefert werden, weil eine dafür geeignete Form der Datenerfassung gar nicht vorgesehen war (siehe hierzu auch die weiteren Schlussfolgerungen unter Pkt. 46 ff.).

6. Die Diskussion ist deshalb bestimmt durch den Verweis auf Einzelfälle und eine besondere Betonung der besonderen Schutzbedürftigkeit von jungen und alten Menschen, die in den unübersehbaren Verweisen auf das Leid sexuell missbrauchter Kinder und in nachdrücklichen Hinweisen auf die außerordentliche Niedertracht einer gezielten Ausbeutung der Schwächen alter Menschen zum Ausdruck kommt.

7. Die auf Einzelfälle gegründete Argumentation weist den Einzelfall als „typisch“ aus, ohne dass dies aber empirisch belegt oder belegbar wäre.

8. Hinzu tritt der Verweis auf die von islamistischen Terroristen ausgehenden besonderen Gefahren. Gerade hier liegen im Übrigen keinerlei Hinweise dafür vor, dass auf Vorrat gespeicherte Verkehrsdaten in den letzten Jahren zur Verhinderung eines Terrorsanschlags geführt hätten. Verkehrsdaten waren vielleicht dazu geeignet, Ermittlungen nach Terroranschlägen in Teilen zu befördern; sie haben aber allenfalls zu der Frage geführt, warum bereits vorliegende und bekannte digitale Spuren der Telekommunikation nicht für eine Verhinderung von Anschlägen haben eingesetzt werden können.

2. Aufklärungsquoten: Trends in ausgewählten Deliktsbereichen

9. Die Untersuchung der deliktsspezifischen Aufklärungsquoten für den Zeitraum 1987 bis 2010 zeigt, dass sich der Wegfall der Vorratsdatenspeicherung nicht als Ursache für Bewegungen in der Aufklärungsquote abbilden lässt. Dies erklärt sich schon aus der großen Zahl polizeilich registrierter Fälle, der gegenüber die Abfrage von Verkehrsdaten nicht ins Gewicht fallen kann.

10. Die deliktsspezifischen Aufklärungsquoten in den Bereichen der Computerkriminalität sowie der so genannten Internetkriminalität geben ebenfalls keine Hinweise dafür her, dass durch die Phase der Vorratsdatenspeicherung Veränderungen in der Tendenz der Aufklärungsraten eingetreten wären.

11. Betrachtet man insbesondere das Jahr 2008, in dem Vorratsdaten grundsätzlich zur Verfügung standen, so kann für keinen der hier untersuchten Deliktsbereiche eine mit der Abfrage zusammenhängende Veränderung der Aufklärungsquote im Hinblick auf das Vorjahr oder den Folgejahren 2009/2010 beobachtet werden.

12. Im Vergleich der Aufklärungsquoten, die in Deutschland und in der Schweiz im Jahr 2009 erzielt worden sind, lassen sich keine Hinweise darauf ableiten, dass die in der Schweiz seit etwa 10 Jahren praktizierte Vorratsdatenspeicherung zu einer systematisch höheren Aufklärung geführt hätte.

13. Punktuelle Vergleiche zwischen Deutschland, Österreich und der Schweiz, also Länder, die gerade seit 2008 unterschiedliche rechtliche Grundlagen im Hinblick auf die Vorratsdatenspeicherung aufweisen (jedenfalls zeitweise), führen nicht zu dem Schluss, dass die sys-

tematische Sammlung und Speicherung von Verkehrsdaten bzw. deren Fehlen mit sichtbaren Unterschieden in der Sicherheitslage verbunden wären.

14. Auch nach der Beiziehung anderer Informationsquellen ergeben sich keine belastbaren Hinweise darauf, dass die Schutzmöglichkeiten durch den Wegfall der Vorratsdatenspeicherung reduziert worden wären.

14.1. Enkeltrick

Im Zusammenhang mit der Untersuchung von Ermittlungen zu „Enkeltrickbetrügereien“ ist deutlich geworden, dass der strafrechtliche Schutz (und Schutzlücken) nicht allein durch den Rückgriff auf Vorratsdaten bedingt sein kann. Dies wird unterstrichen durch nach der Entscheidung des BVerfG erfolgte erfolgreiche Ermittlungen in Deutschland (die durch Polizeiberichte ferner besonders hervorgehoben werden) sowie durch den Vergleich der Entwicklungen des „Enkeltrickphänomens“ in Deutschland, Österreich und in der Schweiz, in denen sehr unterschiedliche Möglichkeiten des Rückgriffs auf Verkehrsdaten gegeben sind. Im Übrigen repräsentiert der „Enkelbetrug“ etwa 0,2 aller registrierten Betrugsfälle und etwas weniger als 0,2% der für Betrug registrierten Schäden. Damit handelt es sich um ein Randphänomen des Betrugs, dem im Übrigen erst in den letzten Jahren durch (offensichtlich relativ erfolgreiche) Anpassungen der Ermittlungsstrategien (Zentralisierung) begegnet wird und dessen besondere kriminalpolitische Relevanz eben in der besonderen Schutzbedürftigkeit alter Menschen gesehen wird.

14.2. Tötungsdelikte

Für Kapitaldelikte sind Veränderungen in den Aufklärungsraten wegen fehlender Vorratsdaten nicht sichtbar geworden. Die gesonderte Überprüfung der in der BKA-Fallsammlung enthaltenen Tötungsdelikte ergibt keinen Hinweis darauf, dass bei schwerster Kriminalität durch die Entscheidung des BVerfG die Aufklärung überhaupt behindert worden wäre. Die als Beispiele für wegen Fehlens von Verkehrsdaten mitgeteilten, nicht oder nur schwer zu ermittelnden Fälle sind überwiegend aufgeklärt worden und ferner bereits abgeurteilt (ohne dass Anhaltspunkte für die Notwendigkeit des Zugriffs auf gespeicherte Verkehrsdaten sichtbar geworden wären). Ferner ergeben sich keine Anhaltspunkte dafür, dass in den bislang nicht aufgeklärten Tötungsdelikten auf Vorrat gespeicherte Verkehrsdaten in den Ermittlungen hätten weiter führen können.

14.3. Kinderpornografie

Ermittlungen wegen der Verbreitung und des Besitzes von Kinderpornografie wird vor allem wegen des dahinter stehenden sexuellen Missbrauchs besondere Bedeutung zugeordnet. Die Aufklärung von Fällen sexuellen Missbrauchs anlässlich von Ermittlungen wegen Kinderpornografie ist aber allenfalls Zufallsprodukt. Es ergeben sich ferner keine Anhaltspunkte dafür, dass kommerzielle Webseiten in die

Herstellung von Kinderpornografie maßgeblich eingebunden sind. Angesichts der in die Auswertung von Datenträgern investierten Ressourcen und angesichts der besonderen Betonung der Bedeutung der Verfolgung der Kinderpornografie für die Vorbeugung von sexuellem Missbrauch dürfte sich schließlich die Frage stellen, ob die hier verausgabten Mittel nicht besser in anderen Maßnahmen zur Prävention und Repression des Kindesmissbrauchs platziert worden wären.

14.4. Stalking

Die Strafverfolgung von Stalking lässt besondere Probleme erkennen. Diese liegen allerdings nicht in fehlenden Rückgriffmöglichkeiten im Hinblick auf Vorratsdaten der Telekommunikation. Worauf sich eine solche Annahme eines Zusammenhangs zwischen Schutz vor Stalking und Zugriff auf Vorratsdaten überhaupt stützen könnte, ist vor dem Hintergrund der Daten zu Ermittlungen und Ermittlungsergebnissen, Strafverfahren und Ergebnissen von Strafverfahren ferner nicht nachvollziehbar.

15. Es kann sicher nicht ausgeschlossen werden, dass in komplexen Verfahren und bei Kapitaldelikten Verkehrsdaten wichtige Indizien repräsentieren oder zusätzliche Ermittlungsansätze schaffen. Derartige Fälle, sollten sie zweifelsfrei identifiziert werden können, wirken sich aber auf die Gesamttrends nicht aus.

3. Ermittlungsmethoden, Ermittlungseffizienz und Aufklärungsquote

16. Bislang liegen nur wenige systematische Untersuchungen zur Effizienz von Ermittlungsmaßnahmen in der Aufklärung von Straftaten vor.

17. Danach erscheint die Fokussierung einer einzelnen Ermittlungsmaßnahme, hier der Abfrage von auf Vorrat gespeicherten Verkehrsdaten, auf der Grundlage empirischer Untersuchungen zu Ermittlungen und Strafverfahren im Bereich komplexer Kriminalität (vor allem organisierter Kriminalität), nicht plausibel.

18. Verkehrsdaten spielen in der Regel nur in Kombination mit anderen Ermittlungsmaßnahmen eine Rolle.

19. Dabei ergeben sich aus der Perspektive von Aufklärungseffizienz und möglichen Sicherheitslücken, ordnet man die bisherigen Diskussionen und Ausführungen zur möglichen Relevanz von Vorratsdaten, 4 Konstellationen:

19.1. Die Nutzung von Verkehrsdaten in der Feststellung von Kontakten bzw. Nähe zu einem Tatort/Opfer. Dies ist vor allem bei Tötungsdelikten thematisiert worden. Die Untersuchungen haben für Tötungsdelikte keine Hinweise ergeben, dass das Fehlen von Vorratsdaten die Aufklärung verhindert hätten.

19.2. Die Nutzung von Verkehrsdaten (insbesondere auch Geo-Daten) zur retrospektiven Identifizierung von Tatzusammenhängen bei Serientaten (insbesondere

durch die Herstellung vergangener Bewegungsprofile). Hier stellt die vergangenheitsbezogene Abfrage von Verkehrsdaten eine unter mehreren Ermittlungsmethoden (in der Erforschung der Zusammenhänge) dar. Für eine Einschätzung ihrer (relativem) Bedeutung in der Identifizierung von Serientaten gibt es bislang keine aussagekräftige Datengrundlage.

19.3 Die Nutzung von gespeicherten Verkehrsdaten zur Feststellung von Zusammenhängen zwischen Tätern (im Einzelfall (mittäterschaftliche Begehung von Raub, etc.) oder bei auf Dauer angelegter Tatbegehung in Gruppen oder durch Transaktionen (Betäubungsmittel, Menschenschmuggel, etc.). Für eine quantitative Betrachtung nicht aufklärbarer Täterzusammenhänge wegen des Fehlens von Verkehrsdaten gibt es keine empirische Grundlage. Jedoch lässt sich ausschließen, dass das Fehlen von Vorratsdaten auf die Gesamtentwicklung beispw. des Betäubungsmittelhandels Auswirkungen gehabt hat[455].

19.4 Die Nutzung von gespeicherten Verkehrsdaten in Verbindung mit Bestandsdaten zur möglichst vollständigen Ermittlung in Volumenverfahren (Kinderpornografie, Urheberrechtsverstöße, Computerbetrug sowie mit Viren, Trojanern, etc. zusammenhängende Angriffe in Netzen). Dabei handelt es sich teilweise um sensible Deliktsbereiche. Allerdings dürfte es sich entweder gleichzeitig um Delikte handeln, die die Sicherheit insgesamt nicht beeinträchtigen, oder um Deliktsbereiche, die tatsächlich sicherheitsrelevant sein können, in denen aber auf die Gegenwart bzw. die Zukunft bezogene Ermittlungen in Datennetzen im Vordergrund stehen werden. Insbesondere gibt es bislang keinen Hinweis dafür, dass durch eine umfängliche Verfolgung aller Spuren, die auf das Herunterladen von Kinderpornografie hindeuten, sexueller Missbrauch über den Zufall hinaus verhindert werden kann.

4. Konsequenzen aus der Perspektive der betroffenen Praktiker

20. Mitunter andere Schwerpunkte zeigen die Bewertungen der befragten Praktiker auf, deren Wahrnehmungen die Einzelfallperspektive betreffen und determiniert sind durch den jeweils eigenen Arbeitsberiech bzw. die Kriminalitätsbereiche, die aktuell bearbeitet werden, sowie die jeweils benötigten Datenarten. Diese Faktoren tragen zu ganz unterschiedlichen Erfahrungen bei. Selbst innerhalb einer Behörde und noch mehr innerhalb eines Bundeslandes weichen auch die Schätzungen bezüglich des aktuellen Aufkommens der Maßnahmen, ob diese zu- oder abgenommen haben, sehr deutlich voneinander ab.

21. Auffällig ist, dass die Gespräche kaum Unterschiede zwischen den Einsatzbereichen der Gefahrenabwehr und der Strafverfolgung aufgezeigt haben. Die Anlässe sind zwar unter-

---

455 Vgl. zu den Zusammenhängen zwischen Strafverfolgung und Betäubungsmittelmärkten Reuter, P., Trautmann, F.: Report on Global Illicit Drugs Markets 1998-2007. Europäische Gemeinschaft, Brüssel 2009.

schiedlich, aber die unmittelbare Zielrichtung der Maßnahmen ist in beiden Fällen identisch: es geht jeweils um die Identifizierung von Personen, die für bestimmte Handlungen verantwortlich sind und deshalb zu identifizieren sind. Der Unterschied ist lediglich, dass es einmal um die Identifizierung von Tatverdächtigen geht und in dem anderen Fall um Störer.

22. Ausfälle beim Zugriff auf Verkehrsdaten sind nach Ansicht der befragten Ermittler in verschiedenen Bereichen festzustellen:

22.1. Fast vollständig weggefallen zu sein scheint derzeit die Speicherung von Verkehrsdaten eingehender Anrufe. Die Zielwahlsuche als mögliches Substitut für Situationen, in denen die gesuchte Nummer bekannt ist, ist nach übereinstimmendem Bericht sämtlicher Befragter bei der deutschen Telekom derzeit nicht möglich.

22.2. Besonders gravierend wirkt sich speziell bei internetbezogenen Recherchen bzw. Auskunftsbegehren der Umstand aus, dass sich TK-Unternehmen auf der Grundlage der aktuellen Fassung des § 113 TKG offenbar regelmäßig weigern, IP-Adressen nach den Bestandsdaten aufzulösen. Damit bleiben zahlreiche Fälle aus dem Bereich der IuK-Kriminalität derzeit offensichtlich unaufklärbar. Dies kann insbesondere auch Ermittlungen in dem Bereich Kinderpornographie tangieren.

22.3. Systematische Ausfälle benennen die befragten Praktiker auch im Hinblick auf konkrete Gerätekennungen. Bei IMSI- und IMEI-Nummern würden viele Abfragen mangels Abrechnungsrelevanz negativ beauskunftet.

22.4. Weitere Einschränkungen werden beobachtet bei Funkzellenabfragen, und dabei insbesondere in der Echtzeitvariante. Die letztere scheint bei keinem der Provider technisch möglich zu sein, sodass § 100g Abs. 3 StPO insoweit totes Recht ist.

22.5. Echtzeitabfragen speziell im Mobilfunkbereich sind derzeit nur auf der Grundlage eines Beschlusses nach § 100a StPO möglich, da eine technische Norm zur Trennung von Inhaltsdaten fehlt.

23. Soweit Daten ungeachtet der vorgenannten Einschränkungen doch noch gespeichert werden, ist die Situation derzeit von beachtlichen Unterschieden in der Speicherpraxis der Unternehmen und in Konsequenz daraus in der Verfügbarkeit der Verkehrsdaten gekennzeichnet. Die Varianzen werden sowohl in den von der Bundesnetzagentur (siehe oben Tabelle C-5, C-6) als auch in den von den Behörden erstellten Übersichten (siehe oben Tabelle F-2) erkennbar. Der drohende Datenverlust erzeugt einen Zeitdruck, der sich bei den Ermittlern spürbar auswirkt und zu unterschiedlichen Reaktionen führen kann (siehe dazu auch gleich unten Pkt. 29 bis 31). Auch Ermittlungsrichter spüren diesen Zeitdruck.

24. Besonders kurze Speicherfristen sind in Bezug auf IP-Adressen festzustellen. Darüber hinaus wird generell auf den häufigen Verlust von Daten verwiesen, die länger in die Vergangenheit zurückreichen. Besonders evident sei dies in Fällen, in denen häufig eine verzö-

gerte Anzeigeerstattung zu verzeichnen ist. Dies sind beispielsweise Fälle des Phishings und des Internetbetrugs, aber auch der sog. Enkeltrick.

25. Die Erreichbarkeit von Verkehrsdaten hängt damit maßgeblich von dem Speicherverhalten und der Auskunftsbereitschaft der jeweiligen TK-Unternehmen ab. Manche Experten haben die Vermutung geäußert, dass sich Täter, die ein gewisses Verständnis für Fragen der Telekommunikationstechnik haben, die unterschiedlichen Speicherpraktiken zu Nutze machen und sich systematisch unverletzlich machen könnten. Die Aufklärungswahrscheinlichkeit kann damit nicht nur zufallsabhängig sein – nämlich von der Frage, bei welchem Telekommunikationsanbieter und unter welchem Gebührenmodell ein Verdächtiger seine Kommunikation abwickelt –, sondern auch anfällig für Manipulation durch die potenziellen Zielpersonen selbst.

26. Keinen adäquaten Ersatz gibt es nach Ansicht der Befragten für löschungsbedingt verloren gegangene retrograde Daten. Dies betrifft vor allem Ermittlungen in den in Teil F unter Pkt. 1.2.3.1. im einzelnen aufgezählten Deliktsbereichen und Gefahrensituationen.

27. Fehlende Verkehrsdaten sind darüber hinaus überall dort nicht ersetzbar, wo ihnen über die ermittlungstechnische Funktion hinaus für den weiteren Verfahrensgang auch Beweisfunktion zukommt und andere Beweismittel nicht zur Verfügung stehen.

28. Speziell bei Ermittlungen mit Bezug auf das Internet kumulieren mehrere Aspekte: die besonders kurzen Speicherfristen bei IP-Adressen, unterschiedliche Rechtsauffassungen zwischen Ermittlern und Anbietern über den Rechtscharakter und die erforderlichen Voraussetzungen für die Zusammenführung von IP-Adresse und Bestandsdatum, sowie technische Lücken betreffend die Konfigurierung von Ports an Hotspots (Stichwort: IP-Sharing). Durch diese Umstände wird die Ermittlungsarbeit im Bereich der IuK-Kriminalität spürbar erschwert. Sinnbildlich hierfür steht das Zitat eines der Experten aus Baden-Württemberg, der die aktuelle Situation im Internet sehr plastisch mit Straßenverkehr ohne Kfz-Kennzeichen verglich. Die Interviews deuten übereinstimmend darauf hin, dass hier derzeit die wohl gravierendste Schutzlücke zu finden ist.

29. Den unter Pkt. 22. aufgeführten Problemen begegnet die Praxis derzeit auf unterschiedliche Weise. Zum Teil – etwa im Bereich Internetkriminalität, wo Verkehrsdaten mitunter der einzige Ansatzpunkt sein können (z.B. Zuordnung von IP-Adressen oder Enkeltrick) – wird häufig von vornherein von einer Abfrage abgesehen, wenn die mutmaßliche Speicherfrist bereits abgelaufen ist. In anderen Behörden wird in dem Bewusstsein um den drohenden Datenverlust schnellstmöglich bzw. sofort ein Beschluss erwirkt. Damit werden unter Umständen mehr Abfragen getätigt als in früheren Jahren, als entsprechende Maßnahmen nicht eilig waren und erst nach vorangegangener Ermittlungsarbeit und sorgfältiger(er) Auswahl von Verdächtigen veranlasst wurden. Der vormals je nach Fallkonstellation recht späte Einsatz der Maßnahme war auch in den Daten der MPI-Studie 2008 erkennbar.

30. Verloren geht nach Angabe vieler Experten häufig auch die Filterfunktion der Verkehrsdatenauswertung im Vorfeld von § 100a-Maßnahmen. Dies könnte in verschiedenen ermittlungstaktischen Situationen zu einer größeren Streubreite und damit einer erhöhten Zahl von Inhaltsüberwachungen führen.

31. Darüber hinaus können, wenn auch nicht auf breiter Basis, die eingriffsintensiveren Maßnahmen gem. § 100a StPO auch als Substitut für die Verkehrsdatenabfrage eingesetzt werden. In diesem Kontext scheint auch die Sonderkonstellation der Auslandskopfüberwachung, die in bestimmten Fällen die problematisch gewordene Zielwahlsuche ergänzen oder ersetzen kann, eine zunehmende Rolle zu spielen. Einige Unternehmen haben von entsprechenden Beobachtungen berichtet. Auch dies könnte insgesamt zu einer Erhöhung bei den TKÜ-Anordnungen führen. Die Verkehrsdatenabfrage würde insoweit durch ein eingriffsintensiveres Substitut ersetzt. Beide Fälle sind allerdings auf die Ermittlung zukunftsgerichteter Daten beschränkt. Retrograde Daten können damit, wie bereits erwähnt, nicht ersetzt werden.

32. Die Feststellung potenzieller Schutzlücken kann nach alledem nicht abstrakt entlang einzelner Delikte oder Deliktsbereiche vorgenommen werden. Tatsächlich hängt dies maßgeblich von sechs Faktoren ab:

- der Deliktsart,
- der Datenart,
- der konkreten Ermittlungssituation,
- dem Einsatzziel,
- dem zuständigen TK-Unternehmen/Provider,
- dem Zeitablauf zwischen dem abfragerelevanten Kommunikationsgeschehen einerseits (tatbezogen oder bezogen auf die erhoffte ermittlungstaktische Erkenntnis) und dem Zeitpunkt der ersten Kenntniserlangung (häufig Zeitpunkt der Anzeigeerstattung); beide Zeitpunkte sind von den Behörden in der Regel nicht steuerbar.

Jeder einzelne der genannten Faktoren wie auch das Zusammentreffen von mehreren kann im Einzelfall zur Unerreichbarkeit von Verkehrsdaten und in der Folge auch zur Unaufklärbarkeit des Falles führen. Besonders häufig ist diese Konstellation derzeit im Bereich der IuK-Kriminalität festzustellen. Eine belastbare Quantifizierung ist derzeit freilich noch nicht möglich. Nach übereinstimmernden Angaben ist der Anteil jedenfalls als hoch einzuschätzen.

33. Im präventiven Bereich stellen sich im Vergleich zu dem repressiven Einsatz der Verkehrsdatenabfrage einige zusätzliche Probleme. Die befragten Polizeiexperten berichteten von mindestens zwei Fällen, in denen die Abwehr einer konkreten Todesgefahr infolge verweigerter Geo- und anderer Verkehrsdatenauskünfte misslungen sein soll. Im Hinblick auf internetbezogene Ermittlungen wurden auch mehrere Beispiele erläutert, in denen die Urheber von Amok- und anderen Gewaltandrohungen, die ihren Ursprung im Internet hatten, nicht identifizierbar gewesen seien. Auch das Fehlen von Funkzelleninformationen kann bei akuten

Gefahrenlagen sehr viel unmittelbarere Auswirkungen haben als im Rahmen von strafrechtlichen Ermittlungen. Ferner scheint es vorzukommen, dass bundesweit tätige Unternehmen Abfragen auf der Grundlage von Landespolizeigesetzen nicht anerkennen und nicht beauskunften, wenn die für die Abfrage zuständige Stelle nicht in demselben Bundesland ihren Sitz hat. Schließlich wurde berichtet, dass Unternehmensmitarbeiter mitunter eine von dem Beschluss oder der Eilanordnung abweichende eigene sachliche Bewertung vornähmen, etwa bei der Beurteilung des Vorliegens einer konkreten Gefahrenlage.

34. Als besonders unbefriedigend wird von Ermittlerseite empfunden, dass man derzeit einer gefühlten Willkür der Unternehmen ausgesetzt sei. Man wähnt sich unzureichend informiert und mitunter mit einer nicht durchschaubaren Beauskunftungspraxis konfrontiert und fühlt sich manchmal, überspitzt formuliert, in die Rolle eines Bittstellers versetzt. Nicht mit dem gewohnten Rollenverständnis als Ermittler lassen sich überdies auch die äußeren Begleiterscheinungen vereinbaren, so zum Beispiel der Zwang, wie private Kunden nur über Call-Center mit den zuständigen Abteilungen Kontakt aufnehmen zu müssen. Insofern unterscheidet sich auch die Unternehmenskultur bei den deutschen TK-Anbietern deutlich von derjenigen z.B. in den USA, wo offensiv und transparent über die Speicherpraxis und Abfragemöglichkeiten informiert wird.[456]

35. Zweifel werden von zahlreichen Praktikern auch an der Richtigkeit von Negativauskünften geäußert. Am deutlichsten wurde hier ein Ermittler aus Österreich, der dezidiert ausführte, die Unternehmen Standortdaten *„lügen uns* [was das Vorhandensein von gespeicherten Daten anbetrifft] an“. Die deutschen Kollegen sprachen vorsichtiger von entsprechenden Vermutungen.

36. Insgesamt erscheint der gegenwärtig wieder aufgenommene Rückgriff auf abrechnungsrelevante Speichergrundätze nicht unbedingt sachgerecht. Die Zielsetzung ist eine gänzlich andere als für die Datenauswertung für Zwecke der Strafverfolgung. Das führt dazu, dass Unternehmen derzeit einseitig die Bedingungen setzen, die sich an den eigenen Interessen orientieren, aber eben nicht an denen der Polizei im Kontext ihrer Aufgabenerfüllung zur Gefahrenabwehr und Strafverfolgung.

37. Als weitere sehr praxisrelevante Regelungslücke wurde von den Experten die Verifizierungspflicht für den Kauf von SIM-Karten im Allgemeinen und Prepaid-Karten im Besonderen identifiziert. Ermittler stoßen auch immer wieder an Grenzen, wenn bei Ermittlungen im Internet ein sog. *„Donald-Duck-Account“* ermittlungserheblich ist.

---

456 Vgl. etwa das Microsoft Criminal Compliance Handbook: Microsoft Online Services, Global Criminal Compliance Handbook, U.S. Domestic Version, March 2008, abrufbar unter http://publicintelligence.net/microsoft-online-services-global-criminal-compliance-handbook/ [Juni 2011].

5. Quick Freeze

38. In einem Quick-Freeze-Verfahren wird von den Praktikern über alle Berufsgruppen hinweg kein taugliches Äquivalent zur Vorratsdatenspeicherung gesehen. Dieser Ansicht waren neben den Praktikern aus Deutschland auch die Experten aus Österreich und Schweden. Zur Begründung führen die Befragten, sinngemäß übereinstimmend, an, dass diese Methode lediglich ohnehin vorhandene Verkehrsdaten selektiv vor der Löschung bewahren, gerade die aus ermittlerischer Perspektive besonders wichtigen retrograden Daten aber nicht ex post generieren könne.

6. Situation im Ausland

39. Auch die ausländischen Interviewpartner verweisen darauf, dass die Verkehrsdatenabfrage heute ein wichtiger Bestandteil im Katalog der polizeilichen Ermittlungsmaßnahmen sei.

40. Besondere Bedeutung haben nach europäischen und außereuropäischen polizeilichen Erfahrungen Telekommunikationsverkehrsdaten übereinstimmend für die Strafverfolgung bei Banden- und organisierter Kriminalität, Telekommunikations- bzw. Computerkriminalität. Wegen der weiten Verbreitung moderner Kommunikationsmittel bieten darüber hinaus Verkehrsdaten in allen Deliktsbereichen zusätzliche Ermittlungsansätze.

41. Der internationale Vergleich lässt (bei vergleichbarer Einschätzung des Nutzens von Verkehrsdaten) Unterschiede in der rechtspolitischen Haltung zur Vorratsdatenspeicherung erkennen. Insbesondere in den USA, Kanada, Australien und Neuseeland sind über vereinzelte und sachlich begrenzte Initiativen hinaus keine Ansätze zur Einführung einer umfassenden Vorratsdatenspeicherung festzustellen. Dies wird zumindest für die USA auch dadurch erklärt, dass Telekommunikationsunternehmen wegen fehlender datenschutzrechtlicher Restriktionen in weitem Umfang Verkehrsdaten speichern, auf die Strafverfolgungsbehörden zugreifen können. Diese deutlich anderen Rahmenbedingungen sind bei der Bewertung des möglichen Potenzials des Quick-Freeze-Verfahrens unbedingt zu berücksichtigen.

42. Die derzeitige Situation der Implementierung der Richtlinie 2006/24/EG in den Mitgliedsländern der Europäischen Union lässt erhebliche Variation erkennen. In einem Teil der Mitgliedsländer ist die Richtlinie noch nicht implementiert oder der Vollzug ausgesetzt worden. Dies hat unterschiedliche Gründe.

43. In Rumänien versperrt nunmehr die kompromisslos ablehnende Entscheidung des Verfassungsgerichts eine Umsetzung der Richtlinie. Die verfassungsrechtlichen Fragestellungen werden mit einer noch ausstehenden Entscheidung des ungarischen Verfassungsgerichts und mit einer Vorlage des Obersten Irischen Gerichts beim Europäischen Gerichtshof (Luxemburg) zur Vereinbarkeit der Richtlinie mit der EMRK weiter verfolgt.

44. Soweit die Richtlinie implementiert worden ist, haben die jeweiligen nationalen Gesetzgebungen zu Unterschieden geführt, die in der Richtlinie allerdings bereits vorgezeichnet

sind. Dies betrifft vor allem die Dauer der Speicherung, die Reichweite (im Hinblick auf die mittels auf Vorrat gespeicherter Verkehrsdaten verfolgbarer Straftaten und der Art und Weise der Festlegung der verfolgbaren Straftaten) sowie die sonstigen Bedingungen, unter denen Verkehrsdaten abgerufen werden können.

45. Jedoch äußern sich vor allem die niederländische und die englische Regierung sehr vorsichtig über das Potenzial der Vorratsdatenspeicherung entlang der Vorgaben der Richtlinie 2006/24/EG. Denn es ist nach diesen Stellungnahmen abzusehen, dass die weitere Entwicklung der Kommunikationstechnologie die jetzige Ausrichtung der Richtlinie überholen und neue Bedürfnisse für den Zugriff auf Kommunikations(verkehrs)daten auslösen wird.

7. Der Evaluationsbericht der Europäischen Kommission

46. Der Evaluationsbericht der Europäischen Kommission geht davon aus, dass die Vorratsspeicherung von Telekommunikationsdaten signifikant zur Sicherheit in Europa beigetragen habe.

47. Die Evaluation der Europäischen Kommission konnte sich allerdings wegen der fehlenden Differenzierung zwischen auf Vorrat gespeicherten und anderen Verkehrsdaten von vornherein nicht auf eine Bewertung der Vorratsdatenspeicherung beziehen. Der Bericht enthält nur solche Daten, die allein die Praxis allgemeiner Verkehrsdatenabfragen beschreiben.

48. Die Beschreibung der Nutzung von Verkehrsdaten bezieht sich auf Daten aus etwa einem Drittel der Mitgliedsländer. Ganz überwiegend können die Mitgliedsländer nicht einmal über einfache Strukturen der Verkehrsdatenabfrage Auskunft geben.

49. Die Statistiken zur Verkehrdatenabfrage lassen nicht unterscheiden zwischen Bestandsdaten und Verkehrsdaten im engeren Sinn. Ferner werden verschiedene Abfragearten nicht differenziert.

50. Die Beschreibung der Nutzung von Verkehrs- und Bestandsdaten unterscheidet nicht nach der Deliktsart oder -schwere. Die Evaluation enthält keine Aussage darüber, ob und inwieweit Vorratsdaten oder allgemeine Verkehrsdaten der Telekommunikation für Ermittlungen im Bereich schwerer Kriminalität Bedeutung haben.

51. Die von den Mitgliedsländern übermittelten Statistiken lassen in keinem Fall eine Aussage darüber zu, ob und in welchem Ausmaß (allgemeine) Verkehrsdaten in strafrechtlichen Ermittlungsverfahren zur Aufklärung von Straftaten beigetragen haben (oder nicht).

52. Die über die wenig aussagekräftigen Statistiken hinausgehenden Informationen und Fallberichte sind weitgehend nicht nachvollziehbar und deshalb als Grundlage für eine Evaluation nicht geeignet.

53. Die von der Europäischen Kommission vorgelegte Evaluation der Richtlinie 2006/24/EG lässt aus den genannten Gründen jedenfalls nicht erwarten, dass das mit der Richtlinie ver-

bundene rechtspolitische Konfliktpotenzial in einem absehbaren Zeitraum ausgeräumt werden könnte.

Anhang A: Ergänzende statistische Materialien

Inhalt:

Bundesamt für Justiz
Referat III 3
4104/1 - B7 178/2009

Übersicht
Verkehrsdatenerhebung
(Maßnahmen nach § 100g StPO)
für 2008

Stand: 24. August 2009

1.	Land	BW	BY	BE	BB	HB	HH	HE	MV	NI	NW	RP	SL [2]	SN	ST	SH	TH	GBA [3]	insges.
2.	**Berichtsjahr**	**2008**																	
3.	**Anzahl der Verfahren**, in denen im Berichtsjahr Maßnahmen nach **§ 100g Abs. 1 StPO** durchgeführt worden sind	1.711	1.405	408	168	150	405	550	330	766	942	311	147	373	306	190	127	27	**8.316**
4.	**Anzahl der Anordnungen zur Erhebung von Verkehrsdaten** [1] unterschieden nach																		
4.1	Erstanordnungen	2.733	1.994	402	199	249	780	740	482	1.155	1.587	617	465	666	358	415	160	424	**13.426**
4.2	Verlängerungsanordnungen	55	30	6	2	0	9	31	11	53	37	7	4	2	1	26	1	203	**478**
5.	**Anlassstraftaten**																		
5.1	nach § 100g Abs. 1 Satz 1 **Nr. 1** StPO	2.578	1.749	393	150	177	765	673	422	1.153	1.370	529	461	555	301	428	138	627	**12.469**
5.2	nach § 100g Abs. 1 Satz 1 **Nr. 2** StPO	205	275	15	51	72	23	99	71	55	242	95	4	113	58	13	23	0	**1.414**
6.	**Alter der abgefragten Verkehrsdaten**																		
6.1	bis zu einem Monat	975	827	76	88	135	259	183	217	284	510	308	151	236	174	105	48	22	**4.598**
6.2	bis zu zwei Monate	283	248	70	25	40	242	45	49	125	149	63	67	98	74	19	20	7	**1.624**
6.3	bis zu drei Monate	655	250	171	40	41	96	235	55	407	528	108	176	88	70	106	24	91	**3.141**
6.4	bis zu vier Monate	154	82	20	12	10	33	14	31	46	45	11	37	33	8	9	6	34	**585**
6.5	bis zu fünf Monate	53	63	6	5	4	29	10	12	30	30	14	0	25	8	9	16	34	**348**
6.6	bis zu sechs Monate	257	288	12	18	6	90	48	4	74	201	93	34	113	19	71	29	46	**1.403**
6.7	bis zu sieben Monate	117	43	6	7	3	7	4	23	13	42	0	0	29	4	11	3	19	**331**
6.8	mehr als sieben Monate	147	138	8	0	10	13	41	5	108	53	6	0	27	0	87	3	8	**654**
6.9	Es wurden nur künftig anfallende Verkehrsdaten abgefragt	142	85	39	6	0	19	23	97	121	54	21	k.A.	19	2	24	12	k.A.	**664**
7.	**Anzahl der ergebnislos gebliebenen Maßnahmen,** weil die abgefragten Daten ganz oder teilweise nicht verfügbar waren	176	131	18	47	0	47	17	97	59	157	60	k.A.	42	68	3	9	0	**931**

[1] Hinweis: Die Summen der Angaben in Rubrik 4 weichen teilweise von den Summen der Angaben in den Rubriken 5 und 6 ab. Dies beruht darauf, dass bei Erst- und Verlängerungsanordnungen, die in einem Beschluss ergehen, zwar unter Punkt 4. sowohl die Erst- als auch die Verlängerungsanordnung gezählt, die Anlassstraftat und das Alter der abgefragten Daten aber nur einmal erfasst wird bzw. nur auf Erstanordnungen abgestellt wurde und bestimmte Angaben (vgl. Fn. 2 und 3) nicht erfasst wurden.

[2] Die Daten zu den Ziffern 6.9 und 7 wurden von der LJV Saarland nicht mitgeteilt.

[3] Die Daten zu Ziffer 6.9 wurden beim GBA für 2008 versehentlich nicht erhoben.

Bundesamt für Justiz
Referat III 3
4104/1

28.10.2010

Übersicht
Telekommunikationsüberwachung
(Maßnahmen nach § 100g StPO)
für 2009

1.	Land	BW	BY	BE	BB	HB	HH	HE	MV	NI	NW	RP	SL	SN	ST	SH	TH	GBA	insges.
2.	**Berichtsjahr**	**2009**																	
3.	**Anzahl der Verfahren**, in denen im Berichtsjahr Maßnahmen nach **§ 100g Abs. 1 StPO** durchgeführt worden sind	1.298	2161	762	358	127	541	689	328	679	931	338	85	422	293	323	91	33	**9.459**
4.	**Anzahl der Anordnungen zur Erhebung von Verkehrsdaten** unterschieden nach																		
4.1	Erstanordnungen	1.982	4.259	747	546	239	1.006	1.004	479	1.390	1.444	670	80	644	399	396	143	279	**15.707**
4.2	Verlängerungsanordnungen	32	52	15	9	0	17	86	16	51	63	8	5	8	1	29	3	124	**519**
5.	**Anlassstraftaten**																		
5.1	nach § 100g Abs. 1 Satz 1 **Nr. 1** StPO	1.875	4.015	741	484	165	997	987	408	1.375	1.222	592	74	559	372	384	106	358	**14.714**
5.2	nach § 100g Abs. 1 Satz 1 **Nr. 2** StPO	139	296	21	71	74	24	103	87	66	285	86	11	93	28	41	33	0	**1.458**
6.	**Alter der abgefragten Verkehrsdaten**																		
6.1	bis zu einem Monat	737	1.541	113	179	140	336	275	194	295	352	387	35	216	123	140	37	14	**5.114**
6.2	bis zu zwei Monate	229	764	116	76	39	260	96	67	90	165	43	8	104	85	71	53	13	**2.279**
6.3	bis zu drei Monate	303	406	328	104	20	154	184	65	344	435	141	31	101	80	40	10	39	**2.785**
6.4	bis zu vier Monate	111	282	48	86	8	37	35	22	61	54	18	3	40	49	9	7	8	**878**
6.5	bis zu fünf Monate	81	173	41	5	7	42	16	5	51	25	13	0	24	17	4	3	6	**513**
6.6	bis zu sechs Monate	323	261	59	46	3	152	373	19	272	240	15	6	83	31	95	18	125	**2.121**
6.7	bis zu sieben Monate	96	328	17	9	1	17	39	6	109	45	6	0	52	2	7	3	5	**742**
6.8	mehr als sieben Monate	69	435	12	4	8	18	63	8	47	47	16	0	21	2	3	5	16	**774**
6.9	Es wurden nur künftig anfallende Verkehrsdaten abgefragt	65	121	28	46	13	5	9	109	172	144	36	2	11	11	56	4	53	**885**
7.	**Anzahl der ergebnislos gebliebenen Maßnahmen,** weil die abgefragten Daten ganz oder teilweise nicht verfügbar waren	74	92	19	89	0	3	37	32	53	46	7	1	37	34	14	20	0	**558**

Bundesamt für Justiz
Referat III 3

Stand: 22. August 2008

Übersicht
Sondererfassung von Ermittlungsverfahren, in denen Anordnungen nach § 100g StPO ergingen
- Erhebungszeitraum 1. Mai 2008 bis einschließlich 31. Juli 2008 -

Lfd. Nr. des Erhebungsbogens und Text		BW	BY	BE	BB	HB	HH [1]	HE	MV [2]	NI	NW	RP [3]	SL	SN [4]	ST	SH	TH [5]	GBA	insges.
Berichtsjahr		**Erhebungszeitraum: 1. Mai 2008 bis einschließlich 31. Juli 2008**																	
Geschäftszeichen (Bund) zu dieser Sondererfassung:		**III 3 - 4104/2-2-B7 296/2008**																	
4.	**Anordnungen nach § 100g StPO, die <u>im Erhebungszeitraum</u> ergingen**																		
4.0	Gesamtanzahl der Ermittlungsverfahren in denen Anordnungen nach § 100g StPO ergingen (= Anzahl der erfassten Einzelerhebungsbögen)	358	359	167	37	31	75	150	67	281	306	71	10	91	91	66	21	5	**2.186**
4.1	Gesamtanzahl der Anordnungen nach § 100g StPO (= Summe aus den Angaben zu 4.1 in den Einzelerhebungsbögen)	716	729	327	43	107	136	265	100	579	708	164	24	148	102	127	45	36	**4.356**
4.1.1	**davon** waren Erstanordnungen (= Summe aus den Angaben zu 4.1.1 in den Einzelerhebungsbögen)	704	703	321	43	107	135	240	100	544	685	160	23	148	102	119	45	32	**4.211**
4.1.2	**davon** waren Verlängerungsanordnungen (= Summe aus den Angaben zu 4.1.2 in den Einzelerhebungsbögen)	12	26	6	0	0	1	25	0	35	23	4	1	0	0	8	0	4	**145**
5.	**"Vorratsdaten"**																		
5.1.a	Anzahl der <u>Verfahren</u> in denen die ersuchten TK-Unternehmen (auch) auf allein nach § 113a gespeicherte Daten zurückgreifen mussten (= Summe der Einzelerhebungsbögen in denen bei 5.1 "Ja" angekreuzt wurde)	189	125	73	19	15	38	32	26	125	163	32	7	36	22	20	11	1	**934**
5.1.b	Anzahl der <u>Verfahren</u> in denen die ersuchten TK-Unternehmen <u>nicht</u> auf allein nach § 113a gespeicherte Daten zurückgreifen mussten (= Summe der Einzelerhebungsbögen in denen bei 5.1 "Nein" angekreuzt wurde)	83	77	69	6	15	16	46	34	61	102	24	3	34	32	19	2	4	**627**
5.1.c	Anzahl der <u>Verfahren</u> in denen eine Angabe dazu ob auf allein nach § 113a TKG gespeicherte Daten zurückgegriffen werden musste nicht möglich war (= Summe der Einzelerhebungsbögen in denen bei 5.1 "Angabe ganz oder teilweise nicht möglich ..." angekreuzt wurde)	86	157	32	11	7	11	29	7	95	41	15	0	13	37	27	8	1	**577**

Bundesamt für Justiz
Referat III 3

Stand: 22. August 2008

Übersicht
Sondererfassung von Ermittlungsverfahren, in denen Anordnungen nach § 100g StPO ergingen
- Erhebungszeitraum 1. Mai 2008 bis einschließlich 31. Juli 2008 -

Lfd. Nr. des Erhebungsbogens und Text		BW	BY	BE	BB	HB	HH [1]	HE	MV [2]	NI	NW	RP [3]	SL	SN [4]	ST	SH	TH [5]	GBA	insges.
5.1.1	Anzahl der (Erst- und Verlängerungs-) Anordnungen zu deren Bearbeitung die ersuchten TK-Unternehmen auf allein nach § 113a TKG gespeicherte Daten zurückgreifen mussten (= Summe aus den Angaben zu 5.1.1 in den Einzelerhebungsbögen)	367	240	162	23	50	49	40	52	185	329	107	9	52	23	31	20	3	**1.742**
5.1.2	Anzahl der (Erst- und Verlängerungs-) Anordnungen bei denen das Auskunftsersuchen (ganz oder teilweise) erfolglos blieb weil die Speicherungs-verpflichtung nach § 113a TKG von dem TK-Unternehmen ganz oder teilweise noch nicht erfüllt wird (= Summe aus den Angaben zu 5.1.2 in den Einzelerhebungsbögen)	43	25	7	0	2	0	5	6	4	17	9	0	1	0	5	5	3	**132**
5.1.3	Anzahl der Verfahren in denen Auskunftsersuchen (ganz oder teilweise) erfolglos blieben weil es sich nicht um Straftaten nach § 100a Abs. 1 und 2 StPO handelte (= Summe der Einzelerhebungsbögen in denen bei 5.1.3 "Ja" angekreuzt wurde)	16	17	6	4	1	7	2	3	9	25	3	0	0	0	3	0	0	**96**
5.1.3.1	Anzahl der (Erst- und Verlängerungs-) Anordnungen in denen Auskunftsersuchen (ganz oder teilweise) erfolglos blieben weil es sich nicht um Straftaten nach § 100a Abs. 1 und 2 StPO handelte (= Summe aus den Angaben zu 5.1.3.1 in den Einzelerhebungsbögen)	10	16	6	4	2	7	0	3	9	33	8	0	0	0	4	0	0	**102**
5.1.3.2.a	Anzahl der Verfahren in denen die Erfolglosigkeit des Auskunftsersuchens die Aufklärung der Straftat vereitelt hat (= Summe der Einzelerhebungsbögen in denen bei 5.1.3.2 a) angekreuzt wurde)	9	8	6	1	0	4	1	3	7	21	2	0	0	0	1	0	0	**63**
5.1.3.2.b	Anzahl der Verfahren in denen die Erfolglosigkeit des Auskunftsersuchens die Aufklärung der Straftat erschwert hat (= Summe der Einzelerhebungsbögen in denen bei 5.1.3.2 b) angekreuzt wurde)	6	7	0	2	0	3	1	0	1	13	2	0	0	0	2	0	0	**37**
5.1.3.2.c	Anzahl der Verfahren in denen die Erfolglosigkeit des Auskunftsersuchens keine nachteiligen Auswirkungen auf das Ermittlungsverfahren hatte bzw. haben wird (= Summe der Einzelerhebungsbögen in denen bei 5.1.3.2 c) angekreuzt wurde)	1	4	0	1	1	0	0	0	2	0	0	0	0	0	0	0	0	**9**

Bundesamt für Justiz
Referat III 3

Übersicht

Stand: 22. August 2008

Sondererfassung von Ermittlungsverfahren, in denen Anordnungen nach § 100g StPO ergingen
- Erhebungszeitraum 1. Mai 2008 bis einschließlich 31. Juli 2008 -

Lfd. Nr. des Erhebungsbogens und Text		BW	BY	BE	BB	HB	HH [1)]	HE	MV [2)]	NI	NW	RP [3)]	SL	SN [4)]	ST	SH	TH [5)]	GBA	insges.
6.	**Anlassstraftaten**																		
6.1 *)	Anzahl der Verfahren denen Straftat(en) nach § 100a Abs. 1 und 2 StPO zugrunde lagen (= Summe der Erhebungsbögen in denen 6.1 angekreuzt wurde)	259	230	114	13	24	59	145	25	176	192	58	9	61	62	51	15	4	**1.497**
6.2 *)	Anzahl der Verfahren denen Straftat(en) nach § 100g Abs. 1 Satz 1 **Nr. 1** StPO zugrunde lagen (= Summe der Erhebungs-bögen in denen 6.2 angekreuzt wurde)	316	151	116	19	17	12	110	32	94	129	39	4	54	13	20	2	3	**1.131**
6.3 *)	Anzahl der Verfahren denen Straftat(en) nach § 100g Abs. 1 Satz 1 **Nr. 2** StPO zugrunde lagen (= Summe der Erhebungs-bögen in denen 6.3 angekreuzt wurde)	54	62	11	9	3	4	24	16	20	41	10	1	20	25	8	4	0	**312**

Die Bezeichnung der lfd. Nrn. 1 bis 3 sind entfallen, da es sich hier lediglich um die Kennzeichnung der ersten drei allgemeinen Spalten handelt.

*) Mehrfachnennungen sind möglich. Baden-Württemberg hat mitgeteilt, dass in Ziffer 6.2 die Verfahren nach Ziffer 6.1 enthalten sind.

[1)] Zu 5.1.c:

Hinzu kommen 10 Verfahren, in denen noch keine (vollständigen) Auskünfte vorliegen.

[2)] Zu 5.1.b:

Bei 2 Verfahren zum Zeitpunkt der Erhebung noch nicht bekannt.

Zu 5.1.2 bis 5.1.3.2.c:

Zum Teil waren Angaben zum Erhebungszeitpunkt noch nicht möglich.

[3)] Zu 5.1.c:

Ein Auskunftsergebnis liegt noch nicht vor.

[4)] Zu 5.1.c:

In einem Fall nichts angekreuzt, aber dahingehend erläutert.

Zu 6.3:

In einem Fall nichts angekreuzt, aber gemäß genannter Vorschrift eingestuft.

[5)] Nr. 5.1.c:

In 3 Fällen liegen noch keine Antworten des TK-Unternehmens vor, in 1 Fall waren die Akten noch zur Bearbeitung beim LKA.

Nr. 5.1.2:

In 2 weiteren Verfahren noch offen.

Bundesamt für Justiz
Referat III 3

Stand: 19. März 2009

Übersicht
Sondererfassung von Ermittlungsverfahren, in denen Anordnungen nach § 100g StPO ergingen
- Erhebungszeitraum 1. August 2008 bis einschließlich 28. Februar 2009 -

Lfd. Nr. des Erhebungsbogens und Text		BW	BY	BE	BB	HB	HH	HE	MV	NI	NW	RP	SL	SN	ST	SH	TH	GBA	insges.
Berichtsjahr		**1. August 2008 bis 28. Februar 2009 - Sondererhebung -**																	
Geschäftszeichen (Bund) zu dieser Sondererfassung:		**III 3 - 4104/1 - B7 626/2008**																	
4.	**Anordnungen nach § 100g StPO, die <u>im Erhebungszeitraum</u> ergingen**																		
4.0	Gesamtanzahl der Ermittlungsverfahren in denen Anordnungen nach § 100g StPO ergingen (= Anzahl der erfassten Einzelerhebungsbögen)	785	793	172	48	69	287	224	168	439	453	130	25	211	161	172	52	16	**4.205**
4.1 [1)]	Gesamtanzahl der Anordnungen nach § 100g StPO (= Summe aus den Angaben zu 4.1 in den Einzelerhebungsbögen)	1.399	1.509	352	131	189	579	445	325	956	1.062	305	32	375	209	298	106	114	**8.386**
4.1.1	**davon** waren Erstanordnungen (= Summe aus den Angaben zu 4.1.1 in den Einzelerhebungsbögen)	1.364	1.458	349	131	187	577	438	308	913	1.016	288	32	370	208	287	103	99	**8.128**
4.1.2	**davon** waren Verlängerungsanordnungen (= Summe aus den Angaben zu 4.1.2 in den Einzelerhebungsbögen)	35	51	3	0	2	2	7	17	44	46	21	0	5	1	25	3	15	**277**
5.	**"Vorratsdaten"**																		
5.1.a	Anzahl der <u>Verfahren</u> in denen die ersuchten TK-Unternehmen (auch) auf allein nach § 113a gespeicherte Daten zurückgreifen mussten (= Summe der Einzelerhebungsbögen in denen bei 5.1 "Ja" angekreuzt wurde)	447	311	95	14	18	252	80	57	195	201	47	19	110	57	11	27	5	**1.946**
5.1.b	Anzahl der <u>Verfahren</u> in denen die ersuchten TK-Unternehmen <u>nicht</u> auf allein nach § 113a gespeicherte Daten zurückgreifen mussten (= Summe der Einzelerhebungsbögen in denen bei 5.1 "Nein" angekreuzt wurde)	188	263	2	19	34	17	95	76	156	165	44	4	68	59	97	20	7	**1.314**
5.1.c [2)]	Anzahl der <u>Verfahren</u> in denen eine Angabe dazu ob auf allein nach § 113a TKG gespeicherte Daten zurückgegriffen werden musste nicht möglich war (= Summe der Einzelerhebungsbögen in denen bei 5.1 "Angabe ganz oder teilweise nicht möglich ..." angekreuzt wurde)	150	219	31	15	12	10	37	35	152	87	39	2	27	45	64	5	4	**934**

Bundesamt für Justiz
Referat III 3

Übersicht

Stand: 19. März 2009

Sondererfassung von Ermittlungsverfahren, in denen Anordnungen nach § 100g StPO ergingen
- Erhebungszeitraum 1. August 2008 bis einschließlich 28. Februar 2009 -

Lfd. Nr. des Erhebungsbogens und Text		BW	BY	BE	BB	HB	HH	HE	MV	NI	NW	RP	SL	SN	ST	SH	TH	GBA	insges.
5.1.1	Anzahl der (Erst- und Verlängerungs-) Anordnungen zu deren Bearbeitung die ersuchten TK-Unternehmen auf allein nach § 113a TKG gespeicherte Daten zurückgreifen mussten (= Summe aus den Angaben zu 5.1.1 in den Einzelerhebungsbögen)	750	563	138	51	38	452	178	119	360	428	122	20	158	78	12	41	7	**3.515**
5.1.2 [3) 4)]	Anzahl der (Erst- und Verlängerungs-) Anordnungen bei denen das Auskunftsersuchen (ganz oder teilweise) erfolglos blieb weil die Speicherungs-verpflichtung nach § 113a TKG von dem TK-Unternehmen ganz oder teilweise noch nicht erfüllt wird (= Summe aus den Angaben zu 5.1.2 in den Einzelerhebungsbögen)	41	71	10	2	2	5	15	10	8	11	2	2	3	5	1	3	0	**191**
5.1.3 [3) 4)]	Anzahl der Verfahren in denen Auskunftsersuchen (ganz oder teilweise) erfolglos blieben weil es sich nicht um Straftaten nach § 100a Abs. 1 und 2 StPO handelte (= Summe der Einzelerhebungsbögen in denen bei 5.1.3 "Ja" angekreuzt wurde)	39	44	5	2	1	26	13	3	21	15	2	2	4	2	2	2	0	**183**
5.1.3.1 [3) 4)]	Anzahl der (Erst- und Verlängerungs-) Anordnungen in denen Auskunftsersuchen (ganz oder teilweise) erfolglos blieben weil es sich nicht um Straftaten nach § 100a Abs. 1 und 2 StPO handelte (= Summe aus den Angaben zu 5.1.3.1 in den Einzelerhebungsbögen)	46	43	7	1	3	28	10	3	23	16	3	2	3	2	3	5	0	**198**
5.1.3.2.a [4)]	Anzahl der Verfahren in denen die Erfolglosigkeit des Auskunftsersuchens die Aufklärung der Straftat vereitelt hat (= Summe der Einzelerhebungsbögen in denen bei 5.1.3.2 a) angekreuzt wurde)	25	24	2	0	0	21	7	3	12	10	2	1	3	0	2	0	0	**112**
5.1.3.2.b [5)]	Anzahl der Verfahren in denen die Erfolglosigkeit des Auskunftsersuchens die Aufklärung der Straftat erschwert hat (= Summe der Einzelerhebungsbögen in denen bei 5.1.3.2 b) angekreuzt wurde)	9	12	3	1	0	5	5	1	8	3	0	0	0	0	1	1	0	**49**

Übersicht

Stand: 19. März 2009

Sondererfassung von Ermittlungsverfahren, in denen Anordnungen nach § 100g StPO ergingen
- Erhebungszeitraum 1. August 2008 bis einschließlich 28. Februar 2009 -

Lfd. Nr. des Erhebungsbogens und Text		BW	BY	BE	BB	HB	HH	HE	MV	NI	NW	RP	SL	SN	ST	SH	TH	GBA	insges.
5.1.3.2.c [5]	Anzahl der Verfahren in denen die Erfolglosigkeit des Auskunftsersuchens keine nachteiligen Auswirkungen auf das Ermittlungsverfahren hatte bzw. haben wird (= Summe der Einzelerhebungsbögen in denen bei 5.1.3.2 c) angekreuzt wurde)	5	6	1	3	0	1	0	0	1	3	0	1	0	2	0	0	0	**23**
6.	**Anlassstraftaten**																		
6.1	Anzahl der Verfahren denen Straftat(en) nach § 100a Abs. 1 und 2 StPO zugrunde lagen (= Summe der Erhebungsbögen in denen 6.1 angekreuzt wurde)	603	545	143	30	53	198	121	103	341	312	94	20	143	112	133	27	16	**2.994**
6.2	Anzahl der Verfahren denen Straftat(en) nach § 100g Abs. 1 Satz 1 **Nr. 1** StPO zugrunde lagen die nicht bereits zu 6.1 erfasst sind (= Summe der Erhebungsbögen in denen 6.2 angekreuzt wurde)	103	129	24	64	10	84	86	51	77	114	22	2	44	28	38	14	0	**890**
6.3	Anzahl der Verfahren denen Straftat(en) nach § 100g Abs. 1 Satz 1 **Nr. 2** StPO zugrunde lagen die nicht bereits zu 6.1 erfasst sind (= Summe der Erhebungsbögen in denen 6.3 angekreuzt wurde)	99	132	5	9	6	5	36	14	26	60	20	3	39	25	5	11	0	**495**

Die Bezeichnung der lfd. Nrn. 1 bis 3 sind entfallen, da es sich hier lediglich um die Kennzeichnung der ersten drei allgemeinen Spalten handelt.

[1] Rheinland-Pfalz: Die Summe der Positionen 4.1.1 und 4.1.2 ist höher als in Position 4.1 ausgewiesen, weil in 4 Fällen Erst- und Folgeanordnungen zu einer Anordnung verbunden worden sind.

Niedersachsen: Die Summe der Positionen 4.1.1 und 4.1.2 ist höher als in Position 4.1 ausgewiesen, weil in 1 Fall Erst- und Verlängerungsanordnungen zu einer Anordnung verbunden worden sind.

Schleswig-Holstein: Die Summe der Positionen 4.1.1 und 4.1.2 ist höher als in Position 4.1 ausgewiesen, weil in 14 Fällen Erst- und Verlängerungsanordnungen zu einer Anordnung verbunden worden sind.

[2] Hamburg: Hinzu kommen 9 Verfahren, in denen noch keine (vollständigen) Auskünfte vorliegen.

[3] Saarland: 3 Antworten stehen noch aus.

[4] Mecklenburg-Vorpommern: Im Übrigen waren bei einer Staatsanwaltschaft Angaben bei Erhebung noch nicht möglich (auf Nachfrage keine Meldung erfolgloser Anordnungen).

[5] Mecklenburg-Vorpommern: Bei einer Staatsanwaltschaft sind noch keine Angaben möglich.

Bundesamt für Justiz
Referat III 3

Übersicht

Sondererfassung von Ermittlungsverfahren, in denen Anordnungen nach § 100g StPO ergingen
- Erhebungszeitraum 1. März 2009 bis 31. August 2009 -

Stand: 25. September 2009

Lfd. Nr. des Erhebungsbogens und Text		BW	BY	BE	BB	HB	HH [1]	HE	MV	NI	NW	RP	SL	SN	ST	SH [2]	TH	GBA	insges. [3]
Berichtsjahr		**1. März 2009 bis 31. August 2009 - Sondererhebung -**																	
Geschäftszeichen (Bund) zu dieser Sondererfassung:		**III 3 - 4104/1 - B7 504/2009**																	
4.	**Anordnungen nach § 100g StPO, die <u>im Erhebungszeitraum</u> ergingen**																		
4.0	Gesamtanzahl der Ermittlungsverfahren in denen Anordnungen nach § 100g StPO ergingen (= Anzahl der erfassten Einzelerhebungsbögen)	607	999	177	49	57	305	246	124	297	364	129	52	184	157	156	44	21	**3.968**
4.1	Gesamtanzahl der Anordnungen nach § 100g StPO (= Summe aus den Angaben zu 4.1 in den Einzelerhebungsbögen)	1.090	1.804	306	93	161	613	413	202	751	945	247	88	329	210	281	109	140	**7.782**
4.1.1	**davon** waren Erstanordnungen (= Summe aus den Angaben zu 4.1.1 in den Einzelerhebungsbögen)	1.066	1.785	278	93	156	605	406	192	729	889	243	87	329	210	259	108	103	**7.538**
4.1.2	**davon** waren Verlängerungsanordnungen (= Summe aus den Angaben zu 4.1.2 in den Einzelerhebungsbögen)	24	19	28	0	5	8	7	10	22	56	4	1	0	0	22	1	37	**244**
5.	**"Vorratsdaten"**																		
5.1.a	Anzahl der <u>Verfahren</u> in denen die ersuchten TK-Unternehmen (auch) auf allein nach § 113a gespeicherte Daten zurückgreifen mussten (= Summe der Einzelerhebungsbögen in denen bei 5.1 "Ja" angekreuzt wurde)	347	398	80	6	37	257	81	48	104	179	43	28	111	56	15	21	16	**1.827**
5.1.b	Anzahl der <u>Verfahren</u> in denen die ersuchten TK-Unternehmen <u>nicht</u> auf allein nach § 113a gespeicherte Daten zurückgreifen mussten (= Summe der Einzelerhebungsbögen in denen bei 5.1 "Nein" angekreuzt wurde)	148	292	71	40	17	20	145	67	133	121	51	16	62	67	120	16	4	**1.390**
5.1.c	Anzahl der <u>Verfahren</u> in denen eine Angabe dazu ob auf allein nach § 113a TKG gespeicherte Daten zurückgegriffen werden musste nicht möglich war (= Summe der Einzelerhebungsbögen in denen bei 5.1 "Angabe ganz oder teilweise nicht möglich ..." angekreuzt wurde)	112	309	26	3	3	16	20	9	60	64	35	8	11	34	18	7	1	**736**

Übersicht

Stand: 25. September 2009

Sondererfassung von Ermittlungsverfahren, in denen Anordnungen nach § 100g StPO ergingen
- Erhebungszeitraum 1. März 2009 bis 31. August 2009 -

Lfd. Nr. des Erhebungsbogens und Text		BW	BY	BE	BB	HB	HH [1]	HE	MV	NI	NW	RP	SL	SN	ST	SH [2]	TH	GBA	insges. [3]
5.1.1	Anzahl der (Erst- und Verlängerungs-) Anordnungen zu deren Bearbeitung die ersuchten TK-Unternehmen auf allein nach § 113a TKG gespeicherte Daten zurückgreifen mussten (= Summe aus den Angaben zu 5.1.1 in den Einzelerhebungsbögen)	617	666	87	3	78	507	144	80	149	435	93	32	193	66	25	32	87	**3.294**
5.1.2	Anzahl der (Erst- und Verlängerungs-) Anordnungen bei denen das Auskunftsersuchen (ganz oder teilweise) erfolglos blieb weil die Speicherungs-verpflichtung nach § 113a TKG von dem TK-Unternehmen ganz oder teilweise noch nicht erfüllt wird (= Summe aus den Angaben zu 5.1.2 in den Einzelerhebungsbögen)	15	36	5	0	4	0	8	1	1	19	1	1	5	3	1	0	0	**100**
5.1.3	Anzahl der Verfahren in denen Auskunftsersuchen (ganz oder teilweise) erfolglos blieben weil es sich nicht um Straftaten nach § 100a Abs. 1 und 2 StPO handelte (= Summe der Einzelerhebungsbögen in denen bei 5.1.3 "Ja" angekreuzt wurde)	32	40	3	0	8	29	7	3	13	18	4	2	3	1	5	2	0	**170**
5.1.3.1	Anzahl der (Erst- und Verlängerungs-) Anordnungen in denen Auskunftsersuchen (ganz oder teilweise) erfolglos blieben weil es sich nicht um Straftaten nach § 100a Abs. 1 und 2 StPO handelte (= Summe aus den Angaben zu 5.1.3.1 in den Einzelerhebungsbögen)	32	41	3	0	9	30	7	3	13	23	5	5	2	1	4	3	0	**181**
5.1.3.2.a	Anzahl der Verfahren in denen die Erfolglosigkeit des Auskunftsersuchens die Aufklärung der Straftat vereitelt hat (= Summe der Einzelerhebungsbögen in denen bei 5.1.3.2 a) angekreuzt wurde)	24	32	0	0	6	15	7	3	9	14	3	2	5	0	5	0	0	**125**
5.1.3.2.b	Anzahl der Verfahren in denen die Erfolglosigkeit des Auskunftsersuchens die Aufklärung der Straftat erschwert hat (= Summe der Einzelerhebungsbögen in denen bei 5.1.3.2 b) angekreuzt wurde)	7	9	1	0	0	5	1	0	1	3	1	0	0	0	0	2	0	**30**

Übersicht

Stand: 25. September 2009

Sondererfassung von Ermittlungsverfahren, in denen Anordnungen nach § 100g StPO ergingen
- Erhebungszeitraum 1. März 2009 bis 31. August 2009 -

Lfd. Nr. des Erhebungsbogens und Text		BW	BY	BE	BB	HB	HH [1]	HE	MV	NI	NW	RP	SL	SN	ST	SH [2]	TH	GBA	insges. [3]
5.1.3.2.c	Anzahl der Verfahren in denen die Erfolglosigkeit des Auskunftsersuchens keine nachteiligen Auswirkungen auf das Ermittlungsverfahren hatte bzw. haben wird (= Summe der Einzelerhebungsbögen in denen bei 5.1.3.2 c) angekreuzt wurde)	1	4	2	0	3	9	0	0	2	1	0	0	1	1	0	1	0	**25**
6.	**Anlassstraftaten**																		
6.1	Anzahl der Verfahren denen Straftat(en) nach § 100a Abs. 1 und 2 StPO zugrunde lagen (= Summe der Erhebungsbögen in denen 6.1 angekreuzt wurde)	492	680	145	31	38	197	178	63	242	264	88	38	137	114	115	21	21	**2.864**
6.2	Anzahl der Verfahren denen Straftat(en) nach § 100g Abs. 1 Satz 1 **Nr. 1** StPO zugrunde lagen die nicht bereits zu 6.1 erfasst sind (= Summe der Erhebungsbögen in denen 6.2 angekreuzt wurde)	56	160	28	8	9	97	96	41	40	76	17	10	20	27	33	12	0	**730**
6.3	Anzahl der Verfahren denen Straftat(en) nach § 100g Abs. 1 Satz 1 **Nr. 2** StPO zugrunde lagen die nicht bereits zu 6.1 erfasst sind (= Summe der Erhebungsbögen in denen 6.3 angekreuzt wurde)	70	159	4	10	15	11	35	20	16	24	24	4	28	17	8	11	0	**456**

Anmerkung: Die Bezeichnung der lfd. Nrn. 1 bis 3 sind entfallen, da es sich hier lediglich um die Kennzeichnung der ersten drei allgemeinen Spalten handelt.

[1] Hamburg: Hinzu kommen unter Punkt 5.1.c 12 Verfahren, in denen noch keine Auskünfte vorliegen.

[2] Die Abweichung zwischen der Anzahl der Verfahren in Nr. 4 zu der Summe der Verfahren aus den Nrn. 5.1.a bis 5.1.c beruht darauf, dass eine Staatsanwaltschaft in drei Verfahren keine Angaben gemacht hat.

[3] Siehe auch die Angaben in den Fußnoten zu 1) bis 2).

Anhang B: Interviewfragen

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Abteilung Kriminologie

Untersuchung möglicher Schutzlücken durch den Wegfall der Vorratsdatenspeicherung

Interviewleitfaden

A. Version Justiz

1. Zunächst als einleitende **Ersteinschätzung**: Wie beurteilen Sie die praktischen Auswirkungen des Wegfalls der Vorratsdaten gem. §§ 113a und 113b TKG für Ihre Arbeit?

- sehr hoch
- hoch
- eher gering
- sehr gering
- keinerlei Auswirkungen
- noch nicht abschätzbar

2. Wie schätzen Sie den **Bedarf** der folgenden **Datenarten** im Hinblick auf die nachfolgend genannten Merkmale für Ihre Arbeit ein?

Haben sich die **Abfragemöglichkeiten** dort erschwert oder sind unmöglich geworden? Wenn ja, in welcher Art und in welchem Umfang

2.1. **Retrograde Daten**

- bezogen auf konkrete Delikte, in Relation mit dem Alter der jeweils benötigten Daten

  (→ welche?)

  (→ Abweichungen im Hinblick auf IuK?)

- bezogen auf konkrete Ermittlungsziele

  (→ welche?)

- bezogen auf bestimmte Informationen

  (→ z.B. konkrete Verbindungsnachweise, gerätebezogene Daten (IMEI, IP, …), personenbezogene Informationen, geographische Informationen, sonstige?)

- Bereiche/Nutzungen

  (→ Festnetz, Mobilfunk, Internet: e-mail, Internet: surfen, Internet: Telefonie, Chat und andere Kommunikation)

  (→ Besonderheiten bei Internetnutung über Mobilfunkgeräte?)

  (→ Sind Änderungen im Nutzungsverhalten auszumachen? In welcher Hinsicht?)

- Art des Anschlusses

  (→ welche?)

2.2. **Echtzeitdaten**?

- bezogen auf konkrete Delikte

  (→ welche?)

  (→ Abweichungen im Hinblick auf IuK?)

- bezogen auf konkrete Ermittlungsziele

  (→ welche?)

- bezogen auf bestimmte Informationen

  (→ z.B. konkrete Verbindungsnachweise, gerätebezogene Daten (IMEI, IP, …), personenbezogene Informationen, geographische Informationen, sonstige?)

- Bereiche/Nutzungen

  (→ Festnetz, Mobilfunk, Internet: e-mail, Internet: surfen, Internet: Telefonie, Chat und andere Kommunikation)

  (→ Besonderheiten bei Internetnutung über Mobilfunkgeräte?)

  (→ Sind Änderungen im Nutzungsverhalten auszumachen? In welcher Hinsicht?)

- Art des Anschlusses

  (→ welche?)

2.3. **Künftig anfallende Daten**?

- bezogen auf konkrete Delikte

  (→ welche?)

  (→ Abweichungen im Hinblick auf IuK?)

- bezogen auf konkrete Ermittlungsziele

  (→ welche?)

- bezogen auf bestimmte Informationen

  (→ z.B. konkrete Verbindungsnach-weise, gerätebezogene Daten (IMEI, IP, …), personenbezogene Informationen, geographische Informationen, sonstige?)

- Bereiche/Nutzungen

  (→ Festnetz, Mobilfunk, Internet: e-mail, Internet: surfen, Internet: Telefonie, Chat und andere Kommunikation)

  (→ Besonderheiten bei Internetnutung über Mobilfunkgeräte?)

  (→ Sind Änderungen im Nutzungsverhalten auszumachen? In welcher Hinsicht?)

- Art des Anschlusses

  (→ welche?)

2.4. **Bestandsdatenauskünfte** gem. § 113 TKG?

3. Bestands-/Verkehrsdaten werden häufig im Zusammenhang mit **anderen Ermittlungsmaßnahmen** erhoben.

3.1. Welche konkreten Ermittlungsmaßnahmen können durch Informationen aus Verkehrsdaten grundsätzlich unterstützt werden? In welcher Hinsicht?

(→ z.B. TKÜ, AKÜ, WRÜ, Einsatz technischer Mittel, Durchsuchung, Beschlagnahme, Einsatz verdeckter Ermittler, Observation, sonstige?)

3.2. Welche konkrete Rolle spielen Bestands-/Verkehrsdaten im Kontext der jeweiligen Maßnahme?

3.3. Welche der oben unter 2. im einzelnen aufgeführten Datenarten und anderen Merkmale spielen dabei eine Rolle?

3.4. In welchen Bereichen kann die Nichtverfügbarkeit von Bestands-/Verkehrsdaten ggf. durch andere Maßnahmen kompensiert werden? Auf welche Weise?

3.5. Wie hoch schätzen Sie den Anteil der Verfahren ohne andere/weitere Ermittlungsansätze (bezogen auf alle Verfahren, in denen Verkehrsdaten relevant sind)?

- Unterschieden nach Bestands- u. Verkehrsdaten bzw.
- Retrogr. / Echtzeit-/ zukunftsger. Daten

(→ bitte jew. %)

4. Wie beurteilen Sie die **Auskunftsbereitschaft der TK-Anbieter** seit Veröffentlichung des BVerfG-Urteils vom 2. März?

4.1. Generelle Einschätzung

- sehr hoch
- hoch
- eher gering
- sehr gering

4.2. Hat sich die Kooperationsbereitschaft im Vergleich zu der Zeit vor dem Urteil verändert?

- In welcher Hinsicht bzw. in welche Richtung?

4.3. Gibt es Unterschiede zwischen einzelnen Anbietern?

- Welche?
- Gibt es einen Zusammenhang mit der Größe des Anbieters?

4.4. Welche konkreten Probleme können Sie ggf. benennen? Gibt es ggf. Unterschiede entlang der oben unter 2. aufgeführten Merkmale

- Keine Auskunft über Vorhandensein von Daten
- Mangelhafte Auskunft über vorhandene Daten
- Mutmaßlich vorhandene Daten werden nicht übermittelt
- Anbieter sitzt oder beruft sich auf Sitz im Ausland
- Behauptung eigener Prüfungskompetenz
- Komplette Kooperationsverweigerung
- Verzögerte Bearbeitung
- Unvollständige Auskunft
- Verzögerte technische Umsetzung (Aufschaltung)
- Kein Rückgriff aus die 'alte' Technik der Zielwahlsuche mehr möglich
- Sonstiges?

5. Sehen Sie auf der Grundlage der gegenwärtigen Rechtslage **mögliche Substitute** für die Abfrage von Verkehrs-/Vorratsdaten, soweit die erwünschten Daten nicht verfügbar sind?

- § 100a StPO
- 7-Tage-Daten gem. § 100 TKG
- § 113 TKG
- Andere?
- Derzeit keine tauglichen/ausreichenden Substitute

5.1. Würden Sie auf der Grundlage Ihrer Erfahrungen der Annahme zustimmen, dass § 100g Abs. 3 StPO einen zügigen Zugriff auf Verkehrsdaten ermöglicht und so funktional dem international unter dem Fachbegriff Quick-freeze diskutierten Verfahren nahekommt?

6. **Folgenbeurteilung** im Detail

6.1. Veränderungen im Rahmen von **Maßnahmen nach § 100g StPO**

- bzgl. der **Vorbereitung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

- bzgl. der **Beantragung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

  (→ insbes.: Hat die faktische **Eilbedürftigkeit der Maßnahmen** (Verfügbarkeit von Verkehrsdaten für lediglich ca. 3 bis 7 Tage in die Vergangenheit) Auswirkungen auf die Antrags-/ Anordnungspraxis? (z.B. Konzessionen bzgl. der Begründungsdichte, der Erforderlichkeitserwägungen, der ultima-ratio-Erwägungen, etc.)?)

  (→ insbes. Wie handhaben Sie den **Umgang mit Vorratsdaten**, die **vor dem 2.3.10** geliefert wurden?)

  (→ Insbes.: Überprüfen Sie bei vorhandenen Daten die **Rechtmäßigkeit der Speicherung** gem. § 96 TKG?)

- bzgl. der **Durchführung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

- bzgl. des **Ertrages** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

6.2. Veränderungen im Rahmen von **Maßnahmen nach § 100a StPO**

- bzgl. der **Vorbereitung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

- bzgl. der **Beantragung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

- bzgl. der **Durchführung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

- bzgl. des **Ertrages** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

6.3. Veränderungen im Rahmen von **Bestandsdatenabfragen nach § 113 TKG**

- bzgl. der **Vorbereitung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

- bzgl. der **Beantragung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

- bzgl. der **Durchführung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

- bzgl. des **Ertrages** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

6.4. Nach weiteren Maßnahmen fragen und nach dem gleichen Schema beurteilen lassen

7. Ist in Ihrem Arbeitsbereich die Anzahl der folgenden **Anträge zurückgegangen**?

- Regelanträge gem. § 100g StPO

  (→ um %)

- Regelanträge gem. § 100a StPO

  (→ um %)

- Regelanträge sonstige entspr. 6.3.

  (→ um %)

- Eilanträge gem. § 100g StPO

  (→ um %)

- Eilanträge gem. § 100g StPO

  (→ um %)

- Eilanträge sonstige entspr. 6.3.

  (→ um %)

- Bestandsabfragen gem. § 113 TKG

  (→ um %)

8. Was wäre Ihr **konkreter Lösungsvorschlag**, wie der Gesetzgeber auf den Wegfall der Vorratsdatenspeicherung reagieren sollte?

- § 113a/b TKG

  (→ möglichst ähnlich erneuern, erweitern (wie?), sonstiges)

- § 100g StPO

  (→ beibehalten, erweitern (wie?), sonstiges)

- Sonstige Ideen
- Keine Änderung erforderlich

9. Gibt es **weitere Punkte**, die noch nicht angesprochen wurden, Ihrer Ansicht nach aber berücksichtigt werden müssen?

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Abteilung Kriminologie

Untersuchung möglicher Schutzlücken durch den Wegfall der Vorratsdatenspeicherung

Interviewleitfaden

B. Version Polizei

1. Zunächst als einleitende **Ersteinschätzung**: Wie beurteilen Sie die praktischen Auswirkungen des Wegfalls der §§ 113a und b TKG für Ihre Arbeit?

- sehr hoch
- hoch
- eher gering
- sehr gering
- keinerlei Auswirkungen
- noch nicht abschätzbar

2. Wie schätzen Sie den **Bedarf** der folgenden **Datenarten** im Hinblick auf die nachfolgend genannten Merkmale für Ihre Arbeit ein?

Haben sich die **Abfragemöglichkeiten** dort erschwert oder sind unmöglich geworden?

Wenn ja, in welchem Umfang?

2.1. **Retrograde Daten**

- bezogen auf konkrete Delikte, in Relation mit dem Alter der jeweils benötigten Daten

  (→ welche?)

  (→ Abweichungen im Hinblick auf IuK?)

- bezogen auf konkrete Gefahrenlagen

  (→ welche?)

- bezogen auf bestimmte Informationen

  (→ z.B. konkrete Verbindungsnachweise, gerätebezogene Daten (IMEI, IP, …), personenbezogene Informationen, geographische Informationen, sonstige?)

- Bereiche/Nutzungen

  (→ Festnetz, Mobilfunk, Internet: e-mail, Internet: surfen, Internet: Telefonie, Chat und andere Kommunikation)

  (→ Besonderheiten bei Internetnutung über Mobilfunkgeräte?)

  (→ Sind Änderungen im Nutzungsverhalten auszumachen? In welcher Hinsicht?)

- Art des Anschlusses

  (→ welche?)

2.2. **Echtzeitdaten**?

- bezogen auf konkrete Delikte

  (→ welche?)

  (→ Abweichungen im Hinblick auf IuK?)

- bezogen auf konkrete Gefahrenlagen

  (→ welche?)

- bezogen auf bestimmte Informationen

  (→ z.B. konkrete Verbindungsnachweise, gerätebezogene Daten (IMEI, IP, …), personenbezogene Informationen, geographische Informationen, sonstige?)

- Bereiche/Nutzungen

(→ Festnetz, Mobilfunk, Internet: e-mail, Internet: surfen, Internet: Telefonie, Chat und andere Kommunikation)

(→ Besonderheiten bei Internetnutung über Mobilfunkgeräte?)

(→ Sind Änderungen im Nutzungsverhalten auszumachen? In welcher Hinsicht?)

- Art des Anschlusses

(→ welche?)

2.3. **Künftig anfallende Daten**?

- bezogen auf konkrete Delikte

(→ welche?)

(→ Abweichungen im Hinblick auf IuK?)

- bezogen auf konkrete Gefahrenlagen

(→ welche?)

- bezogen auf bestimmte Informationen

(→ z.B. konkrete Verbindungsnachweise, gerätebezogene Daten (IMEI, IP, …), personenbezogene Informationen, geographische Informationen, sonstige?)

- Bereiche/Nutzungen

(→ Festnetz, Mobilfunk, Internet: e-mail, Internet: surfen, Internet: Telefonie, Chat und andere Kommunikation)

(→ Besonderheiten bei Internetnutung über Mobilfunkgeräte?)

(→ Sind Änderungen im Nutzungsverhalten auszumachen? In welcher Hinsicht?)

- Art des Anschlusses

(→ welche?)

2.4. **Bestandsdatenauskünfte** gem. § 113 TKG?

3. Können fehlende Bestands-/Verkehrsdaten durch **andere/eigene Instrumente** ersetzt werden (→ z.B. Observation, IMSI-Catcher, etc.)?

3.1. Wenn ja:

- in welchen Situation/bei welchen Gefahrenlagen?
- Durch welche Maßnahmen?

3.2. Wie hoch schätzen Sie den Anteil der Vorfälle/Einsätze ohne andere/weitere Handlungsansätze

- Unterschieden nach Bestands- u. Verkehrsdaten bzw.

(→ bitte %)

4. Wie beurteilen Sie die **Auskunftsbereitschaft der TK-Anbieter** seit Veröffentlichung des BVerfG-Urteils vom 2. März?

4.1. Generelle Einschätzung

- sehr hoch
- hoch
- eher gering
- sehr gering

4.2. Hat sich die Kooperationsbereitschaft im Vergleich zu der Zeit vor dem Urteil verändert?

- In welcher Hinsicht bzw. in welche Richtung?

4.3. Gibt es Unterschiede zwischen einzelnen Anbietern?

- Welche?
- Gibt es einen Zusammenhang mit der Größe des Anbieters?

4.4. Welche konkreten Probleme können Sie ggf. benennen? Gibt es ggf. Unterschiede entlang der oben unter 2. aufgeführten Merkmale?

- Keine Auskunft über Vorhandensein von Daten
- Mangelhafte Auskunft über vorhandene Daten
- Mutmaßlich vorhandene Daten werden nicht übermittelt
- Anbieter sitzt oder beruft sich auf Sitz im Ausland

- Behauptung eigener Prüfungskompetenz
- Komplette Kooperationsverweigerung
- Verzögerte Bearbeitung
- Unvollständige Auskunft
- Verzögerte technische Umsetzung (Aufschaltung)
- Kein Rückgriff aus die 'alte' Technik der Zielwahlsuche mehr möglich
- Sonstiges?

5. Sehen Sie auf der Grundlage der gegenwärtigen Rechtslage **mögliche Substitute** für die Abfrage von Verkehrs-/Vorratsdaten, soweit die erwünschten Daten nicht verfügbar sind?

- § 100a StPO
- 7-Tage-Daten gem. § 100 TKG
- § 113 TKG
- Andere?
- Derzeit keine tauglichen/ausreichenden Substitute

5.1. Gibt es in Ihren (Landes-) Gesetzen eine explizite Rechtsgrundlage, die einen zügigen Zugriff auf Verkehrsdaten ermöglichen und so funktional dem international unter dem Stichwort Quick-freeze diskutierten Verfahren nahekommt?

6. **Folgenbeurteilung** im Detail

6.1. Veränderungen im Bereich der **Verkehrsdatenabfrage**

- bzgl. der **Vorbereitung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

- bzgl. der **Beantragung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

- bzgl. der **Durchführung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

- bzgl. des **Erfolges** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

6.2. Veränderungen im Bereich der **TKÜ**

- bzgl. der **Vorbereitung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

- bzgl. der **Beantragung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

- bzgl. der **Durchführung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

- bzgl. des **Erfolges** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

6.3. Veränderungen im Rahmen von **Bestandsdatenabfragen nach § 113 TKG**

- bzgl. der **Vorbereitung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

- bzgl. der **Beantragung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

- bzgl. der **Durchführung** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

- bzgl. des **Erfolges** einer Maßnahme?

  (→ Gleich geblieben / schwieriger geworden: warum?)

6.4. Nach weiteren Maßnahmen fragen und nach dem gleichen Schema beurteilen lassen

7. Ist in Ihrem Arbeitsbereich die Anzahl der folgenden **Anträge zurückgegangen**?

- Regelanträge gem. § 100g StPO

  (→ um %)
- Regelanträge gem. § 100a StPO

  (→ um %)
- Regelanträge sonstige entspr. 6.3.

  (→ um %)
- Eilanträge gem. § 100g StPO

  (→ um %)
- Eilanträge gem. § 100g StPO

  (→ um %)
- Eilanträge sonstige entspr. 6.3.

  (→ um %)
- Bestandsabfragen gem. § 113 TKG

  (→ um %)

8. Was wäre Ihr **konkreter Lösungsvorschlag**, wie der Gesetzgeber auf den Wegfall der Vorratsdatenspeicherung reagieren sollte?

- § 113a/b TKG

  (→ möglichst ähnlich erneuern, erweitern (wie?), sonstiges)
- § 100g StPO

  (→ beibehalten, erweitern (wie?), sonstiges)
- Sonstige Ideen
- Keine Änderung erforderlich

9. Gibt es **weitere Punkte**, die noch nicht angesprochen wurden, Ihrer Ansicht nach aber berücksichtigt werden müssen?

Max-Planck-Institut für ausländisches
und internationales Strafrecht

Abteilung Kriminologie

Untersuchung möglicher Schutzlücken durch den Wegfall der Vorratsdatenspeicherung

Interviewleitfaden

C. Version TK-Anbieter

1. Zunächst als allgemeine **Einschätzung**: Wie beurteilen Sie die praktischen Auswirkungen des Wegfalls der §§ 113a und b TKG für Ihr Unternehmen?

- sehr hoch
- hoch
- eher gering
- sehr gering
- keinerlei Auswirkungen
- noch nicht abschätzbar

2. Hat sich die **Abfragepraxis der Polizei- und Justizbehörden** im Hinblick auf Verkehrsdaten gem. § 100g StPO nach der Wahrnehmung Ihres Unternehmens seit dem 2. März 2010 verändert?

- Ja / nein

2.1. Wenn ja: in welchem Ausmaß (Zunahme/Rückgang der Abfragen)?

- Schätzung

(→ um %)

2.2. Haben die Abfragen auf der Grundlage anderer rechtlicher Bestimmungen bzw. nach Daten, deren Speicherung auf der Basis anderer Rechtsgrundlagen als § 113a TKG erfolgt, zugenommen?

2.2.1. Abfragegrundlage:

- § 100a StPO

(→ Schätzung: um %)

- Auslandskopfüberwachung (§ 4 TKÜV)

(→ Schätzung: um %)

- Präventiv-polizeiliche Abfragen gem. PolG/PAG/SOG/etc. bzw. BKAG

(→ %)

- Sonstige

2.2.2. Speicherungszweck:

- § 96 TKG

(→ %)

- § 100 TKG

(→ %)

- § 113 TKG

(→ %)

- Sonstige

3. Wie hoch sind in Ihrem Unternehmen die Anteile von **Flatrate- und Prepaid-Tarifen**, und zwar bezogen auf die beiden Sektoren

- Festnetztelefonie
- Mobilfunktelefonie
- Internet

4. Was wird bei Ihnen gegenwärtig auf der Grundlage von **§ 96ff. TKG** zumindest temporär gespeichert?

4.1. Welche Datenarten?

4.2. Wie lange?

4.3. Welche Datenvolumina sind betroffen?

- Durchschnittlich pro Kunde
- Für Ihr Unternehmen insgesamt

4.4. Gibt es bestimmte Datenarten (z.B. Standortdaten) oder Abfragearten (z.B. Zielwahlsuche), die Sie aufgrund des Wegfalls der Vorratsdatenspeicherung aus technischen Gründen derzeit nicht erheben können?

4.5. Gibt es Datenarten bzw. Abfragearten, deren Weitergabe an Polizei bzw. Strafverfolgungsbehörden Sie gegenwärtig im Hinblick auf das Urteil des BVerfG vom 2.3.2010 bzw. aus generellen Datenschutzerwägungen verweigern?

4.5.1. Ist dies ggf. eine generelle Politik Ihres Unternehmens?

4.5.2. Nehmen Sie ggf. Abstufungen vor (z.B. beschränkt auf vorherige richterliche Beschlüsse)?

4.5.3. Machen Sie ggf. Ausnahmen bei speziellen Gefahrensituationen (z.B. Suizid u.a. Formen von Lebensgefahr)?

5. Nehmen Sie bei Eingang einer Anfrage eine eigene **rechtliche Prüfung** der Voraussetzungen vor und ggf. wie häufig?

5.1. Richterliche Beschlüsse

- Regelmäßig
- In Zweifelsfällen
- Nein
- Umfang der überprüften Abfragen insgesamt (→ bitte %)

5.2. Staatsanwaltliche Eilabfragen

- Regelmäßig
- In Zweifelsfällen
- Nein
- Umfang der überprüften Abfragen insgesamt (→ bitte %)

5.3. Polizeiliche Eilabfragen

- Regelmäßig
- In Zweifelsfällen
- Nein
- Umfang der überprüften Abfragen insgesamt (→ bitte %)

6. Wie schätzen Sie die **weitere gesetzgeberische Entwicklung** im Bereich der Vorratsdatenspeicherung ein und welche Erwartungen haben Sie ggf. an den Gesetzgeber?

7. Halten Sie die zur Umsetzung der Vorratsdatenspeicherung **implementierte Technik** in Erwartung einer modifizierten gesetzlichen Neuregelung weiter vor?

Anhang C: Zusammensetzung der deutschen Interviewpersonen

Interviewpartner	**Bereich**
Leiter Polizeidirektion	Repressiv / präventiv
Referent Innenministerium	Repressiv / präventiv
Leiter Kriminalpolizeiinspektion	Repressiv / präventiv
Abteilungsleiterin, LKA	Repressiv / präventiv
Sachbereichsleiter, Internetkriminalität, LKA	Repressiv / präventiv
Oberregierungsrätin im Präsidialbüro, LKA	Repressiv / präventiv
Polizeipräsident	Präventiv
Landeskriminaldirektor, Polizeipräsidium	Repressiv / präventiv
Erster Kriminalhauptkommissar, LKA	Repressiv / präventiv
Kriminalrat, LKA	Repressiv / präventiv
Landeskriminaldirektor, LKA	Repressiv / präventiv
Kriminalhauptkommissar, LKA	Repressiv / präventiv
Kriminaloberkommissar, Polizeipräsidium	Repressiv / präventiv
Leiter Kommissariat für Rauschgiftkriminalität, Kriminalpolizeiinspektion der Landespolizeidirektion	Repressiv / präventiv
Polizeihauptkommissar, Sachgebietsleiter Telekommunikationsüberwachung	Repressiv / präventiv
Kriminalhauptkommissar, Sachgebietsleiter Raub u. Erpressung, LKA	Repressiv / präventiv
Regierungsoberamtsrat im Innenministerium, Sachbearbeitung Polizeirecht, Straf- und Strafprozessrecht	Repressiv

Kriminaldirektor, Dezernatsleiter	Repressiv
Erster Polizeihauptkommissar, Sachgebietsleiter Telekommunikationsüberwachung, Landesamt für Zentrale Polizeiliche Dienste	Repressiv
Kriminalhauptkommissar, Sachgebietsleiter Zentrale Internetrecherche, LKA	Repressiv
Kriminalhauptkommissar, Sachgebietsleiter Telekommunikationsüberwachung, Anwenderberatung, LKA	Repressiv
Kriminalhauptkommissar, Polizeipräsidium, Kriminalkommissariat – Telekommunikationsüberwachung	Repressiv
Kriminaloberrätin, BKA	Repressiv / präventiv
Kriminalhauptkommissar, BKA	Repressiv / präventiv
Kriminalhauptkommissar, BKA	Repressiv / präventiv
Kriminaloberrat, BKA	Repressiv / präventiv
Kriminalkommissar, Service Telekommunikationsüberwachung, BKA	Repressiv / präventiv
Dezernent Kompetenzzentrum Telekommunikationsüberwachung, LKA	Repressiv / präventiv
Dezernent Operative Abteilung –Telekommunikationsüberwachung, LKA	Repressiv / präventiv
Dezernent Organisierte Kriminalität / Rauschgiftkriminalität, LKA	Repressiv / präventiv
Dezernent Wirtschaftskriminalität / Korruption, LKA	Repressiv / präventiv
Dezernent Islamismus / Terrorismus / Staatsschutz, LKA	Repressiv / präventiv
Sachbearbeiter technische Einsatz- und Ermittlungsmaßnahmen, LKA	Repressiv / präventiv
Sachbearbeiter Internet- und Computerkriminalität, LKA	Repressiv / präventiv
Technische Einsatzleitung Verkehrsdaten, LKA	Repressiv / präventiv
Rechtsabteilung, LKA	Repressiv

Polizeioberrat, Leiter Bundespolizeiinspektion	Repressiv / präventiv
Erste Polizeihauptkommissarin, Leiterin Ermittlungsdienst Bundespolizeiinspektion	Repressiv / präventiv
Polizeihauptkommissar, Bundespolizeipräsidium – Zentrale Ermittlungen	Repressiv / präventiv
Erster Polizeihauptkommissar, Bundespolizeipräsidium – Technische Ermittlungsunterstützung	Repressiv / präventiv
Polizeioberkommissar, Bundespolizeipräsidium – Technische Ermittlungsunterstützung	Repressiv / präventiv
Kriminalrat, Revierkriminaldienst	Repressiv
Kriminalhauptkommissar, Revierkriminaldienst	Repressiv
Polizeikommissarin	Repressiv
Kriminaloberkommissarin, Dienststelle Telekommunikationsüberwachung, LKA	Repressiv
Kriminalrat, Sachbearbeiter Internet- und Computerkriminalität (IuK) und Kinderpornographie	Repressiv
Kriminalhauptkommissar, Ermittlungsgruppe Internet, LKA	Repressiv / präventiv
Kriminalhauptkommissar, Telekommunikationsüberwachung – Administration, LKA	Repressiv / präventiv
VA, Amtsleitung, LKA	Repressiv / präventiv
Abteilungsleiter, LKA	Repressiv
Dezernatsleiter, Telekommunikationsüberwachung, LKA	Repressiv
Kommissariatsleiter, Kapitaldelikte, LKA	Repressiv
Erster Sachbearbeiter, Staatsschutzdelikte, LKA	Repressiv
Sachbearbeiter, Organisierte Kriminalität, LKA	Repressiv
Erste Kriminalhauptkommissarin, Sachgebietsleiterin im Landespolizeiamt für grundsätzliche Angelegenheiten der Kriminalitätsbekämpfung	Repressiv / präventiv

Kriminalhauptkommissar, Sachgebietsleiter für Ermittlungen Internet- und Computerkriminalität (IuK) i.e.S., LKA	Repressiv / präventiv
Kriminalhauptkommissar, Sachgebietsleiter, Zentralstelle Telekommunikationsüberwachung, LKA	Repressiv / präventiv
Erster Kriminalhauptkommissar, Dezernatsleiter, Zentrale Auswertung und Analyse Kriminalität, LKA	Repressiv / präventiv
Erster Kriminalhauptkommissar, Dezernatsleiter Operativtechnik / Kommunikationsüberwachung, LKA	Repressiv / präventiv
Sachbearbeiter Elektronische Schnittstelle Behörden, LKA	Repressiv / präventiv
Kriminaloberkommissar, Sachbearbeiter Zentralstelle Internetkriminalität, LKA	Repressiv / präventiv
Kriminalhauptkommissar, Polizeidirektion, Zentraler Kriminaldienst, Fachkommissariat, Ermittlungsfeldführer	Repressiv / präventiv
Kriminalhauptkommissar, Ermittlungssachbearbeiter, LKA	Repressiv / präventiv
Kriminalkommissar, Ermittlungssachbearbeiter, ZD	Repressiv / präventiv
Kriminaloberkommissar, Sachbearbeiter, LKA – Stab	Repressiv / präventiv
Kriminaloberkommissar, Sachbearbeiter Spezialeinheiten Technik, LKA	Repressiv / präventiv
Kriminaloberkommissar, Sachbearbeiter Auswertung / Analyse, LKA	Repressiv / präventiv
Kriminalhauptkommissar, Sachgebietsleiter, LKA	Repressiv
Regierungsrat Stabsleiter, LKA	Repressiv / präventiv
Kriminalhauptkommissar, Sachgebietsleiter Einsatztechnik, Telekommunikationsüberwachung, Mobilfunkaufklärung, LKA	Repressiv / präventiv
Kriminalhauptkommissar, Leiter Mordkommission	Repressiv / präventiv
Kriminaloberkommissar, Sachbearbeiter Telekommunikationsüberwachung, Mobilfunkaufklärung, LKA	Repressiv / präventiv
Kriminaldirektor, Leiter der Abteilung Ermittlungen / Auswertung, LKA	Repressiv
Kriminalrat, Leiter des Dezernats Politisch motivierte Ausländerkriminalität, LKA	Repressiv

Kriminalrat, Leiter des Dezernats Sonderfälle, LKA	Repressiv
Kriminalhauptkommissar, Kriminalpolizeiinspektion	Repressiv
Erster Kriminalhauptkommissar, Leiter des Dezernats Telekommunikationsüberwachung, LKA	Repressiv

Anhang D: Österreichische Gesetzesnovelle 2011 zur Vorratsdaten-speicherung (Auszüge)

1074 der Beilagen XXIV. GP

Beschluss des Nationalrates

Bundesgesetz, mit dem das Telekommunikationsgesetz 2003 – TKG 2003 geändert wird

[Auszüge]

Vorratsdaten
§ 102a.

(1) Über die Berechtigung zur Speicherung oder Verarbeitung gemäß den §§ 96, 97, 99, 101 und 102 hinaus haben Anbieter von öffentlichen Kommunikationsdiensten nach Maßgabe der Abs. 2 bis 4 Daten ab dem Zeitpunkt der Erzeugung oder Verarbeitung bis sechs Monate nach Beendigung der Kommunikation zu speichern. Die Speicherung erfolgt ausschließlich zur Ermittlung, Feststellung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt.

(2) Anbietern von Internet-Zugangsdiensten obliegt die Speicherung folgender Daten:

1. Name, Anschrift und Teilnehmerkennung des Teilnehmers, dem eine öffentliche IP-Adresse zu einem bestimmten Zeitpunkt unter Angabe der zugrunde liegenden Zeitzone zugewiesen war;
2. Datum und Uhrzeit der Zuteilung und des Entzugs einer öffentlichen IP-Adresse bei einem Internet-Zugangsdienst unter Angabe der zugrundeliegenden Zeitzone;
3. die Rufnummer des anrufenden Anschlusses für den Zugang über Wählanschluss;
4. die eindeutige Kennung des Anschlusses, über den der Internet-Zugang erfolgt ist.

(3) Anbietern öffentlicher Telefondienste einschließlich Internet-Telefondiensten obliegt die Speicherung folgender Daten:

1. Teilnehmernummer oder andere Kennung des anrufenden und des angerufenen Anschlusses;
2. bei Zusatzdiensten wie Rufweiterleitung oder Rufumleitung die Teilnehmernummer, an die der Anruf geleitet wird;
3. Name und Anschrift des anrufenden und des angerufenen Teilnehmers;
4. Datum, Uhrzeit des Beginns und Dauer eines Kommunikationsvorganges unter Angabe der zugrundeliegenden Zeitzone;
5. die Art des in Anspruch genommenen Dienstes (Anrufe, Zusatzdienste und Mitteilungs- und Multimediadienste).
6. Bei Mobilfunknetzen zudem
   a) der internationalen Mobilteilnehmerkennung (IMSI) des anrufenden und des angerufenen Anschlusses;
   b) der internationalen Mobilfunkgerätekennung (IMEI) des anrufenden und des angerufenen Anschlusses;
   c) Datum und Uhrzeit der ersten Aktivierung des Dienstes und die Standortkennung (Cell-ID), an dem der Dienst aktiviert wurde, wenn es sich um vorbezahlte anonyme Dienste handelt;
   d) der Standortkennung (Cell-ID) bei Beginn einer Verbindung.

(4) Anbietern von E-Mail-Diensten obliegt die Speicherung folgender Daten:

1. die einem Teilnehmer zugewiesene Teilnehmerkennung;
2. Name und Anschrift des Teilnehmers, dem eine E-Mail-Adresse zu einem bestimmten Zeitpunkt zugewiesen war;
3. bei Versenden einer E-Mail die E-Mail-Adresse und die öffentliche IP-Adresse des Absenders sowie die E-Mail-Adresse jedes Empfängers der E-Mail;
4. beim Empfang einer E-Mail und deren Zustellung in ein elektronisches Postfach die E-Mail-Adresse des Absenders und des Empfängers der Nachricht sowie die öffentliche IP-Adresse der letztübermittelnden Kommunikationsnetzeinrichtung;
5. bei An- und Abmeldung beim E-Mail-Dienst Datum, Uhrzeit, Teilnehmerkennung und öffentliche IP-Adresse des Teilnehmers unter Angabe der zugrunde liegenden Zeitzone.

(5) Die Speicherpflicht nach Abs. 1 besteht nur für jene Daten gemäß Abs. 2 bis 4, die im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet werden. Im Zusammenhang mit erfolglosen Anrufversuchen besteht die Speicherpflicht nach Abs. 1 nur, soweit diese Daten im Zuge der Bereitstellung des betreffenden Kommunikationsdienstes erzeugt oder verarbeitet und gespeichert oder protokolliert werden.

(6) Die Speicherpflicht nach Abs. 1 besteht nicht für solche Anbieter, deren Unternehmen nicht der Verpflichtung zur Entrichtung des Finanzierungsbeitrages gemäß § 34 KommAustriaG unterliegen.

(7) Der Inhalt der Kommunikation und insbesondere Daten über im Internet aufgerufene Adressen dürfen auf Grund dieser Vorschrift nicht gespeichert werden.

(8) Die nach Abs. 1 zu speichernden Daten sind nach Ablauf der Speicherfrist unbeschadet des § 99 Abs. 2 unverzüglich, spätestens jedoch einen Monat nach Ablauf der Speicherfrist, zu löschen. Die Erteilung einer Auskunft nach Ablauf der Speicherfrist ist unzulässig.

(9) Im Hinblick auf Vorratsdaten, die gemäß § 102b übermittelt werden, richten sich die Ansprüche auf Information oder Auskunft über diese Datenverwendung ausschließlich nach den Bestimmungen der StPO

Auskunft über Vorratsdaten
§ 102b.

(1) Eine Auskunft über Vorratsdaten ist ausschließlich aufgrund einer gerichtlich bewilligten Anordnung der Staatsanwaltschaft zur Aufklärung und Verfolgung von Straftaten, deren Schwere eine Anordnung nach § 135 Abs 2a StPO rechtfertigt, zulässig.

(2) Die nach § 102a zu speichernden Daten sind so zu speichern, dass sie unverzüglich an die nach den Bestimmungen der StPO und nach dem dort vorgesehenen Verfahren für die Erteilung einer Auskunft über Daten einer Nachrichtenübermittlung zuständigen Behörden übermittelt werden können.

(3) Die Übermittlung der Daten hat in angemessen geschützter Form nach Maßgabe des § 94 Abs. 4 zu erfolgen.

Datensicherheit, Protokollierung und Statistik
§ 102c.

(1) Die Speicherung der Vorratsdaten hat so zu erfolgen, dass eine Unterscheidung von nach Maßgabe der §§ 96, 97, 99, 101 und 102 gespeicherten Daten möglich ist. Die Daten sind durch geeignete technische und organisatorische Maßnahmen vor unrechtmäßiger Zerstörung, zufälligem Verlust oder unrechtmäßiger Speicherung, Verarbeitung, Zugänglichmachung und Verbreitung zu schützen. Ebenso ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen, dass der Zugang zu den Vorratsdaten ausschließlich dazu ermächtigten Personen unter Einhaltung des Vier-Augen-Prinzips vorbehalten ist. Die Protokolldaten sind drei Jahre ab Ende der Speicherfrist für das betreffende Vorratsdatum zu speichern. Die Kontrolle über die Einhaltung dieser Vorschriften obliegt der für die Datenschutzkontrolle gemäß § 30 DSG 2000 zuständigen Datenschutzkommission. Eine nähere Beschreibung des Sorgfaltsmaßstabs zur

Gewährleistung der Datensicherheit kann der Bundesminister für Verkehr, Innovation und Technologie per Verordnung festschreiben.

(2) Die gemäß § 102a zur Speicherung verpflichteten Anbieter haben zu gewährleisten, dass jeder Zugriff auf Vorratsdaten sowie jede Anfrage und jede Auskunft über Vorratsdaten nach § 102b revisionssicher protokolliert wird. Diese Protokollierung umfasst

1. die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Referenz zur staatsanwaltschaftlichen oder gerichtlichen Anordnung gemäß den Bestimmungen der StPO, die der Übermittlung der Daten zugrunde liegt,
2. in den Fällen des § 99 Abs. 5 Z 3 und 4 die dem Anbieter mit dem Auskunftsbegehren bekannt gegebene Aktenzahl der Sicherheitsbehörde,
3. das Datum der Anfrage sowie das Datum und den genauen Zeitpunkt der erteilten Auskunft,
4. die nach Datum und Kategorien gemäß § 102a Abs. 2 bis 4 aufgeschlüsselte Anzahl der übermittelten Datensätze,
5. die Speicherdauer der übermittelten Daten zum Zeitpunkt der Anordnung der Übermittlung,
6. den Namen und die Anschrift des von der Auskunft über Vorratsdaten betroffenen Teilnehmers, soweit der Anbieter über diese Daten verfügt sowie
7. eine eindeutige Kennung, welche eine Zuordnung der Personen ermöglicht, die im Unternehmen des Anbieters auf Vorratsdaten zugegriffen haben.

(3) Die Speicherung der Protokolldaten hat so zu erfolgen, dass deren Unterscheidung von Vorratsdaten sowie von nach Maßgabe der §§ 96, 97, 99, 101 und 102 gespeicherter Daten möglich ist.

(4) Die gemäß § 102a zur Speicherung verpflichteten Anbieter haben

1. für Zwecke der Kontrolle des Datenschutzes und zur Gewährleistung der Datensicherheit die Protokolldaten gemäß Abs. 2 an die Datenschutzkommission und den Datenschutzrat sowie
2. zum Zweck der Berichterstattung an die Europäische Kommission und an den Nationalrat die Protokolldaten gemäß Abs. 2 Z 2 bis 4 an den Bundesminister für Justiz zu übermitteln.

(5) Die Übermittlung der Protokolldaten hat auf schriftliches Ersuchen der Datenschutzkommission bzw. des Bundesministers für Justiz zu erfolgen; die Übermittlung an den Bundesminister muss darüber hinaus jährlich bis zum 31. Jänner für das vorangegangene Kalenderjahr erfolgen.

(6) Über die Protokollierungspflichten nach Abs. 2 hinaus ist eine Speicherung der übermittelten Datensätze selbst unzulässig.“

Anhang E: Informationsblatt eines Anbieters

Funkzellen:

Zielwahlsuche:

Mit freundlichen G

Telefónica O_2 Ge